

Quantar Solutions Limited



Business Case Presentation

MARINE CYBER RISK ANALYTICS COMPANY

for

Daily Mail and General Trust plc

DMGT

&

dmg :: ventures

27th September 2020

Table of Contents

Introductory Notes	5
EXECUTIVE SUMMARY	6
Covid-19 Impact	8
The Marine Sector-Specific Challenges	8
Cyber Target Systems:	10
Current Maritime Cyber Insurance Cover Methods	10
The challenges	15
Ports	21
Fit to Existing DMGT-V Portfolio	22
Similar or Same Deliverables as RMS & Praedicat:	24
Prior Go-To Market Efforts	24
Why not part of RMS or Praedicat?	26
We Can Do This Ourselves with RMS	27
Long-term Versus Exit Strategy	28
Strategy	29
PHASE 1	30
Strategy/ Operational Model	30
Sample Cyber Threat Data Acquired from EU Insurance Company Network 2017	30
Screendump: Quantar Infrastructure Manager Software Stand-alone Module	31
Sample Existing Quantar Big Data & Blockchain Online Questionnaires	32
Business Model	33
Capitalisation Model Phase 1	35
Financials Phase 1	36
Patent Portfolio September 2020	36
PHASE 2	37
Costs Phase 2	37
Business Model	40
Pricing	42
Revenue Streams	44
Marine Reinsurance Premiums	47
Reinsurance Cyber Analytics Revenues	48
Target Clients and Vessel Volumes	49
Operating Model	51
End-User Operating Model	51
Value Propositions	52
For Vessel Owners and P&I Clubs:	53
For Risk Carriers	53

For Marine Equipment Companies	53
For Ports	54
Market	54
EU Network and Information Security Directive (NIS) DIRECTIVE (EU) 2016/1148	54
P&I Club Market.....	55
Port Inspection Controls (PIC's)	55
Marketing & Branding.....	58
Financial Model	59
Pre-DMGT Investment Valuation:	59
Initial Proposed Capitalisation Table	60
Existing Shareholders and Pre-emptive Rights to New Shares.....	60
Anti-Dilution Protection of A Series Preference Shares	61
Founder Investment.....	61
CAPEX YTD	62
Legal & Tax Jurisdiction.....	63
Tax Structure Where Offshore Required.....	63
1. Group shareholders	64
2. Group holding company.....	65
3. R&D Company.....	67
4. The sales branch/company	67
The System	68
Internet Protocol Threat Assessment Program.....	68
Network Operational Risk Manager	69
Predictive Analytics Engine	70
Implementation of Marine Solutions	70
Hardware Installations on Vessels and at Ports	70
End User Training.....	71
Local Hardware Installations.....	71
Customer Support.....	71
Development Rationale	72
Project Management & Reporting	77
Program Roadmap	79
1) Software/Systems	79
2) Modelling.....	79
3) Industry Engagement.....	80
Program Roadmap: Hardware/Software/Models - Details	80
Potential Marine Installation Issues.....	81
Intellectual Property	85

IP Costs	87
Amortisation of Patent Portfolio.....	87
Patent Encumbrances	88
Program Risk.....	89
Organization	90
Leadership Team.....	92
Founder	92
Product & Analytics.....	93
Engineering.....	94
Operations	94
Finance.....	95
Industry Engagement.....	95
Growth Officer	96
Remuneration & Share Ownership	97
Board of Directors.....	97
Chairman	97
Founder:	98
Investor:.....	98
Reinsurance:	98
Marine Equipment:	98
Advisory Board Members	99
External Adviser	99
Recruitment	99
Competitors	100
Maritime Data Providers.....	100
Maritime-Specific Incumbents	102
Potential Market Entrants.....	104
Marine Equipment Competitors	107
SUMMARY	107
ANNEXES.....	108
INSURANCE LINKED SECURITIES MARKET (ILS)	108
COMPETITOR TO QUANTAR PATENT EVALUATION	111
General Overview of Quantar Patent Methodologies:	111
CYBERPOINT INTERNATIONAL (PivotPoint Risk Analytics)	111
GUIDEWIRE/CYENCE.....	112
SECURE SYSTEMS INNOVATION CORPORATION (SSIC)	115
RISKLENS.....	115
BALBIX.....	118

CORAX CYBER (IP Acquired by Creditor 2020).....	119
NEOPRIME LLC	120
CASE USAGE	123
SELECTED COMPANY CITING QUANTAR PATENTS AS PRIOR ART	125
QUANTAR MARINE IMPLEMENTATION WORKFLOW MODEL	126
QUANTAR MARINE SOFTWARE PLATFORM SUPPORT MODEL	129
Introduction	129
Considerations	130
Priority Responses	130
Process.....	131
Commercial.....	132
QUANTAR MARKET TESTING EXHIBITIONS	133
Indicative Patent Costs - Years 1-5.....	134
INDICATIVE INSURANCE COSTS FOR PERSONNEL SALARY PACKAGE	135
Private Health Insurance Premiums*	135
Dental Insurance Premiums.....	135
External Developer Software Support Costs	135
Vessel Software Installation Guide & Server Pricing	136
Sample 50 Marine Reinsurers, Brokers & Underwriters	145
Example Marine Software Solutions Providers	146
World Container Shippers and Number of Port Calls.....	146
Initial Shipping Lines European Office Locations.....	148
Microsoft Power BI PRO Functionality at £7.50 Per User/Month	149
Proof of Marine Market for Cyber Threat Quantification September 2020	149
ARTICLES OF ASSOCIATION QUANTAR SOLUTIONS LIMITED	151
Reinsurance Annual Premium Workings.....	157
MARITIME SECTOR - CYBER ASSESSMENT & CONTROLS.....	158
IHS MARKIT MARINE SOLUTIONS.....	159
SAMPLE GDPR / ISO DOCUMENTS	160
LUEL RESEARCH - BACK-END SOFTWARE/HARDWARE EVALUATION & DEVELOPMENT.....	161
FINANCIAL STATEMENTS	162

Introductory Notes

1. This business case presentation is intended for DMGT and DMG Ventures only. The content, concept, financial analysis may not be distributed to any person outside of the aforementioned

corporate entities, including, but not limited to, any person employed by, or working for and on behalf of, Risk Management Solutions (RMS) and Praedicat.

2. Financials have been provided within the Annex as well as separately for ease of review. Pdf and xlsx formats have been provided, with the former available where opening macro xls files is not permitted by corporate security.
3. The financial analysis herein is divided into Phase 1, which is a loss-leader and determines the viability of the proposed program, effectively ring-fencing risk. Phase 2 financial analysis also displays some revenue limitations in terms of client acquisition costs. For Year 2 of Phase 2 (year 3 of actual operations), revenue becomes stable and as such only summary financials are included for the following period in order to provide a meaningful insight into the full revenue stream potential.
4. Phase 1 is proposed to be undertaken utilising the existing Quantar Solutions Limited entity, which has been made dormant for the purposes of patent and associated software IP divestment. Long-term debt has directors loan account retained as a tax mitigation in the case of sale. This can be removed and the accounts restated as at 31/12/2019 or 2020. Alternatively, a new entity may be utilised, as planned for the Phase 2 development. This will require an assessment of the IP owned by Quantar Solutions in respect of transfer, ownership and valuation.
5. Founders equity is based upon the current patent portfolio and software source code, with values set at a well-below market rate for the US patent portfolio and a 50% rate of the initial development for the software code. The valuation of the portfolio has been determined by reference to current figures provided by acknowledged sector specialists. Software CAPEX figures relate to invoices paid to external software development houses and university commercial units.
6. The patent portfolio has a specific feature that is now deemed to be best practice by the maritime sector advisory and regulatory bodies, making the IP within the portfolio and the software code developed concurrently with the patents, far more valuable within the maritime sector due to this uniqueness. The USPTO examiner reasons for allowance illustrate in the wording that this feature distinguishes the Quantar patents from all prior art cited. Opportunity has therefore been created by the bodies determining the means of cyber risk assessment and management for global maritime regulatory compliance, unexpectedly.
7. Neither RMS nor Praedicat has IP to protect their models nor are they able to utilise the models developed and patented by Quantar and the Founder. In the US, where most revenue is derived by RMS and Praedicat, there is currently high availability of very low cost litigation capital. This factor, combined with increased non-practising entity litigation activity via the west Texas district courts, creates a scenario whereby the current proposal may also be viewed as a low cost risk management option for protecting RMS and Praedicat against patent assertion entities.

EXECUTIVE SUMMARY

The global supply chain relies upon marine transportation to ship 93% of global goods, via 51 000 vessels and additionally with fuel supplies additionally using fixed or floating marine infrastructure. Each vessel belongs, under International Maritime Organization (IMO) rules, to a Protection and Indemnity Club (P&I Clubs), which function to pool risks in the format of a mutually owned reinsurance captive. It is a requirement in most territories that a vessel be a member of a P&I club in order to enter territorial waters and to dock at a port (e.g. European Union Directive 2009/20/EC mandates membership). There are 13 P&I clubs globally, covering 90% of the global fleet. Failure to comply can result in the rejection from entering a port, or detention of a vessel in a port.

As with all industries, the marine sector is susceptible to electronic threats, but has a specificity of its own due to the method of interaction between on-board information technology and operational technology. In other sectors, the life of capital and operational assets is far less than an average lifespan of 25 years of the marine sector.

This has resulted in aged infrastructure being maintained and added to on a piecemeal basis, resulting in a patchwork of industrial control systems within a vessel's operational technology (O.T.) I.T. and newer technologies in a manner exposing vessels to cyber attack. The impact of a successful attack is also vastly different to shore-based attacks due to vessels being increasingly reliant upon sensors for day-to-day operations, removing human inputs with the objective of reducing operating costs within a sector renowned for thin margins.

A successful system attack may be motivated by a number of factors and actors, including an increasing threat by Nation State actors seeking to specifically target particular routes or vessels. Marine vessels and oil and gas rigs may be weaponised, re-routed, scuttled with massive environmental impact, theft of cargo, or compromised in order to attain safe passage of illicit drugs or persons. The level of skill required by an attacker to access and compromise one or more systems on a vessel is low to medium, exposing the marine sector to a high probability of attack.

Key Points

1. Marine accounts for 93% of global goods transportation; 51-53 000 vessels.
2. From January 2021 vessels must prove they have undertaken and operate cyber resilience.
3. Marine includes vessels, ports, warehousing, inland transport.
4. London is the global hub for marine re/insurance and regulatory bodies.
5. Quantar has software solutions to serve the market rapidly.
6. Quantar owns multi-US patents for cyber threat valuation; RMS/Praedicat remain exposed.
7. Phase 1 is a loss-leader for Phase 2. Year 3 onwards, financial stability & revenue growth.

There is an increasing shift away from manual functions and personnel utilised in marine, towards remote operation and control, with fully autonomous vessels being the long-term objective, this being labelled the advent of smart ships or Bridge0 i.e. no humans. However, contact with ports and their attendant interaction with port and third party systems will remain, as at present, an operation exposing vessels to attack vulnerability.

Ports globally are owned by the municipality in which they are located, with funding of upgrades to systems and security being limited to that provided via local limited budgets, as opposed to a central government funded basis. As a result, ports rely upon basic security, with a primary focus upon physical security and movement of containers and cargo, to resist attempts to smuggle contraband and humans due to the legal burdens upon ports to eliminate such risks.

When at port, vessels systems interact with both port systems and third parties involved within the port-side and bunkering operations. These are regarded, at present, as trusted systems, despite these also interacting with supply chain provider's back-end systems that pose considerable risks of exposure to the vessel's systems; both I.T. and O.T.

Seeking to address and resolve cyber risks within the marine sector, the IMO now requires all vessel owners to "ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021". Failure to comply with this global regulation; RESOLUTION MSC.428(98) "Maritime Cyber Risk Management in Safety Management Systems" will result in a vessel being detained until the owner has proof of compliance with the regulation. In this respect, MSC.428(98) mimics the E.U. GDPR and E.U. NIS, which also apply to the marine sector, in that the burden of proof of compliance falls upon the vessel owners, as opposed to a regulatory body being required to prove a lack of compliance.

Covid-19 Impact

The global pandemic has rapidly changed working practices on a worldwide scale, with remote working increasing the need for secure communications. A further impact is that of re-addressing business continuity risks and in particular, how to manage supply chain interruption, whether caused by reappearance of a pandemic or from other causes such as cyber attacks.

As a result of this, the market for cyber risk identification and management is far more receptive than has been the case with, for example, cyber insurance use for underwriting and pricing. It is therefore urgent to take advantage of this window of opportunity within the marine space to get to market and establish long-term relationships with partnering entities as soon as possible.

Covid-19 has decimated capital reserves of insurers and the reinsurance industry lacks capacity for covering business interruption policies if there is a further outbreak of a Coronavirus. As such, many risk carriers have been forced to recapitalise in order to comply with Solvency II capital adequacy and had eliminated portfolio risks through no longer offering BI and cyber insurance types of products.

Cyber insurance accounts for less than 1% of global property and casualty revenues, whilst having substantial silent cyber risk. This change has resulted in some cyber risk modelling companies, such as Corax Cyber, to enter administration (January 2020), whilst others such as Cybercube are relying upon continued funding from their venture capital owners to weather the storm. Further, others such as Guidewire/Cyence have pivoted to focus upon their InsureTech platform provision to risk carriers and have recruited former cyber risk modellers from companies including RMS.

The Marine Sector-Specific Challenges

A system attack may manifest in the form of a targeted attack upon navigation and communication systems, whether IP based or radio frequency based, since there is a conversion step required, this point being vulnerable to attack. It may also be in the form of an attack against one or more industrial process controllers; the correct functioning of which a vessel relies upon for its survival.

Such controllers have their programmable logic controllers (PLC's) targeted, these providing the automation of electromechanical processes ranging from sensors deployed for ballast control systems, propulsion, steering, cargo monitoring (for shift, fire, seepage, etc). A simulated attack has shown that scuppering a vessel by an agent with a low level of skill is easily achieved, whilst a juvenile, randomly changing inputs to an oil rig's systems, unintentionally took the entire drilling operation offline.

Many of these industrial control systems were never developed with security being embedded within their development, unlike modern day I.T. systems. As a result, many remain unpatched since their

©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

implementation and with default passwords still in place. Similarly, with a minimum of key personnel on board vessels, the cost of an experienced I.T. security professional to monitor and manage on-board security is not one borne by owners. This has resulted in the general practice of relying upon external parties for managing, patching and monitoring on-board systems remotely. Industrial control systems are frequently updated when in port by contractors, using USB keys to access such systems, with the attendant risks of unauthorized compromise being accepted practice in the absence of alternatives.

Recognition of the increasing electronic threats faced by the marine sector resulted in a number of governmental and trade bodies issuing guidelines for cyber security within the marine sector. These included the US Coastguard, the US National Institute of Standards and Technology (NIST), the Oil Companies International Marine Forum, the UK Department for Transport (DfT) and Defence Science and Technology Laboratory (Dstl), plus BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

In June 2017, the IMO's issued RESOLUTION MSC.428(98) "Maritime Cyber Risk Management in Safety Management Systems that mandates every vessel owner to comply with the new law no later than the first annual verification of the company's Document of Compliance after 1 January 2021. This requires cyber risk assessments, identification, mitigation and control through whatever means necessary.

However, as with the E.U. GDPR and E.U. NIS Directives, the onus falls to the vessel owner to prove compliance with the regulation and the steps that have been taken in identification, elimination and controlling cyber risks. The GDPR mandates data protection impact assessments and the use of ISO27001 typically used as the baseline framework for compliance. The NIS similarly mandates "Minimum Security Measures for Operators of Essential Services".

The regulation relies heavily upon best practice and certification guidelines of existing cyber risk management frameworks, in particular, ISO/IEC 27001 Information Security Management Systems Standard; International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) ISA/IEC 62443 Security for Industrial Automation and Control Systems, NIST Framework for Improving Critical Infrastructure Cybersecurity. Each has a linear, tick-box style of execution, well suited to an online questionnaire type of provision. Additionally, the U.K. government has proposed to its fleet that the use of the Government sponsored Cyber Essentials Plus, would provide a sound basis for regulatory conformity.

Each framework requires identification, assessment and quantification of cyber risks and the mitigation actions required to resolve exposure risks. The E.U. GDPR similarly requires the same steps to be taken, utilising differing terminology such as a data protection impact assessment.

In addition to these two impactful regulations impacting upon the marine sector is the E.U. DIRECTIVE (EU) 2016/1148 Directive on Security of Network and Information Systems (NIS). Given the reliance upon shipping for global supply chain continuity, marine has been embodied within the NIS and once again mandates cyber risk management actions for regulatory compliance in an affirmative manner.

Of particular note within the IMO MSC.428(98) regulation is the recognition of "the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management". There is therefore a need by vessel owners to maintain confidentiality of cyber risk management operations whilst simultaneously providing proof of regulatory compliance. Delivering the ability to combine both is therefore a highly desirable factor for a vendor of a cyber risk management solution.

Since 2005 Quantar has developed the systems and software to facilitate regulatory compliance, cyber risk quantification and cost-benefit analysis of mitigation actions. What differentiates Quantar's

solutions from others is in the extrapolation of future predicted threats. The system also utilizes external data in the extrapolation algorithms, all the methods being protected by a number of patents. This IP protection has been maintained utilising continuation filings to prevent competitors engineering around the patents granted to date.

Our intention is to work with co-development partners that cover the spectrum of marine operations; from vessels to offshore fixed and floating structures, to ports and third party suppliers.

Cyber Target Systems:

1. Safe ship operations are reliant on bridge systems such as ECDIS (Electronic Chart Display and Information System); AIS (Automatic Identification System); GPS (Global Positioning System)
2. Main and auxiliary propulsion systems rely increasingly on computers to operate efficiently
3. Ship networks are connected to the internet. As with computers ashore, shipboard systems are vulnerable to cyber-attacks. Hackers can take advantage of vulnerabilities in a network to access servers; this can enable hackers to access, remove and manipulate sensitive data.
4. Even a simple mobile phone charging process using a USB port in the ECDIS system can cause a virus to render a system inoperable.
5. A cyber-attack could catastrophically impact the safe navigation of a vessel, both in terms of its ability to avoid hazards and in terms of its stability and cargo operations.
6. A cyber-attack could lead to collision, personal injury, property damage, pollution or even to a shipwreck.

Are cyber risks excluded from P&I cover? No. As a general rule, P&I liabilities, nor is the International Group Pooling Agreement subject to a cyber risk exclusion.

Current Maritime Cyber Insurance Cover Methods

As a general rule, neither P&I liabilities, nor the International Group Pooling Agreement are subject to a cyber risk exclusion.

The cover is pooled by the IG under a Supplemental Pooling Agreement and is limited to US\$30 million in the aggregate any one event. If there is more than one entry in the Club and/or any other IG insurer in respect of the same ship, insured for cyber risks under the Bio-Chem covers, each such entry's cyber risks claims are pro-rated accordingly.

Some maritime cyber risks, however, do not come within the scope of P&I because they do not arise from the operation of a ship. An example is the risk of monetary loss where a shipping company is blackmailed to pay a ransom for the restoration of IT data or restoration of IT systems that have been compromised by cyber-attack.

P&I clubs are not the primary underwriters of war P&I cover, which is often provided as an ancillary cover to an owner's hull war cover. Liabilities arising out of a cyber-attack on a vessel may therefore fall within the war risks exclusion in P&I cover.

IG Clubs do provide a P&I war risk extension cover of up to US\$500 million in excess of the amount recoverable under a vessel's primary war P&I policy, but does not extend to losses under CL380.

The Institute Cyber Attack Exclusion Clause (CL 380) 10/11/2003, or a variant of that clause, has appeared on marine policies for the past 10 years: "in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software program, malicious code, computer virus or process or any other electronic system".

In practical terms, therefore, and to the extent that cyber would be covered by the applicable insurance, any loss or damage (including consequential loss and business interruption) or liabilities attributable to a breakdown of a computer system would prima facie be recoverable from insurers.

However, if the loss, damage, or liability was caused either directly or indirectly by the use of a computer and its associated systems and software "as a means of inflicting harm," such loss, damage, or liability would be excluded from coverage.

Some P&I claims resulting from cyber risks may be excluded from cover by virtue of exclusions relating to paperless trading, or exclusions relating to P&I war risks.

Normal P&I cover is subject to an exclusion in respect of liabilities, losses, costs and expenses arising from the use of any electronic trading system, other than an approved electronic trading system to the extent that such liabilities, losses, costs and expenses would not have arisen under a paper trading system:

Approved Electronic Trading Systems:

- Bolero
- ESS
- E-Title

Electronic trading systems could be vulnerable to cyber-attacks. Although the exclusion does not expressly refer to cyber risks, any liabilities, losses, costs or expenses arising out of a cyber-attack (such as hacker attacks) affecting a non-approved electronic trading system are not covered.

P&I claims arising from cyber risks are covered by UK P&I in the normal way, subject to any separate exclusion under the Rules such as those in respect of war risks or non-approved electronic trading systems.

P&I cover is subject to an exclusion in respect of P&I liabilities, costs or expenses arising from war risks. Depending on motive, a cyber-attack could constitute an "act of terrorism" or even in warlike circumstances a "hostile act by a belligerent power".

A cyber-attack on an individual ship is, however, likely to be regarded as a hostile act of a belligerent power only in the context of civil war or where a rebellion extends to the occupation of territory and organised political authority over military forces.

A cyber-attack on an individual ship could arise for a variety of reasons that do not engage the war exclusion – including, for example, commercial sabotage, or the malicious act of an individual with a grudge against the owning company – and in any such cases a Member's normal P&I cover will respond.

The UK War Risks Club excludes cover for any losses, liabilities, costs or expenses directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer virus. Cyber risks caused by a "computer virus" are therefore excluded. However, the

computer virus exclusion will only apply once claims within the scope of the clause exceed a certain level in the aggregate in a policy year and this is similar across P&I Clubs.

P&I war risks claims resulting from cyber risks may be covered by primary war risks underwriters – for example the UK War Risks Club (where incurred by the member of that club), but in the case of that club subject to a limit of US\$50 million in the aggregate across all such claims of all members arising in the 2020 policy year.

Additional cover is available from UK P&I for P&I war risks claims resulting from cyber risks where such claims are in respect of crew liabilities or legal costs falling within the scope of the Bio-Chem exclusion, subject to a limit of US\$30m in the aggregate any one event.

Excess War Risks P&I cover is subject to a combined Cyber Risk and Bio-Chem exclusion which bars recovery of “losses, liabilities, costs or expenses directly or indirectly caused by or contributed to by or arising from any chemical, biological, bio-chemical or electromagnetic weapon or the use or operation, as a means for inflicting harm, of any computer virus”.

Number of Ships Per London P&I Club

1. Britannia P&I Club (London)	3465
2. Japan P&I Club Liaison Office (London)	4198
3. Gard UK	6600
4. The London P&I Club (London)	3400
5. North of England P&I Club (Newcastle & London)	5000+
6. The Shipowners Club (London)	8398
7. Skuld Underwriting (London)	5789
8. Standard Club (London)	11065
9. Steamship Mutual (London)	9000+
10. The Swedish Club Team London (London)	1699
11. UK P&I (London)	3471
12. West P&I Club (London)	3700
Totals	65785

Source: P&I Clubs

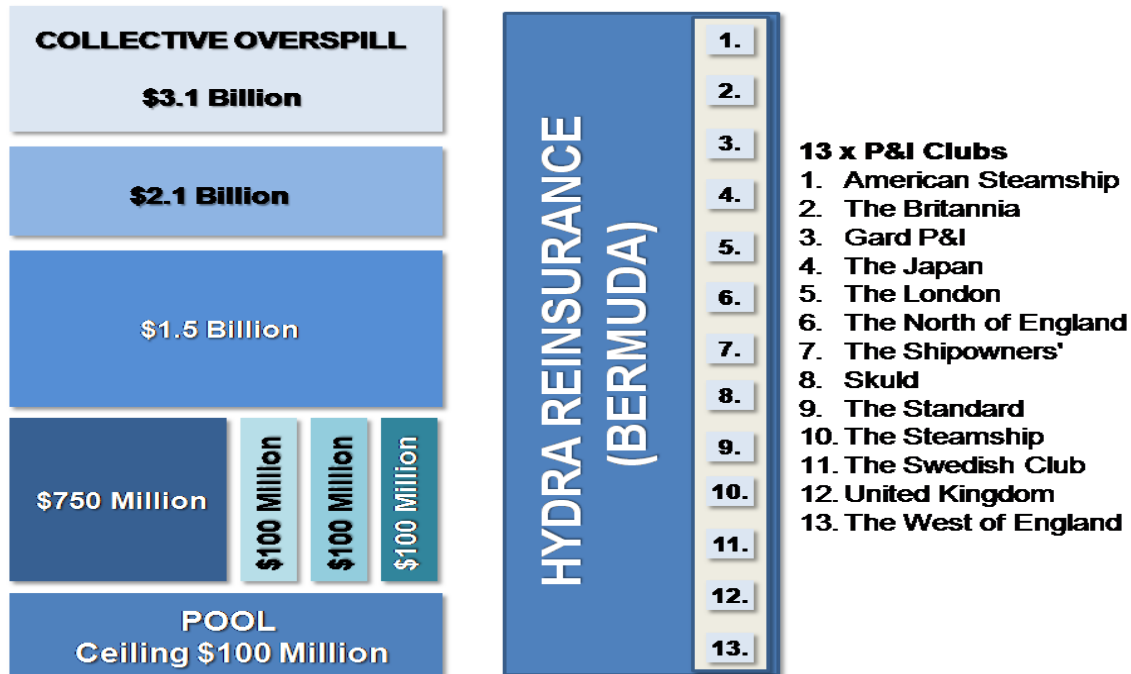
International P&I Club Reinsurance Structure

The structure of the Group’s claims-sharing arrangements (the “Pool”) and the commercial market and captive (Hydra) reinsurance arrangements for the 2020/21 policy year are depicted in the diagram below.

Key Points

1. P&I clubs already use ART, using private placements, for individual and pooled reinsurance.
2. The clubs compete for members and reinsurance rates are a key differentiator.
3. Cyber attacks: covered, but with a \$30 million limit in the aggregate, leaving high risk exposures.

The Pool is structured in three layers from US \$10 million to US \$100 million. Excess of US \$30 million, the Pool is reinsured by the Group captive reinsurance vehicle, Hydra Insurance Company Limited.



Hydra is a Bermuda incorporated Segregated Accounts company in which each of the 13 Group Clubs has its own segregated account (or “cell”) ring fencing its assets and liabilities from those of the company or any of the other Club cells. Hydra reinsures each Club in respect of that Club's liabilities within the Pool and reinsurance layers in which it participates. There are currently three multi-year 10% private placements within the first GXL layer (US \$650 million excess US \$100 million).

Through the participation of Hydra, the Group Clubs can retain, within their Hydra cells, premium which would otherwise have been paid to the commercial reinsurance markets. This reduces the annual premium per P&I Club as well as delivering higher levels of reinsurance cover.

However, the reinsurance cover for cyber is limited to a \$30 million ceiling with the limit placed on the aggregate in the whole per incident. By comparison, a company such as Yahoo has paid out on \$32.5 million in legal fees alone as a settlement for the 2014 data hack. A cyber attack resulting in spillage would be likely to incur many multiples of this figure due to the environmental impact not covered in the reinsurance pool.

Reinsurance Rates IG P&I 2020-2021

Tonnage category	2020 rate per gt – in US cents
Persistent Oil tankers	57.47
Clean Tankers	25.82
Dry	39.71
Passenger	321.61
Chartered tankers	21.58
Chartered dries	10.54

Source: IG P&I Club 2020

Further Marine and Port Risk Background

Vessels have increasingly depended on information technology (IT), taking solutions that offer high functionality at moderate cost out of the office environment. One central concern when delivering

electrical propulsion systems, electrical generation and protection equipment, and automation and advisory solutions is how all these are connected in a network architecture and how the network is connected with other systems on the ship and on land.

Traditionally the different technical solutions have not been connected together in a proper computer network; this has been used to argue that cyber security is not relevant to vessels. This is only partially true. In a disconnected system, there is no risk of a problem occurring during normal operations.

However, typically these systems will occasionally be connected to a maintenance computer, a USB stick or a modem. In these instances, the system is as vulnerable as a connected system. And if a security culture and measures are not in place, malicious code could end up disrupting the system.

Typically, all these marine automation systems will be located in one inner security zone. Other equally important security zones could include the navigation system network. At the next level up, a zone connects some of the most critical areas, which could also include systems not as critical for running the ship safely. This zone is called the ship Technical Net. It could be connected through a firewall to an open ship network, which is then connected to the world through a satellite link.

Many people access an open ship intranet, such as that of a cruise ship or ferry. On other vessels, off-duty crews use the network for getting news, contacting friends and family, etc. Such generic Internet traffic is valuable and should, of course, be used; however, use should be restricted to the part of the network where malicious code or simple mistakes cannot influence the operation of the vessel.

There are stronger incentives for digitally enhanced operations than crew cost. If for example machine-assisted viewing gains acceptance, requirements for line-of-sight from the bridge could be relaxed, and container ships could take more containers thereby providing a direct and immediate business case.

Vessel Digitisation

As for every digital industry, shipping is exposed to malware and multiple other cyber threats. However, the viruses that threaten to break the maritime supply chain and delay cargo delivery carry additional risks. Infected systems can compromise navigation or propulsion, threatening ship safety itself as well as the marine environment. With broadband internet connectivity available for vessels globally, and viruses such as NotPetya and Wannacry expose vulnerabilities within older, legacy systems found on vessels globally.

Shipping's well-publicized journey towards digitalization and greater automation therefore demands an accompanying commitment to increase IT security and mitigate cyber risks through system robustness, but also through additional training and continuous awareness-raising. The need for advanced maritime cybersecurity is expanding in both IT and Operational Technology (OT).

Maritime traditionally has large volumes of data that is not utilised, with legacy equipment data typically not correlating with digital systems. Maritime digitalization process typically starts by addressing cost savings, providing tools for analytics of routes, fuel consumption, emissions, and fleet management.

Increasingly common however is the use of digital sensors. The technology for monitoring ship operations and performance has been building in sophistication. Ships of the future will have a complete network of sensors to measure all aspects of operations, including detecting faults and identifying areas needing maintenance or repair. Allied to this, increasingly powerful ship to shore

communications will mean that most aspects of the ship's operation can be controlled by a land-based team of fleet managers.

The challenges

There is increasing convergence between the IT and OT, with Industrial IoT expanding. Closed networks are no longer air-gapped and as Covid-19 has demonstrated, can be rapidly transformed to networks connected to office networks and cloud. This introduces multiple risks for the marine sector, affecting the entire Industrial Automation and Control Systems (IACS) beyond marine e.g. utilities, rail networks, airports.

Marine industrial facilities increasingly integrate computer networks previously isolated control systems, connecting all of the organization's computer systems based on open networking standards to operate more efficiently and effectively. Integrating sensor and enterprise data into vessels increases visibility throughout the ship, with 24/7 systems availability, assisting in rapid resolution of problems, and reducing operational and support costs in a sector with constant margin pressures.

Among the control systems connected to the integrated marine networks are Supervisory Control and Data Acquisition (SCADA) systems, Plant Distributed Control Systems (DCSes), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), intelligent field devices and drives, smart meters, and other embedded industrial control and monitoring systems.

Key Points

1. Industrial control systems are not designed with security in mind; lacking basic protection mechanisms.
2. Industrial protocols are developed for trusted networks; reliability and availability as main priorities.
3. Emerging technologies expose industrial devices to heightened risk of a cyber attack.
4. Risk carriers and modellers are not active in PLC risk models: an opportunity for Quantar.

These fulfil a variety of functions ranging from sensor data collection to centralized monitoring and control of entire vessels, warehouses, or complexes of systems over large geographic areas, such as ports. Due to budget limitations, such control networks are often managed by remote employees, contractors and vendors increasing cyber vulnerabilities.

Many ICS have moved towards the use of open, standards-based functionality which provides outstanding integration and operational benefits, but in turn expose them to security threats ranging from malicious code and attacks by hackers, to operator error and technology failures.

Cyber security has not traditionally been a primary consideration in developing industrial control systems. Human-Machine Interfaces (HMIs) typically utilize unsecured networking stacks, common operating systems and applications that are seldom patched after initial deployment. Many of the forms of remote access used in the marine sector by control networks also create vulnerabilities

Another further marine security challenge is presented by the ubiquity of wireless systems that are vulnerable to threats including eavesdropping, rogue access points, interference from natural forces or reconfiguration of the physical space. With the advent of wireless-capable devices, as well as access through modems, radio and cellular links, the traditional physical security perimeter organizations once relied upon has more or less disappeared altogether.

The interconnectedness of shipping with the global internet and equipped with industry 4.0 create specific marine risks including ghosting of GPS systems, taking over of command-and-control systems, disruption attacks, ransomware and even cyber commercial intelligence gathering. Official records lack attack data because marine companies are reluctant to report for fear of reputation damage, in the same manner that companies such as Control Risks Group operate covertly in corporate kidnapping cases. However, there is evidence that a successful cyber attack may cost a shipping company the equivalent of losing one or two ships. Lloyd's of London has warned that a serious cyber attack could cost the global economy more than £92bn from disruptions, theft on ships, ports, refineries, terminals and support systems. An oil tanker is able to carry up to \$100m-worth of crude, container vessels are frequently loaded with perishable fruit and vegetables; a vehicle carrier with 1,200 luxury cars can be worth \$53m.

In the recent past, most ocean-going vessels operated with isolated dedicated industrial control systems with customised network protocols and a virtual absence of security systems within the safety-critical systems. This lack of security did not matter much as long as physical security of the endpoints and communications were maintained.

Vessels today are equipped with a range of electronic navigation, command-and-control systems interconnected to the global internet via satellite. However, satellite communication terminals are easily hacked. Additionally, crew member access to the internet creates connected and automated systems exposed to attack; internally and externally.

There are many access routes on a vessel for cyber attackers to access including all points where connected devices and systems intersect and interact with employees; laptops, tablets and mobile phones to share operational manuals and chart updates. These access points radiate via many devices to application groups and onwards to service sectors and locations, affecting supply chains, headquarters, ports, terminals and ships.

A vessel's navigation system is crucial to its operations and the most vulnerable to a cyber attack such as spoofing, because it is based on an electronic chart display and information system (ECDIS), along with inputs from satellite positioning systems such as GPS and from AIS, the automatic identification system used to provide information about vessels to other ships and coastal authorities. Ships with a tonnage over 10 000 tons are required to use the automatic identification system (AIS) that, if breached, could cause collisions and losses globally.

One widely reported example of this kind of disruption occurred in 2017. Here, a master of a ship positioned off the Russian Black Sea port of Novorossiysk, noted that his global positioning system placed his ship over 32km inland, at Gelendzhik Airport. The AIS (automatic identification system) used to track vessels also placed at least another 20 ships at the same airport in this incident.

Adoption of IoT technology within the marine sector, coupled with use of weak default passwords, failure to apply software updates and a lack of encryption opens the way to a variety of attacks. Such shortcomings may explain the 2017 cyber attack on the world's biggest container fleet operator, Danish shipping company Maersk. In June 2017, Maersk was the victim of a major cybersecurity incident: an attack with NotPetya malware, which forced the company offline for ten days, shutting down several ports and forcing the company to handle 80 per cent of its operations manually. This attack caused a \$250-300m impact, and 50,000 devices had to be updated.

Onshore, leading UK shipping broker Clarksons was the victim of a hacking and blackmail incident in November 2017. According to Clarksons, hackers accessed its systems through a single user account

demanding a ransom to prevent public release of the information and for the return of stolen information.

Another example is the hacking into the Port of San Francisco Electronic Information System, “moving the port” in cyberspace twenty miles north which became problematic in the foggy weather.

In June 2017, the International Maritime Organization (IMO) Maritime Safety Committee adopted Resolution MSC.428 (98) on Maritime Cyber Risk Management in Safety Management Systems. This resolution, for implementation by 1 January 2021, introduces regulatory measures to “make sure that cyber risks are addressed in existing safety management systems (as defined in the International Safety Management (ISM) Code)”.

The legislation requires that ships are issued with a cyber-security certificate by an approved body or flag or port state. In addition, to raise the compliance rate, vessels without such a certificate could be detained. The Document of Compliance holder is ultimately responsible for ensuring the management of cyber risks on board each vessel. The onus under the new law is placed upon the vessel owner to prove compliance, as per GDPR, rather than a regulatory authority having to prove non-compliance.

For Europe, the EU has taken the first step with introducing the General Data Protection Regulation, which applies to all commercial firms including shipping companies. Under this regulation, it requires shipping companies to be more proactive in their cyber security. This is because they now must make sure data subjects’ consent is not only freely given but also as easy to withdraw as to provide, and they must use secure systems for the storage and processing of data.

In addition, with implementing the EU’s Networks and Information Systems directive (NIS Directive EU 2016/1148), ship-owners, as “operators of essential services”, are liable for failing to “take proper and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies”.

To cope with operational issues such as denied physical access, quarantined vessels and travel restrictions, ship-owners are now actively developing remote access capabilities and implementing remote digital survey tools and encouraging shore stations to work remotely from home. This process has been sped up by the Covid-19 crisis.

An added issue is that shore-side and onboard personnel may be unaware that some equipment manufacturers maintain remote access to shipboard equipment and network systems given most vessels do not carry a specialist on cost grounds.

Some IT and OT systems can be accessed remotely and may have a continuous internet connection for remote monitoring, data collection, maintenance, safety and security. These can be “third-party systems”, whereby the contractor monitors and maintains the systems from a remote location and can be both two-way data flow, or, upload-only. Unknown and uncoordinated remote access to an operating ship is clearly a third party risk that is frequently unrecognised in managing electronic threats on vessels.

Four Main Risk Categories:

Machinery:

- Remote condition monitoring of electronically controlled engines (propulsion, power generation, steering systems, etc.)

Communication systems

- Ship’s administration system
- Crew welfare system
- Public network for passengers
- Communication via GMDSS considered

- Can shut down systems in case of operation beyond set parameters
- Remote control for troubleshooting
- low risk
- Unprotected port Wi Fi systems and 4G are high risk

Cargo and ballast control systems

- Remote control of valves, pumps, compressors, etc.
- Reefers and other high value cargo stowed in containers being fitted with GPS tracking systems

Other

- Paperless trading (e Bs /L, e Manifest)
- Cruise vessels : passenger data and payment systems

Examples of systems/workstations with remote access:

1. Bridge, engine room computers, workstations on a vessel's administrative network
2. Cargo such as containers with reefer temperature control systems; specialised cargo tracked remotely
3. Vessel stability decision support systems
4. Hull stress monitoring systems
5. Navigational systems including Electronic Navigation Chart (ENC) Voyage Data Recorder (VDR)
6. Dynamic positioning systems (DP)
7. Cargo handling and stowage, engine and cargo management, load planning systems
8. Safety and security networks, such as CCTV (closed circuit television)
9. Emergency Shut-down (ESD) for gas tankers, submarine cable installation and repair.

Examples of common marine-specific cyber vulnerabilities:

1. Obsolete/unsupported operating systems
2. Outdated/ missing antivirus software and protection from malware
3. Inadequate security configurations, best practices and ineffective network management
4. Use of default administrator accounts and passwords
5. Shipboard computer networks lacking boundary protection measures and network segmentation
6. Safety-critical equipment/systems permanently connected to the shore side
7. Inadequate third party access controls; contractors/service providers

Additionally, all navigation systems are unencrypted and thus vulnerable to attacks:

GPS	AIS	Gyro
ECDIS	Radar	VDR

Switchgear on vessels is increasingly networked via Simple Network Management Protocol (SNMP) cards. SNMP is not secure. In the case of switchgear systems, the US Industrial Control System – Computer Emergency Response Team (ICS-CERT) has reported specific cases of switchgear being attacked via its SNMP port. the SNMP security features of the switchgear were easily fooled by IP spoofing.

The current, supposedly more secure SNMPv3 has been fully compromised by hackers taking only a few minutes of medium skill to break into an SNMPv3 device; or a few seconds to break into an SNMPv1 or v2 system. In addition, many switchgear systems employ the use of Modbus Communications. Modbus is a protocol that is designated as “Insecure by Design” (IbD) because it has no security within its structure whatsoever.

Fortunately, most switchgear does not allow a remote user to actually change settings on the switchgear. But, this is not the case with Programmable Logic Controllers (PLC's). PLC's allow anyone

with the capability to program the unit to execute control code to open and close switches, breakers, etc. Most PLC's also use Modbus as their standard communications interface and some use SNMP as well.

A further serious concern is the fact that a number of PLC's have been found to have flaws in their design that allows remote users to reprogram the unit to do as they wish, without having any security authorization. A recent example of this can be seen in the Eaton ELCSOFT programmer.

Security body PLCNCCIC/ICS-CERT issued the following alert in respect of the flaw:

"buffer overflow vulnerabilities affecting Eaton ELCSOFT, a PLC programming software for Eaton Logic Control (ELC) controllers - a hacker of even modest skill can use the Eaton programming software to place their own code onto the PLC with no authorization".

There are a number of PLC's that have been found to be vulnerable to similar exploits.

Key Point:

The majority of global power control systems are similarly vulnerable due to this type of controller. Whilst vessels may have several PLC's on-board, or possibly hundreds in the case of ultra-large cruise vessels, the number per major utility location may run into multiples of this.

As such, whilst the marine sector alone is large enough to sustain a business, the natural fit to utilities and smart cities, for example, makes a compelling case for commencing in marine and expanding as the company's capabilities and experience develop.

The side effects of disasters caused by a hacked port system or deluded on-board ship system include environmental threats. Serious damage resulting in closure of trade ways leads to complications including shifting of long-term trade and shipping routes and may require rebuilding the infrastructure such as locks and dams as well as commercially established networks. The automatic identification system (AIS) has several (in some cases up to seven) key systems dependent upon it, including radar and the chart plotter. Further, the human control of the ship and port is being reduced while the Internet of Things (IoT) plays an increasing role in ship and port governance, surveillance and monitoring systems.

The state-of-art ship technology minimizes traditional navigation and communication systems and the role of officers and engineers of modern merchant ships is deferred to monitoring. This increased automation and the decrease of human intervention on ships and in ports provides fertile ground for security breaches.

As the internet becomes more and more part of port operations and as the internet enters all commercial ships the AIS aboard ships will be increasingly more vulnerable to cyber-attacks. The nature of the industry provides many challenges particularly with many operators and users. A terminal operator may be concerned about a large number of local agents, ships and operators that have shared access to key backend systems. This shared access inadvertently gives users an ability to penetrate the terminal operators overall corporate systems. In addition to shared access, each user may have their own cyber infrastructure platforms which may interfere with the terminal operators' platform.

The most common manipulation to the AIS system is "spoofing." Spoofing occurs when either the authentic AIS is overlaid with a signal of greater power and of different content to capture the receiver

or the AIS is simply jammed by generating a cluster of false AIS messages and create a new message at another time delay and/or frequency. It is also possible for the AIS monitoring system to disappear due to cutting, or reducing, electrical power on the ship. Further, when electrical power is manipulated the AIS system may send the wrong information.

A future trend is towards full autonomous shipping and by the end of the decade, it is expected that the world's first autonomous container ship will have embarked on its maiden voyage, moving goods around the coastline of Norway. Together with other initiatives currently underway, such as the development of remote controlled vessels, this will mark a new era of connected shipping technology in a \$210 billion industry.

One of the most difficult challenges with maritime cybersecurity is that every ship is different. There's little standardisation, especially when it comes to on-board control systems, and a high mix of legacy systems – many of which were never designed with security in mind – and additional networked technologies which have been added over time.

Many vessels have a 'flat' network structure, in which new internet connected systems for navigation and communications have been placed on the same networks as older control hardware. This introduces multiple vulnerabilities into systems which do not have adequate built-in protections.

In addition, the operating environment is also much more challenging than typical industrial setups. Most ships rely on Very Small Aperture Terminal (VSAT) satellite communications for connectivity, which is low bandwidth and high latency. It can carry some communications, such as email and navigational data, but isn't reliable enough for the most effective security measures recommended to shore bound industries: regular patching and updates.

Manual patching still takes place, but the current nature of the industry, seeking cost reductions where they can be found, means that ships spend as little time in port as possible. When they are docked, and bandwidth is available, security updates come a long way down the list of priorities, behind upgrades to navigational software and downloading new digital entertainment for the crew.

Critical ship control systems, including IP-to-serial converters, GPS receivers or the Voyage Data Recorder (VDR), tend to be easily compromised; some on-board devices for instance still run Windows XP and even Windows NT, with converters rarely having their admin passwords changed.

Those that do have non-default credentials will likely have such out of date firmware that they're easily exploited anyway: Many of the industrial serial device servers, used for serial port to ethernet connectivity commonly found aboard vessels, have been found to be vulnerable to firmware downgrade attacks allowing trivial compromise. This includes the Moxa brand of marine serial device servers that are extremely common on vessels.

Password security and patch management are so poor at sea that compromise does not require significant expertise. There is, for example, a documented case of a youth finding a mobile drilling platform control system using the search engine Shodan that reveals specific types of computers connected to the internet (routers, web servers, servers, etc). Upon clicking buttons to see what happened, the platform's dynamic positioning system was taken offline.

These easily hacked devices communicate with a large number of control systems via a standardized messaging system, called NMEA 0183 messaging (a superset of the messaging format that GPS devices use). These include autopilot systems, propulsion control, dynamic positioning, engine control, ballast control and digital compasses; all can potentially steer a ship off-course, or cause catastrophe.

The messages are usually exchanged using RS485 serial datacomms, either directly or encapsulated, over IP networks. In some cases, control area network (CAN) is used as a bridge between IP and serial. Any point where serial meets IP is an exploit point for hackers. Access to control systems can be attained remotely or locally. Serial network attacks can be carried out remotely via the satellite communication systems connection, or by physically locating the converters.

Ports

Port authorities manage the flow of ships in and out, and the flow of cargo off and on each of those ships. Currently, these processes are primarily human directed; an incoming ship will typically check in with a harbourmaster and its freight is signed for using paperwork. With local authority budgets small, the broad scale of inefficiencies embedded within port operations, there is an ongoing drive to seek out automation opportunities throughout the operational chain within ports.

The key for port operation lies in establishing identity and tying that identity to the supply chain. This commonly entails taking images of each vessel's serial number, attaching that marker to its cargo, the dockworker checking it in and continuing tracking down the chain to the vehicle that collects each container. Most of the IoT systems being put in place to digitize this process were not built with security in mind and are very easy to penetrate using low level of hacking skills. Where such systems can be compromised, high-risk security events occur. Documented examples exist where a bad actor instructs the system to permit specific containers to pass through a port unsearched.

Digital transformation requires all systems and sensors to be interconnected to achieve the desired business automation. However, with disparate operations within a port, linking all together is complex and offers potential for creating exploitable weak points. The primary functions within ports are:

Port Operations

- Port Control & Administration
- Security Control & Administration
- Customs & Border Control
- Cargo Reception, Handling and Storage
- Supply Chain Facilities

Risks posed to ports include:

Port Risks

- (a) loss or theft of assets, including documents and storage media;
- (b) unauthorised access to data or information;
- (c) loss, compromise, unauthorised manipulation or change of data or information;
- (d) loss or compromise of port assets connected to its systems;
- (e) planting of bugs or other surveillance devices;
- (f) accidental or deliberate Global Navigation Satellite System (GNSS) jamming or interference; and
- (g) insertion of malicious software.

Example of Port Volumes Per Country - Main UK Ports:

1. AB Ports	46. Liverpool
2. Aberdeenshire Council Harbours	47. Leith
3. Able Humber Port	48. Inverness Harbour Trust
4. Argyll & Bute Council Harbours	49. Lowestoft
5. Associated British Ports	50. London

6. Ayr	51. Lerwick Port Authority
7. Barrow	52. London Gateway
8. Barry	53. Marine Resource Centre
9. Belfast	54. Manchester Ship Canal
10. Berwick Harbour	55. Medway Ports
11. Bird Port	56. Methil
12. Birkenhead	57. Milford Haven
13. Bristol	58. Newhaven Port
14. British Waterways	59. Newport
15. Burntisland	60. Northern Lighthouse Board
16. Cargo Marine	61. Montrose Port Authority
17. Cardiff Harbour	62. Peel Ports
18. Chatham Docks	63. Peterhead Port Authority
19. Clydeport Ltd	64. Perth Harbour
20. Comhairlie Nan Eilean Siar	65. Orkney Islands Council
21. Cromarty Firth Port Authority	66. Poole
22. Dover Port	67. Port Talbot
23. Douglas Port	68. Portland Port
24. Dumfries and Gallosway Council Harbours	69. Plymouth
25. Dundee	70. Portsmouth Port
26. Fairlie Quay	71. Rosyth
27. Falmouth Harbour Commissioners	72. Scrabster Harbour Trust
28. Fleetwood	73. Scotland & Ireland Division
29. Felixstowe	74. Southampton
30. Fraserburgh Harbour	75. Shetland Islands Council
31. Fowey Harbour	76. Sherness Port
32. Forth Ports PLC	77. Shoreham Port
33. Garston	78. Silloth
34. Grimsby	79. Swansea
35. Grangemouth	80. Stornoway Port Authority
36. Goole	81. Sunderland
37. Kishorn Quay	82. Tees
38. King's Lynn	83. Tilbury
39. Heysham Port	84. Teeside Port
40. Holyhead Port	85. Teignmouth
41. Hull	86. Warrenpoint Port
42. Hartlepool	87. Whitby
43. Highland Harbours	88. Troon
44. Immingham	89. Wick Harbour
45. Ipswich	90. Whitehills Harbour

Fit to Existing DMGT-V Portfolio

DMGT already owns or holds interests in risk modelling firms; Praedicat and RMS. Each of these is a specialist in their respective fields, although RMS has expanded into cyber risk modelling, personnel have joined competitor Guidewire/Cyence and the cyber insurance market currently offers no scope for growth or revenue opportunity as a direct result of Covid-19. The erosion of Solvency SRC across the risk carrier spectrum, allied to the increased silent cyber risk posed by the massive uplift in remote working, has removed cyber risk modelling for underwriting as a priority.

DMGT has a recent history of selling interests in entities that are no longer within the reduced portfolio focus; from 10 down to 5 in 2020. These include the sale of Genscape to Verisk for £298 ©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

million, with revenues of \$100 million, following its acquisition in 2006 for £73 million. Verisk may play a part in a divestment strategy option and having this prior commercial relationship would benefit the current proposed development.

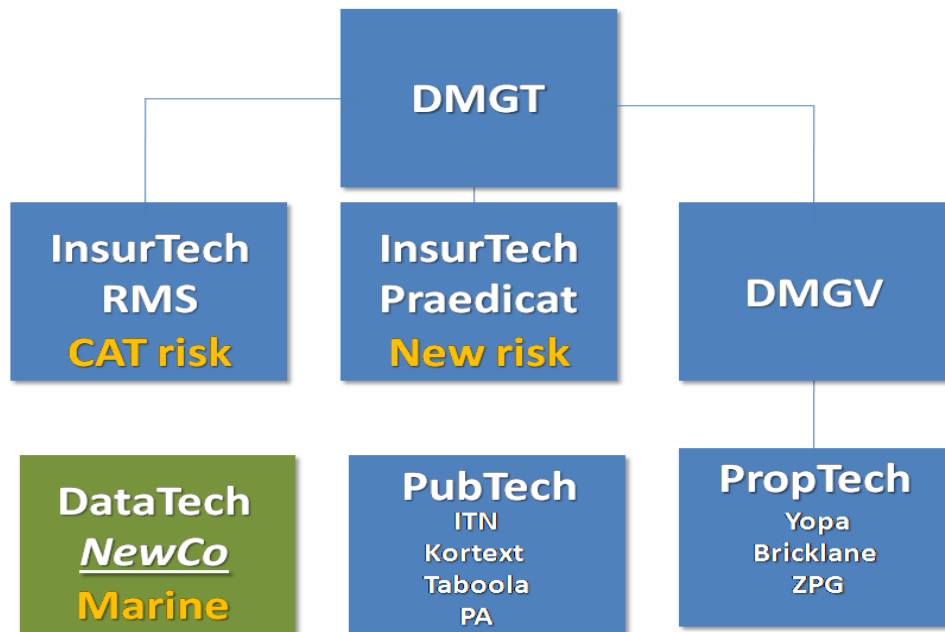
Key Points:

1. Phase 1 will result in loss; the objective is to attain installations per vessel/per major carriers and acquire marine-specific cyber threat data that no other company has, using Quantar patented backend software and hardware;
2. Exit model is 3-5 year horizon, with true revenue streams coming from Phase 2, Year 2 i.e. Year 3 of operation. A year 4-5 time horizon is more realistic for divestment to a risk carrier or shipping company i.e. mid-term view required in assessing plan;
3. As with RMS and Praedicat, the older and larger the volume of total data, the greater the value of the company, with the addition of the degree of difficulty in acquiring marine-specific cyber threat data creates extreme switching and transfer costs for shipping companies as well as risk carriers.

Further, one of the potential parties in discussion with DMGT for the sale of Genscape was IHS Markit; a data company that is heavily involved in the marine sector, albeit not within the segment proposed herein. IHS Markit has been responsible for the allocation of IMO numbers to vessels globally and therefore has a strong link to the Regulator. It also has a marine data subscription service that would benefit from the data provided by the proposed entity. This would make IHS Markit a strong potential divestment target in the future.

Additional recent DMGT divestments of On-Geo and Real Capital Analytics, despite remaining in PropTech, illustrates the strategy of DMGT in focussing upon a specific set of B2B products and services, to which the current proposal is aligned, yet separate to existing offerings. It also demonstrates the ability to monetise from investments, which may apply to the proposal herein within a 3-5 year period of trading.

With Covid-19 having long-term implications for DMGT operations such as Exhibitions, this proposal may be viewed as a low-risk mitigation option against falling revenues from that unit, with long-term stable potential and a potentially high exit margin.



Similar or Same Deliverables as RMS & Praedicat:

ENABLEMENT FOR RISK CARRIER CLIENTS:

- Efficient use of capital and maximizing of return on that capital
- The equitable and transparent transfer of catastrophe risk from risk holder to risk taker
- Expansion into new insurance products

TARGET CUSTOMERS RISK MANAGEMENT LIFE CYCLE:

1. Identify
2. Select
3. Price
4. Optimise
5. Profit & ROI
6. Mitigate
7. Manage
8. Understand
9. Regulatory Compliance

Platform Rationale:	Product development cycles	Functional Spend: % Expenses
Open Future-proof Modular Allows differentiation Value to partners and clients	New Models in development 1-4 years New data & analytics products take up to 6-12 months for first versions, then iterate per quarter	Selling, General & Admin (SG&A) 27% COGS 22% Product / R&D 51% (74% of all expense is employee and related)

Prior Go-To Market Efforts

Quantar Solutions launched market test in November 2009, in London as a sponsor of the Business Continuity Institute conference and exhibition. It subsequently exhibited at the International Security and National Resilience exhibition in Abu Dhabi in 2011 and at the Risk and Insurance Managers

©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

conference and exhibition in Boston in 2011. The resulting leads were followed up by presentations in Kuwait at the National Bank of Kuwait, the National Guard and the Central Agency for Information Technology.

Additionally between 2011- 2013, presentations were made to Willis, Marsh, Swiss Re, Munich Re, Achmea, Dresdner Kleinwort Wasserstein. Joint venture or patent licensing/exit discussions were undertaken with SAS Corporation, Oracle, IBM and NetDiligence. Between 2013 - 2016 company and patent portfolio sale were negotiated with Cyberpoint International, GTT Group, Intellectual Ventures, Tangible IP, Iceberg IP, RPX Corp, Allied Security Trust, and Pluritas.

In 2017- 2018, pitches to market were made at Board/C-suite level at Nestlé, Vevey Switzerland, Hiscox, London, Lloyds Lab and Magnum Capital. Aggressive non-practising entities (patent trolls), Iceberg IP, Siskin Capital, Parallel North IP, N&G Consulting, Vitek Intellectual Property, Dynamic IP Deals and Acacia Research contacted Quantar Solutions to seek out patent infringement and licensing opportunities.

The rationale for the disparate markets for initial testing was due to the depth and breadth of cyber risk management; IT Security, business continuity, regulatory compliance (Basel II, Solvency II, GDPR, AML, NIS, etc), cyber insurance underwriting, cyber risk transfer product development, carrier portfolio risk management. When reviewing the above, it is clear that exactly the same areas are covered today; in 20 years, the scenarios have not altered, indeed, there is a greater demand than ever to manage cyber threats, requiring assessment, quantification and identification as the underlying requisites for cyber risk management.

Quantar was unable to execute a go-to-market strategy for the following reasons:

1. Too early for cyber insurance 2000 - 2013; still viewed as an IT security issue and not a corporate one until major US hacks and subsequent financial penalties/reputational damage;
2. Silent cyber perils prevent risk carriers from offering the level of cyber insurance cover required by major corporations; a situation that continues today, with low ceilings and a lack of cyber reinsurance capacity globally;
3. The US cyber market has a clear and continued focus upon the E&O market as an extension of existing products, with a cyber addition. There is no business case for expanding into core cyber insurance products when the global cyber insurance market accounts for less than 1% of global P&C revenues when risk of loss remains high with cyber;
4. A lack of belief in the models developed by cyber risk modelling companies, such as Cybercube, Corax Cyber, Risklens, SSIC, etc, since they utilise a top-down approach and peer grouping to arrive at risk exposures; a completely incorrect form of modelling cyber risks due to the use of underwriters and actuaries to develop models;
5. Covid-19 has pushed many risk carriers and most reinsurers into precarious Solvency II ratio levels. This is particularly the case where business interruption was included within P&C policies and requiring increased capitalization or a culling of product portfolios to reduce overall portfolio exposures;
6. The patent case of Alice Corporation V CLS Bank International put at doubt the patentability of business methods. Incorrect advice from the company's IP attorneys on not going to market in the US without patents having been granted, coupled with "Alice" created uncertainty of direction. Patent assertion entities had their business models eliminated e.g. Intellectual Ventures, removing portfolio divestment and reducing the ability to attain joint venture partners;

7. Lack of runway; all development over the past 20 years has been through the Founder utilising consulting revenues to fund CyCalc and IP development; a lack of continued traction resulted in pausing the company's operation until alternative strategies were formulated.

The continued lack of traction for cyber insurance modelling within the core corporate market is demonstrated by the still-low ceilings on offer by carriers. Typically, \$250 million limits are still imposed by carriers, with a sparse number offering up to \$500 million, but with narrowly defined trigger and points. Attachment point remain high, leaving clients with exposure gaps that are difficult or impossible to cover.

This has resulted in cyber modelling companies failing, such as Pivotpoint Risk Analytics, Corax Cyber, SSIC, despite backing of big-tech in some cases such as SSIC with Unisys and Risklens with Dell RSA. No cyber risk modelling entities have made operating profits, with some pivoting in their business models, such as Guidewire after their acquisition of Cyence for \$270 million in 2017 for its cyber analytics software and having to transition away and to offering an InsureTech platform instead.

Fortunately for both Praedicat and RMS, their core service offerings of modelling pandemic risks and natural catastrophe events have strong demand as a result of Covid-19 and the losses incurred in 2019 from global weather events impacting the carrier market. Indeed, Praedicat has been utilised to place two recent successful ILS products by Achmea Re (former employer of the founder) covering natural wind risks for windmills across Europe - see Annex for ILS data. Operating margins have reduced for RMS in the period 2019-20; from 22% to 16% as a result of Covid, requiring them to optimise their ongoing platform development as soon as possible, without additional distractions.

Why not part of RMS or Praedicat?

Our proposal is to focus upon a specific sector, marine, using the same model as with the two complementary companies within the portfolio. Within the marine segment, the risks are highly specific to the use of industrial control systems with proprietary implementations due to the differences between vessels. Insurers and reinsurers are concerned with aggregation risk for their risk portfolios comprised of cyber policies, whereas with the marine sector operating risk pooling and captive reinsurance, the P&I Club operations are more concerned with environmental risks arising from cyber attacks.

The data and models required for marine are the same as for other sectors, however, the additional development of the existing software and systems will create bespoke marine sector products. Quantar's models could potentially benefit from inputs from both Praedicat and RMS given marine supply chain continuity is dependent upon both health-related pandemic risks and natural catastrophes. There are therefore synergies to be extracted from the proposed structure separate from RMS and Praedicat.

RMS utilises external parties for model development, such as:

- **Model Partners:** Applied Research Associates, Catalytics, CATRisk Solutions, COMBUS, ERN, JBA Risk Management, Risk Frontiers, QuakeRisk.
- **App Partners:** Analyze Re, SpatialKey.

It would therefore be necessary to manage IP created by the new entity and how it would be utilised by RMS and Praedicat where there is a requirement for collaboration, given the dependence of RMS upon third party supplies of IP to its products. A stand-alone entity would resolve this potential issue, whilst still offering scope for collaboration.

RMS does already provide modelling services for the marine sector, but in a different segment; platforms and cargo loss modelling, plus a proposed CAT modelling product for ports. These are very distinct and separated within the risk carrier sector; cargo losses are GIT whereas cyber impacts upon protection and indemnity. How each is modelled and covered can be regarded effectively as two different sectors.

In 2017, under the previous CEO, RMS was partnering with 7 clients within the marine sector to build a modelling solution. This was however, an analytics solution for moveable risks and not for regulatory compliance, nor for marine cyber, despite the forthcoming cyber regulations being published in 2016. As such, RMS has no focus upon the same market segment as proposed herein, nor does RMS address P&I Club risk transfer solutions and development of ART.

Praedicat does not offer bespoke marine services, however, the use of externally sourced data is an area that the current program could draw upon to add to the means the software and systems currently acquire and model from such external data.

Further, the marine sector is so extensive in its depth and breadth that it is one that does not offer a “winner takes all” possibility. Under the new IMO regulations, marine now also includes warehousing and inland shipping (normally labelled inland marine and distinct from vessels and offshore operations). This extension of the applicability of the cyber regulations increases the total market exponentially.

Key Points

1. The proposed development is complimentary to RMS and Praedicat; potential for data sharing.
2. Portfolio risk reduced by ring-fencing new operation as a separate legal entity until developed.
3. New entrants such as Jupiter¹, CelsiusPro AG² pose threats to RMS through high specialization.
4. Future integration could be a development path option where required.
5. The business model is the same as for RMS & Praedicat and is therefore a known format.
6. Guidewire & PCS own cyber threat patents; RMS does not. Quantar's patents can protect RMS.
7. Quantar: previous JV discussions with Guidewire, Cybercube, Verisk for cyber/ IP 2017-2019.

The overall business models of the proposed program, RMS and Praedicat remains the same, in that value is contained within the data acquired; from specific clients plus external data. In all cases, the ability to capture and model from such data creates both a barrier to entry as well as a high switching cost for clients.

At present, there would appear to be an absence of data collaboration across the separate corporate entities. However, in developing marine risk transfer products, the opportunity to create some form of internal data transfer may well arise. How this is executed will only become apparent as the program progresses. Internal charging structures may be required, or an entirely new data-holding entity established.

We Can Do This Ourselves with RMS

There is the opportunity to develop the same concept within RMS, however there are a number of reasons why this may not be practical or cost-effective:

¹ Jupiter ClimateScore Global backed by ILS company Nephila Capital

² CelsiusPro AG, the Swiss headquartered weather index insurance and parametric risk transfer specialist

©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

1. RMS has to pivot away from traditional cyber due to Covid-19 and focus upon epidemiological modelling and CAT risk to make up for lost 2020 revenues as a result of Covid and the effective closure of the cyber underwriting market;
2. RMS does not have models that suit the purpose of marine cyber; their models are lacking the bottom-up methodology and developing them would incur higher R&D and execution costs due to the OpEx structure of RMS as a larger entity;
3. The ability to move fast is necessary and RMS has a reputation; internally and externally for being incapable of do so, with internal friction between the modelling side of the business and the developer side (see RMS One as a prime example and execution failure);
4. Network traffic capture is simple; the means of so doing without compromising the integrity of the data and the risk of data privacy breach means RMS would need to also develop the back-end system instead of utilising a ready-made software product;
5. The methods of the back and front end of Quantar's products are patented and RMS has no such patents; going it alone would open up RMS to exposure to a competitor or an NPE that acquires the portfolio in order to capitalise Quantar for an entry into marine;
6. The proposed program ring-fences risk to the overall DMGT portfolio of companies;
7. A stand-alone company/program enables a build fast / fail fast agile method of development and offers ongoing windows to close down the program and limit losses; running the program within RMS would be far more difficult to built and then close down.

NOTE: As at September 14, 2020, global brokers Guy Carpenter assessed the impact of business interruption insurance claims as being highly unlikely to be settled before January 2021 (the global reinsurance renewal period), creating further uncertainty for the insurance risk markets.

Further, they note that although there have been single no stand-out catastrophic events to date in 2020, there have been a sufficient number of events of significance impacting upon risk carriers, Hurricane Irma; California/Oregon Wildfires, events in Japan. This has created further uncertainty in the present risk models. The consequence of this is a requirement to re-assess pre-existing CAT models and thus will impact upon RMS and Praedicat directly.

Long-term Versus Exit Strategy

The marine and utilities sectors are sufficiently large to support a supplier for long term growth (3-5 years before exit), with stable revenues i.e. the global fleet does not vary in count or volume in the manner of other sectors. As such, the intention at the outset is to develop and build the company with a long-term ownership objective as a privately listed company.

However, there may be opportunities to divest to entities such as P&I Clubs, marine equipment companies, competitors, or to fold into RMS within a short period (3 years onwards), due to the revenue potential to add to existing lines of associated business. DMGT-V has extensive experience of both build-to-keep and build fast and exit models and the company will be guided by such experience as it develops its products and builds the client-base e.g. Chemist Direct/Pharmacy2U; PA Media Group; Taboola; Bricklane, all of which rely upon data for their business models.

As described above, other modelling companies such as Verisk and IHS Markit are also potential acquirers due to their operations within the marine sector. Where there is sufficient data acquired over time by the proposed new entity, it would create a credible opportunity for DMGT to sell with the same multiples attained for Genscape due to the portfolio fit for Verisk and IHS Markit.

Careful consideration of the IP owned by the entity requires assessment where it is used to protect RMS from patent infringement contentions from competitors and NPE's.

Mission & Vision

Vision: to become the only source for cyber risk data for financial risk quantification to the marine sector and others vulnerable to industrial control system attacks, for risk management and regulatory compliance.

Mission: to develop systems and models that exactly meet and align with the requirements of sectors with high degrees of specialization and proprietary cyber risks enabling each client to measure and value the unknown.

Ethos:

Do the most with the least

Build upon solid data foundations

Be far too unique, relevant and accurate to ignore

Strategy

The IMO regulations take effect from January 2021. This does not leave sufficient development time for a full rollout of a new platform within the intervening period. As such, there are two phases of launch proposed, in order to get to market as soon as practicable. In Phase 1, there will be very few resources required, with only minimal software development required to be fully operational within a short space of time.

The only caveat to this is the configuration of the software on-board vessels will require more technical knowledge by the installer, which may increase external supplier costs, but by a limited amount. The Founder is able to undertake the task where required, in conjunction with remote assistance where necessary. This Agile approach, effectively acts as a form of rapid prototyping of the Phase 2 development concept and also embodies working collaboratively with clients, who will have a greater degree of buy-in to the Phase 2 roll-out of the platform they will utilise.

The existing software is fully functional, with small work-around actions required at the user level and it is proposed that a service is provided in place of the marine operators having to learn and operate the system and software from the outset.

There will be a requirement to install hardware, as in Phase 2, on a target number of vessels and ownership and control of the hardware will remain with the company (Quantar Solutions Limited in Phase 1).

Cost-containment will be the focus in this initial period, with only an industry engagement team member and the Founder being active within the company, with the former responsible for securing the first clients and the Founder in executing on the orders and fulfilling the hardware and software requirements using external low-cost contractors, as in the 2020 re-testing of the patented updated backend software for data acquisition solution.

Key Points:

- Rapid go-to-market execution;
- Utilise current patented software systems for proof of concept and field trials for clients;
- Potential for quick wins and subsequent adaptation of Phase 2 development - simpler/cheaper;
- Low cost, low risk for DMGT with Phase 1 ring-fenced to validate Phase 2 developments;

Once the concept has been validated according to agreed terms between the Founder and DMGV, Phase 2 can commence, with the establishment of a new entity to facilitate the desired capitalisation model for DMGT, the Founder and the employee share option scheme that cannot be attained with the current capital structure.

There are therefore two sections for the proposal herein, which can be regarded as almost two separate operating models, with the second only commencing once Phase 1 milestones have been achieved. This document is therefore divided into two sections, labelled PHASE 1 and PHASE 2 and should be read as separate, but related, content. The detailed content is contained within Phase 2 of this document due to the single year, simplified operation within Phase 1. The financial model of Phase 1 is contained within the Annex and should be reviewed as a one-year plan leading to the 5-year Phase 2 financial plan.

PHASE 1

Strategy/ Operational Model

The objective is to validate the Phase 2 proposal through a quick-win strategy of securing 2-4 trial clients, installing the patented software systems on-board vessels in order to acquire marine-specific cyber threat data from inbound network traffic to each vessel.

ObservedThreats2017-12-18.xml - XML Marker version 1.1

File Edit View Options Navigate Help

Tree View 0 warning(s), 0 error(s)

Ready

ObservedThreats

2 Attributes:

Name	Value
ObservationStart	2015-04-06T00:00:00
ObservationEnd	2015-04-12T00:00:00

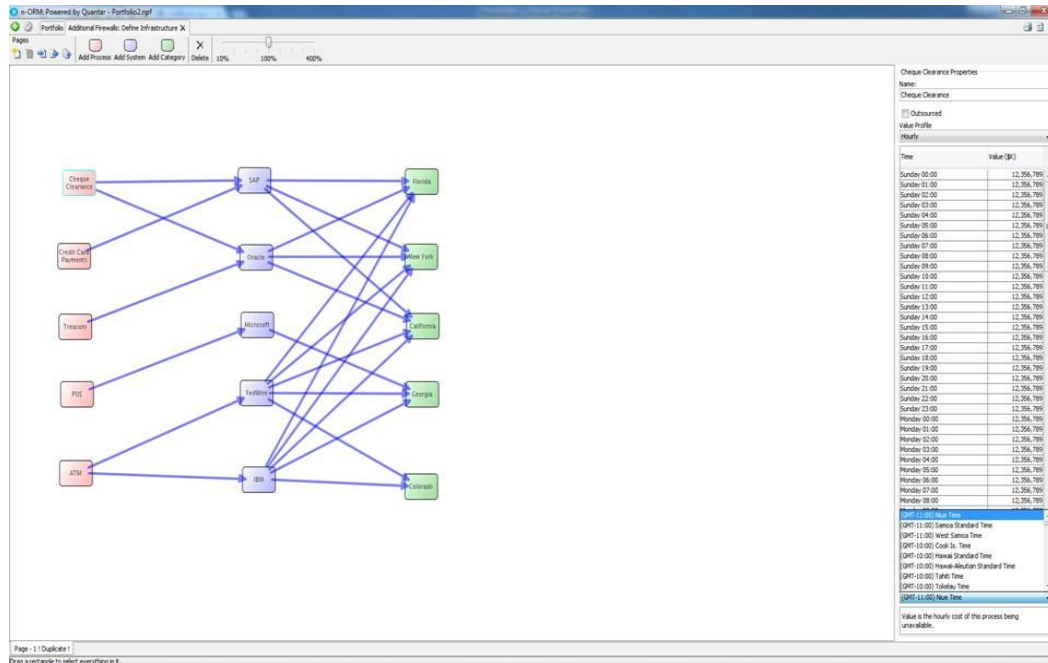
14 Subtags:

Tag name/Text	ID	Category	Target	SeverityScore	Observation
Threat	1408	Indiscriminate	Unknown	7	Observation (163 occurrences)
Threat	2417	Indiscriminate	Unknown	4	Observation (163 occurrences)
Threat	472	Indiscriminate	Unknown	7	Observation (163 occurrences)
Threat	2050	Indiscriminate	SQLServer	1	Observation (163 occurrences)
Threat	2003	Indiscriminate	Unknown	7	Observation (163 occurrences)
Threat	2466	Indiscriminate	Unknown	4	Observation (163 occurrences)
Threat	2924	Indiscriminate	Unknown	10	Observation (163 occurrences)
Threat	2404	Indiscriminate	Unknown	10	Observation (163 occurrences)

Sample Cyber Threat Data Acquired from EU Insurance Company Network 2017

The client will augment the captured threat data with proprietary data through a stand-alone patented software product, named "Infrastructure Manager". This maps the vessels individual processes and systems onboard and will vary from ship to ship. The means of configuration of this application was designed to be extremely simple, with drag-and-drop functionality, with other values typed into the fields. The application was created to be small enough to be emailed between the client and the operating company.

End users responsible for the data inputs will have access to video instructions hosted by the company and accessed using identifiable credentials, providing proof of access and credibility of the vessel data.



Screendump: Quantar Infrastructure Manager Software Stand-alone Module

The data will be assessed using the patented front-end cyber risk analytics data and reports issued to the client. These will be in two formats; paper-based and online. The paper-based report will be sent electronically to each client to use for IMO regulatory compliance purposes. This will act as auditable proof of having undertaken the requisite cyber risk analysis and additionally provide proof of ongoing cyber risk management, as per the regulations. The intended use of the original software was for Basel II and Solvency II regulatory compliance and as such will serve the marine sector for the same purpose.

Additionally, the client will access online interactive reports for their own internal risk management purposes. These will be provided as Microsoft Power BI Pro files (see Annex for functionalities), accessed via a web browser or on a mobile device. These reports will facilitate feedback to Quantar to customise reports as the program evolves and the clients make specific requests for report content/layout, etc, and will also inform Phase 2 developments.

Within the reports will be additional content resulting from online self-help compliance tools in the form of GDPR and ISO27001 online questionnaires. These already exist offline and can be rapidly deployed online, with very little operational cost, whilst providing value-added to the marine clients.

NOTE: The maritime professional and regulatory bodies refer almost exclusively to ISO27001, GDPR, OHSa, ISO 9001, and marine-specific ISO standards. See Annex for ISO27001 and GDPR master document records already created for Quantar consultancy in information security, data governance and GDPR compliance, which will be repurposed at low cost for self-help documentation and audit.

DISTRIBUTED LEDGER DATA GOVERNANCE 2020

Distributed Ledger Technologies (DLT)

*Required

1. Which DLT is employed? *

Choose ▼

2. How is the blockchain used i.e. what for exactly; *

☐ Secure transactions
 ☐ Regulatory compliance
 ☐ Increased operational efficiency
 ☐ Strategic partnering
 ☐ Cost reduction

DISTRIBUTED LEDGER DATA GOVERNANCE 2020

Distributed Ledger Technologies (DLT)

*Required

1. Which DLT is employed? *

Choose ▼

2. How is the blockchain used i.e. what for exactly; *

☐ Secure transactions
 ☐ Regulatory compliance
 ☐ Increased operational efficiency
 ☐ Strategic partnering
 ☐ Cost reduction

BIG DATA GOVERNANCE 2020

DG Big Data

*Required

1. What best describes how you govern big data today? *

	No, not at all	Somewhat	Case-dependent	Yes, totally
Security and monitoring	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Information Integration	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Protection & masking of sensitive data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data quality	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Master data management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Profiling data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

15. In the assessment of the necessity and proportionality of the processing operations in relation to the purposes and the risks to the rights and freedoms of data subjects: *

	Yes	No
Are individuals made aware of the use of their personal data?	<input type="radio"/>	<input type="radio"/>
Could analysis involve sensitive personal data - for example, in the analysis of social-media posts?	<input type="radio"/>	<input type="radio"/>
Are the datasets representative and accurate?	<input type="radio"/>	<input type="radio"/>
Do you have retention policies for the data?	<input type="radio"/>	<input type="radio"/>
Are the datasets held across multiple and disparate systems?	<input type="radio"/>	<input type="radio"/>
Will your organization be able to explain all the reasons behind any decisions it makes that result from the processing of data?	<input type="radio"/>	<input type="radio"/>

Sample Existing Quantar Big Data & Blockchain Online Questionnaires

The Founder has over twenty years of creating such forms of questionnaires for research purposes as well as for commercial development of various programs for major corporations. The cost therefore to create the self-help options for marine clients is limited to man hours of the Founder. Additionally, as a certified GDPR practitioner and ISO27001 Lead Auditor, the Founder has already developed the relevant content to facilitate the system rapidly.

Working in conjunction with the operators, feedback to refine the self-help system will also provide insight into which specific areas are of most concern for shipping companies and assist the focus of iterative software functionality and model development.

In earlier developments of the software system, the small business market in the US was targeted, in conjunction with assistance from the US Small Business Association (SBA) whilst research was being conducted at the University of South Florida, Department of Information Systems and Decision Sciences.

Since small businesses do not have the same complexity of interdependencies between their business processes and IT systems, an online system was developed by the Founder whereby the configuration data required for the front-end systems was acquired by way of an online questionnaire system.

Threat data was non-proprietary to each small business, but the outcome was the proof of concept for the same software as proposed herein, to be utilised without recourse to a full deployment of the hardware and software on-site. This will inform the current Phase 2 development for vessels not having the hardware/software installed and will function alongside the **Infrastructure Manager** component of the software. As such, the field trials of this approach have been attained, with the remaining issue to be resolved being the adequacy of the threat data and peer-grouping for actuarial valuation to be acceptable to risk carriers.

Key Points:

- Phase 1 deliverables will provide a go/no-go decision on Phase 2;
- Feedback will inform Phase 2 requirements;
- A low number of installations are required to validate the functioning and deliverables to clients;
- The solutions have low or no costs and utilises existing capabilities and assets;
- Acquired marine-specific threat data enables early formulation of Phase 2 options without cost.

Business Model

The business objective of the Phase 1 rollout is to validate the operating model, as opposed to the revenue model, the Phase1 period will incur loss, limited to the salary of the industry engagement member (salary based upon UK positions for Technical Sales Director; Marine £55-70k) and a minimal remuneration of the Founder, who will be contributing the software, patent licences, and be employed to execute all aspects of the plan, as agreed with DMGV.

The amount paid to the Founder will be subtracted from the non-cash contributed in the Phase 2 new entity contribution calculation, as agreed with DMGV. The Founder will serve as an external consultant, on a self-employed basis, to reduce the NI & PAYE burden on the company.

Where necessary, there may be a trade-off between consultancy fees and shares allocated in lieu of payment, as per the case with DMGV's Cudoni share allocation.

The hardware and office equipment acquired for the initial client installations will be owned by Quantar and transferred to the new entity at the end of Phase 1 as the new owner, with the acquisition value input as part of the DMGT contribution value.

Costs will be maintained at the lowest possible level, summarised with indicative summary costs as ([see Annex for Phase 1 financials](#)):

Item	Total Cost Phase 1
Salary NI & PAYE Industry Engagement Member	65000
Fees Billed by Founder on Self-Employed Basis	35000
Microsoft Power BI Per User/PA Based upon 5 Clients/5 Users	225
Training and Self-Help Questionnaire/Video Hosting	120
Laptop Industry Engagement	1300
Mobile Telephone Industry Engagement Member	700
Mobile Telephone and Data Industry Engagement Member + Founder	720

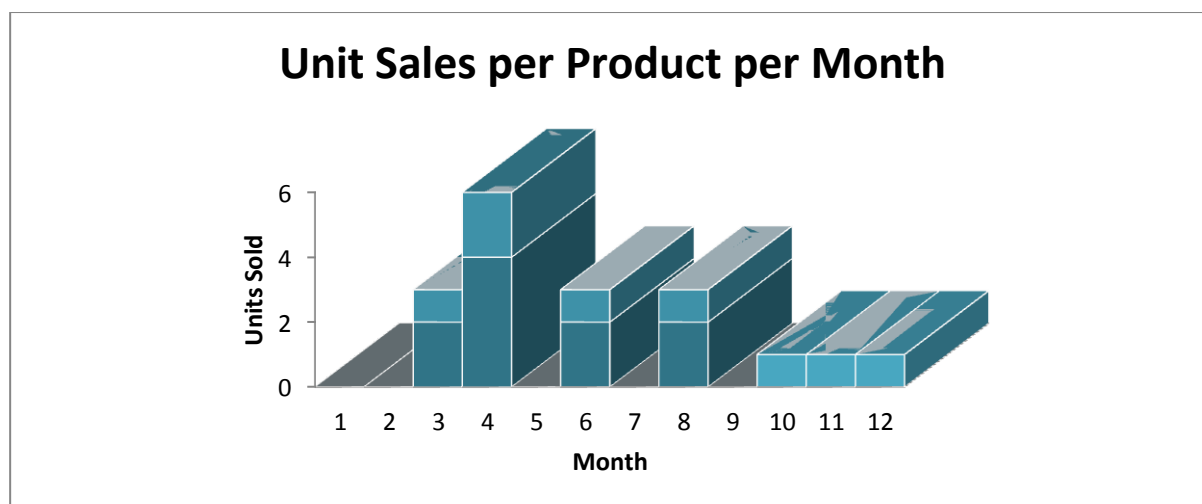
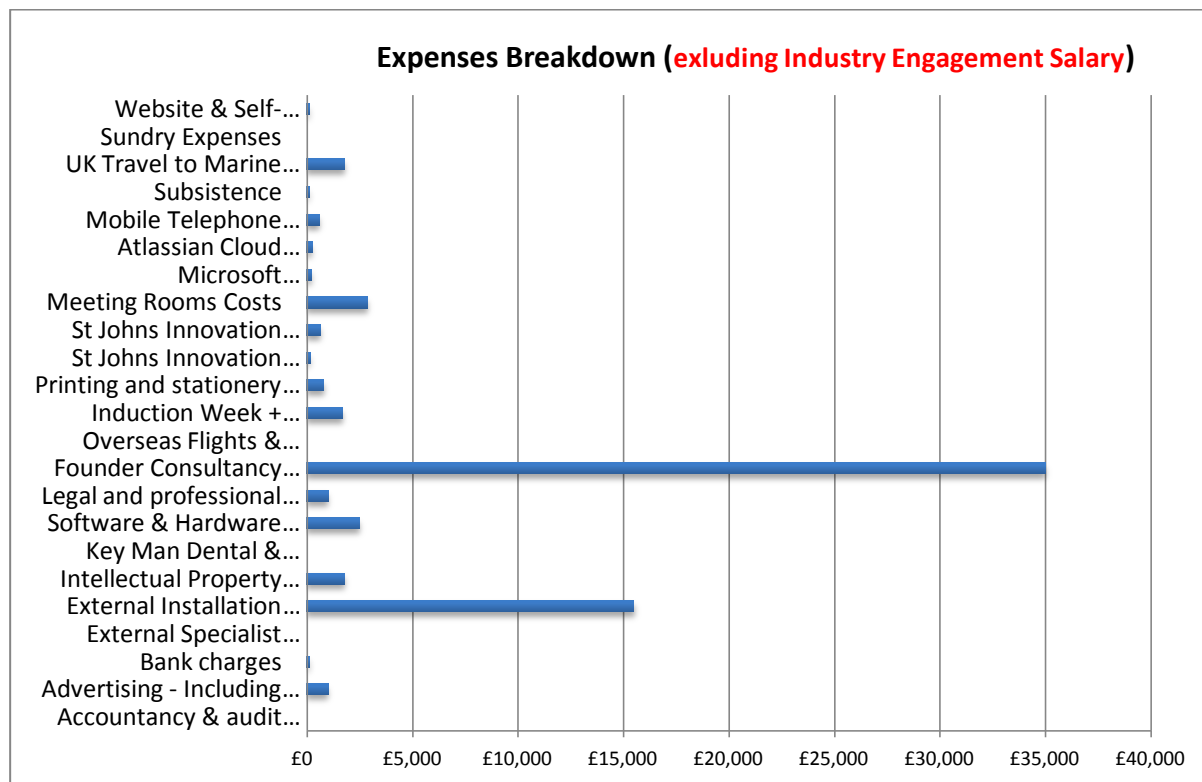
Atlassian Project Management Subscription Confluence + Jira + Trello	240
St. Johns Innovation Centre Virtual Office/Postal Service/Registered Office	631
1 Week x 1 Person Hotel Induction Period Industry Engagement	500
3 Days x 1 Person Hotel Review Post-Induction Period Industry Engagement	300
5 x Hardware/Software Installations	7500
External Contractor 5 x Hardware/Software Installations	2500
Operational Review at 3 Months - 2 x 3 Hours Per Day Meeting Room	390
Zoom Subscription	0
Accountancy	600
Travel PA - Industry Engagement Member (Home Location to London Marine Zone)	3500
Sundries and Supplies (business cards, office stationery etc)	700
	119926

The revenues assumed from Phase 1 clients is assumed to be:

Assumptions	Revenue
5 Clients; 1 Vessel per Client	30000
5 Clients; 1 Office per Client	30000
1 x Port	6000
	66000

This results in a loss-leader for Phase 1, plus the booked depreciation for the hardware, with the depreciation being:

ITEM	YEARS OF USEFUL LIFE	DEPRECIATION CHARGE PHASE 1
Patent Portfolio	10	TBD (nominally £98832)
Office Equipment	3	666
Installed Hardware on Vessels	2	3750



With Quantar Solutions having losses to carry forward, there is an opportunity to mitigate future NewCo revenues through utilising the 2-company structure over the initial term via intra-company invoicing.

Capitalisation Model Phase 1

At present, Quantar Solutions has an equity and capital structure as befits a UK small business of:

Quantar Solutions Limited

Company Number: 06978018

Authorised Share Capital:

£1000.00 Ordinary A Management Shares of £1 Each

£1000.00 Ordinary B Shares of £1 Each

Issued A Shares 100

Issued B Shares 100

Given there will be the appointment of an Industry Engagement Member from the outset to secure initial sales, the share option for this employee will not be offered in Phase 1. There will be an adjustment to the vesting period for their share option in Phase 2 to account for this.

For Phase 1 the proposed equity and capital structure is proposed as an equity holding of 25% DMGV; 75% Founder of Class A shares; and 50% Founder; 50% of Class B shares. The 2 outstanding shares will be returned to Quantar. The outstanding £100 000 outstanding debt as directors loan will be filed as amended accounts to zero, leaving no debt within the company and assets comprising the patent portfolio. The rationale for the proposed structure is to protect the assets within Quantar Solutions, whilst allowing them to be utilised for protecting RMS and Praedicat in an increasingly litigious period within the insurance modelling sector; both from competitors and by non-practising entities. The structure may be altered according to the requirements of both parties, but the proposal follows other DMGV investments in recent periods, such as GP Nutrition in 2020.

The patent portfolio will be licensed for a period of 1 year to RMS and Praedicat, which will lapse at the end of the period. Where Phase 2 is implemented, the patent portfolio will be transferred to the new entity, with agreement between DMGT and the Founder on licensing to RMS and Praedicat and the patent portfolio being entered as part of the Founder's non-cash contribution. The protection of the 2 major investments by DMGT for the following decade and longer via continuations and new filings forms part of the valuation and risk assessment of the current proposal.

Financials Phase 1

The presented 1-year financial plan is based upon the closing financials submitted to HMRC to 31/12/2019 and adds the present proposed Phase1 revenues and costs, as listed above. This should be regarded as separate to the Phase 2 plan also enclosed within the Annex.

Patent Portfolio September 2020

The current patent portfolio, provisional patent filing excepted, is currently under continued review, as notified by a non-practising entity as at 15th September 2020. An exclusivity period from 21st - 29th September 2020.

There is considerable doubt that the portfolio will be divested due to the current economic climate and limited budgets by potential infringers to acquire the portfolio. However, should the opposite occur and there is divestment (notification by 29th September 2020), then the Phase 1 and 2 plans will require review.

Of note is that there will be a grant-back licence to Quantar Solutions Limited for the entire portfolio, for commercial exploitation. However, the non-cash contribution of the founder would be limited due to the below-market price of the submitted portfolio to the NPE earlier in 2020 when early Covid-19 conditions depressed the secondary IP market to a greater extent than at present.

Where there is an opportunity to allow the grant-back to be attributed to NewCo, a rapid decision will be required by all parties for Phase 1 & 2 as to whether to establish a new entity and exploit the patent IP. The software source code registered copyright remains within Quantar Solutions, regardless of the outcome.

There would be a reduction in the value of the proposition from a protection of RMS and Praedicat perspective, however, an agreement may be made with the NPE, where possible, to exclude the two entities from and future patent infringement prosecution based upon the patent portfolio acquired by the NPE.

PHASE 2

Costs Phase 2

Although, as with all early stage entities, costs are estimates, in the case of the marine sector actual and historical values are notorious for being difficult to acquire due to the global nature of the sector and the offshore registration of the volume of entities within the supply chain and risk transfer markets.

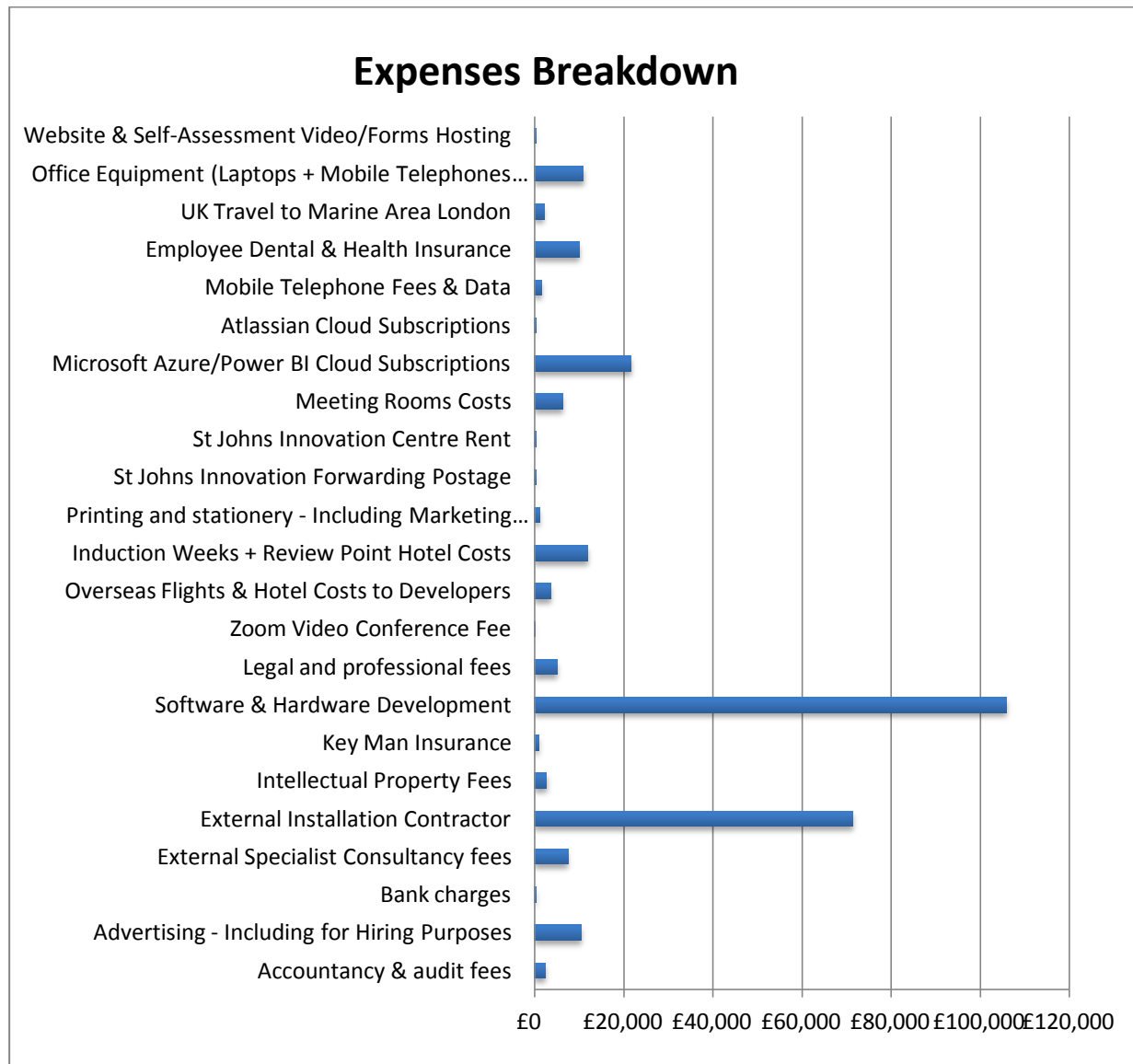
However, the operational costs within the financial plans herein are based upon actual known values, which have been attained from P&I Club annual reports, the Bermuda Monetary Authority reports, SEC filings and Companies House filings.

For the case of operational costs, most cyber risk analytics entities are still venture capital owned or private. The costs associated with operating a cyber risk analytics cloud-based platform are therefore based upon industry known values that validate the use of costs extracted from the liquidation of former competitor, Corax Cyber Security & Corax Cyber Security Holdings Limited, dated 15th September 2020.

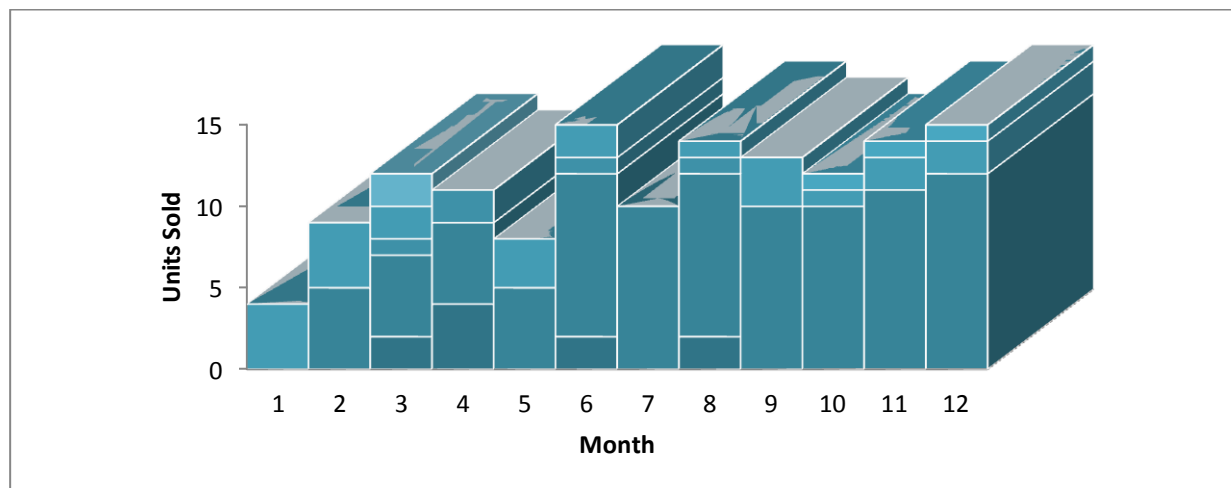
The marine sector costs for implementation are based upon daily UK rates for experienced software developers at a median cost of £500 per day, plus travel and associated costs. Where initial evaluation in week 1 determines an alternative mode of implementation, it is anticipated that such costs would reduce, not increase.

The majority of operational costs are personnel-related and are again based upon data extracted from sector-specific company websites as at 17th September 2020, together with travel-related data from mainstream sources for meetings with offshore software developers in either Estonia or Poland.

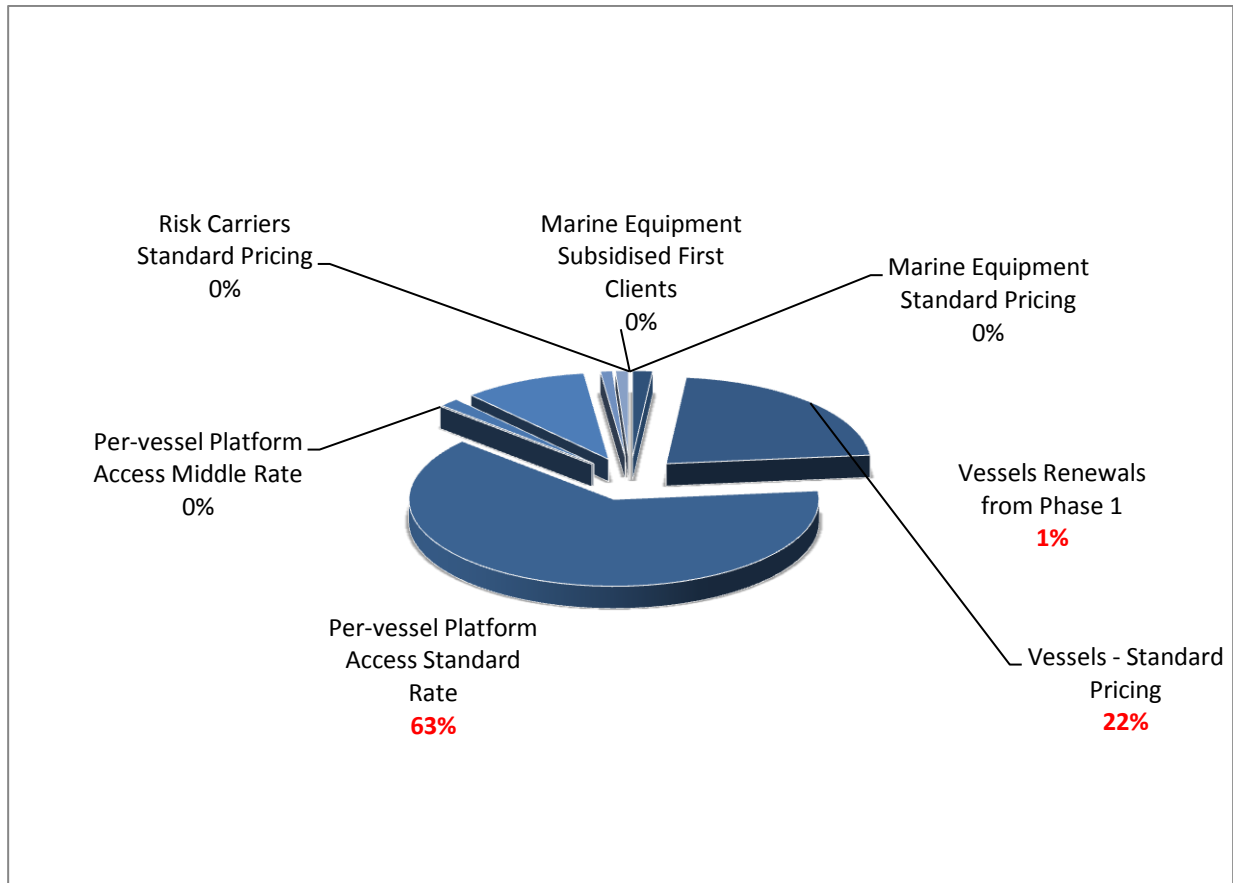
Software development costs are based upon the historic costs from a leading UK software development firm that created the initial front-end Quantar application over a number of years. These costs have been allocated a per-man hour software cost and amended to account for the substantially lower hourly cost of software houses in both Estonia and Poland. These figures have been validated by the costs per hour of Guidewire-Cyence and Cybercube, who outsource to each of these countries.



Unit Sales per Product per Month



Sales Contribution Per Product



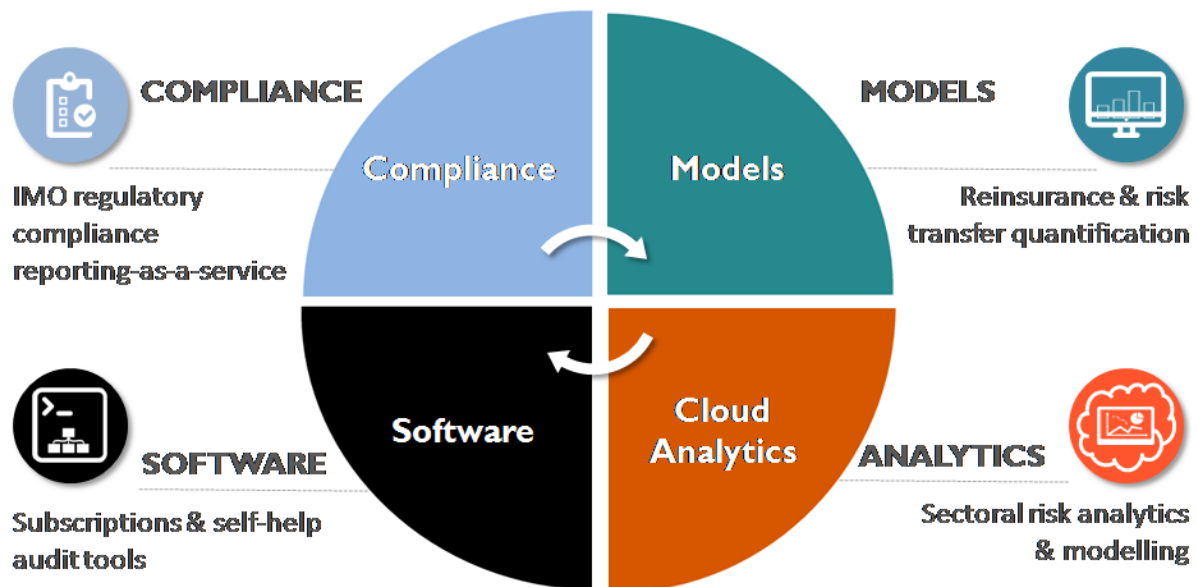
Current cloud-enablement and enterprise application costs as at August 2020 are as follows:

Servers		Storage					
Server type		Storage Type					
Number of virtual machines		Raw Storage Capacity					
CPU cores		Percent Accessed Infrequently (for Object Storage)					
Memory in GB		(Rows may be added for multiple server and storage types where necessary)					
Hypervisor, Guest OS, and DB Engine							
Provider (Per Hour Costs)		Small	Medium	Large	XL	2XL	
Amazon		\$0.07	\$0.11	\$0.21	\$0.42	\$0.84	
Microsoft		\$0.06	\$0.11	\$0.21	\$0.45	\$0.89	
IBM SoftLayer		\$0.05	\$0.11	\$0.21	\$0.39	\$0.72	
Google		\$0.04	\$0.09	\$0.18	\$0.35	\$0.71	
Intermap		\$0.01	\$0.02	\$0.04	\$0.09	\$0.18	
1&1		\$0.01	\$0.04	\$0.07	\$0.18	\$0.48	
Provider	Storage Type	GB/Month					
1&1	Default SAN Storage	\$0.07					
Amazon	EBS Cold HDD	\$.03					
	Optimized HDD	\$.05					
	EBS General Purpose SSD	\$.10					
Google	Standard Provisioned Space	\$0.04					
	SSD Provisioned Space	\$0.17					
IBM	Endurance Block Storage	\$.15/\$.35					
Intermap	Persistent Block Storage	\$.30					
Microsoft	Standard Disk LRS	\$.05					
	Standard Disk GRS	\$.10					
	Standard Disk RA GRS	\$.012					

Business Model

The overall business model is a variation of the RMS / Praedicat models. In the case of the former, there has been a move to a platform, away from the traditional fixed fee licensing model following the failure of RMS One and the development of Site IQ.

THE MARITIME SERVICE PORTFOLIO



The proposed business model covers the following functionalities within a platform accessible by multiple parties for a variety of purposes:

Function	User
IMO regulatory compliance	Vessel/fleet owner + P&I Clubs
Cyber risk management	Vessel/fleet owner + Marine Equipment Companies
Mitigation cost-benefit analysis	Vessel/fleet owner
Self-assessment tools	Vessel/fleet owner
Maritime standard forms library	Vessel/fleet owner
Third party controls	Vessel/fleet owner + Port Authorities
Underwriting	P&I Clubs + Risk Carriers + ART/Captive Participants
Portfolio risk management	P&I Clubs + Risk Carriers + ART/Captive Participants
Risk transfer (reinsurance / captives / ART)	P&I Clubs + Risk Carriers + ART/Captive Participants

As the proprietary data acquired grows over time, the revenue model will change with additional revenue streams generated through data access and use. This follows the RMS and Praedicat model and is allied to rollout of new products or functionalities year-on-year.

There is opportunity to utilise the models developed by both RMS and Praedicat as quick wins. An example is the litigation model of Praedicat that could be adapted for use in the marine sector utilising the new platform. The input from Praedicat would offer the potential of internal synergies and internal charging, without disclosure to external parties of the underlying model.

The business model is applicable to the global maritime sector, with the initial periods having a solely E.U. focus, followed by the U.S. To put the total market into perspective, the E.U. market, of known vessels over 100 000 tons, relative to the global market is only 12.9%, yet provides sustainable revenues for present and long-term operations.

Vessel Type	World Fleet	E.U. Fleet
Container	5164	1144
Tanker	10420	1410
Gneral Cargo	19613	1973
Bulk	11125	1461
Other Type	47847	7419
Total	94169	13407
Container	5164	1144
Tanker	10420	1410
Gneral Cargo	19613	1973
Bulk	11125	1461
Total	46322	5988
<i>E.U.Fleet 14.24% of Global Fleet</i>		
<i>E.U.Fleet 12.92% of Specified Types Global Fleet</i>		

With the E.U. market geographically providing ease of access to vessels, ports and the London market the marine P&I Club, regulatory and reinsurance sectors, the scalability of other markets is addressed through the global network utilised by the maritime sector.

The European routing of vessels provides ample opportunities to install the limited number of hardware instances per ship owner, whilst the remainder of the proprietary data is input remotely and simply, thereby removing obstacles to gaining market access in domains outside of the EU and US.

With the Asian market being by far the largest, there is vast scope to acquire a large number of users within this segment. EU destinations for Asian-owned vessels ensures that IMO regulatory compliance, together with EU maritime regulations relating to cyber, provide sales opportunities and the P&I Club headquarters in London ensures point of contact is feasible for all geographies - see Annex for number of European port calls per container shipping company as an example.

Pricing

The different target segments within marine require pricing strategies that fit to the sector norms, with the exception of the vessel pricing. For this latter, the Phase 1 prices are used to gain access and marine-specific data for a minimum two year period, without which, the whole business model fails. As such, the losses incurred in Phase 1 will return in subsequent operating years during Phase 2 where hardware is installed.

For ports and shipping company offices, prices reflect the competitive nature of the marine industry and low margins. Again, the gaining of data is of prime importance in developing data prices for the reinsurance and ART sectors, which carry higher margins than the actual marine operator segment.

Marine equipment pricing is nominal, since the value is derived from collaboration in terms of future vessel developments and the ongoing need to align the systems and models with such changes. By establishing a commercial relationship, opportunities will remain in the longer term to acquire marine data relating to trends such as changes resulting from 5G, autonomous vessels, sensor evolution, etc.

Reinsurance and ART/ILS function with high volumes and low rates through aggregated risks and a diversified portfolio for carriers. This has the effect of offering larger premium margins for risk carriers, but also for the P&I Clubs, using retained excess premiums to smooth long term pricing for their members. This is despite each P&I Club effectively having ring-fenced risk exposures within the reinsurance layers i.e. an amalgamation of individual risks per club that remain identifiable as separate entities within the overall reinsurance pool.

The availability of granular data relating to the global fleet, each P&I Club, down to individual vessels offers the potential for risk carriers to underwrite the total risk for cyber and for other categorised per-vessel/operator risk in a manner that reduces total exposure. Given the sector covers and entire global industry, pricing of data and modelling reflects this unique scenario where small reductions in exposure result in disproportionate increases in revenues.

Access to marine data and models increases in value over time, with greater volumes of historic data to model from. This is reflected in the growth rate of access over the initial five year period projected prior to a future defined exit strategy being executed. However, the price of marine-specific data for risk carriers will not be of the order of the fees of RMS and Praedicat; the market is substantially smaller than the global property and chemical litigation reinsurance sectors. With over 400 clients and revenues of £250 000 000, RMS, for example, has an average monthly data fee of £52 083. The marine sector, by contrast can sustain around 15% of that monthly value.

Revenue Segment	Price Sensitivity
Vessels	High
Operator Offices	Medium - High
Ports	High
Marine Equipment	High
Risk Carrier	Medium - Low (over time used)

A summary of the service pricing is as follows:

USER	DISCOUNTED RATE PM	FULL RATE PM
Vessels With Hardware	250	500
Per Vessel Platform Access & Use	50	100
Ports	500	750
Marine Equipment Manufacturer Platform Access	50	100
Reinsurance Data & Analytics	2000	3500
Alternative Risk Transfer/ILS Company Access	2000	3500
Utilities Platform Access	2000	3500

However, for the per-vessel pricing, the use of pricing bands will be implemented to incentivise shipping companies to include as many of the respective fleet as possible, as per volume licensing models within the software sector. With fleet sizes of the major operators being sufficiently large, the inclusion of at least 25% of their fleet is the primary objective for the top ten companies within the EU and US initially. This constitutes a significant number of users for the platform and generates sufficient revenue to support the company without the future addition of reinsurance revenue.

- Average E.U. Fleet Size: 348 vessels
- Target 25% per company fleet: 97 per company
- Top 10 E.U. shippers at £100 per vessel per month: £1 164 000

Pricing Strategy

Vessel Installations	Ports	Platform Subscribers	Risk Carrier/ART
Below Cost (loss leader)	Below Cost (loss leader)	Market Price	Below Market Price

Phase 2 Tiered Pricing Structure

1-75 Vessels	76-150 Vessels	151+ Vessels
£125 Per Month	£100 Per Month	£75 Per Month

Revenue Streams

In Phase 1, a subsidised rate for the service will allow for validation of the system for end-user companies, with a 2-year contract ensuring the continuous acquisition of marine-specific cyber threat data, regardless of the final outcome. However, it is anticipated that the low cost/high perceived value and switching cost will result in very high retention rates.

As such, in Phase 2, Year 1, there will be a continuation of the initial subsidised revenue flow to be added to the new entity revenues, mitigating Phase 1, Year 1 losses. Further, it is also expected that the number of vessels per company, per fleet, will be expanded in Phase 2, Year 1, once the value to the operating companies has been proven; the greater the number of installations, the better the modelling for the benefit of the fleet owners, plus a greater volume of auditable proof for IMO regulatory compliance.

The usage will therefore result in data and system revenues, regardless of whether a vessel has a hardware installation or not; the platform will be used by a greater number of vessels than there are hardware installations, since the compliance and risk management functions, together with the self-help audit questionnaires are independent of the hardware itself.

In Phase1, a small number of office installations is also planned due to the same IMO regulations applying to such locations. The operators, in general, operate offices at each port location they utilise on a frequent basis. It is therefore logistically easier to undertake installations concurrent with vessel installations, with the end-users becoming familiar with the UI and functionalities for their office use as well as for the fleet. The rate of growth of office installations is anticipated to be at a far lower rate than for vessels and is reflected in the financial forecast accordingly. This is due to a lack of Port inspection controls being carried out at operator offices. The same applies to installation rates at ports.

For each instance, there will be a fee charged for the use on a per-office basis, as well as per vessel, with there being a subscription cost, plus a data usage cost. This will ensure the decoupling of hardware installations versus vessels without installations does not impact upon the revenues i.e. in effect the same use of the system, regardless of having hardware on-board or not.

Contract will be for a fixed term of 2 years, renewable, again ensuring continuity of threat data acquisition, allied with per-vessel proprietary data.

Growth will be attained, after the initial focus upon E.U. operators, from the U.S. market due to the similarity in operations, language, compliance structures, and availability of external contractors able to fulfil roles remotely.

The issue in accounting for sales volumes in the U.S. lies in the use by U.S. operators of flags of convenience, making actual fleet and type numbers difficult to attain. The U.S. Bureau of

©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

Transportation, for example, has a very low number of U.S. registered vessels. In order to attain meaningful data for the financial analysis, the figures used have been extrapolated based upon accurate data from other sources in order to arrive at a starting point for the U.S. fleet size. Only relevant vessel types are accounted for in the calculations and use.

US Fleet By Country (Flags of Convenience)	Deadweight Tonnage in Millions
USA	11
Panama	320
Marshall Islands	253
Bahamas	66
World Total	1966
EU 28	811
US Total	650
US Share %	33.03%
EU Share %	41.25%
EU 28 - Total Number of Vessels	13407
EU 28- Total Number of Vessels Container + Tanker + General + Bulk	5988
EU 28 - % of EU Total Vessels Container + Tanker + General + Bulk	44.66%
World Total Number of Vessels	94169
World Total Vessels Container + Tanker + General + Bulk	46322
*Extrapolated Number of US Vessels Container + Tanker + General + Bulk	5725

* U.S. Assumed at 95.61% of E.U. fleet in size and same composition for reinsurance calculations

Extrapolating the fleet number arrives at a figure not dissimilar to the size of the E.U. fleet comprised of the same types of vessels. It is therefore assumed that the E.U. plans are attributable to the U.S. market, with a similar mode of operation to that within Europe. Further, the expansion into the U.S. will entail engaging the Growth Officer for the company, with the person being employed on an external contract basis, which is a heavily utilised model in the US and removes issues with establishing U.S. employment contracts and avoiding costs and risks.

The proposed revenue generation in the first three years from the platform is as follows:

Year 1:

Fixed subscription per vessel basis (includes initial installation and configuration costs)

Fixed subscription + data usage per operating company to data for internal use; fleet risk

Fixed subscription + data usage per operating company to data for own cyber risk management use

Fixed subscription + data usage per P&I Club

Year 2:

Per Year 1:

+ Fixed subscription & data usage fee per risk carrier

+ Fixed subscription & data usage fee per marine equipment company

+ Additional product with additional access costs per use (e.g. litigation model for regulatory breach)

+ Fixed subscription fee per port authority

Year 3:

Per Year 1 & 2:

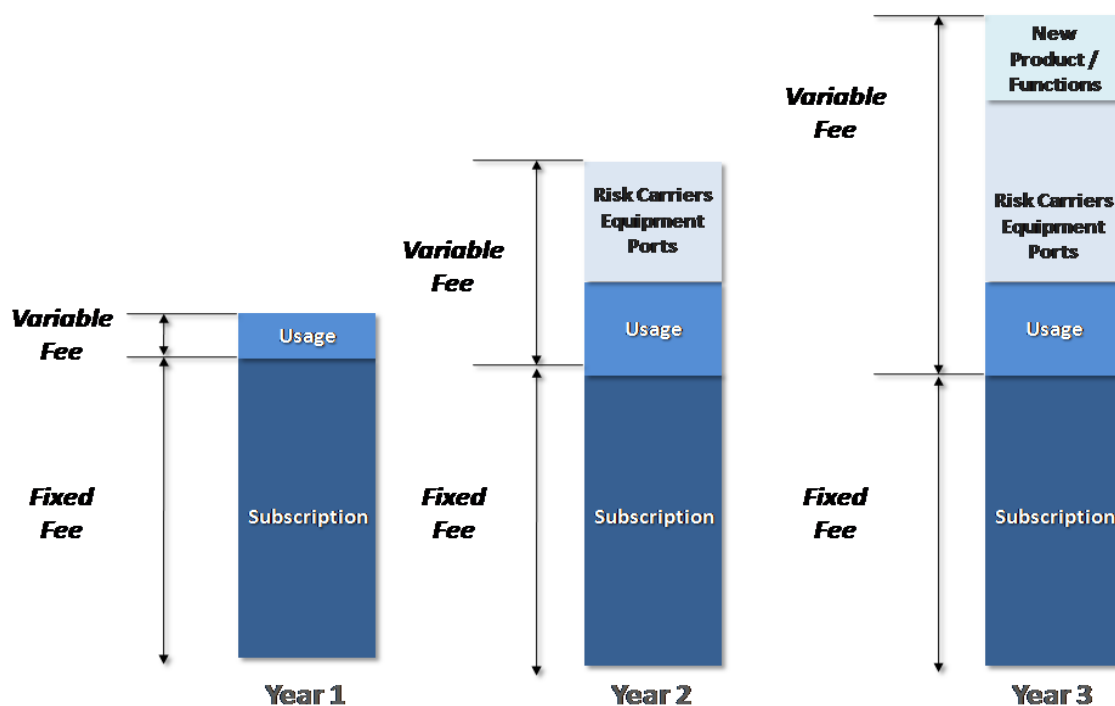
+ Additional products with additional access costs per use (e.g. 5G risk management analysis tool)

- + Additional functionalities with additional access costs per use (e.g. reporting for portfolio risk; sectoral benchmarking analysis/data)
- + Development of ART/ILS securitisation with commission fees.

The ship owner companies will have a number of their total respective fleet installed with the relevant hardware and software. The remainder will have their proprietary data input into the software and each vessel will have a unique ID, using the existing IMO registration number to ensure interoperability with other users' systems for identification, together with a further unique ID for internal data use when modelling and data analytics is run (due to the incompatible IMO ID with large data sets; cost increase impact).

As with RMS and Praedicat, the fee model is based upon a per-user model, with the marine case using a per vessel designation in place of user. The cost per month for each vessel is modest, with a tiered rate commencing at £125 per month and reducing to £75 per vessel per month according to the volume of vessels included in the use per company, to ensure both uptake and continued use. Contracts per vessel will run for a fixed two year period, with an option of 12 months at a higher rate by 33.3%. With the net fleet size after deducting for hardware-installed vessels, of 2025 for only the initial six E.U. target clients, this still amounts to a significant number of potential vessels within the system. The objective is to attain a 25% vessel usage rate from the top ten EU ship owners as a commencement point. By the end of Phase 2, Year 1, there will be additional targeting of US ship owners.

The pricing model will need to evolve as trends and vessel replacements impact upon the sector, with ultra large and mega large builds in progress, with changes to navigable waterways (e.g. Suez, Panama, Beijing-Hangzhou, White Sea-Baltic, Kiel and Rhine-Main-Danube canals), the volume of fleets is set to decrease over the medium to long term. A commercial vessel has an average life expectancy of 25 years, with the global fleet having approximately 50% at the 10 years and older point.



The revenue model is based upon switching costs once data is acquired and the platform is used by a number of different entities across sectors, thereby also reducing the risk of new competitors entering the same markets. As with most current digital ventures, the value of the accumulated data and the ability to utilise it increases its value over time. In the case of cyber, this needs to remain modelled as present and future predicted activity and losses due to the constant evolution of attack types.

Key Points

- Year 1&2 Data acquired from E.U. operators from their Ultra-Large Fleet: 60% of global fleet
- Top 4 E.U. operators initial targets for practicality, execution & serviceability; goals attainable
- Statistical significance can be attained rapidly; gain buy-in and fleet installation expansion
- Potential for hardware customisation by suppliers; creates switching costs/retention rate
- Reinsurance premiums for E.U. + U.S. alone = \$250 million, offering scope for significant commission revenues in medium term & ART reinsurance structure development validity.

As with RMS, the financial objectives will be to generate 70%+ of revenues from large clients, such as the P&I Clubs and reinsurance entities, but with a low concentration level of not more than 7.5% being generated from the largest client. The contract term will be for two-year periods due to the time lag between contract conclusion and meaningful data acquired per client fleet. Where there is reticence to engage on this basis with the first clients, a concessionary pricing model may be required to ensure data is attained; the true value from the enterprise.

Target year-on-year compound revenue growth is targeted at 2.5% over the long-term, with a target operating margin of 42% over the same period. In the initial phase of development, with the IMO regulations impacting from January 2021, there will clearly be a very high growth rate anticipated in order to secure market share and with first mover advantage. The overall trend however will allow, steady rate, as for RMS and Praedicat.

Marine Reinsurance Premiums

The calculation of current reinsurance premiums is based upon the 2019 figures provided by the International Group of P&I Clubs, which summarises the overall reinsurance tranche coverage, as provided elsewhere herein. The \$ per cent premium per vessel type has been applied to known values from government sources. For the U.S., overcoming the majority use of flags of convenience, together with an absence of division of vessel types has resulted in using the E.U. data to extrapolate U.S. values. These should be regarded as having a high probability of under estimated values due to the predominance of bulk cereals and oil vessels relative to the E.U. fleet, with higher reinsurance rates per deadweight ton.

Tonnage Category	2020 rate per gt in US cents	EU Fleet Tonnage	\$USD (Millions) EU Fleet Annual Reinsurance Rate	US Fleet	\$USD (Millions) Annual Reinsurance Rate	US + EU Fleet Reinsurance Premiums P.A. \$ Mln
Persistent Oil Tankers	57.47	68209000	39.199	65214624	37.478	
Clean Tankers	25.82	0	0	0	0	
Dry	39.71	223000000	88.553	213210300	84.665	
Passenger	321.61	0	0	0	0	

Chartered Tankers	21.58	0	0	0	0	
Chartered Dries	10.54	0	0	0	0	
Totals			127.752		122.143	249.895

Reinsurance Cyber Analytics Revenues

The targets for the risk carrier market are primarily those within the reinsurance market and entities engaged within the alternative risk transfer market (ART) such as within the insurance linked securities segment, since the International Group of P&I Clubs utilise these for risk coverage.

However, within this broad description are other players that are concerned with the actuarial valuation, underwriting, placement and managing the risk cover operations. These include the Lloyds managing agents, ILS bond issuers and sponsors, Bermuda reinsurance/ILS market as an entity, reinsurance brokers, property and casualty (P&C) commercial insurers, and the primary insurance carriers.

The Market for these types of entities may be summarised as at 2019 as:

Reinsurance Companies Bermuda	47
Lloyds Managing Agents	53
Lloyds Brokers	335
Lloyds Syndicates	93
Insurance Linked Securities Companies Bermuda	21

Bermuda plays a major role within the reinsurance and ILS markets due to the tax structures permitted by laws that are accepted by all countries. As such, the Bermuda stock exchange (BSX) accounts for 77.3% of global market capitalisation of ILS issuance. In Q1 2020, there were 21 ILS issues, with a range of \$10 - \$496 million and an average value of \$187 million. Other countries are seeking to enter this rapidly increasing market, such as Singapore, Guernsey and the UK London market through tax reforms to facilitate the holdings and dispersals without the standard tax regime applying.

This presents an opportunity to utilise the London market in conjunction with the marine sector presence in establishing relationships to collaboratively develop ART/ILS products for the P&I Clubs and their members for cyber risk and IMO regulatory compliance.

Comparison with RMS In/Reinsurance Clients

RMS	NewCo Target	
Current Client Data	Phase 2 Year 2	Phase 2 Year 3-on
90% Top P&C Commercial Reinsurers	5	9
90% Top Global Reinsurance Brokers	3	9
90% Bermuda In/Reinsurance Market	4	12
70% To P&C Primary Carriers	2	4
70% Lloyds Managing Agents	15	25
85% Top Reinsurers	5	12
Total Number of RMS Clients 400+	Totals 34	Totals 71
RMS Revenue: £250 Mln P.A.	Annual Fee £24 000	Annual Fee £42 000

ART/ILS revenues will be derived from commission percentage payments, as with the current pricing structure within the marine sector. Since there is no product or data from which to derive estimates from, this additional revenue stream is not included at the present time in the financial model.

However, the scope for an ILS product to cover marine cyber risks presents a model with a high probability of success. Developing such a product would enable the International Group of P&I Clubs to offer global coverage for cyber threats and IMO compliance risks, at a low cost relative to premiums and ceilings outside of the marine sector. The low correlation between standard corporate network exposures to cyber risks and their consequences, is such that a risk carrier's portfolio, whether via reinsurance, a captive structure or an ILS product, will be sufficiently diversified to offer sufficient volume coverage to the sector. Further, revenues may be by way of a per-placement fee for each ILS product successfully launched and taken up by investors. This may also apply where a captive structure is utilised for the reinsurance tranches that have a capital markets component.

Target Clients and Vessel Volumes

The objective is to build, develop, then operate a sound, stable model with sustainable dividend income and low retained earnings outside of R&D for ongoing model development and software updates/new functionalities. Headcount will be maintained at a stable level, with additional operational requisites being met via third party outsourcing, reducing fixed overhead and shifting expansion and flexibility to OpEx.

- | | | | |
|---------------------------------|--------|----------------------------------|--------|
| • No. of P&I Clubs | 13 | • No. of E.U. Ports | 175 |
| • P&I Club Fleet Size | 65,785 | • E.U. Fleet Size | 13,407 |
| • No. of U.K. Operational Ports | 90 | • No. of Global Shippers in E.U. | 38 |

The marine sector poses considerable access and installation issues for the company to overcome in the short-term but it is anticipated they can be overcome by working with the operators. The issue for the early period of development of sales is that the data subscription model cannot commence without there being a representative volume of data from which to model. Taking the minimum percentage of 9.5% for there to be statistical relevance and *P*-value correlation and with a fleet size of 65 000 vessels (thus, 6175 vessels required), this clearly creates operational and cost issues.

However, taking only the EU companies and a sub-set of super-large vessels within their fleets as well, it will be possible to commence with a low volume unless otherwise required by the clients, whilst the data still being representative of their individual fleets.

COMPANY	COUNTRY	FLEET SIZE	ULTRA LARGE VESSELS	TARGET NUMBER
APM-Maersk	Denmark	681	97	3
MSC	Switzerland	574	110	2
CMA CGM Group	France	533	93	2
Hapag-Lloyd	Germany	238	45	3
Unifeeder	Denmark	62	0	0
Grimaldi Group	Italy	40	0	0
Totals		2128	345	10

Table: Initial Target Shipping Companies Phase 1: Year 1 - Vessels with Hardware Installed

COMPANY	COUNTRY	FLEET SIZE	ULTRA LARGE VESSELS (ULV)	TARGET NUMBER ULV	TARGET NUMBER non- ULV
APM-Maersk	Denmark	681	97	10	15
MSC	Switzerland	574	110	12	12
CMA CGM Group	France	533	93	10	10

Hapag-Lloyd	Germany	238	45	5	10
Unifeeder	Denmark	62	0	0	5
Grimaldi Group	Italy	40	0	0	4
Totals		2128	345	37	56

Table: Initial Target Shipping Companies Phase 2: Year 1 - Vessels with Hardware Installed

The initial target in Phase 1 and Phase 2 is the Ultra Large Vessel fleet since the total global fleet size is 580 vessels, with 4 of the E.U. shipping companies representing 60% of world total Ultra Large Vessels (December 2019 figures).

This is a highly significant figure when modelling from proprietary data in order to extrapolate future values for both attribution to the remainder of the fleet and for cyber risk quantification. It also provides the companies with auditable proof that the overall cyber risk management programs run within their respective fleets is sufficient to satisfy the criteria for the IMO regulatory compliance dictate.

By using a 10% sample of the E.U. fleet at 35 vessels, the volume of hardware to be installed is manageable for a start-up operation. Additionally, such vessels have the highest value to the shipping companies, who will be more likely to engage in the added cyber protection offered by the system being installed. Further, since the top 4 E.U. companies own 2028 vessels in total, it will be easier to expand installations once the proof of concept to them has been attained in the first two years of trading.

Of note is that the total cost per installation will incur loss and should be regarded as a loss-leader. Without the highly specific marine cyber threat data, the models have low levels of relevance to the sector. Conversely, acquiring and owning the risk data and associated per-vessel parameters and data creates a unique data set that cannot be replicated by any other company. This creates high data values to both the end users (through the provision of comparative data) and third parties such as risk carriers, marine equipment manufacturers and the broader ILS market.

The break-even on a per-installation cost will be attained at the end of the two-year contract for the vessels in which the hardware has been installed. Loss is therefore capped at the cost of capital in purchasing the hardware as inventory plus the depreciation booked over the two-year period. Additionally, where there are renewals for vessels with the hardware installed, the subsequent periods result in a positive revenue post-installation for the remaining contract period.

The data will be used to provide the basis for all other shipping company vessels through importing the proprietary system inputs from every vessel and use the actual data collected from the target group as the basis for the other vessels.

In addition, the development program will include additional modelling parameters to enable the shipping owners to run change the data parameters in order to undertake "what-if" scenarios.

As the number of vessels with the hardware installed increases over time, so the value of the data to external parties such as P&I Clubs, reinsurers, marine equipment suppliers, increases in its validity and usefulness.

It is therefore planned to not make data access available outside of the reinsurance/ART sectors until year three of operation, in order to gain credibility within as short a period as possible within the modelling sectors.

Operating Model

The company will benefit from a simple operating model, relative to manufacturing or complex on-site services organizations, since the functioning is platform-based once initial installations are completed during an initial period. As such, the high-level description of the operating model can be summarised as following (additional details are included within the Annex).

1. Sale to shipper or port:
 - a. Contract establishes status and sets conditions for installation of hardware and platform access; users; price per user; contract length; conditions for removal of hardware and termination at the end of the contract; conditions for renewal; ownership of rights, hardware, IP.
2. Sale to risk carrier or data client:
 - a. Contract establishes status and sets conditions for platform access; users; price per user; contract length; conditions for termination of the contract; conditions for renewal; ownership of rights, hardware, IP.
3. Sales passes case to engineering and finance for execution of the contract performance.
4. Engineering establishes installation timeline, inventory for installation; re-ordering of stock, advises finance, creates new user account on platform; executes third party contract for installation of hardware where required, advises finance on inventory and contract terms and costs.
5. Finance issues invoicing to client, contract, third party payables logged, purchase order issue for inventory re-stock.
6. Post installation and/or user account testing; client acceptance test per contract terms; engineering go-live sign-off by client. Finance advised for invoicing schedule and credit control.
7. Contract overseen by finance, sales, engineering and renewals plus expansion of contract pursued over first period post go-live date.
8. Analytics interfaces with client to ensure ongoing acceptance, receiving data for model reviews, proposing ongoing additional model inputs, functionalities and self-help tools. Provides iterative feedback to team for R&D of products and services. Finance advises on cost and new product/service viability.
9. New software versioning planning as per RSM/Praedicat roll-out schedule; engineering develops software development architecture and submits to third party development houses for costing. Feedback to finance; measured against plan; Board sign-off or return for adaptation and resubmission or new options.
10. Presentation of new options and versions to clients for feedback and acceptance. Clients undertake acceptance testing and sign-off. Go-live date set with clients. Contracts renewed, expanded or closed; new entities signed on to platform. Cycle repeats.

End-User Operating Model

The operational model for end-users is similarly simple, again for the same reasons as for the company itself i.e. platform operations are intended to make life easy for users.

Aside from the normal contractual and pre-installation, acceptance testing and sign-off by clients, the additional steps required within a marine environment are:

1. Port and vessel security access;
2. Server/IT room on-board security access;
3. Security of installation agreement;
4. Removal and replacement of storage media and routing via courier of media to U.K. office.

Aside from this, the end users will simply access the system via a browser, in the usual manner of platforms and as per RMS and Praedicat. Access control will be provided via the company using industry-standard software (at present the software is locked via a hardware encryption key). There are no underlying issues in operating and controlling the platform for end users.

Software and platform operations are simple and lies behind digitisation within the FinTech, InsurTech, EdTech, PropTech markets, which are areas of focus for DMGT. The slimness of the operation of platforms enables rapid rollout of new products and services, such as with Praedicat within the past 12 months being a prime example of nimbleness and reacting to market demands.

The intention is to mimic how RMS and Praedicat continue to roll out new offerings to existing clients. However, with marine being far broader in scope than the NatCat category, the same products will be repurposed for other sectors/clients, such as the energy and industrial control system sectors.

Value Propositions

The marine sector is undergoing a slow transformation through digitisation as part of the ongoing search for cost reductions. Simultaneously, there are very substantial additional operating costs being forced upon the sector by the IMO (IMO2020) via the International Convention for the Prevention of Pollution from Ships (MARPOL Convention). From January 2020, vessels have been regulated in the percentage of sulphur content within the fuel oil burned. This was reduced from 3.5% to 0.5%, resulting in an estimated additional fuel cost burden of \$60 billion.

An alternative to switching fuels is to install scrubbers which cost \$5-\$10 million, take 6+ weeks to install and are only made by a limited number of manufacturers around the world.

A third option is to switch to LNG, however the tanks fitted take up more physical space (up to 3% of total cargo space). Further, analysts anticipate swings of up to 50% in the price of LNG over a sustained period. This would increase the cost of port-to-port sea freight costs by 10-20%.

Dependent upon the carriage contract terms (IncoTerms) at the time of shipment, the additional cost between leaving a port and arrival for unloading goods could be borne by the shipper, with no opportunity to pass these additional costs on.

Additional costs to cover for environmental protection via the mandatory membership of a P&I Club, coupled with the statutory requirement to undertake cyber risk assessments and mitigation actions from January 2021 places the marine sector into the position of margin pressures at a higher rate than in the past 25 years.

With a regulatory dictate to undertake and manage cyber risks within the marine sector, which includes vessels, ports, warehouses and transportation, the need to minimise costs has an increasing importance to both vessel owners and P&I Clubs.

For Vessel Owners and P&I Clubs:

Using the company's cyber risk quantification and valuation products by individual ship owning entities and the P&I Clubs on an ongoing basis will create a number of opportunities for both:

1. An accepted measurement of risk will reduce reinsurance premiums for P&I Clubs, thereby reducing premiums charged to members;
2. An accepted method of measurement of risk per vessel offers potential for alternative risk transfer using capital markets;
3. Ongoing collection of data creates a sectoral risk database for underwriters to draw upon to determine re/insurance pricing of the sector within the overall risk portfolio of a carrier – greater insight and data leads to greater certainty and lower premiums over a sustained period.
4. Segmentation of risk values per category of vessel may reduce an aggregated risk since the accuracy of the per-segment quantification facilitates use of differing actuarial models as opposed to setting of an average/median value for all;
5. Alternative risk transfer options outside of ART/ILS may be created, such as industry loss warranties, with a trigger set by the company – utilising the data held for a large number of members within a P&I Club.

For Risk Carriers

For a risk carrier/reinsurer, the ability to have a standardised means of financially quantifying risk per vessel, category and in the aggregate is something that has not been attained previously. A risk carriers' ability to model overall portfolio risk for an entity is a means of competitive advantage via premium differentiation.

Additionally, partnering with one entity to deliver consistent, sustained risk data that can be relied upon allows a risk carrier to offer bundled solutions e.g. cyber risk assessments with risk cover. This is the existing model for a number of carriers, such as Achmea with Willis, RMS with Brit Insurance, Hiscox with Praedicat.

The cost for using the company's software products is low relative to the potential losses either from cyber attack in some form, or from regulatory compliance failure e.g. detainment or prohibition from docking/bunkering.

As such, the value proposition for marine is simple to communicate; low cost cyber risk management for regulatory compliance together with the most efficient use of capital allocated to membership of a P&I Club. For the risk carrier sector, it is one of reduced portfolio risk coupled with partnering for additional risk transfer product development utilising the proprietary data acquired over a sustained period.

For Marine Equipment Companies

The marine equipment sector is already engaged in developing cyber security systems and the use of the company's products, services and licensed patents represent a quick-win situation for them. The timeline to January 2021 is short and although the number of competitors is limited, added-value services are seen as highly desirable. This is linked to the trend towards digitisation and automation of the global fleet.

The impact of the reduction of sulphur content in fuel oil for vessels is anticipated to speed up the process of retirement of older vessels in favour of modern, efficient ships. These have an increased I.T. Content within their systems and thus have a higher exposure to cyber attacks. By bundling equipment and cyber risk control, the marine equipment sector is seeking to assure potential purchasers when specifying hard and IT systems in new vessel builds.

For Ports

Ports are in the invidious position as having liability for security, but with very limited budget from local authorities. Where a P&I Club or other professional body determines the risk to vessels is higher at one port than another, the revenue stream reductions resulting from less port traffic will have a high impact. As such, using the company's products and publicising the fact that they undertake constant cyber risk assessment will be of value at a low cost to ports.

The ability to model mitigation actions and undertake cost-benefit analysis of each will also assist in securing the necessary funding from their local authorities. The low cost of subscribing to the service will be more than offset by the ability to demonstrate to regulators and P&I Clubs the ability to manage cyber risks, both from a port and a third party perspective.

Market

The initial market will be the marine sector. This has a high degree of specificity to a number of elements of the industry, making it similar to the markets for RMS and Praedicat in that the size and volume is sufficient to sustain a company operating solely within it.

However, there are similarities across a number of sectors that rely upon the same underlying technologies as in marine. These include heavy industries such as utilities and transport. Warehouses and haulage have been included within the IMO regulations, with a high number of operators within each.

Additionally, the E.U. NIS Directive addresses risks within the utilities sectors, creating the same market opportunities as that created by GDPR and the IMO regulations. Utilities entities are increasingly requesting non-damage insurance cover i.e. protection from cyber attacks. This trend has increased very rapidly within the U.S. renewable sector; solar and wind in California being a prime example.

EU Network and Information Security Directive (NIS) DIRECTIVE (EU) 2016/1148

The Directive covers operators in the following sectors relevant to this proposal:

- Energy: electricity, oil and gas
- Transport: air, rail, water and road
- Financial market infrastructures: trading venues, central counterparties
- Health: healthcare settings
- Water: drinking water supply and distribution

Industrial control systems (ICS) underpin the functioning of utilities companies. With each being comprised of programmable logic controllers, the risks are the same as within the maritime sector and can therefore be marketed to in the same fashion.

The incremental cost of addressing the utilities sectors is low, given the similarity to the value proposition for the marine sector. This follows the ethos of RMS in expanding their modelling to associated CAT risks, from NatCat and pandemics, into cyber in more recent periods.

P&I Club Market

The Protection and Indemnity Clubs operate to pool risks and cover liabilities through, effectively, captive insurance frameworks and traditional reinsurance layers. They also pool on an aggregated basis via the International Group of P&I Club, that in turn reinsurers using the pooled risk to achieve the lowest possible reinsurance premium rate per ton per vessel type.

As such, the number of ships under the umbrella of P&I Clubs is an important consideration of the market size and targeting. However, the majority of vessels do come under the membership of a club:

Ship Type	IGP&I		Non IGP&I		Total	
General Cargo Ships	34,864	2.8%	22,868	19.3%	57,732	4.3%
Specialized Cargo Ships	3,680	0.3%	781	0.7%	4,461	0.3%
Container Ships	231,015	18.8%	8,912	7.5%	239,927	17.8%
Ro-Ro Cargo Ships	46,324	3.8%	3,444	2.9%	49,768	3.7%
Bulk Carriers	430,229	35.0%	27,293	23.1%	457,522	33.9%
Oil and Chemical Tankers	322,839	26.2%	22,084	18.7%	344,923	25.6%
Gas Tankers	75,275	6.1%	1,390	1.2%	76,665	5.7%
Other Tankers	1,881	0.2%	496	0.4%	2,377	0.2%
Passenger Ships	34,042	2.8%	6,738	5.7%	40,780	3.0%
Offshore Vessels	42,149	3.4%	13,246	11.2%	55,395	4.1%
Service Ships	5,595	0.5%	5,179	4.4%	10,774	0.8%
Tugs	523	0.0%	501	0.4%	1,024	0.1%
Fishing Vessels	1,746	0.1%	5,438	4.6%	7,184	0.5%
Total	1,230,162	100%	118,370	100%	1,348,532	100%

Table - P&I world fleet GT≥500 status : gross tonnage (in 1000 GT) of ships, by type

From the above, it can be seen that the initial target market of cargo, container, bulk and tanker fleets operated by E.U. shipping companies, has a high rate of membership of the IGP&I Club. This provides tangible data relating to the total addressable market per sé but also for the initial sales focus.

The business model requires that the fleet market within the E.U., covered for losses and indemnity via P&I Clubs remains stable. The values have remained without large fluctuations until Covid-19 impacted the sector, as for all others. However, the historic trend ensures future shipping volumes will remain as per pre-Covid or higher, given the increase in traffic as there is a fulfilment of earlier orders. This is borne out by the number of new ships on order at present and their size.

Vessel size is constrained by two primary factors; the availability and desirability to utilise deep water ports; the size capacity limits of the Panama and Suez canals. Whilst these have been altered to accommodate ever-larger vessels over a substantial number of years, these remain as the limits of future vessel builds.

The current rate of growth in exports in China, the highest level at 1st September 2020 since 2011 is a strong indicator of global demand recovering and driving higher rates of shipping than for the past decade. This presents a market ready to have a new product and service rolled out for regulatory compliance and a consequent reduction in lost revenue from time taken at ports for the additional cyber inspection burden.

Port Inspection Controls (PIC's)

Given the value proposition for ship owners and operators is based upon the requirement to comply on an ongoing basis with the new IMO regulations from January 2021, it is necessary to ensure that the threat posed for non-compliance is a valid reason to use the new entity's service.

Ships are inspected by port authorities and have legal powers to inspect a foreign ship. Various IMO conventions e.g. SOLAS, Marpol, STCW define the roles of port state controls in ensuring the implementation of these conventions.

There are port state control MOU's in place that contain common documented standards and procedures for vessel inspections, with a common database for inspected ships. e.g. <https://portal.emsa.europa.eu/web/thetis/ship-risk-profile-calc> of the European Maritime Safety Agency.

The MOU's and allied database reduces the inspection burden of vessels and upon port authorities through having the agreement in place. Where a vessel has been inspected and found to be satisfactory, the other ports within the agreement are bound by the inspection and the ship may dock at the ports within the group agreement without further inspection.

Each vessel is assigned a risk profile according to:

1. Type of ship
2. Age of the ship
3. Flag of the ship
4. Classification society of the ship
5. Performance of the Ship's ISM company
6. History of the ship

Ship-risk-calculator:

Ship Risk Profile Calculator

Generic Parameters

Type of Ship ▼

Ship is older than 12 years: ☒ Yes ☐ No

Flag ▼

Flag Performance: ▼

Flag is IMO audited: ☒ Yes ☐ No

All Certificates issued by Flag: ☐ Yes ☒ No

Recognized Organization: ▼

Performance: ▼

Is EU recognized: ☒ Yes ☐ No

ISM Company Performance: ▼

Weighting

Historic Parameters from the last 36 months

At least one inspection: ☐ Yes ☒ No

All inspections with 5 or less deficiencies: ☐ Yes ☒ No

Number of detentions: ▼

Result

Total weighting point to high risk profile

Eligibility to high risk profile (>=5)

Eligibility to low risk profile

Ship Risk Profile

5

Yes

No

High Risk Ship

Of key importance for the business model is that it is not solely a vessel's performance that acts as a factor for ship risk profile. The performance of the shipping company is also taken into account (as is

©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

the case within the aviation industry that has potential for global catastrophic impact in a case of failure).

When a Port State Control (PSC) inspector boards a vessel, they will conduct one of four types of PSC inspections:

- Initial Inspection
- More detailed inspection
- Expanded inspection
- Concentrated inspection campaign

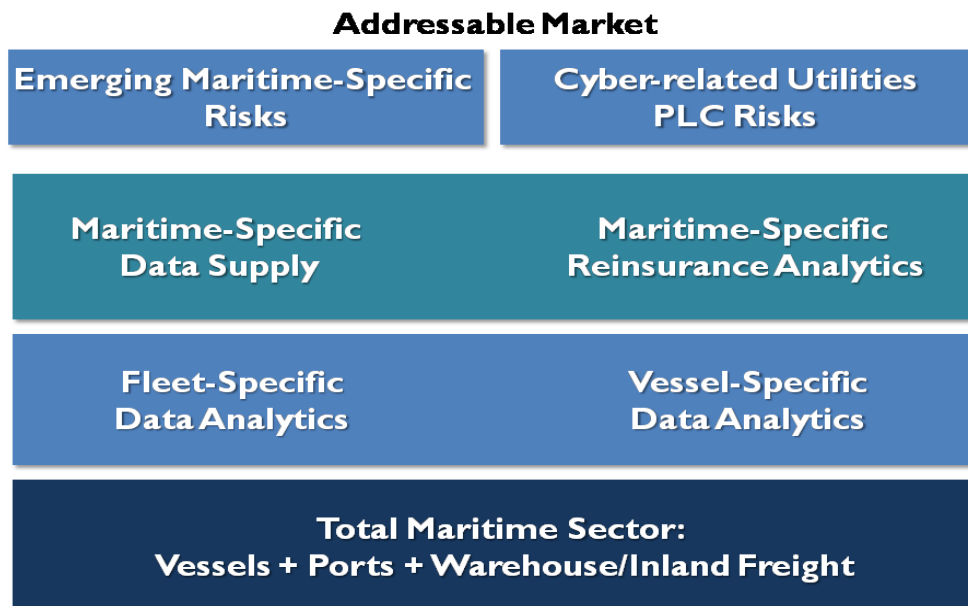
In the case of the forthcoming regulations, there is a very high probability of inspection for compliance, as with the safety inspections, since the risks posed by cyber attacks comprise safety and pollution damage risks. The incidence of inspections is therefore at the core of the current value proposition, which is founded upon the data relating to vessel inspection rates:

Ship Type	Global Number	Inspected	%	Very Large Ships Inspected %
General Cargo	17956	6979	38.9	100
Heavy Load	114	92	80.7	40
Container	5077	4430	87.3	98
Bulk Carrier	10544	9483	89.9	97.3
Oil Tanker	9664	3964	41	85.6
Chemical Tanker	4907	3335	68	100
Combination Carrier	52	27	51.9	100
Gas Carrier	1931	1371	71	83.4
NLS Tanker	332	324	97.6	100

From the table above, it can be seen that the initial target market of very large ships, operated by E.U./CH based shipping companies, as a 100% inspection rate. Further, the secondary fleet type markets of containers, heavy load, bulk, and tankers also have considerable rates of inspection.

Having a new regulation to comply with will add to the burden of inspection on both sides; the vessel/owner and the port inspection authorities. This provides ample opportunity for the new entity to build trust with each party by effectively providing a set of agreed frameworks, methods of proof of compliance and ongoing auditable proof.

The market has no IMO cyber regulatory compliance frameworks at this time and there is therefore a market opportunity to establish this and create, effectively a centre of excellence in cyber risk management, acceptable to vessel operators and Port State Control inspection authorities.



Marketing & Branding

The company operates as a downstream supplier to end user clients within the marine and utilities sectors, whilst also will operate as an upstream supplier to the risk carrier and capital markets. As a B2B supplier of a specific product and service supplier, acting in co-ordination with large-scale partners, there is no requirement for above line advertising whatsoever.

The role of the industry engagement member is more crucial, since both the marine and re/insurance/broker sectors have traditionally relied upon face-to-face meetings, professional relationships and networks built over a period of time. As such, only where there is a need on the part of partner entities, for example from the marine equipment sector, will there be visibility of the company name.

Below-line marketing may be used, as per RMS with its role as prime sponsor in 2020 for InsureTech Connect. However, previous experience as a corporate sponsor of a targeted event has not yielded a positive cost-benefit and the prime lesson learned was to attend specific events and targeted sessions with targeted attendees and to network face-to-face at a fraction of the cost of being an event sponsor.

Where it is felt that a higher awareness, for example specific to the marine sector, an evaluation of the most beneficial means will be undertaken. With an increasing number of major global events, such as the Geneva Motor Show moving to an online format, major events within the heavy marine sector may well follow.

As with RMS and Praedicat, the brand will depend solely upon attaining clients within the target markets and leveraging from the initial client base to attain brand awareness. The founder of the company has extensive marketing and brand building experience across Europe within the re/insurance and banking sectors and will draw from this and contacts within the corporate communications sector where required, such as founders of digital media companies Hard Reality (now within Leo Burnett), Ossian Productions (now OMG Media), suppliers to major corporates such as Sky UK.

Financial Model

Post Brexit Transition Period

The financial model takes a position assuming that the rules on VAT will remain very close to the current scenario in the event of a no-deal Brexit on 31st December 2020. The HMRC guidance on the issue states that there may be a requirement to register for VAT in each E.U. country that an entity sells service into.

However, the UK government also states that in the event of a no-deal Brexit, there will be an intention to align as closely as possible with the current rules and regulations. As such, the financial model accounts for VAT payable on services as if the current scenario is maintained.

It will be important to ensure that the hardware installed is not judged to be classified as exports goods into the E.U. This will require contracts to be correctly structured and worded. Further, where commissions are paid by risk carriers or the capital markets for reinsurance and/or ART/ILS it will be necessary to assess whether such revenue is classified as financial services payments, since this class is treated differently in respect of VAT post-31st December in the case of a no-deal.

Hardware will remain as the property of the company, since the purpose of it is purely to acquire marine cyber threat data and has is a loss-leader financially. The depreciation schedule for installed hardware is set at a high rate, justified by the harsh operating environment, reducing book profitability, but in reality having an operating life of at least two contract terms i.e. 4+ years from installation to replacement. Inventory churn rate will clearly also be affected by the accounting figures for the depreciation rate.

How the contracts are constructed and with which company is contracted with for the provision of the marine services will also require careful tax analysis since marine entities have their operations located offshore, typically in Guernsey, Jersey, Luxembourg and Lichtenstein. For risk transfer, the entities are located primarily in Bermuda, the BVI and Luxembourg. ILS taxation treatments are the reason for such locations. The current UK government is continuing to restructure the tax regime for ILS within London and this also needs analysis for future potential ART marine risk transfers within the London market.

Pre-DMGT Investment Valuation:

There is a requirement to establish a pre-investment valuation given the contribution by the Founder of the IP developed YTD and to account for the structure of share options as part of remuneration/lock-in of team members. As such, the proposed equity structure is a commencement point and open for discussion with the DMGT-V members. The pre-investment valuation includes an unallocated option pool for the team members to be recruited.

There may be future additional investment, or a divestment by DMGT to a third party, or an internal sale to another investment such as RMS. It is therefore necessary to establish an agreed valuation at the outset of the new entity.

Quantar has two share classes; class A of ownership and the B shares for control and it is envisaged that share classes of ordinary and preference shares, with voting and non-voting rights will be used for the company, for DMGT, the Founder and key team members as part of their recruitment.

Initial Proposed Capitalisation Table

The intention is to issue the key team members with a number of ordinary shares within an employee share option scheme, at zero charge, with the shares vesting upon attainment of specified targets that are to be agreed between DMGT and the Founder prior to the incorporation of the new entity. The percentage of shares allocated for the employee share pool will not exceed 4% of ordinary shares. No Series A preference shares will be allocated to any employee share option scheme.

share allocation will not be subject to UK stamp duty, however if there is an increase in ordinary shares issued in future periods, the value of the second issue of shares may be above the £1000 HMRC limit and will therefore be subject to 0.5% stamp duty at the time of them vesting. The burden will not be onerous for the transferees and may be offset by adjustment in the form of a salary bonus at the appropriate time. In all cases, an exit by the company will trigger capital gains tax on the sale and transfer of shares.

The authorised number of shares at incorporation will be agreed between DMGT and the Founder, with the following ownership and investment structure being proposed as a guide to the establishment of the new entity:

Shareholders	Common Stock	Common %	Series A* **	Series A %	Total Shares	Total %
Issued Shares	1000000	100	1000000	100	2000000	100
Paid Up Shares	1000000	TBD	1000000	TBD	2000000	100
Nominal Price per Share	£1.00		£1.00			
Investors						
DMGT	480000	48	500000	50	980000	48
Founder	480000	48	500000	50	980000	48
Employees - Share Options When Vested						
Finance	10000	1	0	0	10000	1
Engineering	10000	1	0	0	10000	1
Analytics	10000	1	0	0	10000	1
Industry Engagement	10000	1	0	0	10000	1
Maximum Equity Incentive Scheme	40000	4	0	0	40000	4

***Series A Converts into Common Stock at 1:1 Undiluted**

****Series A converts into Common Stock Using Broad-Based Weighted Average Formula Where Additional Series A Shares are Issued in Future Periods for Anti-Dilution Protection**

Existing Shareholders and Pre-emptive Rights to New Shares

The majority shareholders; DMGT-V and the Founder shall hold shares with such pre-emption rights as agreed at the outset of the new entity. It is proposed that an open offer is contained, without provision for third parties to take up any unallocated newly issued shares, unless under a private placement, as agreed by DMGT-V and the Founder .

Where Quantar Solutions Limited is utilised in place of a new entity, such rights will be conferred by amendment to the Articles of Association, by Special Resolution, as provided upon incorporation (and subject to the provisions under the Companies Act 2006).

New Share Issuance

New share issues shall be subject to an agreed subscription agreement between DGMT-V and the Founder, together with an agreed updated constitution within the Articles of Association and additionally within a Shareholders' Agreement.

Anti-Dilution Protection of A Series Preference Shares

In order to provide anti-dilution protection to DMGT-V and the Founder in the case of future funding rounds, or for other purposes, it is proposed that a broad-based weighted average formula is implemented to eliminate the impact of dilution.

This would result in the number of shares of common stock that each Series A preference shares is convertible into, is equal to the original price per share paid by DMGT-V and the Founder, divided by the conversion price, which is initially equal to the original price per Series A share (i.e. a 1:1 conversion rate).

When there is a future requirement for anti-dilution protection by DMGT-V and the Founder, the conversion price per Series A share shall be adjusted using an agreed formula to calculate the new conversion price of the existing Series A preference shares upon the issuance of the new Series A preferences shares.

Employment Related Securities Scheme (ERS)

For an HMRC qualifying employee share option scheme, it will be necessary to ensure that the shares allocated to the scheme are the same ordinary shares as held by DMGT-V and the Founder, with no variation of rights in order to avoid taxation implications. There will no variation of the maximum total number of shares allocated to the employee share option scheme, unless agreed between DGMT-V and the Founder.

As with RMS and Praedicat, the major cost component will be personnel-related costs, either as salaries for in-house team members, or through the provision of services by third parties. In the case of RMS, the cost is presently at 74% of total costs and this would be an indicative level for the current proposal.

Founder Investment

The founder will input the intellectual property developed YTD into the new entity as equity, in exchange for a percentage of preference shares. The valuation of the patents and software code should reflect the direct expenditure YTD, allied with the cost to develop new software at today's rates, with the original development time taken as a baseline.

At present the values as at 1st September 2020 are listed below. Patent valuations are renowned for the difficulty in establishing market values. However, IAM Media and in particular, Richardson Oliver are acknowledged leaders in the field. Using the latest valuation figures, each US patent has a present estimated value of between \$125 000 - 250 000 (September 2019 figures). Quantar currently owns 7 granted patents, with 135 granted patent claims for cyber risk management systems and methods, with 2 continuations and 1 provisional patent filed (with a 1 year deadline to file a definitive non-provisional utility patent).

With the present patent market weak due to Covid-19, lower level valuations should be applied to the portfolio. An approach from non-practising entities (NPE) in the US have indicated a valuation in the region of \$500 - 600 000 is valid for purposes of sale to an operating company within the cyber risk management sector at this time. The portfolio is being considered at present, as noted in Patent Encumbrances below.

Where the founder places the assets of Quantar into the new entity in exchange for preference shares, an agreed earn-out period may be applied to ensure stability and lock-in of the originator. Further, where patent assistance is available from within DMGT-V, the founder will work to ensure a full understanding of the models and systems embodied within the patents, to ensure continuity, irrespective of future outcomes.

Additionally, the patent protection provided to RMS by the Quantar patents will be in the form of annually renewable licensing during the development of the new entity. The year in which the company begins making repayments of the initial investment by DMGT, there will also be a contribution for the payment of the patent portfolio, with shares being surrendered by the founder in exchange for payment. Over future trading periods, ownership will therefore pass from Quantar to DMGT in full, in the same manner as the repayment of the initial investment.

Where a sale of the entity, or absorption into RSM, or Praedicat, occurs, the valuation of the portfolio will be accounted for on the same basis as for the exit/transfer valuation for DMGT i.e. sale price of a defined multiple of revenues.

For the software source code, this will be valued at 50% of the original cost of development.

NOTE: Quantar Solutions was listed at Companies House as a dormant entity to facilitate a potential IP sale. There is a long-term creditor, however this is merely directors loan, which was retained as a tax mitigation item in case of sale. This outstanding amount can be written down to zero where required, either for 2019 or 2020.

UK Example of Current IP Valuation - Corax Cyber (Insolvency Report September 2020)

Corax Cyber, was a UK limited liability company operating within the cyber risk modelling segment since 2016 and a competitor of RMS within the cyber risk modelling space. The company failed in 2019, entering administration in 2020.

The company was sold pre-packaged, with the two patents it owned accounting for the only value sold on by the administrators, KRE Corporate Recovery LLP, in London. The two limited patents were sold with a value of £163 349 to a US entity in 2020.

Taking the patent values at £81 500 in insolvency, Quantar's 7 US patents and 2 continuations in this model amount to £570 500 for the 7 granted patents, £80 000 for the 2 continuations, totalling £650 500.

CAPEX YTD

Expenditures YTD comprise two primary categories; intellectual property; and software/systems development. Intellectual property includes UK trademarks, patents, certified US code copyright.

Within the IP segment, costs are primarily patent attorney fees, patent renewal costs, ongoing patent continuation applications, PCT and USPTO prosecution associated fees.

For the software systems development, these costs are primarily actuarial consultancy, modelling consultancy, security research and actual software development.

Intellectual Property	£217 724
Software & Systems	£317 602
OpEx	£77 622
Totals	£612 948

OPEX is limited to field trials and market testing across countries and sectors, plus basic operating costs such as accountancy, office location, printing, with figures approximated due to the period of time covered and the number of day-to-day transactions related to them.

Legal & Tax Jurisdiction

Due to the nature of the maritime sector, most companies within it are registered limited entities in offshore jurisdictions. This applies to both the actual vessel operating companies, as well as the risk carriers.

In the case of the latter, this is standard practice for reinsurance, captives and sidecars and alternative risk transfer vehicles such as insurance linked securities. This is due to the tax burden that would otherwise reduce the total available cover within every layer or vehicle as a fund.

The most common locations are Bermuda, due to its global prominence for expertise in the reinsurance and ART sectors, as well as Luxembourg for captives and sidecars, Guernsey & Jersey for marine brokers, and Switzerland for other reinsurance operations.

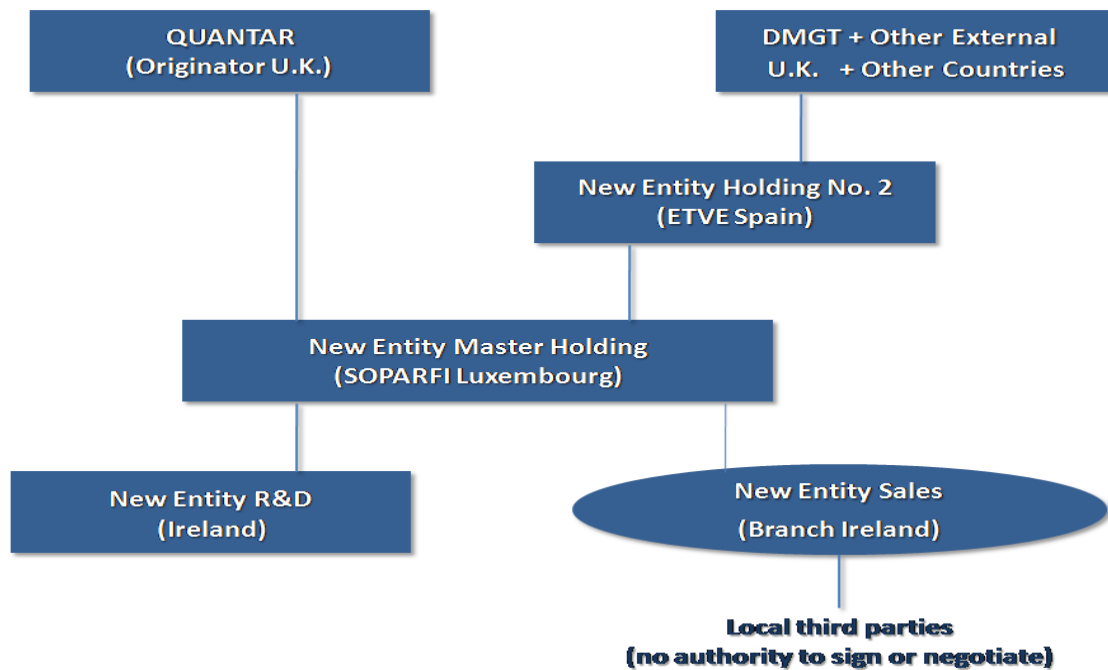
It is not envisaged that there will be a requirement for the entity to be established in an offshore location, unless deemed necessary by the client organizations. Given the company will be providing cyber risk modelling and not at the outset involved in any financial trading activities, it will be operating in an unregulated market.

If there is a later requirement by the sector, the founder has extensive knowledge of the offshore establishment mechanisms due to the predecessor of Quantar being located in both Luxembourg and Jersey. Where required, the London office would simply be a sub-division of the offshore entity, in the same manner as with RMS US and UK.

Tax Structure Where Offshore Required

Due to the nature of the maritime sector, with vessels operating in international waters, coupled with Bermuda-based risk transfer operations, it may be necessary to review the tax structure for the entity, dependent upon client requirements.

Given the potential need for an alternative structure, Quantar engaged tax specialists Nauta Dutilh to review operations and activities, to propose a relevant tax structure should this be required.



Where there are External Investors across a number of sectors, their tax domicile is highly unlikely to be in the U.K. For the marine equipment sector, this is likely to be Switzerland; for the P&I Clubs, Luxembourg; for Ports, this will be a disbursed tax domicile for obvious reasons.

Further, due to the geographic disbursement of shipping companies, it will be necessary to contract with local third parties for installation of the requisite hardware. This aspect of operations has also been embodied in the initial royalty tax structure.

NOTE: The final outcome of Brexit will have an impact upon the overall tax position in relation to all points listed herein. This structure has been defined according to the pre-31st December 2020 tax status of all the listed countries. Output VAT is assumed to be at 0% due to the parties invoiced being registered in offshore jurisdictions.

1. Group shareholders

Identification and tax residency

The identification of the top tier shareholders and their tax residency is important to locate the top tier holding company in a tax efficient way. There will be two types of shareholders, *i.e.* the initial shareholders of Quantar and DMGT (Originator) and potentially, additional external shareholders (External Investors). For the purpose of this overview, the Originator (Quantar and DMGT) are assumed to be to be U.K. tax resident.

The External Investors will be sought in different sectors, for which only one investor per industry will be eligible. These industries are ports, reinsurance, marine equipment vendors, P&I Clubs, Technical partner.

External Investors are likely to be Company X (tax resident in the Switzerland), Company Y (tax resident in the Luxembourg) and Company Z (tax resident in Bermuda). Other investors still have to be determined. Other investors may be US tax residents.

2. Group holding company

It is proposed that a Luxembourg company is used as the group holding company that holds the intellectual property rights taking into account the following elements:

Participation percentage, equity contribution and voting rights

The External Investors will hold a percentage in the Master holding. The Originator will hold the remaining percent at the outset, but this percentage may diminish over a period of 2-5 years after the launch of the commercial product on the market. Over such period, the External Investors could increase their stake by up to 52% percent, as in the case of Praedicat, with DGMT retaining 24% and Quantar 24%.

Since the Originator should contribute a small amount in comparison to the External Investors, but hold majority of voting rights, it is envisaged that there will be the creation of two types of share classes (Class A & Class B shares). Class A shares, to be held by the Originator, represent a small contribution and high voting rights, whereas the Class B shares, to be held by the External Investors, represent a high value contribution and low voting rights.

Luxembourg holding companies can be structured with different classes of shares, as indicated above.

Dividend distribution

The location can be determined based on the tax residency of the currently known External Investors. It is not the intention to seek more investors / shareholders than the initial identified external sector investors. Nor must an IPO of the holding company be taken into account, since this may jeopardize the commercial attractiveness of the product. One of the important issues to be taken into account is the dividend distributions; it is not the intention to retain the earnings.

Based on previous facts, the holding company should be located in a jurisdiction with a good tax treaty network and low or no taxation of outbound dividends.

Luxembourg has a good treaty network and has a low or no taxation on outbound dividends.

Interposition of a Spanish holding company (ETVE)

Depending on the tax residency of the external investors, Luxembourg may not always provide for a tax-free exit to the investors. For instance, a 5 percent dividend withholding tax will be due in Luxembourg to dividends paid to the US shareholders (provided they hold at least 10% of the voting shares). Therefore, it could be of interest to interpose a Spanish holding company (ETVE).³ Spain

³ A special tax regime applies to companies that obtain foreign portfolio holding company (*entidades de tenencia de valores extranjero* or *ETVE*) status. An ETVE is an ordinary Spanish company whose principal purpose is the administration and management of participations in the equity of non-resident entities. To obtain ETVE status, a company must submit to the Spanish General Director of Taxes an application containing specified documentation concerning the company and its subsidiaries. The following are the principal tax benefits granted to an ETVE:

- no withholding tax is imposed on distributions of foreign-source dividends;
- interest payments are fully deductible;
- no capital duty is imposed on the issuance of share capital by ETVEs located in certain provinces or on share-for-share exchanges;
- foreign branch income is exempt from tax;
- advance rulings are available with respect to transactions;
- dividends received from non-resident companies and capital gains derived from disposals of shares are exempt from Spanish tax, if the following conditions are satisfied:

allows a zero percent dividend withholding tax on dividends paid to non-residents of Spain, provided they are not resident in a tax haven (which will be the case).

The interposition of a Spanish ETVE is not necessary for the Investors identified as tax resident in the U.K. and Switzerland, to the extent that a certain minimum participation is held in the Luxembourg group holding.⁴ With respect to the investors resident in the US, the withholding tax can only be reduced to 5%. Therefore, the interposition of an ETVE is inevitable if any withholding tax is to be avoided.

Non-recurrent capital tax

In Luxembourg, a non-recurrent capital tax of 1 percent will be due over the contributed share capital. In the event a Spanish holding company is incorporated, a 1 percent capital tax would also be due. However, contributions in kind, such as the contribution of shares in a foreign entity, made to the capital of an ETVE are exempt from capital tax if, as a consequence of the contribution, the contributor holds an interest of at least 5 percent in the capital of the Spanish holding entity.

Location of the IP and respective taxation

The intellectual property must be located in the holding company, not in the New Entity R&D company that deals with operations and R&D. The technology is currently held by a U.K. limited company, but should be transferred as soon as possible (*i.e.*, before distribution of the business plan to potential external investors) to the group to avoid the occurrence of taxable capital gains. Since no R&D, marketing, etc. has been undertaken by Quantar in its current dormant state, there should not be a capital gain issue. Consequently, it is the master holding company that will grant licenses and collect royalty income.

Ideally, the IP should be located in a jurisdiction that has a low taxation of royalty income. There is, however, no specific tax treatment for royalty income in Luxembourg. Subsequently, the income will be taxed at the rate of 30.38 percent. It should be noted, however, that it is not possible to let the royalty income strike in an offshore company, because they do not avail of treaty protection for any income received causing withholding tax to be withheld; and because the distribution to the shareholders/external investors of such income as dividends, would cause full taxation in the jurisdiction of the shareholders/external investors. Moreover, E.U. tax law entails a fiction of law

-
- at the time of the distribution of the dividend or the generation of the capital gains, the ETVE has owned, directly or indirectly, at least 5% of the share capital of the non-resident company for an uninterrupted period of at least one year;
 - the non-resident company is subject to and not exempt from a tax system that is similar to Spain's corporate tax system, regardless of the rate of tax imposed on corporate income;
 - the non-resident company is not resident in a country identified by the Spanish tax authorities as a tax haven;
 - for capital gains, if the purchaser is resident in Spain, the seller and the purchaser are unrelated, and;
 - income derived by the non-resident company is connected with business activities conducted outside

Spain.

⁴ Under the EU parent-subsidiary directive, withholding tax is not imposed on dividends distributed to a parent company resident in another EU state, if the recipient of the dividends holds directly at least 10% of the distributing company for at least one year. This holding period need not be completed at the time of the distribution if the recipient commits itself to eventually holding the participation for the required period. Subject to the above conditions, dividends paid to the Swiss, E.U. and UK investors are not subject to withholding tax. With respect to the dividends paid to Switzerland, the 0% rate applies, if at the time of the distribution, the recipient has held at least 25% of the share capital of the payer for an uninterrupted period of at least two years.

©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

according to which any transfer of, *i.a.*, intangibles to non-taxed jurisdiction, or a jurisdiction where the company benefits from an advantageous regime for the income from the transferred intangibles, is not opposable to the tax administration. This means that an E.U. tax administration may act as if no transfer has occurred that consequently the income should be taxed in an E.U. State i.e. Luxembourg and potentially Switzerland.

3. R&D Company

R&D companies are often situated in high-tax countries, since that is where most IT specialists can be found. Amongst the different examples proposed, it would currently be preferable to locate the R&D Company in Ireland.

An Irish R&D company is likely to benefit from a 12.5 percent tax rate (as of 27th.08.2020) to the extent the income is regarded as trading income.

The Irish Revenue gives its opinion on the characterization of the income, based on a ruling request filed by the company. Such opinion, however, is not binding, but it gives a certain degree of comfort as to the applicable tax rate.

4. The sales branch/company

It is not specifically the intention to create a separate sales company. The proposal is based on the HP model and their use of transfer pricing. A sales branch/company should be located in function of an EU market penetration, given the focus of the market being U.K./E.U. in the first years of trading.

In a further stage, the Group may focus on the US market and the Asia Pacific market, for which a separate sales structure will be put in place. It should be further determined whether this would be done via another holding company or via a sister sales branch/company of the same master holding.

It is not clear whether the new entity would specifically need a sales company. Therefore, it is suggested that a sales branch is considered, this allowing for the contracting of third parties for hardware installations and any local support activities.

This has the advantage to give more flexibility in allocating the income/profits. At the level of the master holding company, only board meetings will be held and the contracts with clients be signed. A 5 to 10 percent of the global profit could be attributed to the head office. At the level of the branch, the sales/third party contracted personnel will assist and install at new clients, propose (not accept or offer) terms and conditions of sale, etc. The branch does not bear any risk and should be able to work on a cost-plus basis. The currently preferred location for the branch is in Ireland as well.

A company not resident in Ireland is also subject to corporation tax if it carries on a trade in Ireland through a branch or agency. The liability applies to trading profits of the branch or agency, other income from property or rights used by the branch or agency, and chargeable gains on the disposal of Irish assets used or held for the purposes of the branch or agency. It is therefore necessary to determine what margin the sales branch should report.

In all instances, it is advisable to maintain legal jurisdiction of the Courts of England and Wales via contract terms and conditions, with legal representation determining the best manner to attain this.



The development of the overall system commenced in 2000, created by 3 network security experts working for Belgian I.T. security firm Uniway S.A. (later Paradigmo), now acquired by French Euronext listed I.T. services company Devoteam (€762 Mln revenue 2019).

With a fourth member joining the group to forward develop the overall concept of cyber risk quantification, external suppliers were engaged from the actuarial, software simulation and intellectual property sectors:

- **NSC** (<https://www.nsc.co.uk/>): Award-winning military software simulation developers and consultants. Suppliers to British Army, Kuwait Army, UK Defence Science and Technology Laboratory. Based in Camberley.
- **Risk Capital Research and Technology (RCRT)** World leading quantitative analytical modellers in financial modelling applications, risk management and portfolio analysis. Currently assigned as portfolio risk management for the sovereign wealth fund of the Abu Dhabi Investment Authority (ADIA).
- **Lane Clark & Peacock LLP** (<https://www.lcp.uk.com/>): Award winning actuarial consultants, working within the re/insurance and energy and technology sectors, developing risk models.
- **Loughborough University Enterprises Limited** (<https://www.lboro.ac.uk/enterprise/consultancy/luel/>): Engaged to study network traffic and security, packet capture and develop the original back-end software application into a scaleable commercially deployable product.
- **Venner Shipley LLP** (<https://www.vennershipley.co.uk/>): Internationally recognised by IP Stars ranking of IP management expertise. Managed initial patent development and filing of applications globally on behalf of Quantar.

The applications developed YTD are:

Internet Protocol Threat Assessment Program (IP-TAP):

Back-end system developed in conjunction with Loughborough University Computer Science Department; collects, analyzes and outputs threat data per client installation for front-end applications (see Annex for detailed research report on traffic analysis).

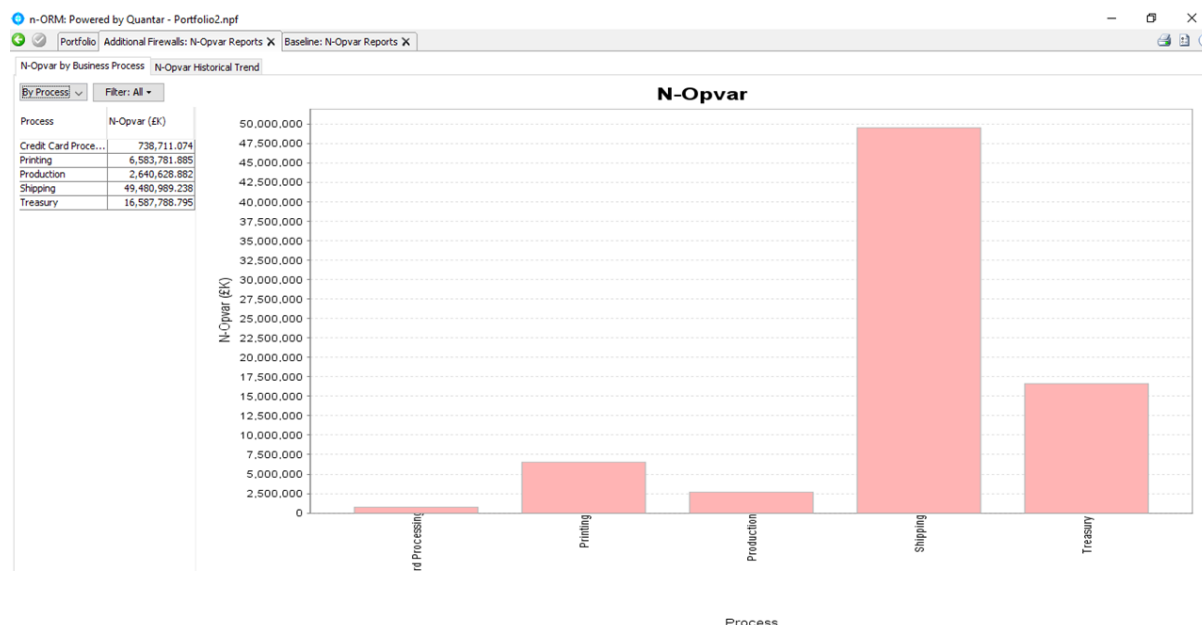
The screenshot shows the XML Marker application displaying threat data. The tree view on the left shows a hierarchy starting with 'Crimson', followed by 'ObservedThreats', 'ObservationStart', 'ObservationEnd', 'Threat', and 'Observation'. The main view shows the XML structure with attributes like 'ID', 'Category', 'Target', 'SeverityScore', and 'Observation'. A table at the bottom lists 14 subtags with their respective values.

Tag name/Text	ID	Category	Target	SeverityScore	Observation
Threat	1408	Indiscriminate	Unknown	7	Observation (163 occurrences)
Threat	2417	Indiscriminate	Unknown	4	Observation (163 occurrences)
Threat	472	Indiscriminate	Unknown	7	Observation (163 occurrences)
Threat	2050	Indiscriminate	SQLServer	1	Observation (163 occurrences)
Threat	2003	Indiscriminate	Unknown	7	Observation (163 occurrences)
Threat	2466	Indiscriminate	Unknown	4	Observation (163 occurrences)
Threat	2924	Indiscriminate	Unknown	10	Observation (163 occurrences)
Threat	2404	Indiscriminate	Unknown	10	Observation (163 occurrences)
Threat	579	Indiscriminate	Unknown	7	Observation (163 occurrences)
Threat	1918	Indiscriminate	Unknown	4	Observation (163 occurrences)
Threat	1002	Indiscriminate	Unknown	10	Observation (163 occurrences)
Threat	1113	Indiscriminate	Unknown	7	Observation (163 occurrences)
Threat	2570	Indiscriminate	Unknown	7	Observation (163 occurrences)
Threat	1852	Indiscriminate	Unknown	7	Observation (163 occurrences)

Sample xml Threat Data System Output

Network Operational Risk Manager (n-ORM):

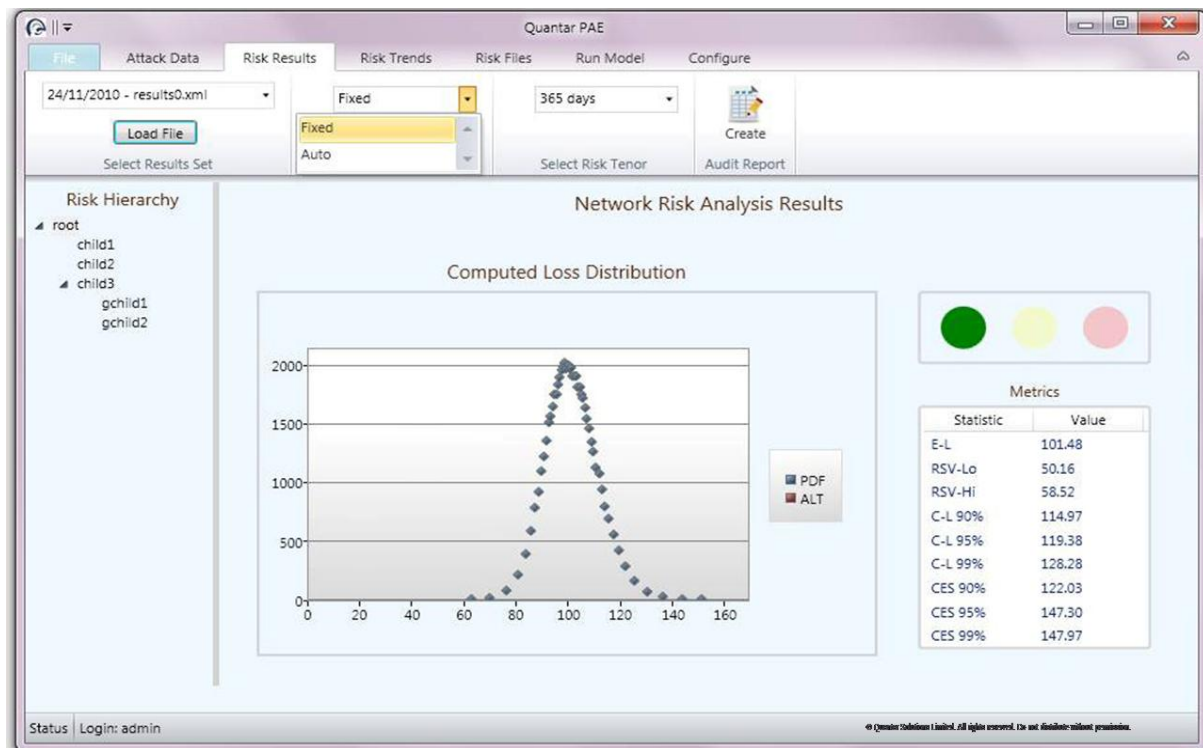
Developed in conjunction with NSC to model system/process/category interdependencies, derive a financial risk exposure from cyber threats, allows capital modelling efficiencies from what-if scenario changes for cost-benefit analysis of mitigation actions.



Example Screen Process Vulnerability Hierarchy

PAE Predictive Analytics Engine (PAE):

Developed in conjunction with RCRT. Utilises the same data as n-ORM but uses a different series of models and model control systems to account for fat-tailed risks from cyber. Projects loss values and attack rate forecasts up to a maximum of 9 months ahead of present, facilitating risk pricing for current and future periods.



Example Computed Loss Distribution

Implementation of Marine Solutions

Hardware Installations on Vessels and at Ports

Logistically, the marine sector poses major problems to be overcome in order to acquire sufficient data to create value for the end user and the company overall. Ships only generate revenue for owners whilst in transit, with port time kept at an absolute minimum. This creates a small time window, infrequently per year for the installation of the relevant hardware.

However, it is the intention of the company to install within the target group of companies that are located in the EU in year one. Further, the number of extra large vessels is limited and with the volume owned by EU operating companies, the opportunity to model a series of sub-sets per category and size is available from the outset.

If the company is able to gain buy-in from the operators to have sufficient volumes of hardware to be installed, it may be possible to have bespoke units created by the vendor/s that would be only available, under contract terms, to the company, creating competitive advantage, as well as switching costs.

Working in conjunction with the shippers, the company will have lead time to enable allocation of resources to execute the installation and configuration tasks on an ongoing basis. Once credibility and usefulness has been established, it is anticipated that a mass roll-out to the larger fleet would be made over the first two years of operation, generating far greater data sets.

End User Training

As has become increasingly the norm, end-user training will be conducted remotely via online training using the Moodle, or similar platform, allied to one-to-one video training. Most technology companies have switched to self-paced online training in recent years. With Covid-19, the digitisation of training has been vastly accelerated, resulting in global acceptance of the use of online training and certification.

There will be a requirement to deliver training in multiple languages, with a gradual roll-out of this once assessment of need has been completed. Where there is a language need, this will be a one-off cost in the creation of the customised training solution. It is not envisaged that this cost will be high, given previous experience of creating software in various languages, including Arabic.

Additionally, the creation and delivery of multiple language training will not require more than 1 week of engagement with a third party for voiceover of existing video training. There will be an additional cost for developing self-assessment tools, which is included in the financial plan, as well as new and/or revised documentation.

Local Hardware Installations

There will be a requirement to have a ready-configured managed switch installed on each vessel required by the client. This is a simple plug-and-go task, with a power supply to be activated, together with 3 short cables. This task will be outsourced where required, with the probability that a UK installation will be undertaken by a team member in the short term.

Costs for external third parties to undertake the task are based upon those levied by external developers during the Covid period and as such are valid for the purpose of establishing total installation costs per instance.

Quantar has 20 years experience (and in its previous guises of Web-gain sprl [Belgium] and IP-TAP Ltd [Jersey]) of hardware and software installations across the EU and in the US. Further, with some installations being in highly secure environments as well as needing to comply with SEC regulatory functioning, the company has long-established process flow and other related documentation to control and maintain quality per installation (see Annexe for samples). This will be adapted for use in the marine environment.

With the platform and applications being cloud-delivered, there are no other constraints for local installations aside from local assistance where necessary. Access to the platform will be via a simple browser with access control by way of hardware devices at the platform end. Support will be provided remotely (see Annexe) with the system not being mission-critical in operation, removing a high degree of urgency for response.

NOTE: See Hardware Section Below for Marine-Specific Potential Hardware Installation Issues

Customer Support

©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

The company will use open source trouble ticketing software as part of the overall troubleshooting and customer service process; previously OTRS and Spiceworks have been used to good effect for major corporate customers. This will limit the operating overhead substantially, whilst providing a high level of service and issue management.

Telephone and email support will also be provided, with the method and basis being included within the Annexe herein.

Development Rationale

Remote working will become part of working practices across sectors, including within the re/insurance and broking sectors, marine administration and management and port operations. This will require previously in-house accessible software applications to be accessible remotely. A corporate shift to cloud operations was previously in progress, but the current operating environment has created urgency. The existing software applications therefore require a similar redeployment within a cloud environment for ease of remote access by multiple user groups across sectors. RMS and Praedicat utilise the same operating model whereby the greater the number of clients, the more use their data is to overall model development.

The overall business model requires data to be acquired from client organizations and stored for data aggregation and modelling. By using a cloud solution, the data is non-sensitive and therefore carries no regulatory risk, whilst providing secondary revenue opportunities from the same data sets used by clients.

The approach in developing the initial products was based upon evaluating and selecting best in class regardless of the sector of the supplier; commercial; military and academic. Additionally, in 2000-20014 there was little existing data or competition to base selection criteria upon in the cyber risk financial quantification segment. During this period, there was no pure cyber insurance available and a C-level mindset that cyber was purely an I.T. security issue as opposed to a corporate/enterprise/compliance risk management requirement.

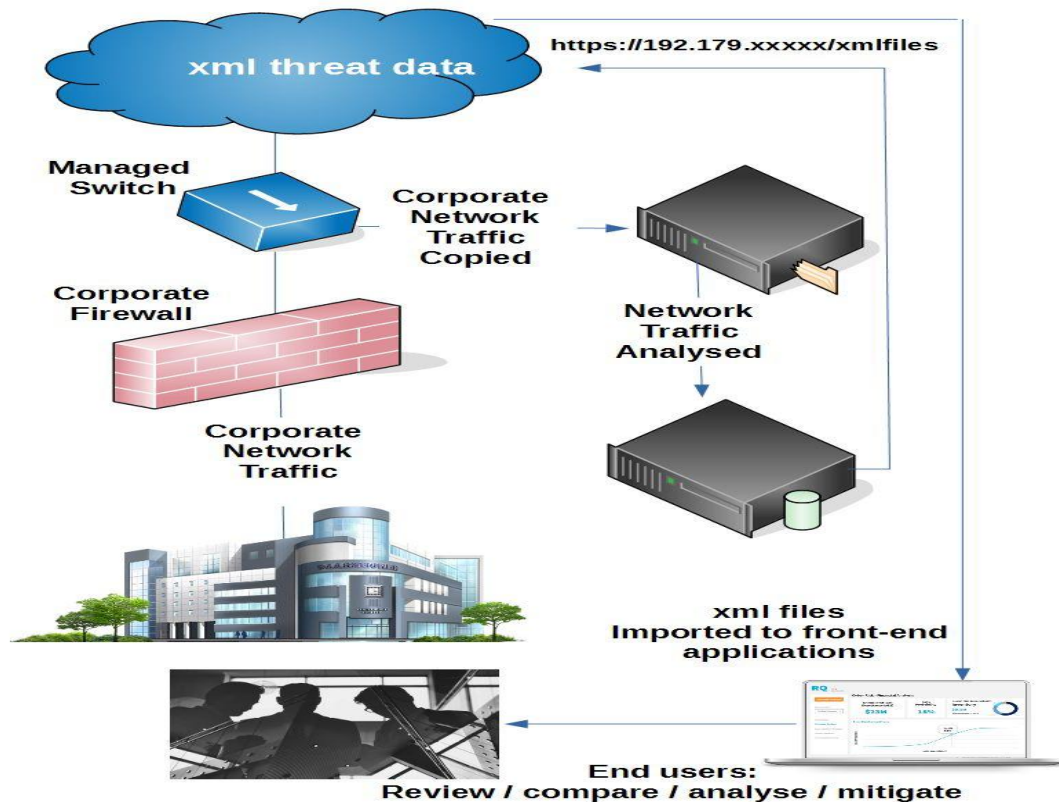
As a consequence of this approach, disparate applications were developed using different programming languages to run on different platforms. This was not an issue given the original intended users would use the applications for different functions within an organization.

By comparison with RMS's software solutions, these are also developed in C# and Java, validating the language used in such enterprise software solutions.

1. **IP-TAP:** FreeBSD + Ubuntu Server
2. **n-ORM:** Java
3. **PAE:** C#

The main development period 2005-2009 was pre-cloud delivery and the intention is to further develop the applications and to then deploy them using a major cloud provider. As cloud developers have sought to open up their platforms to support an increasing number of languages, those used by the applications in their current state could be used as-is.

Current Installation and Operational Framework:



However, the intention is to add functionality to the applications, create a consolidated and cohesive single UI/UX, together with leveraging the data generated per client and maintaining a low operational cost.

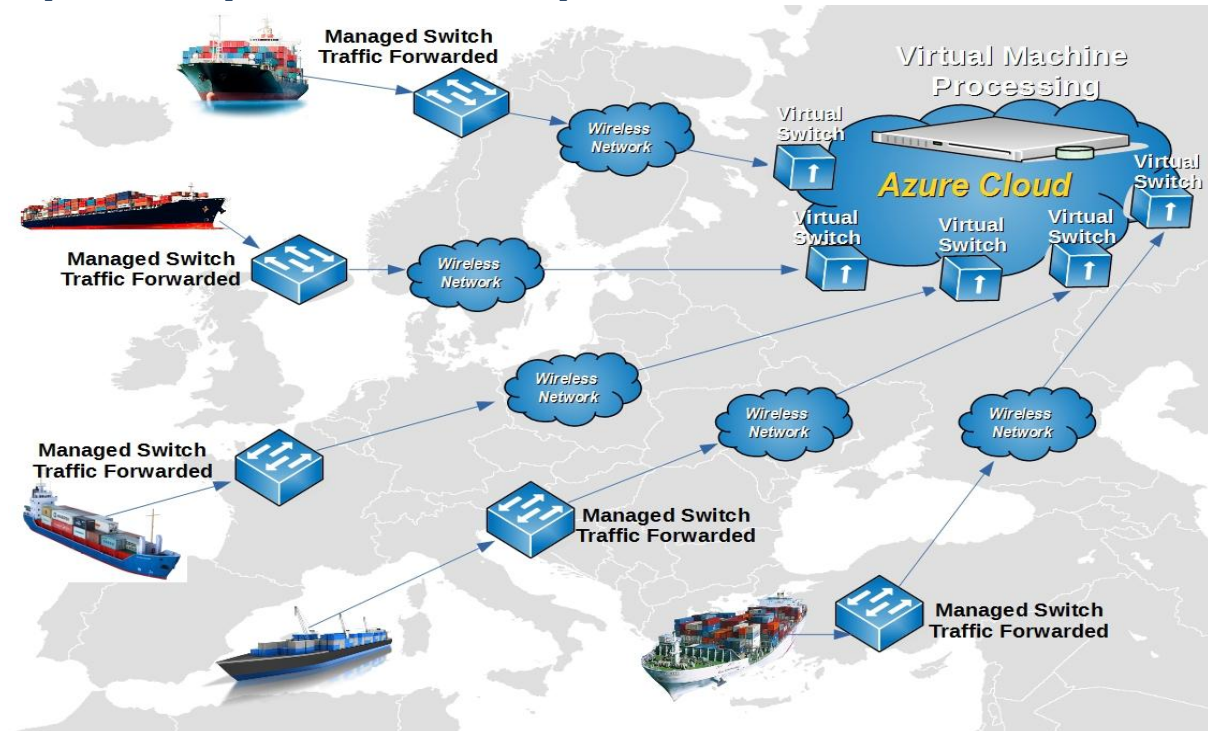
In the initial re-development phase of the proposed program, evaluation of different languages, migration and architectures will be undertaken. The final decision will be encapsulated within the product specification document.

It is programmed that year 1 will be a development and incremental roll-out year, with year 2 generating meaningful revenues, as with RSM with the RMS One and RMS IQ platforms and as such is an accepted development path for DGMT.

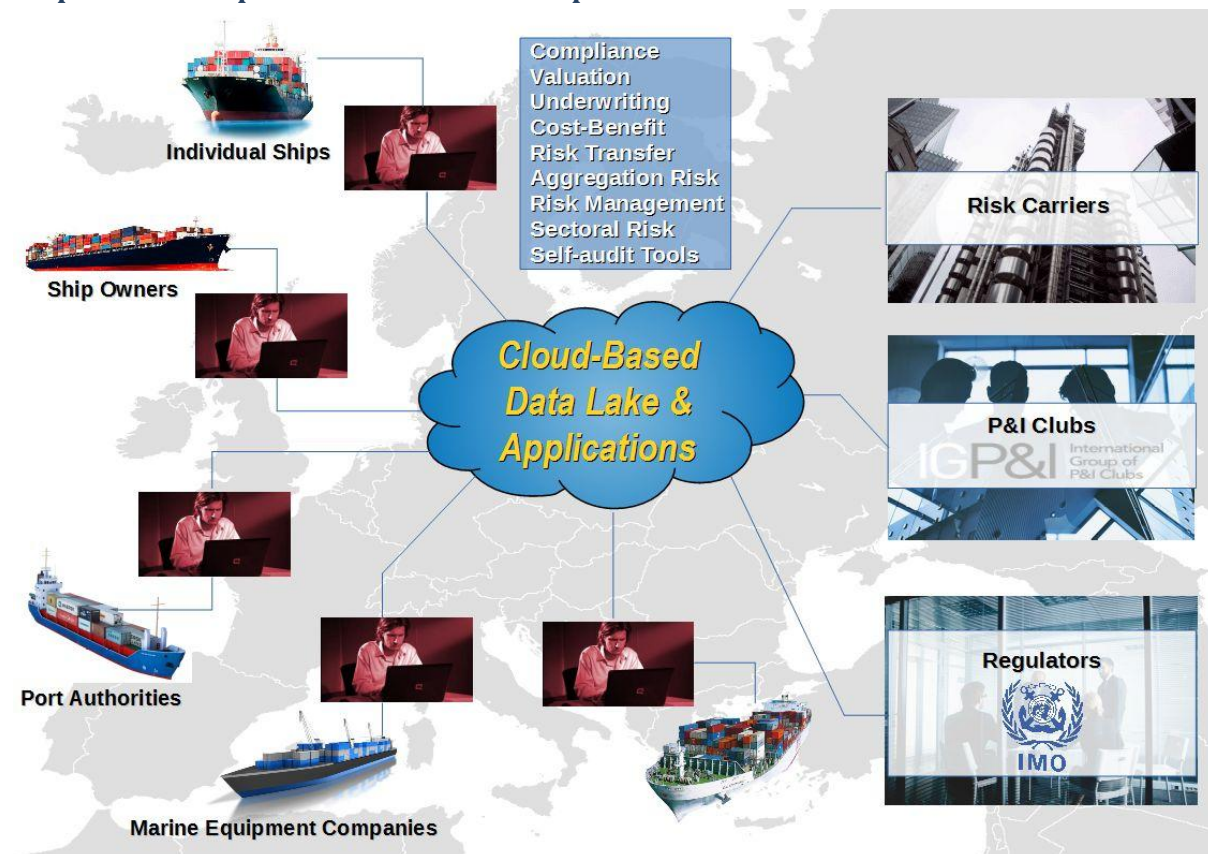
Best practice will be followed in determining the architecture and operation, with the web tier being stateless to facilitate rapid future changes, respond to demand shifts, customise for use within other sector-specific segments (see target markets) and above all, cost-limitation. In a cloud environment, an operator only pays for the server resources actually used. Risks from hardware failure will be managed using horizontal scaling, which also provides flexibility and cost limitation.

The initial evaluation would propose use of Microsoft Azure as a platform, as opposed to Amazon Web Services, with Tableau, based upon the ability to integrate with Microsoft Power Business Intelligence for high value-added services for clients. This would include highly customisable and interactive reporting as well as in the provision of self-help tools such as standards-based online questionnaires for self-assessments, impact assessments and gap analysis. These are low-cost functionalities with high perceived value and are well-established as value-added services within the re/insurance/broker sectors.

Proposed Development Installation and Operational Framework Part 1:



Proposed Development Installation and Operational Framework Part 2:

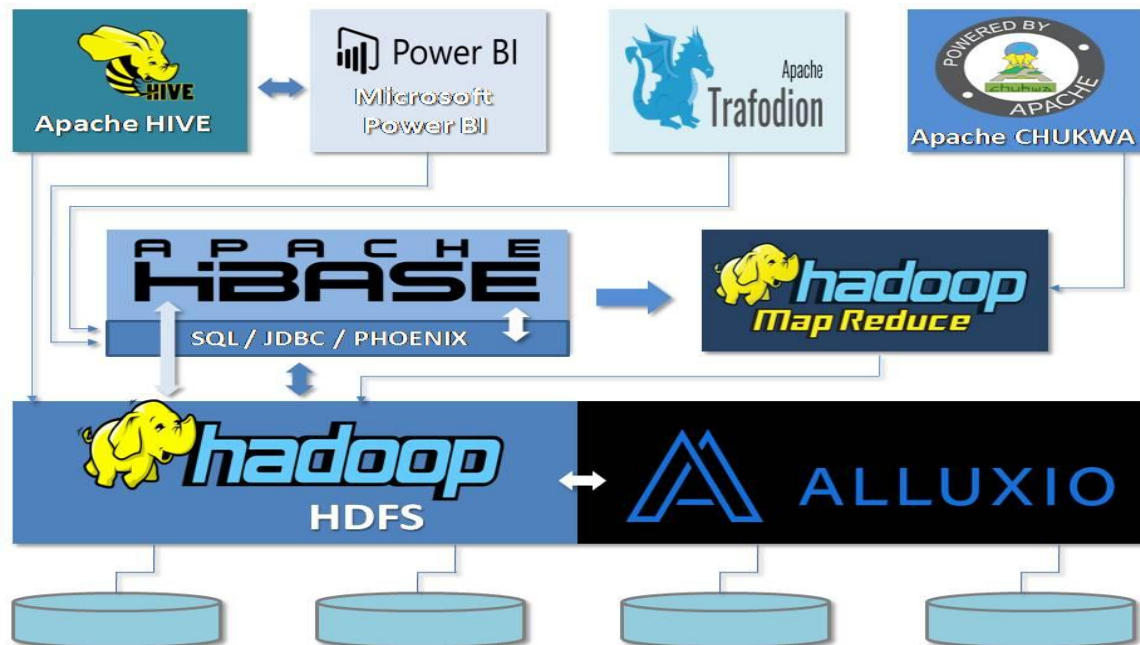


Since the intention is to acquire large volumes of data and to model from it, a Hadoop infrastructure will be implemented in the cloud. This will serve the company over a sustained period given the open

source nature of the software, with ongoing development and additional software applications and resources being added.

Hadoop is a well-accepted data repository system and has a number of modelling and presentation tools available; for the data modeller and for the end-user creating reports. As such it is a low-cost option for the data aspect of the program. Using a cloud provider for data manipulation converts CAPEX to OPEX, with usage per Mb/Tb determining cost, i.e. scalable with no fixed overhead.

Proposed Development Data Lake Framework:



It is both the intention and objective to utilise open-source, non-proprietary solutions whenever possible. This has always been the ethos, with the systems utilising open source operating systems such as FreeBSD and Ubuntu to good effect. Within the past 3 years, there has been an increasing shift towards open-source software development due in part to the major technology companies adopting this as a means of developer engagement in the face of increasing competition for skill sets and resources.

For the new entity, this approach serves several purposes:

1. Low cost of development through external contractors and free code;
2. No lock-in to a supplier of highly proprietary code;
3. High volumes of API's and libraries to speed development, deployment and support;
4. Adaptability of solutions to use within other sectors e.g. energy;
5. Interoperability of systems and ease of access for end-users.

The major players and their competitors have, since 2018 in particular, embraced the whole concept and ethos of free and open source, with revenues being created through added value services, such as support and customisation (e.g. Canonical; Red Hat, Microsoft), or through migration to the cloud e.g. AWS, Azure, Service Cloud, Zoom, Alibaba, etc, and monetizing through processing/storage.

Menu Search **Bloomberg**

Stay informed with Bloomberg as we track the post COVID-19 economy. **Enable desktop notifications.** Allow

Deals

Microsoft Buys GitHub for \$7.5 Billion, Going Back to Its Roots

ZDNet CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITERS

MUST READ: 7 top Windows 10 annoyances and how to fix them

Why Microsoft is buying GitHub: It's all about developer relationships

Microsoft's move to acquire GitHub isn't all that surprising given that the company is a top contributor and has worked well with developers in recent years. Now can it keep GitHub the Switzerland of code?

Microsoft | Official Microsoft Blog Microsoft On the Issues The AI Blog Transform

Microsoft + GitHub = Empowering Developers

Jun 4, 2018 | Satya Nadella - Chief Executive Officer, Microsoft

This is counter to RMS's strategy, which is founded upon proprietary software from a limited supplier for analytics and business intelligence (Qlik), as well as owning its own development team in-house, which requires ongoing recruiting and on-boarding for development of its own products, platform and the analytics provided by Qlik, creating substantial overhead that could not be borne by a new entity.

Qlik Products Solutions Learn Support Partners Company

- Data Analytics
- Platform & Products
- Qlik Sense
- QlikView
- Value Added Products
- Developer Platforms
- Platform & Products
- Qlik Analytics
- Platform

Accelerate data - on

Turn raw data into relevant insights and analytics solutions. Close the gaps between data, insights, and action.

9/1/2020 Search all Jobs | LinkedIn

in Search

Jobs RMS Date Posted Experience

Noida, IN
Actively recruiting
1 month ago · 31 applicants

RMS Software Development Engineer: Java, Scala
Promoted
RMS
Newark, CA, US
1 connection works here
5 days ago · 17 applicants

RMS Client Success Executive
Promoted
RMS
London, England, United Kingdom
Your profile matches this job
2 weeks ago · Easy Apply

RMS Qlik Developer
RMS
Noida, IN
1 connection works here
1 month ago · 16 applicants

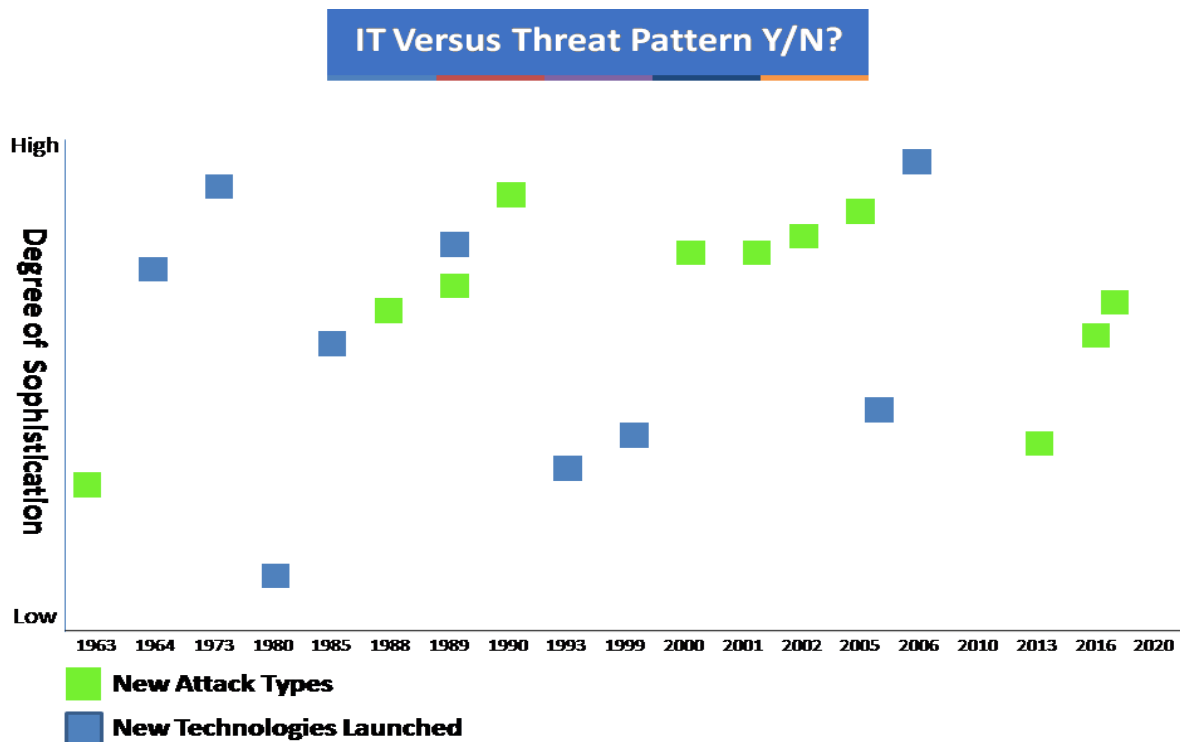
RMS Software Development Engineer II
RMS
Noida, IN
1 connection works here
1 month ago · 23 applicants

RMS C#/Java Developer
RMS
Newark, CA, US
1 connection works here
1 month ago · 6 applicants

RMS Sr. Modeler
RMS
Noida, IN
1 connection works here

New technologies will also need to be accounted for, including autonomous control systems for vessels, changes to PLC's, changes to navigation and propulsion systems, communications systems such as 5g.

Of note is that attack types and evolution, since the 1960's onwards, have not developed in a linked and linear manner. The company has extensive experience in assessing threats and their evolution, spawning numerous models and patents over the past 20 years. As such, mapping of potential security issues into future periods and adapting models and software will not pose an insurmountable problem for the in-house team, supplemented where required by external sources e.g. university divisions.



© Phillip King-Wilson / Quantar Solutions. Do Not Distribute Without Written Permission

Project Management & Reporting

The leadership has long-term experience of managing software development at distance, with the three main software and systems development having been managed across countries. Each contractor operated completely independently, but under the guidance of Quantar. As such, project risk management is reduced and further by the shift or working practices to using remote developers in Eastern Europe by US/UK entities within the same sector and more recently by the impact of Covid-19.

The combined team will utilise well-accepted cloud based project management software from Atlassian Software for all aspects of the program. The program will employ a combination of Prince 2 and DSDM Agile project management frameworks.

Prince2 is a long-established means of managing complex projects, with the end result being the focus. This framework operates well in larger programs, but the reporting and issues handling mechanisms remain suited to software projects as an over-arching framework. Dynamic Systems Development Method (DSDM) Agile is the most used software development project management method currently. This requires projects to be broken down into time blocks with a development defined within the block. Like many management methods, Agile and Prince 2 are simply a codification of long-standing practices, with Agile merely being a documented method of previously PM methods of defined work packages.

Use of Atlassian Jira software for the Agile software development ensures a sectoral-best tool is utilised for the software project management. Jira is ranked as the top software tracking and issues tool for agile software development.

Use of Atlassian Confluence is a top collaborative working software package. Both Jira and Confluence have a low per-user cost base, with each costing £60 for 15 users of each package. The use of other remote working packages such as Zoom will enable remote working practices for a number of the program members and eliminate office and facilities overheads whilst providing optimal flexibility for ongoing program and company growth.

Regular reporting to the Board and program sponsor will be facilitated through access to both software tools, providing transparency and insight into development speed, issues and features developments as feedback is taken account of by the development team.

Where in-person meetings for the team are required, these can be arranged at low cost in view of the numerous options now widely available for facilitating such group discussions. This may include the use of the existing St. John's Innovation Centre meeting rooms, or a mutually convenient location for the individuals concerned.

Office & Equipment

Since substantial remote working and utilisation of external third parties is intended, the cost impact of office space and working equipment will be limited to absolute basic needs. This comprises laptops and associated office productivity software (the team will use free LibreOffice and other open source applications). The use of cloud-based services will not require high specification machines, again limiting initial CAPEX spend. Basic laptops will be utilised by all team members, with a ceiling per machine based upon MS Windows pre-installed. Productivity and program management tools will be cloud based, with mobile app capability to ensure no lost work time.

Mid-range mobile telephones and laptops are fairly generic in specification and cost and as such, whether a team member opts for one type over another i.e. Mac or Windows/Android is irrelevant to the start-up costs. In line with Praedicat, this slim operating model will be leveraged wherever possible to optimise operating margin.

To reduce initial costs to the minimum, the Founder will utilise their own equipment for the new entity and take a lower salary than the other members of the team, with the trade-off being at the point of exit.

Office space will be limited to team meeting points, with typical hot-desking costs at St. John's Innovation Centre, as an example, being £12 per week, with the ability to rent meeting rooms on an ad hoc basis.

For in-house testing and concept development, the company will have an initial 2 sets of servers and managed switches that have been field tested and updated to the current specification of software during the period of July - August 2020, with the work being undertaken by German networking specialist company LX Systems, based in Düsseldorf. This work was undertaken remotely, underpinning the concept of remote device management for the new entity.

Although the intent is to operate primarily as a virtual team, some early team-building time and space has been allocated to the financial plan. Covid-19 has amply demonstrated the lack of need for fixed overheads for a technology start-up and failure risk is therefore limited.

Additional equipment will be required in the form of managed network switches and potentially network packet broker units for evaluation, configuration and learning how these will be installed at client premises. This is still substantially less than was originally required for the development of systems and software at multiple locations.

Program Roadmap

The program will be divided into functional areas, although the horizontal structure will involve all members within each area. The initial activities are summarised as:

1) Software/Systems

The current installation method places too heavy a burden upon the clients in the provision of an ability to install multiple hardware devices and the associated cabling and power supplies. The open source movement and associated virtualisation allows a redevelopment of the hardware installation into a single small profile box with limited cabling and a single standard power supply. The systems development will be outsourced, at speed and is anticipated to take one month to complete.

The front-end applications will be redeveloped into a cloud-based application set, with a unified UI/UX aligned with current GUI fashions. Benchmarking will lead development in this area, however, the use of open source tools, such as Wordpress, MS Power BI, etc already provides much of the required information for user-friendly interfaces. As such, the task will be quick to execute using a third party contractor.

The software has an encryption algorithm embodied with it, secured by a hardware dongle. This was implemented to control trial versus fully paid versions as well as ensuring the per-seat pricing model was maintained. Additionally, for regulatory compliance, the ability to control who is able to configure or make changes to the system at the user end also requires physical control. The German company concerned, Matrixlok GmbH, is able to supply the necessary information to remove this functionality from the software during redevelopment. However, it will also be considered to secure user access in the future and compared with security delivered by current access control systems.

Technologically, the requirements are simple and require input for additional and/or revised functionalities, multi-language support, wireless tap in addition to traditional hardwired networks; exporting into various data formats (for multiple models and technologies in future development such as blockchain); integration of self-help reporting, audit and questionnaires.

The timeline set for this activity is 4 months, utilising an external contractor. Proof of concept will be in month 5 and the first test client location at month 6. Commercial roll-out will also commence in month 6.

2) Modelling

There are additions to the models that can be incorporated into the existing software. These include marine-specific attributes, a previously developed series of refinements and optional inputs to the models (e.g. using Markov and Autoregression as a pre-processor within n-ORM and using the Founder's developed model using an epidemiological models to increase threat data accuracy).

Additions to the models must be facilitated and the development of an appropriate data model will be important in this area. This will involve the engineering member and founder. The first developed models will be passed to the software development external party within the first month of modelling, with a second set of updates being issued by the end of month 3 due to the complexity of the models being integrated without error.

©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

There will be ongoing, iterative development, taking feedback from the marine and risk carrier sectors in order to update and uplift the software, as per RMS and Praedicat.

An allied activity will be the development of additional patent filings in order to protect the software as it is being developed. This will be carried out in-house, with external validation only once the specification and claims are complete. The Founder has extensive experience in this field and will hold responsibility for company IP. A marine-focussed patent is being filed as a provisional patent, covering all of the areas developed to date, with a deadline to file a non-provisional utility patent of September 2021.

3) Industry Engagement

It is important that the marine sector inputs are acquired as soon as possible after program commencement. This will require a concerted activity within the London territory by the industry engagement member. It is envisaged that personal contacts and meetings will be required, with a need to have a field and market test client being secured and contracted by month 4. Commercial sales to clients must be attained by month 5, with implementations commencing by the end of month 6.

This is a sales activity, with a heavy reliance upon the experience and knowledge of the holder of the position. The time-intensive nature of the task will take the majority of the member's calendaring, however the need to understand, in depth, the workings of the software, the benefits to a client and integrating with the other team members will consume most of the first month as a training and on-boarding process.

Program Roadmap: Hardware/Software/Models - Details

Hardware

The initial hardware configuration from 2005 onwards required two servers and a managed switch. The cost per installation was therefore a function of the number of perimeter security devices (firewalls primarily) multiplied by the package. Taking an average cost per medium-large sized organization installation as being*:

Network Tap Server: HP DL360 Gen x	£1400
Threat Database Server: HP DL360 Gen x	£1800
Managed Port Mirroring Switch HP	£300
Total Single Point Installation	£3500
Enterprise with 5 External Network Access Points	£17 500

* Simplified costing. Each server requires manual hardware transformation, with additional hardware and software installed, each with additional costs e.g. additional network interface cards, RAID controllers, installation of proprietary Quantar software code in FreeBSD and Ubuntu server.

Subsequent years has provided the capability to remove the fixed costs associated with installations, through the use of virtualisation allied with cloud processing of large volumes of data.

The first stage of engineering research will be in the area of virtual switches (v-switch), ports and virtual LAN's, with traffic forwarding to a cloud hosted v-switch. Where it is possible to attain sufficient

performance, the requirement for hardware on each vessel and at each port would reduce the burden on the client in terms of cost, management and accommodation.

A key issue will be in determining the packet drop rate using a physical switch with a virtual port, since the traffic will be forwarded as entire traffic streams. Compliance with GDPR and other data privacy regulations requires an extremely low packet drop rate, in order to prove data losses are not attributable to it being acquired by a third party.

In a normal corporate environment, this may be difficult, if not impossible to achieve due to data volumes. However, within the maritime sector, bandwidth is such that data volumes are very limited.

With a v-switch it is possible to span a single interface, a range of interfaces or even a whole vlan on the v-switch to a destination. However, it is necessary to be aware that if there are multiple sources at the output end, then the destination port in the cloud as a v-port may need sufficient capacity to complete the traffic forwarding i.e. 10 sources of 1 Gbp/s each, and a destination port of 5 Gbp/s will result in potential data loss. Since cloud costs are based upon usage, it will be necessary to understand the actual computing cost using virtualisation versus physical infrastructure. Since it will not be necessary to capture egress; only ingress then this should not be an issue.

Other areas to be investigated will be vlan tagging and whether this will be necessary, together with the configurations of the v-switch and trunk port. The other main issue to be addressed will be how the security features of the v-switch can be utilised or dropped to ensure all traffic is forwarded, rather than being blocked partially, or in whole, by such features.

The end objective should be to overcome the physical server requirement and monitor inbound network traffic and store in a data-like environment (elastic search, azure log analytics, etc) to be collected and processed by the various processors at a later stage.

How this is to be achieved is the question to be answered on the hardware side of the development. However, it should be noted that most major suppliers have the requisite capabilities to arrive at the desired goal.

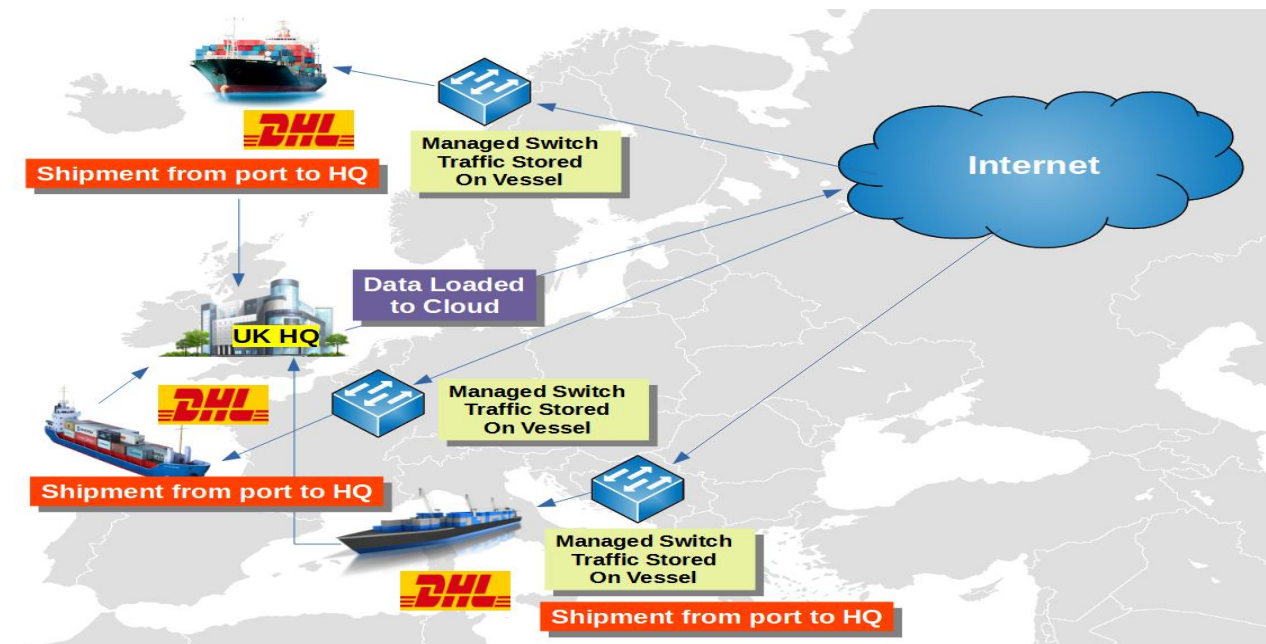
Potential Marine Installation Issues

The marine sector is hampered by digital transmission limitations. This manifests itself in a number of areas, as listed above, that limit data reception and transmission. In the current and proposed hardware development, the assumption is made that it will be possible to re-transmit the inbound data to the cloud via a locally installed switch with a virtual port to another virtual port in the cloud.

There is a risk that the extremely low bandwidth available to vessels on their global routes will either be insufficient or asymmetrical in availability, rendering the proposed method of data acquisition and use impractical. Where this is found to be the case during the initial engineering analysis stage of development, a simple alternative is available. This will make installations as simple as the proposed development path, but with an additional step in the collection process.

A further assumption is based upon the roll-out globally of 5G networks, which will offer respite to the marine industry with far higher network traffic volumes being made possible. However, with some countries blacklisting the global leading supplier, Huawei, there is also the potential for a delayed roll-out of up to two years as well as the same potential for asymmetrical network availability globally whilst the vessel is in transit.

A hardware installation will simply dump all inbound data to a storage mechanism that is either accessed remotely each time the vessel docks and has high volume data access when at port, or the physical storage media will be swapped out and the data collected sent physically to the new entity.



The operational impact downstream in modelling risk and providing compliance data would function in the same manner, but with a time delay between the acquisition and centralised storage and processing. The time lapse will obviously be a function of the time between port docking. However, since the entire system is non-critical in its real-time operation, the impact upon operations is minimal; the impact will be on the start-up phase and cashflow impact.

However, the mitigation option for both control of the hardware and the up-front cost may be via leasing the hardware from a major supplier that views the opportunity to partner for volume sales. Typical leasing costs from Juniper Networks for hardware costing £1500 for example are:

24 months £56.09	36 months £40.06	48 months £32.14	60 months £28.35
---------------------	---------------------	---------------------	---------------------

Finance Lease Basis

24 months £62.5	36 months £41.67	48 months £35.71	60 months £29.53
--------------------	---------------------	---------------------	---------------------

Pay fixed prices on a rent -to -own agreement Basis

This method of hardware acquisition within the marine environment where tracking of hardware is potentially problematic, may also be viewed as a risk management option where the volume of installations poses financial risk to the company. The potential for developing a longer-term relationship with the vendor would also offer an opportunity for bespoke development for marine-specific solutions.

The data would, in this case, be acquired via a low-cost managed switch and the entire network traffic stored on a local device. This will be couriered to the UK HQ where it will be uploaded to the cloud environment.

* Shipping to UK HQ from:	DHL Cost £
----------------------------------	-------------------

Italy	77
Spain	77
Norway	72
Turkey	72
UAE	80
USA	63

* 30cm x 30cm x 30cm x 5KG

It may therefore be more cost-effective, where it is possible to swap storage drives at a low or no cost, to utilise this method than the proposed upload to the cloud. A cost analysis will be undertaken in weeks 1-2.

At this point, the potential is to utilise products from a leading technology, due to their use across various geographies i.e. support is available. The lack of available product liability due to the offshore nature of the installations is therefore mitigated by such a company's products and provides assurance to shipping operators.

It may be advantageous to have the hardware installed to be certified by the marine certification body, the DNV GL in Norway. This body certifies for a number of sectors, including marine. Currently, the DNV GL is authorized by 130 maritime administrations to perform certification or verification on their behalf. The company would work in conjunction with the suppliers to investigate and certify the product used, since this would be in the interests of the supplying entity.

Software

The development path for the software will follow four prongs of:

1. Updating and integrating the existing software products and functionalities;
2. Migration from existing local installations into cloud-based processing/stored data;
3. Developing new functionalities and UX for marine/utility specific use & self-help tools;
4. Developing the data models for analytics, AI/ML and big data storage/processing.

These will require in the initial phase a redevelopment of the software architecture. Commencing with the high level design, the engineering member will work in conjunction with the modelling, reinsurance members, and the founder. This task will take into accounts all components to be integrated into the new and future versions of releases for the initial maritime sector as well as potential other sectors, such as utilities.

Benchmarking against the RMS product roll-out rate of 3 new products out of 300 per year, the objective will be to launch a revised version of the current software, plus an additional new product in year one.

Further functionalities will be delivered within a unified UI, which will appear as new products, including self-help tools from year two onwards. There will be extensive use of open source software, which may require proprietary API's to be developed where there are no existing libraries. However, since the current software has been developed in the most common programming languages, this is not likely. Review will be at the outset of the software redevelopment planning.

The major task for the team will be in building virtualisation and data lake skills. However, there are a number of existing publicly available schemas to draw upon and this is not envisaged to require a major level of investment. Utilising external developers with the appropriate skills will reduce development, training and budgetary burdens.

Key Points:

1. Existing software is fully functional; short-cut to new version.
2. Anticipated model developments are covered within existing patents i.e. no infringement.
3. Virtualisation simplifies system installation & operation, with significant cost reductions.
4. RMS - already developed a similar integrated platform with i.e. proven concept to follow.

Marine Cyber Risk Models

There are several marine-specific cyber risks that are not modelled outside of the sector. These include, but are not limited to, the following:

1. Marine propulsion systems have a number of programmable logic controllers and electro-mechanical systems that have been targeted by brand of marine engine;
2. Certain geographical routes have been made specific targets of cyber attacks, typically spoofing of GPS location;
3. Types of vessel are routed to specific ports due to their cargo and port systems are targeted via staged attacks exploiting third party network access e.g. brokers, payment providers;
4. Vessel records are easily accessible, disclosing refits and age/type, exposing them to defined attacks by ship age/equipment age.

It is for this reason that the development requires input from the marine industry from a physical vessel perspective as well as from a risk one. However, of note is that there are models that already exist, that account for the risks listed, albeit in different sectors that can be assessed and adopted where relevant.

The company has already developed some of these and already has developed models to be incorporated into the current software that can be implemented rapidly and at a lower cost than from a standing start.

The role of the modeller will be to assess and test which increase accuracy of risk values output from the models and which would be accepted by the reinsurance/ART sectors in order to attain credibility of the models and subsequent reductions in premiums/fees for placement to cover risk. Credibility within the reinsurance markets, especially the Bermuda market is also the main focus of RMS in its ongoing model developments and subscription renewal rate.

Reinsurance & ILS Development

The current marine reinsurance structure, as outlined above, utilises a pooled risk concept at both the individual P&I Club level and at the global level. The objective is to create suitable layers of reinsurance protection at the lowest possible cost, whilst using funds accumulated from premiums to invest and offset future changes in reinsurance premium rates.

At the individual P&I Club level, the degree of efficiency in this operation acts as a differentiator between P&I Clubs and similarly, the larger the fleet number per club, the greater the premium income per club with a consequent greater fund to invest and maintain lower premiums per ton, benefitting the members of the club.

The use of reinsurance is achieved through the usual channels of cover i.e. the major reinsurers, together with private placements, thereby removing regulatory constraints for some layers of the

cover. The pooling of risk is made on the same basis as for captives within major multinational corporations with large product/service lines across numerous geographies.

The private placements may be regarded as a move towards increasing use of insurance linked securities (ILS). There has been a growth in this sector over the past 2 years within the NatCat segment of reinsurance and in particular where there is clearly identifiable and quantifiable risks such as windmill ILS placements (Achmea Windmill II in 2020 for example).

For cyber, there has been zero growth in the use of ILS due to the nature of the risk and the rapid and constant shift in attack types and targets. The retrocession risk has long been recognised and with legal cases for business interruption from Covid ongoing, risk carriers are unwilling to cover demand for cyber risks due to silent cyber. For the same reasons, ILS for cyber is similarly at a near-zero rate, with risks demanding a coupon rate that is not acceptable to the market.

There are, however, other modes of providing cover, in whole or in part, that have not been developed due to a lack of data and market acceptance (risk carriers). In the case of marine, such data is almost totally absent. This presents an opportunity for a certain product type to be developed. There is an general acceptance by experts in the field, as well as sector commentators that such products would serve to expand cyber cover, but the carriers remain at odds due to the shift in focus from Covid and its impact upon revenues.

Neither RMS or Praedicat have assessed this type of product and the new entity's data acquisition will facilitate the product development. With the sector controlled in a flatter regulatory and control structure than other industries, buy-in will be easier to attain globally than for other markets. Further, it is in the best interests of all parties operating within the maritime sector to accept and promote the proposed product development, due to the new risks posed by the IMO regulations, coupled with a new need for non-compliance reinsurance protection.

The term will develop the product concept at the outset, with reinsurer input, coupled with discussions with market makers e.g. Goldman Sachs, J.P Morgan for product underwriting and placement. The opportunity in this area for large-scale revenues over time should not be underestimated, but have not been exaggerated within the financial model.

The ILS market has been evolving and this is reflected in the tables provided within the Annexe.

Intellectual Property

Quantar developed its patents in parallel with the software in order to protect the invented solutions, commencing in 2002 with a PCT filing, extended to cover the E.U., U.S., Hong Kong and China for the back-end system (IP-TAP). These were further extended with applications covering the systems and methods employed within Network Operational Risk Manager (n-ORM) and Predictive Analytics Engine (PAE).

The applications filed in 2010-2011 for the front-end applications were only allowed in 2015, with substantial patent attorney costs being incurred during the intervening period. From 2013 onwards, a number of cyber risk modelling companies appeared on the market due to the launch of cyber-specific insurance policies by major risk carriers, allied to a number of high-profile cyber attacks. This refocused C-suite minds that cyber is an enterprise risk, with increasing financial liabilities.

In 2015, Quantar held discussions with one particular competitor in the U.S. that sought to acquire the patents and continuing applications of Quantar due to the recognition of their software infringing Quantar's patents. A failure to agree terms resulted in the company (a major U.S. military and UAE
©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

military supplier of network security products) failing to attain Series A funding for this spin-off entity, which then was closed.

This serves as an indication of the importance of holding patent protection within this sector, either for offensive or defensive purposes (typically, disputes result in mutually beneficial cross-licensing).

Key Points:

1. RMS 60% revenue in U.S.; exposed to patent infringement litigation from competitors & NPE's
2. Quantar: 135+ granted U.S. patent claims for cyber risk
3. Continuations facilitate ongoing protection for Quantar + RMS; Offensive or defensive purposes
4. Investment in Quantar proposal = low cost of access & ownership of early dated cyber IP

Example: Current Offer to Quantar for Litigation by U.S. Non-Practising Entity
Patent Litigation Defence Options
DEFENDANT OPTION 1: File an IPR (costs per patent assertion)

In-house legal review of patent assertions	\$200 -250 000
IPR filing costs	\$15 000
IPR legal costs	\$300 – 600 000
Totals Minimum	515 000
Number of patents 7	3,605,000.00

DEFENDANT OPTION 2: Wait and defend patent infringement claim in court

Defending assertion	\$1 – 4 000 000
---------------------	-----------------

DEFENDANT OPTION 3: Pay licensing fee

Licensing cost -all current & future patents	\$200 000
Quantar Income 1 st Tranche Infringers	
Corax + SSIC + Cyberpoint + Risklens + Cyence + Arx Nimbus + Evolver+ Cybercube, RMS, PCS.....etc	20 X \$200 000
Commission payment to legal entities	52%
Net Totals for 20 Licenses	\$1,920,000

Quantar has maintained patent protection of the two primary families through continuation applications. These serve two purposes; eliminating competitor's efforts to engineer around the granted patents; expanding the scope of protection and identifying areas in competitor's products infringing and filing targeted claims within continuations.

The patent system provides for subsequent patents within the same family benefitting from the priority date of the parent applications. Since Quantar's patents were filed in 2007 and 2009, any claim assertions against Quantar by competitors would be disqualified by the 2007/09 priority of Quantar's applications. Further, Quantar may assert against competitors, leveraging the priority dates, forcing either withdrawal of their products or licensing from Quantar for an agreed annual revenue or percentage.

A comparison of competitor's patent claims against Quantar's is included within the Annex, a listing of patent infringement contentions is also within the Annex. CAPEX YTD for generated IP is also disclosed. Patent ownership will form part of the value proposition to DMGT-V and also forms part of the program risk mitigation strategy.

The current market value of the patent portfolio has been established through benchmarking of values provided by IP market specialists from IAM Market and Richardson Oliver Insights, based upon the most recent figures available from 2019. At present, there are 7 granted patents and 2 continuation applications.

Upon the establishment of the new entity, DMGT and Quantar should immediately investigate the opportunities provided by the patent portfolio for licensing from infringing companies (approximately 29 at the current time). Forcing licensing or cross-licensing will provide additional program revenue, reducing overall program risks. Litigation may be required to facilitate this, however, Quantar has experience in establishing litigation capital funding as well as contingent fee litigation with top tier US patent firms; Fish & Richardson, Studebaker Brackett, Morrison & Foerster, Knobbe Martens.

In the current Covid-19 environment, major corporations are unwilling to acquire patent portfolios and prefer to license to reduce exposure. The licensing strategy should therefore to act with speed and keep licensing fees below the cost to counter claim validity via the Patent Trial and Appeal Board (PTAB) by filing multiple applications for inter partes review - see diagram above.

IP Costs

There is ample scope to develop a number of marine-specific patent applications over the first five years of the company's development. These will be filed under the patent convention treaty (PCT) to ensure protection is attained in all geographies where significant revenues are derived.

The costs of filing PCT's is significantly higher than for purely national filings, but the value increases in a non-linear manner and may also increase protection provided to RMS and Praedicat by attaining these. Costs are listed, in detail, in the Annex. Further, as with the current patent portfolio, once one set of claims for a given patent have been allowed, there is then the opportunity to file additional, continuation patents, based upon the same specification as the patent application.

In all cases, it is essential to pay the maintenance fees for the current patent portfolio and to maintain continuations to expand the scope of protection on an ongoing basis, as has been the policy to date. Additionally, since the products and methods utilised for the marine sector are the same as for the general cyber risk quantification and valuation segment, continuations may now be filed with an emphasis on marine risks, since the specification offers this opportunity through the drafting of the original specification. The repurposing of the current patent portfolio for marine will be the responsibility of the founder.

A provisional patent application has also been filed in the US with a marine-specific emphasis in both the drafting of the specification and in the claims as filed. By filing the provisional utility patent application, there is now a year in which to refine the claims and file the non-provisional application. The current filing gives a priority date to the subsequent non-provisional filing, thereby providing a form of limited protection from other entities filing to cover the marine sector in the short term.

Amortisation of Patent Portfolio

From a UK tax authority perspective, corporate intangible assets that have sums written off are usually deductible so long as their treatment is in accordance with GAAP. All receipts from the assets are

revenue items for corporation tax purposes. For the portfolio, the valuation is input as non-capital assets introduced at the commencement of the new entity and as such have not been written down and then re-valued upwards and thus there are no HMRC past tax deductions to be recovered.

Under HMRC guidance, in general, the tax rules for intangible assets follow the accounting treatment and if expenditure on qualifying assets is written off, normally by way of amortisation, the appropriate deduction for tax follows, in line with the accounts treatment.

For the new entity, there will be no revenues directly accruing from the patent portfolio, such as in the form of royalties, therefore from a capital and accounting perspective, the impact will only be in the form of the amortisation values input per year.

Since the current portfolio has 2010-11 initial filing dates, with a patent life of 20 years from the filing date, the useful life of the balance of the period will be via linear amortisation rates since these assets are not consumed at an accelerated rate. However, the salvage value or transfer value at the point of exit will impact upon the capital gain on the transfer of the intangible asset. Therefore external advice on the best form of amortisation of the portfolio is required before the end of the first trading period.

Patent Encumbrances

All patents are assigned to Quantar Solutions Limited, with no litigation having been instigated neither against an entity nor as a challenge to the validity of the portfolio. This is despite a competitor negotiating with the company to acquire the patents, as opposed to filing for inter-partes review at the US PTAB, thereby demonstrating the strength of the patents.

The patents have been submitted to a US defensive patent aggregation entity, as part of the intention to divest the portfolio to release capital for Quantar Solutions. There is a fixed exclusivity period between September 20th-30th 2020. The value attached to the portfolio is a heavily discounted one in order to take advantage a speed of sale and grant back by the NPE.

However, it is highly unlikely that the portfolio will be sold for the following reasons; 60% of corporate patent officers expect IP acquisition budgets to be slashed as a result of Covid-19 for the foreseeable future; the entity is a defensive aggregator of patents and has a trend of only acquiring patents that have already been used to instigate patent infringement proceedings against one of the members of the group, typically Microsoft, Google, Uber, Intel, IBM and Facebook. The rationale for submitting has been with the intent to raise fast capital if the portfolio is sold and in the absence of a sale, there are zero costs for submitting the portfolio.

Should the portfolio be unexpectedly sold, there is an automatic grant-back of the patent license to allow commercialisation by Quantar. Should DMGT wish to accept and execute this proposed program, it will be necessary to determine the best structure to allow the grant-back license to provide IP protection for RMS at the same time as enabling the new entity to develop. One option would be to create a sub-division within RMS, albeit a separate entity, with the license thereby being directed to RMS.

Discussions with other companies have been conducted under the standard Quantar Solutions NDA. To date, the current companies that Quantar is under an NDA are:

Oracle	Acacia Research Group	Dynamic IP Deals
SAS	Intellectual Ventures	Parallel North IP
GTT Corporation	Knightsbridge Cyber Security	Tangible IP
RPX Corporation	Cyberpoint International	

Product Specification Document

An initial product specification document will be developed and will evolve with the input from co-development partners to create marine/industrial control system specific systems and products, albeit based upon the existing software.

The use of the Dynamic Systems Development Method (DSDM) form of Agile program management will be used to fulfil the PSD as a matter of urgency in order to ensure the infrastructure and software architectures can be created for cost estimates and timelines within the initial operating period.

There will be a number of PSD's initiated at the outset; each with a different component to be delivered and each with a team member accountable for each, as well as having input into other PSD's. These will be signed off by the Board prior to execution of them.

Reporting will refer to the PSD's to ensure variations from the originals are agreed and signed off at each stage of the launch of the program, as per normal project management practice.

Program Risk

Basing the program around existing products and business models substantially reduces program risks. The potential exists to commence field trials with co-development partners from the onset i.e. the existing systems and software are fully functional commercial grade modules. These can be evaluated for additions and integration, with quick wins to get to market within a short period.

Due to the broad and long experience of managing the software and systems development, coupled with creating and prosecuting patents to allowance, program management risk is substantially lower than from unproven leadership.

Utilizing software developers in Estonia or Poland with fixed pricing further reduces program risk and eliminates fixed overheads. This model is used by a number of risk modelling competitors, including Guidewire/Cyence, with 80 developers contracted in Krakow and Cybercube with 60 developers contracted in Tallinn.

Financial exposure is mitigated to a certain extent through ownership of an expanding patent portfolio that may be used to acquire licensing fees from competitor cyber risk modelling companies. Alternatively, the portfolio may be viewed as an on-book intangible asset with a market value near or equivalent to the initial period of investment. Additionally, the patent portfolio may be viewed as a means of covering litigation risk posed to the RMS cyber modelling division from competing risk modelling entities that have patents that may be asserted against RMS.

Using the Dynamic Systems Development Method version of Agile project management (DSDM Agile), program risk management is contained within development stage envelopes, with a defined outcome per stage. Where it is clear that a stage will fail, development and investment may be curtailed more rapidly than using other forms of project management, such as Prince II.

Building the program in conjunction with partner organizations with Board representation may create governance and control risks. Contractual stipulations on control and voting rights will require mutually agreed terms and commitment prior to commencement of the program. An advantage of having Advisory Board Members alongside Board Members from each domain will alleviate and indeed strengthen the program direction through drawing upon resources and knowledge from large-scale program co-developers.

Organization

The organizational structure is akin to that utilised by Praedicat, in that the number of personnel is very limited, especially in the first period of establishment and growth. Praedicat has maintained a core top level management team formed of the original five team members; each delivering individual expertise for the company's product and sales expansion.

The proposed program does not require a large headcount due to the use of partnering and external developers for products. The focus of personnel will be in creating long-term relationships across sectors within the marine sector, later moving to include other sectors heavily reliant upon industrial control systems. A summary of the roles at start-up are listed below. Some will be fulfilled as combined roles until sales require additional dedicated headcount.



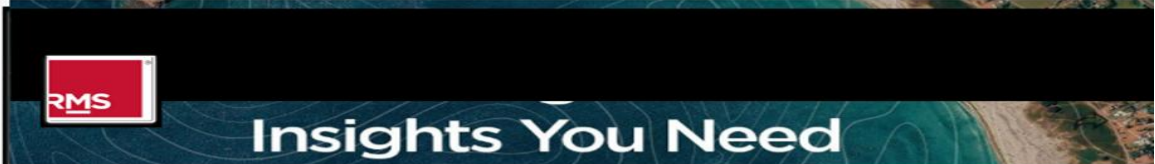

Key Points:

Small specialist team, as per Praedicat approach to development & growth.
Recruitment eased due to Covid-19 reducing London underwriting department headcount.
Below market salaries bolstered with stock-options for personnel commitment & lock-in.
Remote working core to cost limitations, but with frequent on-site team meetings.
No permanent office overhead; pay-as-you-go renting per day basis.

Further, limited physical space will be required for the team and may also be housed in office space under a sub-contract at the location of RMS if this is viewed as viable and desirable by DMGT-V. An out of London location would serve the purpose of the team, as well as reducing OPEX for the program. Only the Industry Engagement Office will be required to access the City insurance district on a regular basis due to the location of the marine P&I Clubs and the risk carrier sector.

The salaries anticipated to attract the relevant personnel have been based upon the rates offered by RMS in the London office, with some variation to take account of both the start-up position of the company and the share option scheme offered at the outset.

The attraction of joining a start-up in this particular case is founded upon the backing of a major corporate entity in the form of DMGT. As such, it poses some risk, but heavily mitigated by this, together with the offer of share options in a company with an investor that has both a long track record of building start-ups, as well as owning long-established modelling entities.

9/1/2020		(43) Director of Product Management - Exposure Analytics RMS	
 <input type="text" value="Search"/>			
			
Description		Seniority Level	
Director of Product Management, Exposure Analytics		Director	
Location: United States		Industry	
		Information Technology & Services	
 Estimated salary For Director of Product Management in Newark, CA, US at RMS			
Base salary		Total compensation	
\$174,000/yr Range: \$106K – \$285K		\$197,000/yr Range: \$118K – \$329K	

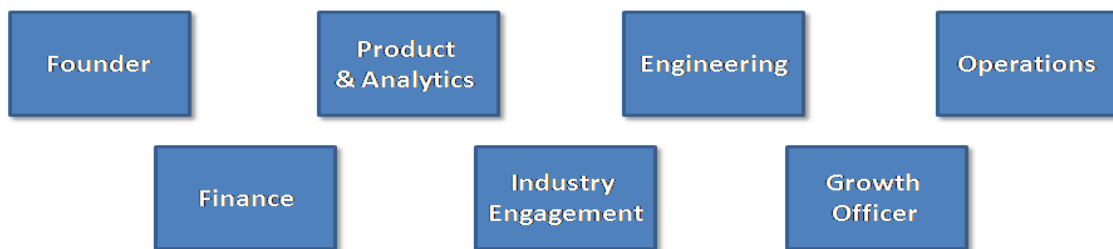
UK salary levels are substantially lower than in the U.S. at present due to the impact of Covid-19 on the supply of suitable qualified and experienced personnel within the risk modelling sector and in particular the cyber risk modelling segment. Q4 2019 salary levels for the Head of Cyber in London, was advertised at the level of £120 000, with the same position now around £90-100 000. At present, by way of comparison, RMS is seeking 27 new members of staff:

RMS Hiring Need September 2020

Software	12
Modelling	9
Sales & Marketing	6

This emphasises the churn rate of staff within entities that do not have a form of lock-down, such as share options, whereas Praedicat still has the same team as at the launch of the company in 2011. Salary sacrifice in lieu of share options therefore offers a greater level of attractiveness than in the previous trading periods.

Leadership Team



Board of Directors

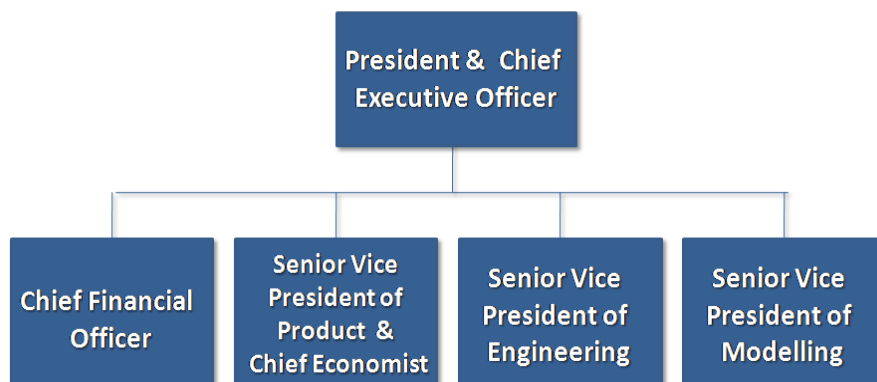


Advisory Board Members



Comparison with Praedicat Organizational Structure:

PRAEDICAT MANAGEMENT STRUCTURE



Onboarding Process

There will be a requirement for the initial team members to work intensely at the outset in order to create the relevant documentation, policies, procedures, development plans and product specification documentation. It is therefore envisaged that the team will work over the first month in a suitable location, where necessary with breaks for research reading and individual task completion. The first tasks will be led by the founder, followed by collaborative discussions, presentations and documentation proposals. This will include:

Pre-Week 1:

Background reading by each team member on the overall concept, SWAT analysis of the concept, their own specialist area, industry journals, regulations, competitor intelligence, trend analysis, future trends, financial and budget analysis for each team member activity for the first 3 years financial plan (own and other member's).

Week 1 On-Site Meeting:

Presentation by each member of the findings from the pre-meeting activities. Feedback and input to outline plans; updating of development, financial and budget plans. Proposals for amendments and/or additional activities required. Group training and establishment of accounts for the Atlassian project management web-based tools with use from week 2.

Agreement on next meeting deliverables. Location will be central London within Marine sector head offices: P&I Clubs, IMO, Lloyds Maritime, to create group understanding of the sector. Where possible, the DP World Port, the London Gateway will also be visited by the team, meeting with the port commercial manager; Mr. R. Moodie and his cyber security colleagues.

Week 2; Partial Off/On-Site:

Part week individual work off-site. Convening Thursday & Friday to review from week 1 plus work undertaken Monday-Wednesday week 2. Presentations of early part week's work by each member, receiving input from all team and updating work requirements for week 3. Specific focus upon 3rd party management, development of management tools, policies, templates, for software development, acceptance and delivery tests.

Week 3 Off-Site Working:

Individual work to complete all tasks. Completion of all requisite documentation, planning, budget, requirements, in detail for year 1; outline for year 2-3; sensitivity and risk analysis for all plan components of the program for the individual's core activities.

Week 4 On-Site Meeting:

Collaborative working; presenting to the team by each member. Detailed Month 2 plans agreed, with execution and deliverables for months 2-12 set and proposed to Board for sign-off. Controlled plan update after Board review and re-submission where required for sign-off.

Leadership Team

Founder

The more usual title of CEO is avoided since the company will operate a fairly flat structure, with each member fulfilling a crucial role. As such, the vision of having a founder who leads the overall company direction and product development remains, but without the stereotypical hierarchical structure.

This will assist in recruiting each core program member, since the perception is that they will have full accountability and responsibility for creation, development and execution of their individual program components.

Having both a Board and an Advisory Board will eliminate any perspective of a lack of overall ownership and control, with the Founder present at Board level.

The founder has the historical data and experience to draw upon, with the primary function being to ensure the program adheres to the agreed plan and manage issues as they arise. Strategic direction will be set at the outset, but with the knowledge that regulations, technologies and commercial considerations will change; potentially simultaneously, thereby requiring the Founder to have the capability to research and extrapolate data for ongoing changes to strategy. Regular briefing at Board level will therefore be an important component of the day to day tasks, to ensure changes are agreed unequivocally.

In addition, the founder will work closely with each member in defining tasks, scheduling and in the overall product definition. Negotiations with third parties will fall under the remit of the founder, collaborating with the finance member in this area.

Top 10 Tasks for Founder Phase 1

- 1.) Hire Industry Engagement Officer no later than 31 January 2021.
- 2.) Identify and contract with software developer for updating of current versions for installations and replications.
- 3.) Work month 1 with Industry Member to create initial target clients, sales approach and execution.
- 4.) Collaboratively work with Industry Member on sales calls and secure/contract first test clients.
- 5.) Evaluate and order hardware per confirmed installation; bench test and attain client sign-off to install.
- 6.) Install and test first set of hardware & software; train relevant client personnel, activate and evaluate.
- 7.) Acquire data from clients. Test and develop future platform based upon data type. Review data with external underwriter for feedback.
- 8.) Create appropriate patent licence for RMS and Praedicat and execute between the parties.
- 9.) Create and file non-provisional marine-specific utility patent from the provisional patent before the expiration of the priority date of September 2021.
- 10.) Commence recruitment process for three additional team members Q4 Phase 1 to commence in new entity January 2022

Product & Analytics

The products are software models that provide key information to a user viewing via a simple web browser. Existing software will be supplemented with 3 additional developments within the models and will require input from a risk modeller, such as an underwriter or actuary, to ensure the end results are fit for purpose within the marine risk management segment.

In-house model development will be undertaken, with only a final external validation being required, as per the current model developments to date. In the absence of the external validation by an accepted leader in the field, the industry engagement process will be more difficult.

The analytics member will lead all model developments and work in conjunction with the engineering member to ensure integration and deployment is executed in the correct and most efficient manner.

Since there will be ongoing model refinement, development and technology impacts, the role will be served by a mid-level model developer, preferably with experience within the marine sector, or in the absence of this, within the underwriting or actuarial markets. Clearly a need for comprehensive model and statistical expertise is required. As the company develops, the role will grow further, with a need to understand how large data (and potentially receiving data from Praedicat and RMS) can be leveraged going forward in modelling within other sectors such as utilities.

Within the London market, a large number of suitably experienced personnel exist and rotate across the various risk carrier and modelling sectors, as such this is not a position that will be difficult to fill, but may require heavy incentives to join a start-up enterprise.

Engineering

The engineering member fulfils the role of software development and infrastructure architect. This is a skilled position and determines how the company will be able to implement its systems and products on-site at client locations.

Due to global demand exceeding the supply to fill this position, it may be necessary to utilise sub-contracted personnel during the initial start-up phase. Although this is not the desired solution, a sub-contracted individual from RMS would remove some risk in recruitment as well as retaining costs in-house from a BDMGT-V perspective.

Since the systems and software will develop as client needs dictate, allied to technology changes, the role will also require up-to-date knowledge and skills e.g. marine use of 5G is anticipated by with 5G network deployment varying by nation, the overall impact is currently difficult to determine. Other commercial data transmission providers are also close to market launch, such as Amazon and SpaceX, with Oneweb also having strong data/navigation impact going forward.

An advantage for the company in developing its products is the increasing move away from proprietary technology, towards open standards, as evidenced by the Microsoft shift to open standards under the current CEO.

This removes a substantial product development risk in that the selected programming language will be suited to a write once run anywhere operating environment. As such, the degree of utilisation of a full-time engineering member will be limited and offer greater opportunity for contracting out. The role may be a contractor and combined with that of the product & analytics member in the initial period. The financial plans utilise a man-hour rate based upon contractor costs for the evaluation and planning.

Operations

The role of operations member will only be implemented when there is a need within the company, such as after attaining contracts from the first batch of customers. Only at this point will the management and control of multiple third parties at a larger scale, plus customer support provisions require this role being filled by an additional team member.

Since Quantar will be utilising a small team, supplemented by external parties and co-development partners, part of the definition of the role will not become clear until the type of initial clients and their requirements are also defined by contract.

Working with external companies, such as marine equipment suppliers, will assist determining the day-to-day activities aside from the general functioning of the company. The member will work in conjunction with the finance, industry engagement and growth officer to ensure feasibility of delivery and maintaining supply to clients and in supporting them in the use of the products.

A typical profile for this role would be any product based operations manager from a background that includes a quality management component. Prior experience in seeking and recruiting suitable personnel and managing their activities within an industrial setting makes the recruitment of a suitable person not viewed as a major task for Quantar.

Finance

The finance member will be required to fulfil 2 distinct functions; the first as the financial officer of the company, however, given the size of the organization and the financial activity, there is ample capacity to undertake a secondary role. This will require analysis of potential risk transfer models during development of the products and their potential use.

In particular, the finance member will understand and develop in-house models for securitization of the cyber risk exposures posed to individual entities and an aggregate risk for a particular group of entities. Whilst this may be viewed as requiring two skill sets the ability to undertake financial modelling is well suited to the secondary task and should be regarded as complementary.

The role will require taking input and direction from other members of the program, in particular from the Founder, Industry Engagement and Product and Analytics members in fulfilling the secondary role.

Industry Engagement

The role of industry engagement will be fulfilled by an experienced marine insurance sector professional. The mode of operation of the marine and London markets within the insurance sector results in small numbers of specialists who rotate between companies in very similar positions. The specificity of segment leaves little room for shifting across specialties. Marine has a number of separate lines within the space, with cargo, for example, being distinct in knowledge and skills from P&I Clubs.

This role is envisaged to be the most difficult to fill due to the constraints listed above. However, the rate of growth of the company represents an opportunity for a candidate that cannot be derived from remaining in their role aside from moving from one risk carrier to another.

The industry engagement member will contact and interact with the key stakeholders within the marine sector from vessel owners, P&I Clubs and each P&I Club membership, ports, and the risk carrier market. They will seek to engage their contacts to work with the company is developing individual solutions for each one.

Where there is an existing relationship that precludes immediate acquisition as a client, the objective will be to maintain dialogue until such time as an opportunity to tender opens. Further, due to the structure of the market, entry to one entity will inevitably lead to opportunities to engage with others and it is this facet that will play an important part in early go-to-market activities.

The industry engagement member will also work in conjunction with the founder, products and analytics and the finance member when holding discussions with risk carriers and the capital markets in developing potential reinsurance or securitization products.

In particular, the potential for different forms of risk transfer such as industry loss warranties (ILW) requires working in conjunction with the risk carriers directly, whereas securitization via insurance linked securities (ILS) requires working with investment banks, a book runner and a deal structuring agent (this may be the same entity such as a capital markets division of a brokerage such as AON Benfield).

The company will take its lead in this area from the Board and in particular from the knowledge gained by DMGT-V through RMS ILS securitization of Achmea's Windmill CAT bond working in conjunction with Willis Re for placement. This represents a quick win for the company in its development, given the same key contacts within the ILS/ILW sector will be receptive to working collaboratively with Quantar. A proof of concept can be developed for the P&I Clubs far quicker than a competitor in this instance, with low risk for any party in commencing discussions and formulating a framework for co-developments.

Although an ILS/ILW product development ambition may appear beyond the scope of a program focussed upon cyber risk management, the scale of the marine risk market is such that there is currently a growing recognition of the opportunity to move P&I Clubs towards securitization and away from risk pooling and captives for risk transfer. The value proposition to P&I Clubs and their members is consequently a very significant reduction in cost structures of their existing risk transfer vehicles and an area as yet unexploited by the ILS/ILW markets.

Growth Officer

This role will only be created and filled at the appropriate time, with an initial start point in year 3. During the initial phase of creating and launching market-ready products to the first clients, there will not be a requirement to grow the company's capabilities. Once the company has attained its go-to-market goal, the risk associated with executing a growth strategy into secondary markets will be reduced sufficiently to commence the activity.

The role of the growth officer is to instigate and expand on existing contacts from the industry engagement member and in creating alliances within the target segments. These will include ports, marine equipment and secondary market targets as the company develops its capabilities. The secondary markets will be those utilising the same types of industrial control systems and programmable logic controllers as within the marine sector since they contain the same vulnerabilities.

The initial effort will be in engaging with companies within the marine equipment sector in order to co-develop cyber risk systems that are matched to their marine product portfolio. The key contacts within this sector act as gatekeepers to other sectors, especially to ports and ship owning entities due to the reliance upon the marine equipment sector by these actors.

An example of the type of target the growth officer would target would be ASEA Brown Boveri (ABB Group). This particular enterprise operates in all the target markets of Quantar, both initially and into future periods. They service the marine & ports, power, industrial automation & production, oil & gas, railway and other heavy industries that Quantar could serve. Similar entities and competitors include Siemens, Schneider Electric, Emerson, GE, Danfoss, Eaton, Honeywell, Rockwell, Yokogawa, Lear, Rolls Royce.

The total number of companies operating in this product/service sector that have in excess of \$2 billion annual revenues exceeds 50 and represents broad scope for engagement by the growth officer. The member will collaboratively work with the other members since each will be impacted by any collaboration attained by the growth officer, in terms of the products developed and in the financial and operating environment of the company.

Remuneration & Share Ownership

The objective of the program is to build the systems and software rapidly, with a fast go-to-market strategy all at the lowest initial operating cost as a means of reducing execution risk and program failure. With this in mind, members of the team will be recruited at a lower than average market salary cost, with the incentive of joining and continuing in each role coming in the form of share options to benefit the holder upon exit or within a defined period for vesting, rather than in the expectation of dividend income, although this will form part of the remuneration.

The conversion of the options will be subject to a number of conditions. The forward vesting period will be set at 5 years, with the strike price agreed with the HMRC at the outset under an Enterprise Management Incentive (EMI) scheme in order to reduce the future tax liability for the company and employee. There will be a 24 month cliff whereby a leaver, within this period, has zero vesting options. A quick exit for DMGT in years 3 or 4 will require a certain degree of certainty and continuity of personnel for an acquirer, requiring a short-term perceived lock-in period.

For the Founder, there will be a share allocation at the outset to reflect the transfer of the patent portfolio plus the software code that will be used to develop the final marine products. There will also be a Founders vesting period, but with a cliff after 12 months, resulting in a higher percentage being vested than in the subsequent 24 months, where there will be a linear vesting basis. The maximum percentage shareholding will be capped at 4% of authorised share capital.

There will also be a small number of shares issued to the external adviser, also with an agreed vesting period, during which time the adviser must attain specific introduction targets for the company. Failure to achieve them will result on the loss of external investor ordinary shares or with an extension of the vesting period.

Anti-dilution methods will be agreed and used to maintain DMGT-V and other external investor's share holdings, using share classes where it is felt appropriate and agreed by all by the investors and founder. Quantar currently has A & B class shares with reverse ownership and voting rights for each class, formulated for a future exit strategy. The potential use of Advisory shares being issued to the Founder and DMGT will be considered within the overall anti-dilution strategy.

The cost of establishing a share option scheme for between 5-10 members in the UK currently falls between £1500 – 3000.

Board of Directors

Chairman

The role will be fulfilled by a member of DMGT-V or their assigns, to oversee the correct functioning of the Board. The voting structure will be part of the development of the investment structure and will impact upon the weight given to Board members. Since there is no intention to divest the company at the outset (rather to establish a long-term entity), the voting rights in view of no substantive dilution,

will be relevant primarily to ongoing development and budgeting for the continued growth of the company.

Founder:

The role of the Founder in the context of Board membership will be to brief the Board at the agreed intervals and take the resulting input from the board members forward in the development of the company.

A board sponsor for the project will be appointed by mutual consent. The sponsor will work closer with the Founder than other members, to ensure delivery of expectations of other members and to feed back to them where any issues arise.

Investor:

A Board representative of the investors will be appointed with the mutual agreement of the overall investor group. Their role will be to ensure that their capital is secure and any rises posed to the return on said capital is addressed in accordance with the stipulations within the program plan. Fundamental deviations from plan will require agreement of the investor representative. Definitions will be defined within the investor contract documentation.

Reinsurance:

The board member from the reinsurance sector will play the role of providing input to the overall board as to the state of the market in marine and any issues that may be foreseen by a risk carrier in the market as early as possible in the program. Additionally, they will review the overall program, business model and concepts and provide feedback from the perspective of the reinsurance market.

This role is important, given that reinsurance is a cyclical business and the hardening or softening of premiums within the market are directly correlated to risk events. The cycle will therefore be a determinant of the profitability of the company, given the model of revenues based upon a percentage of written premiums.

Further, the intention of the company in its development is to work closely with the reinsurance and capital markets to co-develop risk transfer products that would suit to needs of the marine sector. These include securitization of consolidated group risk (e.g. ILS) in place or allied to the existing captive usage; insurance loss warranties that can be created with sufficient volume of parties covered, or other capital markets products.

Having expertise in these areas and oversight of product viability in development will be key to ensuring expenditure is focussed on the correct areas over a sustained timeline and operation of the company.

Marine Equipment:

A vessels' technical equipment facilitate its fundamental operation and as such, the trends within the marine equipment segment are a vital area of continual assessment for the company. Where, for example, industrial control systems develop fundamentally away from their present status, Change will impact upon cyber resilience and risk and input from this sector is therefore invaluable.

Further, as co-developers of the systems and software, it is in the interests of the marine equipment representative to ensure that there is appropriate ongoing development of the systems and models to take account of trends. The rate of change however, is not expected to be rapid, due to the market

conditions and the limits on capital expenditure on retrofitting vessels. A move towards increased automation will actually increase the need for more robust cyber risk assessment systems and risk models.

Advisory Board Members

There will be a panel of advisory Board members whose role will be in oversight of the program, ensuring Board representatives views are taken fully into account and not subverted, as well as providing input from the perspective of their individual specialisations.

Within this panel will be representatives from the P&I Clubs and the ports sectors. This is due to the symbiotic relationship between vessels and these entities. Their views should inform at Board level and thence to the company officers. Additionally, such representative members shall provide direct access to the wider P&I Club and ports sector bodies and persons of influence. The composition shall be:

- Group Investor
- IMO
- Group Equipment
- P&I Clubs
- Ports

External Adviser

The company will also employ on a per day contract basis a world-renowned strategy and technology leader in the form of Professor Soumitra Dutta; current co-chair of the World Economic Forum, founder of the Samuel Curtis Johnson school of Business at Cornell University and current Professor.

As a global consultant to major corporations around the world, to governments in defining technology policy, the company will use the standing of S. Dutta to attain immediate credibility with the IMO, P&I Clubs and risk carriers through his liaising with target clients. There will be no permanent tie and use will be on a per instance requirement.

Additionally, S Dutta will be able to contribute to the development of the company and providing ongoing input based upon his global contacts. Within the WEF, there may also be opportunities for the company to leverage introductions to heads of corporations present at WEF events through each year. This will be particularly important in establishing the company in the U.S. and Asian markets given S Dutta has been a prominent academic and business consultant in those geographies, with contacts at the very highest levels.

The appointment should be viewed in much the same vein as Cudoni with Lord Mervyn Davies as a shareholder, or GP Nutrition with Sir Charles Dunstone, Nick Jenkins and Sir Keith Mills as shareholders and advisers.

Recruitment

The company will utilise online advertising and recruitment firms to recruit suitable team members, coupled with networking contacts. This will limit the cost per member acquisition overhead. Taking the following online recruitment and re/insurance specialist websites, the costs comprise an average of £3500 per member recruited within the business plan:

Recruitment Websites:

- Indeed
- Glassdoor
- LinkedIn
- Dice

Payment Model:

Per click
Monthly fee
Per day budget limit
Monthly fee

Re/Insurance Industry Websites:

- Artemis
- Insurance News Daily
- Insurance Business
- Insurance Insider
- Captive.com
- Insurancejobs

Monthly Advertising Cost:

£500
£500+ placement dependent
£500 (uses Indeed within Jobs Section)
£1000+
Free + Sponsorship Opportunities
£450+

Due to Covid-19, there are a larger number of available re/insurance personnel available in the London market than is the norm. The opposite is true of technical, data and networking professionals, with this being reflected in the remuneration for the 2021 period. However, skilled reinsurance professionals still maintain a higher than average salary due to the specialist knowledge and network contacts they possess and this is reflected in the uplift in remuneration from year 2 as a means of retention.

Competitors

Competitors may be categorised into two groups; the incumbents and potential entrants as the impact of Covid-19 reduces the market opportunity for cyber risk modelling within the traditional cyber insurance sector.

Maritime Data Providers

Lloyds Register:

Historically, marine data was provided by the Lloyds Register, which categorised ship hulls by grade and later expanded into other areas relating to maritime safety, providing a body for maritime quality assurance. This is attained through the Lloyds Register Rules, which include:

- Materials used for construction of the vessel
- Ship structural requirements and minimum scantlings, depending on ship type;
- Operation and maintenance of main and auxiliary machinery;
- Operation and maintenance of emergency and control systems.

These categories have expanded and now include (see Annex for example rules):

- Lloyds Register Guidance Note Cyber Enabled Ships (February 2016);
- Procedure for the Assessment of Cyber Security for Ships and Ships Systems (September 2019);
- Cyber Enabled Ships ShipRight Procedure - Autonomous Ships (July 2016)

Whilst the Lloyds Rules govern safety and operational standards for numerous merchant, military, and privately owned vessels, they do not provide marine data. The data available is limited to the entities seeking accreditation, certification and classification via the Lloyd's Register Group Limited (a subsidiary of the Lloyds Register Foundation).

IHS Markit

A joint venture with IHS Markit was established to provide marine-specific data in the form of the totally marine focussed magazine Fairplay. This entity expanded over a number of years and owners, to include data and data management and becoming a digital offering and acquired by IHS Markit in its entirety in 2009.

Since 2009, IHS Markit has expanded its digital offerings to the marine and other sectors, with data relating to:

Vessel, tracking;
Ship and Port Data;
Risk and Compliance;
Maritime Shipping Intelligence;
the IMO vessel numbering scheme;
Engineering intelligence;
Trade data;
Commodity Tracking and forecasting;
Workflow automation data.

However, despite the range of data available to subscribers, there is no current cyber risk management offering, nor cyber-related threat data to add to the existing threat data relating to ports, threats posed by other ships, routes, etc.

Maritime Industry Bodies

There are maritime industry bodies that issue guidelines to the sector, but these are not mandatory, only best practice. However, ship owners, ports and associated segment players belong to such bodies due to their representation at the international and national regulatory body level.

One such body, the International Chamber of Shipping states within its objectives that it seeks to:

- Promote the interests of shipowners and operators in all matters of shipping policy and ship operations.
- Encourage high standards of operation and the provision of high quality and efficient shipping services.
- Strive for a regulatory environment which supports safe shipping operations, protection of the environment and adherence to internationally adopted standards and procedures.
- Promote properly considered international regulation of shipping and oppose unilateral and regional action by governments.

One of its publications, "Guidelines on Cyber Security Onboard Ships" gives a detailed explanation of what shipowners should do to secure their vessels from cyber attack.

Crucially for the present business proposal, this set of guidelines at Page 48 states:

" It is recommended to place a sensor on the internet-facing segment, because the public servers are a visible target to attackers. Another sensor should be placed behind the firewall, to monitor traffic between the internet and the internal network. An IDS/IPS sensor could also be placed by a remote access segment, for instance a Virtual Private Network (VPN)" (see Annex).

This sensor placement is exactly the location required to capture, analyse and assess cyber threats by the backend system that is then used by the front-end applications. By referring to this set of best practice guidelines, the value proposition for regulatory compliance and adoption of best practice of the leading industry body is greatly increased.

The Industry Engagement member has therefore a number of references to establish credibility of the sales proposal made to shipowners and ports.

Key Points

1. There is no marine -specific cyber data or risk management product available within the sector;
2. IHS Markit is a good fit for a divestment in year 3-4 or a high potential threat to the RMS marine product offering;
3. Industry bodies stipulate sensor placement within the demilitarised zone (DMZ) - this is the requisite for Quantar data acquisition and therefore removes potential objections i.e. NewCo helps them comply with Industry Body guidelines.

There may also be opportunities to collaborate with the marine sector bodies in developing future guidelines, as with private companies such as SOFTImpact, Improsec and Aspida Group, that have contributed to Chamber of Shipping cyber security guideline development that match their security assessment and compliance services i.e. piggybacking their company services on the recommendations they themselves have stipulated as being best practice and delivered by an authoritative marine body.g

Maritime-Specific Incumbents

The main focus of the incumbent competitors is on the supply of encrypted email. This is due to the limited bandwidth available on the majority of commercial vessels used for goods transportation (as opposed to cruise liners, where the customer expects high bandwidth availability).

The "traditional" attack techniques used by attackers, are the main focus of secure email for the maritime sector.

Top eMail Attack Types

Trojans
Phishing
Spear Phishing
Spyware
Scareware
Malware
Viruses
Pharming

Top Secure Maritime eMail Providers

1. Duolog
2. CompassAir
3. GT Maritime
4. Nordic IT
5. Netpas

As the IMO regulations have been communicated and the deadline for compliance has approached, a number of new entrants or incumbents expanding their service offerings have emerged. The types of services typically offered are listed below. However, these are, in the main, based upon standards developed by national institutions and organisations such as the U.K.'s Cyber Essentials Plus; NIST, ISO27001 (information security), ISO31000 (risk management).

The approach is very much paper based evaluations against standards for gap analysis in order to address missing security within the vessel's operations. There is no use of network traffic per vessel to analyse and predict outages and process downtime.

Further, the services rely upon the vessel' personnel for security integrity and maintenance, despite the lack of skills and abilities being renowned within the sector. Operating cost pressures require head count to be as low as possible, with low skilled personnel from low income countries being heavily utilised within the industry. As such, training and awareness programs may be viewed more from a regulatory compliance perspective than actual risk management.

Typical Service Provision by Cyber Security Maritime Providers

- Enterprise Cybersecurity Assessments
- Cyber Risk Awareness Training
- Confidential Executive Briefings
- Vulnerability Assessments
- Cyber Risk Communications (crisis communications; incident response planning; execution)
- Tailored Cyber Crisis Incident Response Training table-top exercises)
- Cyber Risk Management Planning and Development
- Cyber Risk Business Continuity & Disaster Planning
- Cyber Security Technology Selection, Procurement & Solution Implementation
- Cyber Incident Response
- Cyber Security Operations Centre Support
- Cyber Threat Intelligence Support
- Virtual CISO Services
- Capacity Building (Organizational and National)
- Technical Solution Evaluation and System Design Support
- Enterprise / Advisory Program Management Office (PMO) Support

Some P&I Clubs have commenced partnerships with cyber security companies that have launched as marine-specific entities, with a training/audit solutions base. These include :

P&I Club	Cyber Security Company	Base Offering
West of England P&I Club	Astaara (UK)	Cyber Essentials Plus
North of England P&I Club	Hudson Cyber (USA)	Proprietary Check Box Audit

Another sector seeking to enter the cyber security segment within marine is the traditional maritime equipment industry. With companies having historically designed and built vessels latterly involved with the design and specification of advanced technologies within ships, these companies are also seeking to add cyber as a complementary service.

Part of the rationale is derived from the increasingly onerous fuel burning limitations mandated by the IMO, which requires, in many cases, retrofitting of alternative means of using lower sulphur propulsion systems. By adding newer technologies simultaneously with the retrofit, such entities are able to differentiate themselves from competitors. Examples here include ABB, Rolls Royce, Mann.

Other specialist military ship builders such as Qinetiq have also expanded their complementary services to include cyber. However, as with the previous sector, the cyber security service comprises of consultancy, gap analysis, training and ISO/NIST benchmark analysis, rather than a system and analytical modelling.

One sector that could, but as at present has not, entered the cyber security segment is the marine software sector. There are a number of players within the space, with differing products serving to resolve a number of different marine-specific needs. These include:

Supplier	Software Solution
QSP	Hydrographic data collection to piloting
Netpas	Maritime Mail Analyzer
Trigonal	Post Fixture Management e.g. Voyage and Fixture Management
Danaous Maritime Software	Multiple products e.g. crewing systems, cargo operations
Nordic Maritime Solutions	Web-based quality, safety, risk platform
LGMAR	Maritime messaging solutions software
Bass	Fleet management software, inventory app, risk management
Shipnet	Maritime ERP

Of the entire number of providers, only a small number have the breadth of offering that makes them potential competitors. The majority have highly focussed and specialised products that have no natural fit to a combination with cyber threats. Bass, Danaous and Shipnet are the three companies that may offer distribution potential or some form of joint venture. However, it is not the intention at this stage to enter into dialogue with these downstream providers.

Potential Market Entrants

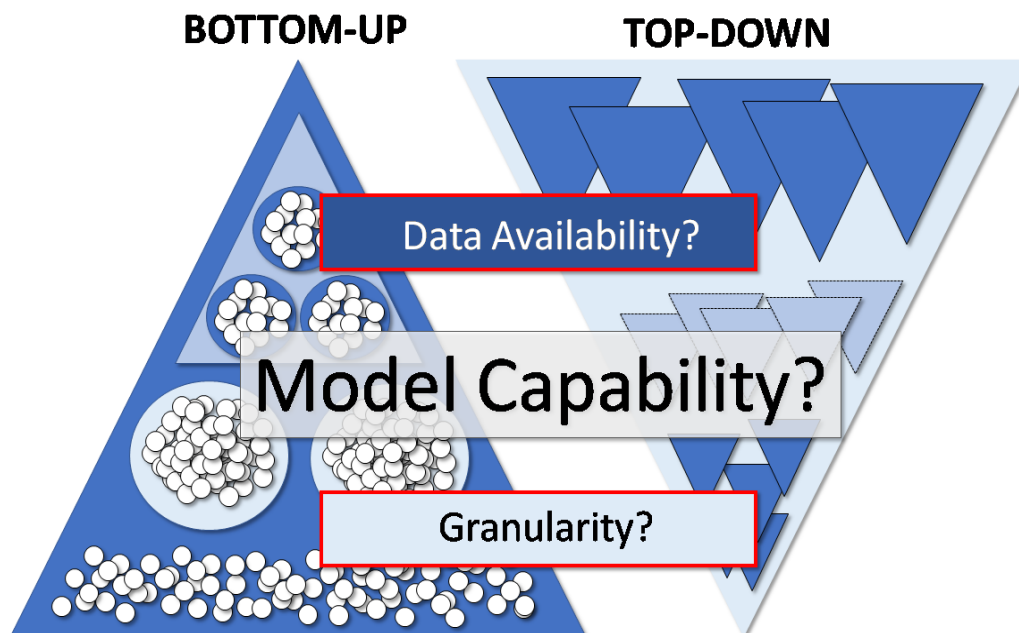
There are a small number of cyber risk modelling companies that could enter the marine market, including RMS with its current cyber models. However, the models used by competitors are not applicable to the marine sector and in particular fail to meet the compliance requirements that shipping companies are seeking urgently for the January 2021 deadline.

This is due to the target of these competitors who entered the market from 2014 and from 2016 in earnest. Their foundation and business models are based upon the need by risk carriers to understand their portfolio risks through offering cyber insurance in a market demanding high levels of cover. This requires an understanding of the aggregation risk and thus matching similar companies with profiles based upon the erroneous belief that IT infrastructure, processes, IT security personnel can be grouped into profiles that have the same exposure.

Key Points:

- Marine sector incumbents are focussed upon secure email and communications.
- Existing cyber modelling firms do not have the appropriate technology and/or models for marine.
- Cyber modelling firms are pivoting due to Covid, towards NatCat and Environmental change.
- Corax Cyber liquidation releases patents for assertions against NatCat modellers e.g. RMS/Praedicat.
- Other potential entrants include marine shipping equipment companies; ABB, Qinetiq.

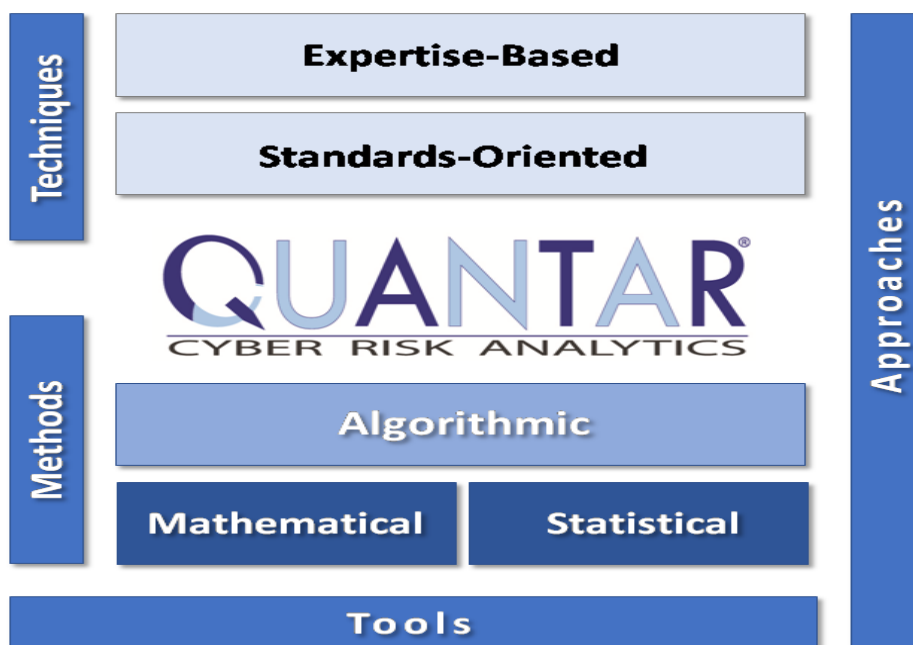
This does not function as a model for IT security for a number of reasons; the primary one being on the lack of actual similarity between the entities (Quantar has a history of high security skills, serving SWIFT, NATO, Eurocontrol, Belgian Government ID Scheme, retail banks). The difference in model approach can be seen below:



All competitors, without exception, use a top-down approach, based upon the needs of risk carriers to have a single risk exposure figure for a given product line delivered by the models.

By contrast, Quantar commenced its development in 2000 based upon the need for banks globally to quantify their operational risks, including IT and cross-border electronic transactions, in order to quantify for the Advanced Measurement Approach (AMA) to risk capital reserves under Basel II.

This requires a fundamentally different approach, with a bottom-up method taking the proprietary data of each entity and extrapolating into future periods. combining this with proprietary data inputs from the client to attain a valid series of figures.



It was only in later years of development that cyber insurance grew to the point where new entrants, backed by Silicon Valley VC capital, commenced operations. These have included:

©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

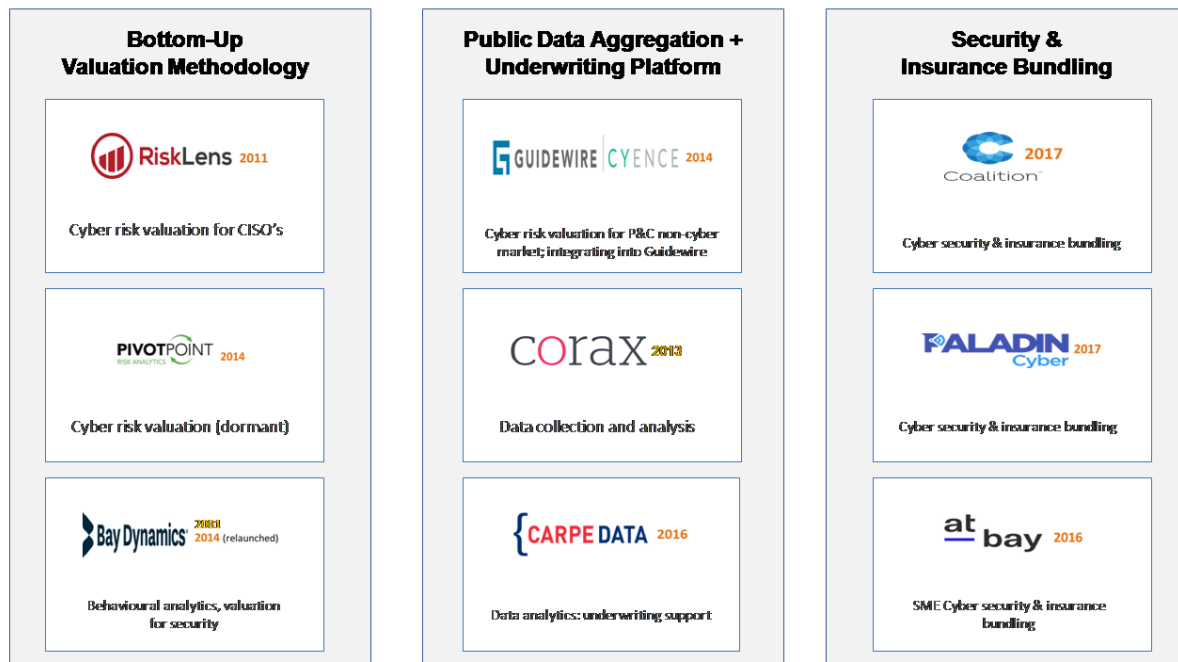
Cyence
Risk Lens
Corax Cyber
Cybercube
Paladin Cyber
Bay Dynamics
Cyberwrite

PivotPoint Risk
Analytics
Carpe Data
atBay
Secure Systems
Innovation Corp
Arx Nimbus

Risksense
Nehemia Security
Vivo Security
Neo Prime
Cytegit
Axio
Cura

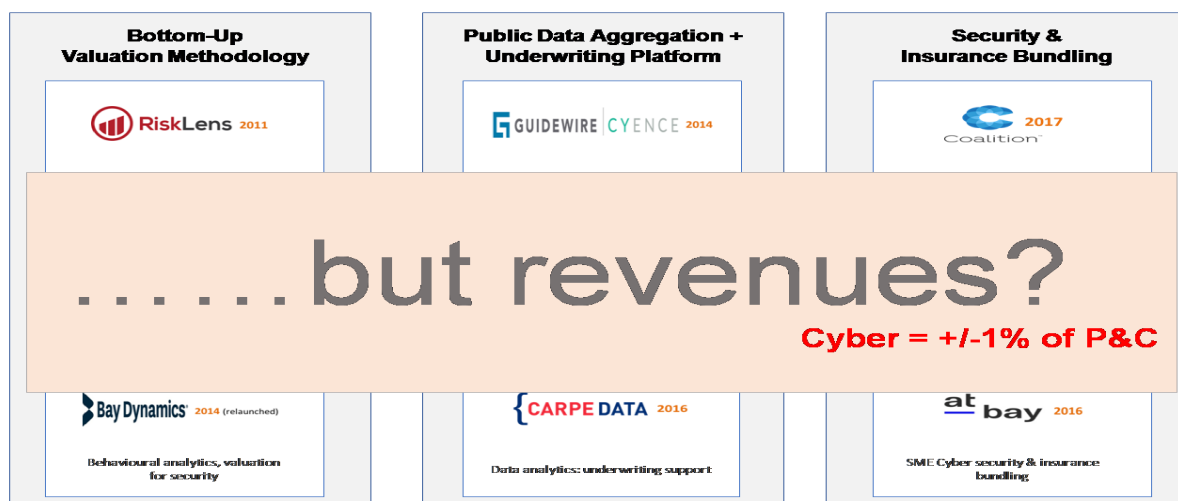
Avaluation
Alyne
Balbix
Continuity Logic
Emergynt
Pericertum
Six Thirty Cyber

Competitor Model Approach



In addition to these, major players such as IBM, SAP, Oracle, Verisk, AON Benfield, WTW, RMS, Unisys, Dell/RSA Archer, L3 entered the market, often in conjunction with a start-up to limit early exposure.

Of note is that despite this high level of activity and numerous publicity announcements, none has derived net profit from their cyber risk modelling operations. A prime example of this is Corax Cyber and its entry into administration and onward sale as a pre-packaged entity in 2020.



The failure of Corax is, in the opinion of the sector commentators, only the first of a number that will either fail, pivot or be acquired. Cybercube, as an example, have been seeking to acquire the client base of Corax Cyber. Cybercube is now seeking to acquire the two patents from the sale of Corax to Wells Market Square Management LLC in Texas, US.

The strategy of Cybercube, unlike other modelling companies, is that of taking a "last man standing" approach to the cyber threat modelling market. Cybercube has significant venture capital funding from Forgepoint Capital and has reduced expenditures as well as having already pivoted to the broker market.

Further, if Cybercube is successful, they have an expressed intent to utilise the patents to litigate against catastrophe modelling companies, given their recent shift into this more traditional market. This may include patent assertions against both RMS and Praedicat.

Quantar entered into discussions with US security company Cyberpoint International with a view to a sale of the patent portfolio due to this posing an obstacle to securing Series A funding. A lack of agreement curtailed negotiations and Cyberpoint failed to secure the necessary funding for expansion of its cyber modelling spin-off, PivotPoint Risk Analytics and still has only one client, paying a mere \$250USD per month.

Marine Equipment Competitors

The major marine equipment manufacturers have recognised the market opportunity afforded by the forthcoming IMO regulations relating to cyber threat management. However, despite this, there is little investment in developing service/product capabilities beyond basic services.

Covid-19 heavily impacted capital-intensive industries, including vessel building companies with shipping companies seeking to recover turnover, then margins, before contemplating renewing or refitting their fleets.

Top 11 Global Shipbuilding Companies:

Sumitomo Heavy Industries Fincantieri SpA Samsung Heavy Industries	Daewoo Shipbuilding & Marine Hyundai Heavy Industries CSSC United Shipbuilding Corp	STX Offshore & Shipbuilding Sembcorp Marine Ltd Mitsubishi Heavy Industries Tsuneishi Shipbuilding
--	--	---

Similarly, the marine equipment sector is constrained at present by the same lack of investment by ship owners. Additionally, the forced refit for IMO fuel sulphur emission reductions has added to the issue of capital allocation prioritization.

For the proposed program, this offers a distinct opportunity to leverage the relationships that the two segment incumbents have with ports, ship owners and regulators, to establish a form of collaborative development. Attaining the backing of one global player through the offer of comparative advantage to the party, will provide instant credibility of the new entity within the marine sector, aiding expansion of contacts and relationships.

SUMMARY

There are very few opportunities for market entry on a global scale, where the operators within that market have a legal obligation to undertake specified activities outside of the core skills required to operate. The IMO regulations, in effect from January 2021 is one such opportunity.

©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

Covid-19 has reduced the number of potential new entrants from the risk modelling, maritime and equipment sectors in the short term, thereby offering a short-term, quick win scenario to an entity able to react with sufficient skills, knowledge and existing products.

As with cyber insurance, demand exceeds supply within the marine sector; as with GDPR, the IMO law places responsibility to prove compliance upon the operator; guilt until auditable proof demonstrates otherwise. Failure to comply will result in ship detention or banning of entry, costing very significant financial losses for shipping companies.

Basel II and Solvency II were the last regulations with global impact upon individual sectors. The outcome was concerted and ongoing investment from those sectors, which continues today. Marine operators, be they vessel owners, ports, inland marine (warehousing and transport) will all similarly invest to comply.

Margin pressures in the industry are renowned, requiring low cost solutions for operators whilst regulatory breach cover in the form of reinsurance through risk pooling and alternative risk transfer methods provides additional revenue streams from the P&I Clubs.

Marine is a global sector, with a sufficient total addressable market to sustain a specialist entity providing compliance, audit, cyber threat management, data and modelling to shippers, reinsurers, ports, equipment companies over an indefinite period.

Efficiency (cost) of pooled risk and reinsurance defines comparative advantage between P&I Clubs, each seeking volume tonnage to increase funds under management. The current lower layer of reinsurance is insufficient to cover legal liability risk, offering opportunities for arbitrage between the clubs and risk financing entities.

Existing products and models, protected by multiple patents, created specifically to fulfil the needs of quantification, compliance, cyber threat management and underwriting already exist. Rapid redeployment, utilising third parties for speed and cost limitation, presents a unique situation of low risk, high and long-term reward.

Potential synergies between existing entities is provided, with at the least, delivering protection to RMS and Praedicat via intra-firm licensing; eliminating potential IP infringement litigation from increasingly assertive competitors and non-practising entities in a period of limited sales opportunity.

Quantar Solutions will enter the marine market. There are 4 companies; 3 located in London and all 4 with London-based marine operations that may partner with Quantar. DMGT is the prime target for Quantar to create a new entity for this market, due to prior conversations with RMS in relation to potentially joining that company as head of cyber and optionally for joint ventures in cyber. DMGT is therefore logically offered this opportunity first, before being offered to the three other companies with similar profiles in the absence of interest.

ANNEXES

INSURANCE LINKED SECURITIES MARKET (ILS)

RMS lags AIR in issuance, however ILS is not a core focus for the company. AIT, by contrast, has focussed increasingly on this securitised risk market for a considerable period. PCS is increasingly doing so for the core P&C market as well s via their Verisk sub-brand.

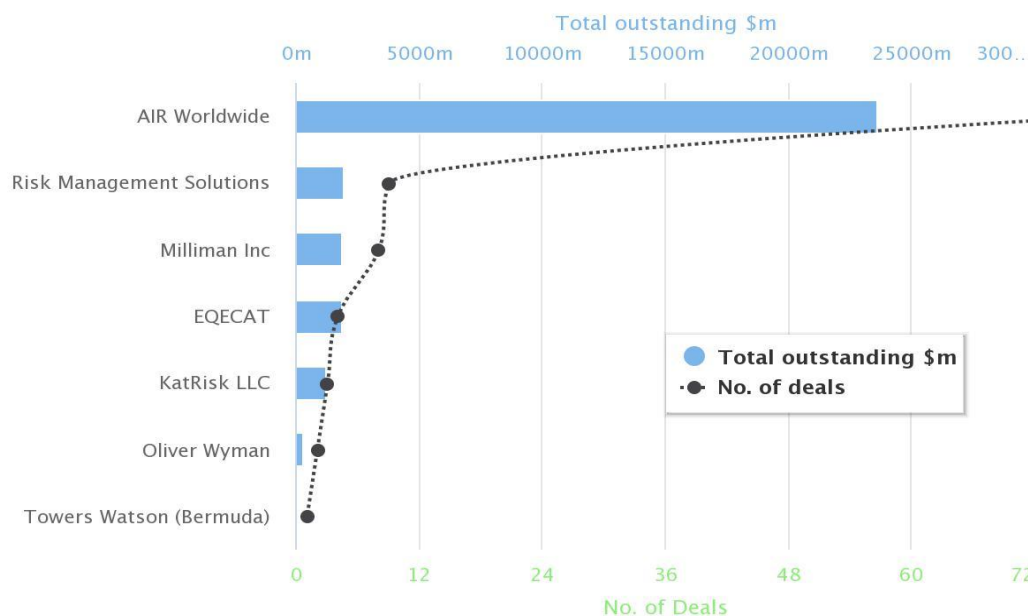
Smaller players are also beginning to launch a greater number of niche products, such as Achmea's Windmill II Re DAC at €100, placed by Willis Re that will provide Achmea with a source of European windstorm reinsurance protection, on an indemnity trigger and per-occurrence basis across a four-year term.

This follows on from their Windmill 1 cover at \$46 million in 2017, which successfully matured and gave investors a positive result and providing for the second bond issue.

The significance of this particular ILS bond was that it was the first Euro peril cat bond to hit the market for a long period and was a good test case for investor appetite for a diversifying region (the US has a glut of U.S. peril deals).

The Windmill II Re DAC cat bond occupies a layer of Achmea's reinsurance tower attaching at EUR 365m and exhausting at EUR 615m (EUR 250m layer).

With little room at present for investors tom operate within, with central bank rates at record lows, investors are more receptive to alternative vehicles, leading the way for the proposed marine sector product development within a short period of time.

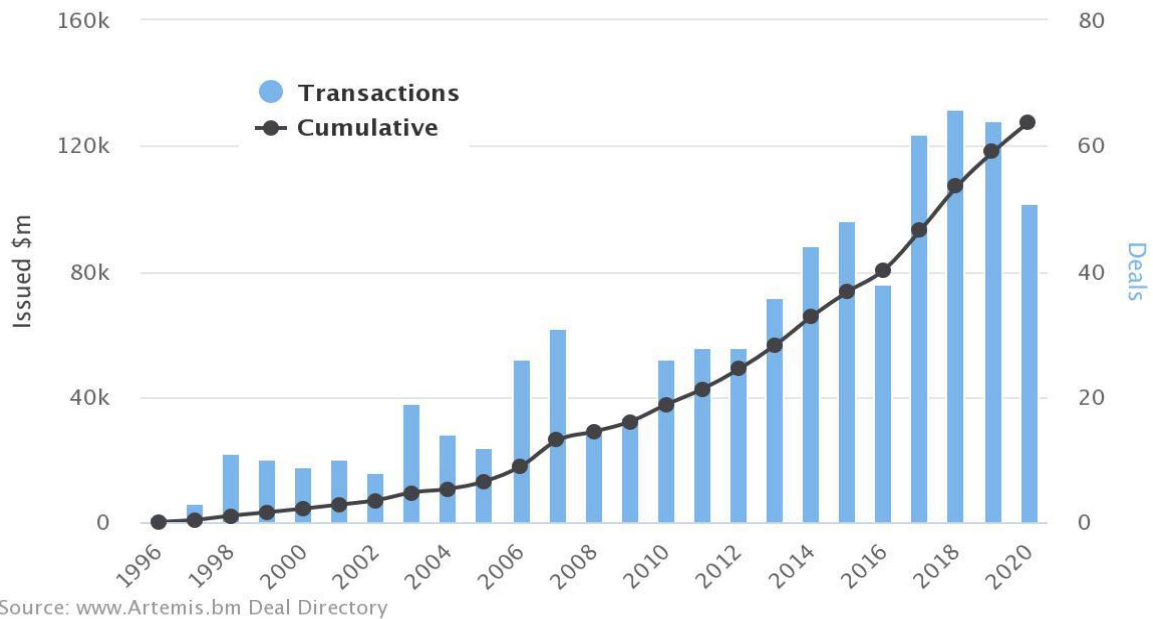


Source: www.Artemis.bm Deal Directory

The period 2018-20 has seen a rise in the number of ILS transactions; primarily in the NatCat wind and known perils segments. There has been no growth in cyber ILS market, despite this being launched by Credit Suisse over a decade ago.

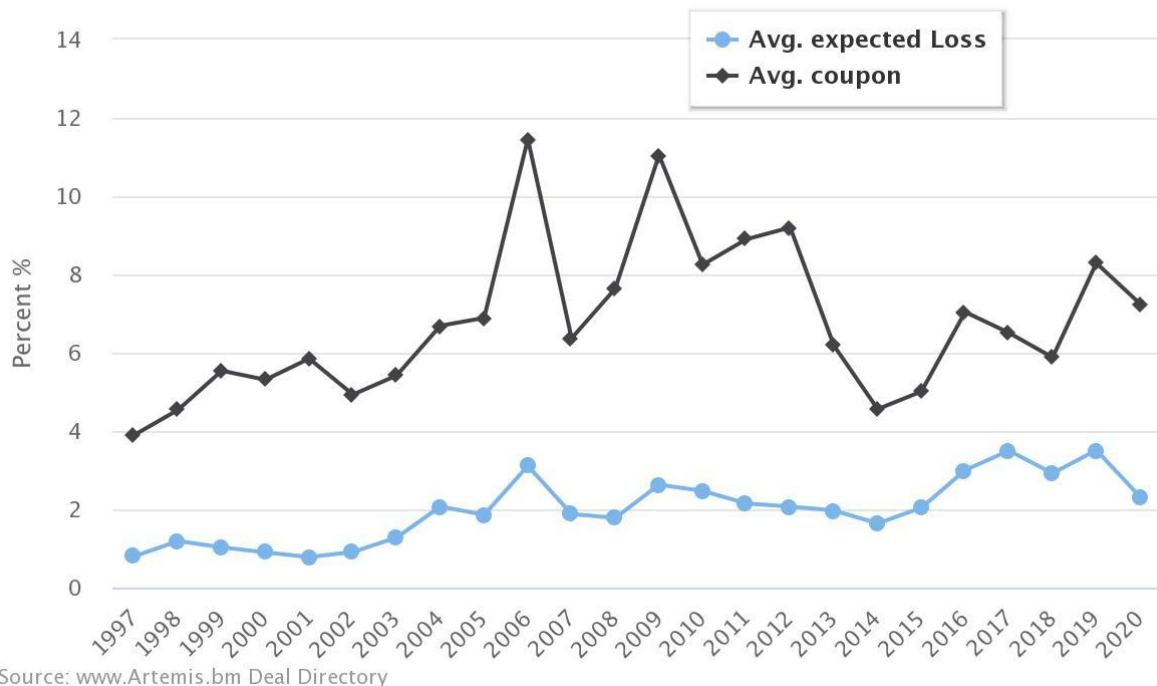
Catastrophe bonds and ILS cumulative issuance by year

Cumulative cat bond issuance and number of deals by year – From the Artemis Deal Directory



Although there has been a recent softening in the coupon rate as well as within the traditional reinsurance markets over the recent years until Covid-19, there is now a hardening of the rates due to the increase in NatCat events such as fires in Australia and California; multiple typhoon and hurricane events, plus business interruption cover due to Covid.

Catastrophe bonds & ILS issuance average expected loss and coupon by year



COMPETITOR TO QUANTAR PATENT EVALUATION

Companies Covered:

1. CyberPoint International (PivotPoint Risk Analytics)
2. Guidewire/Cyence
3. Secure Systems Innovation Corporation (SSIC)
4. Risklens
5. Balbix
6. Corax Cyber
7. Neo Prime

All cross-references to Quantar patents are to Quantar INDEPENDENT CLAIMS ONLY. Other references to drawings and specifications are indicated herein.

General Overview of Quantar Patent Methodologies:

Quantar patent specifications include a fundamental of risk assessment used by the risk and insurance industry for generations. These have a target, a threat, the frequency, impact and subsequent consequential financial loss.

They also account for actions taken to reduce risk exposure through mitigation actions.

All the claims map the interdependent relationships of systems, business processes, threats, frequencies, mitigations, dependencies, loss and aggregated loss.

The development of the models was in parallel with the allied software applications, from 2000 onwards, with the first back-end application being filed in January 2002. Because the initial risk valuation applications were made in 2010 and 2011, they predated all other similar applications/claims. These latter have been formed as a result of recent recognition of cyber risk quantification as a critical component in managing cyber threats and pricing of cyber insurance. As such most of the later application specifications contain elements of Quantar methods. Claim language has been obtuse in the phrasing, but correspond to the claims or specification of Quantar.

Of note is that due to the earlier filing dates of Quantar applications, they have been examined both pre and post Alice and are tied to a specific machine, whereas some/most competitor claims are method patents only.

Below is a high-level view of the current top-ten target companies for an acquirer of the Quantar patent portfolio.

CYBERPOINT INTERNATIONAL (PivotPoint Risk Analytics)

US 9,537,884 Application 15/170,369

CyberPoint International created a spin-off entity, labelled PivotPoint Risk Analytics.

CyberPoint realized that they were infringing Quantar's patents and sought to file their own, which was executed by Fish & Richardson LLP, with issue acquired within six months.

Of particular note is that Quantar's patents were listed by the applicant in their application.

©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

The listed inventor of the CyberPoint application is Mark V. Raugas, who is subsequently listed in a further competitor's prior art (see Corax Cyber below).

CyberPoint's patent utilises the same methodology, with the application listing a dynamic Bayesian network model. This is not the same as a Bayesian network and takes inputs within time-steps in the same manner as the Quantar patent families.

The claims mimic those of Quantar's with the use of wording such as "dynamic Bayesian network", which relates variables to each other over a given time period; and "nodes" in place of business processes and IT systems of Quantar's patents.

Further, the claims of CyberPoint include reference to the use of Monte Carlo simulations to sample outcomes and to determine a distribution of loss, as per Quantar 13/322,298; 15/012,182; 15/696,202.

Loss is determined using measures of impact and aggregated as per Quantar 12/811,298, 13/322,298, 14/827,712, 15/012,182 and 15/017,645.

Mitigation measures are included within CyberPoint's patents, which are embodied within Quantar's 15/696,202 patent, independent claims 1, 9 and 17.

Temporal components of the patents are the same, with CyberPoint's using the term "data indicating a time window" rather than the term temporal profile in Quantar 15/012,182 and 15/696,202.

GUIDEWIRE/CYENCE

US 9,253,203 Application 14/585,051;
US 9,373,144 Application 14/931,510 (CIP);
US 9,521,160 Application 15/141,779 (CIP);
US 10,050,990 Application 15/374,212 (CIP);
US 10,230,764 Application 15/371,047 (CIP);
Continuation in Part Application 15/972,027 (Published)

Quantar identified Guidewire/Cyence potential infringement of its patents in 2017 and contacted (then) Cyence with no response. Cyence was acquired by NASDAQ listed Guidewire in 2017, at which time Quantar contacted the lead venture capital backer at New Enterprise Associates. The contact inquired as to whether the potential breach had been disclosed during the M&A due diligence process (sale price US\$275 Mln).

As a result of the contact, co-founder and Cyence patent lead, George Ng met with Quantar in London in early 2018. At the meeting, Dr. Ng sought to convince Quantar that Guidewire were not using the systems and methodologies embodied in the Cyence patents nor Quantar's. Quantar intimated that the company would be open to patent divestment. No response from Guidewire has subsequently been received.

The overall concept behind all of the Guidewire/Cyence patents is the use of external data to create peer groups of entities. This enables insurance companies to understand portfolio risks created through issuing new policies to new companies that will be assigned to a particular peer group.

The risk of financial loss to the insurer of claims arising from a single IT outage/breach that can affect all within a peer group with the same level of impact (financial loss) can increase with each new insured.

To reduce overall portfolio risk i.e. the total risk exposure arising from issuing cyber insurance policies, risk carriers need to diversify the portfolio. If there is a clear delineation between peer groups through each having distinctly different risk exposure levels to cyber threats/breaches, then this can act as the tool to create a more diversified portfolio.

To achieve this, an aggregation of the total risk exposure arising from cyber threats/breaches is required. Quantar 12/811,208; 13/322,298; 14/827,712; 15/012,182; 15/017,646 all have risk aggregation embodied within the independent claims.

Guidewire 14/585,051 was filed without reference to loss, however the following CIP's do so. Similarly, mitigation actions are not embodied within the initial application, but does so in the CIP's.

The wording of all the applications is sufficiently obtuse as to make comparison initially difficult. However, the terms in Guidewire and Quantar are in fact directly comparable. Reference to the relevant paragraphs in the specifications provide clarity when reviewing Guidewire's patents.

US 9.253,203 Application 14/585,051

Column 4; Line 16: "In one embodiment, the variables can include technologies a company might employ (e.g., internally and externally for Internet communication such as e-mail, website, and social media presence) such as CDN provider, cloud service provider, server type, OS type".

Column 4; Line50: "The data collecting device may be a server, router, firewall, switch, or repeater, or may be a software agent or routine that monitors traffic and/or performs packet inspection. The data collecting device may be on the company's network and/or its periphery, and may collect and/or analyse the data while also transmitting it to system **105**".

Column 6; Lines 36 -52:

Mitigation to reduce risk following provision of the risk score to the user ("actionable feedback").

US 2016/0189301 Application 14/931,510 (CIP);

Figure 6 is an addition to the original specification and introduces loss to the model. Reference is therefore made herein to the related paragraphs in the specification as follows:

[0091] FIG 6 illustrates a flowchart **600** for an exemplary method for determining a probably maximum loss for a group of entities.

[0093] assigns categories to assets as IT systems.

[0094] assign assets to groups with dependency upon the IT systems

[0095] determining financial loss arising from process dependency where loss of IT systems occurs. Assigns predicted threat activity to determine a range of loss.

[0096] - [0098] Delivers loss value to user and enables changes to be made to mitigate loss exposure.

[104] Changes as per above can be re-modelled using Monte Carlo simulation.

[106] Prediction of threats over a temporal profile.

[107] Use of Monte Carlo using model parameters, random variables and threat prediction to generate future loss values.

US 2017/0085595 Application 15/371,047 (CIP)

This application covers assignment of risk to an entity by using data acquired indicating if the entity is a target or not and where it is a target, automatically recommending a change to the entity's cyber security policy or the entity's computer network.

There is no specific method indicated in the independent Claim 1, aside from "cross-referencing data in the collected information to confirm or infer that the entity is referenced in the circumstantial or indirect information that is indicative of the entity being referenced in the circumstantial or indirect information; and

Increasing or decreasing the assessed risk if the circumstantial or indirect information is respectively negative or positive;"

Reference to [0169] provides:

"Cyber security policy" is an insurance policy;

[0182] provides that the circumstantial or partial referencing data are items such as newspaper items mentioning an entity.

However, the application specification introduces at Fig 5, a "Commercial Estimator Module 550" which provides a commercial risk assessment resulting from a technology outage.

At [0103] "The exemplary assessment system may provide recommendations to an entity to improve their cyber risk assessment by, for instance, reducing their cyber risk."

[0104] Implementing the recommendations may impact an entity'sexpected commercial impact of a security failure (e.g. a cyber attack,..."

[0113] "To be sure, the system 505 can be used to automatically change technical aspects of the entity, such as computing diversity, content distribution and delivery and other technical attributes.!

[0114] In some embodiments, the system 505 comprises a commercial estimator module 550 that is configured to estimate a commercial impact to the entity for a simulated security failure (e.g. a cyber attack,..."

Referring to the specification, in conjunction with the claim language, it is possible to determine that the application uses the same methodology within Quantar 12/811,208, 13/322,298, 1/827,712, 15/0122,182, 15/017,645 in relation to determining financial/commercial loss.

The effect of reducing assessed risk is embodied within Quantar 15/696,202.

In relation to automatic changes to technical aspects of the entity [0113], this is embodied in Quantar continuation 16/129, 820

US 2017/0093905 Application 15/374,212

The remainder of Guidewire/Cyence's patents follow the same path, with additional elements, such as catastrophe modelling being included with each iteration of the specification/drawings.

This being the case, the arguments provided above apply equally to all Guidewire/Cyence patents other than those listed above.

All require prediction of cyber threats; aggregation; mitigation effect measurement, sophistication measures (which can be regarded as being a severity score, as per Quantar).

SECURE SYSTEMS INNOVATION CORPORATION (SSIC)

US 9,747,570 Application 15/259,084

Continuation in Part Application 15/651,377

Continuation in Part Application 15/651,407 (Notice of Allowance)

SSIC has developed a product labelled X-Analytics, which purports to be unique in its' ability to quantify cyber risk. It is currently rebranded by Unisys as its' Trustcheck product. As such, infringement by SSIC includes contributory infringement by Unisys.

SSIC patent claims use the fundamental concepts of the Quantar application method, with the exception that SSIC's model applies a percentage allocation of threats to a system out of the total number of experienced threats. Quantar allocates a fraction as opposed to a percentage scale. Clearly a fraction is expressed in percentage terms within the mathematical model of Quantar (Figs 5A and 5B all patent application drawings)

SSIC patent independent claims utilize the same methodology as Quantar patents as follows:

A model taking inputs comprising predicting threats for a threat, the impact upon a business process, the severity, threat type and its target, data specifying the relationship between systems, processes, threats and mitigation actions taken by an entity.

All Quantar patents utilize the method of predicting threats; predicting a business impact for a scenario comprising "a threat type and a targetable system."

Quantar patent 15/696,202 also has mitigation actions embodied within it. All patents have the adjusted exposure from mitigation actions in the drawings at Fig 7.

15/696,202 also has temporal component to independent claim 1:

"each simulation involving propagating data through stochastic modelling for a given time window having a beginning and end;"

"simulations generated using a Monte Carlo method according to the series of threat events within a series of temporal profiles, each having a beginning and end;"

RISKLENS

Application 10/912863 (abandoned)

Applicant Jack A. Jones filed an application titled Factor Analysis of Information Risk (FAIR) in 2004, with a single claim. This was rejected in light of prior art which was fundamentally copied in Factor Analysis of Information Risk:

Jones, Jack, A. 10/912,863	Cole E. 10/426,908
----------------------------	--------------------

<p>Factor Analysis of Information Risk (FAIR)</p> <p>1. A method of measuring and representing security risk, the method comprising:</p> <p>(a) selecting at least one object within an environment;</p> <p>(b) quantifying the strength of controls of at least one object within that environment by:</p> <p>(i) quantifying authentication controls;</p> <p>(ii) quantifying authorization controls; and</p> <p>(iii) quantifying structural integrity;</p> <p>(c) setting global variables for the environment [e.g., whether the environment is subject to regulatory laws];</p> <p>(d) selecting at least one threat community [e.g., professional hacker]; and</p> <p>(e) calculating information risk by:</p> <p>(i) performing a statistical analysis, using the strengths of controls of said at least one object, the characteristics of at least one threat community, and the global variables of the environment, to compute a value representing information risk.</p>	<p>Methodology, system and computer readable medium for rating computer system vulnerabilities</p> <p>Claim 1 (Jones) rejected under 35 U.S.C. 102(e) as being anticipated by Cole, US-PGPUB 2004/0221176.</p> <p>As per claim 1:</p> <p>Cole discloses a method of measuring and representing security risk, the method comprising:</p> <p>(a) Selecting at least one object within an environment;</p> <p>(b) Quantifying the strength of controls of at least one object within that environment by:</p> <p>(i) Quantifying authentication controls;</p> <p>(ii) Quantifying authorization controls; and</p> <p>(iii) Quantifying structural integrity (paragraphs 0033-0048);</p> <p>(c) Setting global variables for the environment (paragraph 0049);</p> <p>(d) Selecting at least one threat community (paragraph 0050); and</p> <p>(e) Calculating information risk by:</p> <p>(i) Performing a statistical analysis, using the strength of controls of said at least one object, the characteristics of at least one threat community, and the global variables of the environment, to compute a value representing information risk (paragraph 0050).</p>
--	--

In light of Cole, originally assigned to Sytex Inc and thence to Bank of America, Jones allowed the application for Factor Analysis of Information Risk (FAIR) to be abandoned.

Risklens (formerly CXOware, rebranded Risklens in 2015 with Series A US\$5 2018 and Series B US\$20.55 Mln 2019) markets its software product as being the only product built upon the FAIR methodology. However, since FAIR infringed Cole and applications have been built based upon Cole, this is a marketing statement only.

The Risklens product is currently being provided white labelled to Dell Technologies for its' RSA Archer Cyber Risk Quantification application. This is currently being further integrated into the overall RSA Archer suite of applications/platform.

As such, infringement by Risklens results in Dell Technologies being in contributory breach. Similarly, Evolver Inc also utilises the Risklens product and also stands on the same basis.

The methodology of FAIR incorporated into the Risklens product remains unprotected by patents and is therefore highly vulnerable to the proliferation of new entrants with their own applications at USPTO and PCT levels.

Both Cole and Jones were cited in Quantar applications as prior art. The accepted differentiation being that both Cole and Jones (FAIR) only model a risk that is actually occurring at a present point in time (see applicant arguments to non-final rejection Quantar). This being the case, any forward projection of risk valuation by the Risklens product would breach this difference between the FAIR methodology and the Quantar patent claims.

The FAIR method is described:

“[0188] Factoring Risk. FAIR defines information risk as occurring at the intersection of two primary probabilities (FIG. 1):

1. The probability of a loss event (exposure)
2. The probable loss magnitude (impact)

[0191] Factoring Exposure. The probability of a loss event is dependent upon two primary contributing factors (FIG. 2):

1. The probability of a threat agent acting against an asset (**threat event frequency**)
2. The probability that the asset is vulnerable to the action taken against it (**vulnerability**)

However, the FAIR method also utilises exposure to a threat event as a proxy for probability of exposure:

[0222] Within FAIR, exposure represents the probability of a loss event.

FAIR also utilizes Monte Carlo analysis to derive risk:

[0240] Deriving Risk. Risk is derived using Monte Carlo (MC) analysis of two probability distributions—the probability of a loss event (exposure), and the probable loss magnitude (impact).

Exposure also uses MC analysis:

[0243] Just as risk is computed by combining exposure and impact through MC analysis, exposure is derived by MC analysis of Threat Event Frequency

In determining financial impact:

[0272] Deriving Impact. Impact reflects the probable loss magnitude of an event in financial terms.

With reference to the Quantar model for the relationships between IT systems, business processes and threats, resulting in dependence and downtime effects:

[0279] Measuring Operational Impact. As defined within this model, operational losses are those losses in productivity associated with lost integrity or availability of data or systems, as well as the costs of recovering degraded data or systems capabilities.

[0280] **The first step is to identify**, through interviews with the business stakeholder(s) **how much loss is expected per day of outage**. The second step is to identify, through discussions with appropriate staff, the expected recovery time and the expected costs associated with recovery. **The loss per day (LPD) and expected recovery time (ERT) are multiplied, and then the recovery costs added. This provides a baseline for operational impact** that then is modified (up or down) based upon additional operational loss domain factors (FIG. 8).

In terms of the mathematical modelling within FAIR, this includes:

[0412] A method of measuring information security risk based upon;

[0416] A statistical method that derives risk values based upon mathematical processes of modeling the risk factor relationships.

[0417] A software program interface.

[0418] In support of claim 1, a method of measuring risk based upon the intersection of loss event probability (exposure) and the probable loss associated with the event (impact).

[0430] The volume and level of threat agent activity

[0441] In support of claim 2, a method of measuring loss magnitude probability based upon a combination of the following loss domains:

[0442] Operational losses.

[0502] In support of claim 32, a method of measuring risk within a simulated computer software program that:

[0503] Applies mathematical formulas to emulate the relationships and interactions between the objects and threat communities defined by the user.

The above references to the original application, 10/912,863 are provided given the ongoing insistence that the Risklens product is built using the FAIR methodology of the said patent application.

As such, in the absence of detailed knowledge of the operating software, reference reveals that the Risklens application breaches Quantar patented methods.

BALBIX

US Continuation in Part Application 15/383,656
15/473,418
15/234,980 (Issue Notice)
15/234,970 (Notice of Allowance)

Balbix applications abstract indicate that the concept is to identify and categorize assets on a network in order to identify levels of security risk per node of similar types of assets (15/473,418). In

15/383,656, there is an additional component of understanding how a security breach is distributed and interdependent upon the nodes on a network. 15/234,970 and 15/234,980 introduces mitigation to the modelling of risk, as well as quantification [0019].

The specification specifies a risk modeller server **190** or **192** [0044] that receives network data (“analysis data”) from an agent on the network and uses this data for analysis. The risk modelling utilizes an enterprise risk model, labelled an “enterprise risk layer”, with an additional “mitigation” layer 15/234,970 [0050] “that models a reduction in risk to the enterprise network in response to the performance of potential mitigative actions”.

The enterprise model **500** predicts future compromise of nodes on the network. The model maps the likelihood and impact of an event in a graphical format to an end user [0081]. Assets on the network are assigned an impact score as to their importance to an organization, that is, the model multiplies the predicted likelihood with the impact value to quantify risk. Where mitigation actions are taken, the impact score is reduced, thereby reducing the overall risk score for that asset.

The overall risk model for the applications is **Fig 11.**:

Observations:

User
Device
Environment
Asset



Risk:

Impact
Likelihood

This is summarized 15/234/980:

[0064] FIG 11. Is an illustration of observations used to model risk to network assets according to an embodiment of the invention. As depicted in FIG 11, analysis data of an embodiment may comprise data that describes for each node: attributes of the user of the node, hardware and software features of the node itself, the environment in which the node is deployed, and the assets stored on the node. Such information will be used by enterprise risk model 500 in assessing the risk of a security breach, and its impact, posed by each node.

Although the main use of the method is to determine risk to nodes on a network in order to prioritize which have the greatest exposure and thus not directly infringing Quantar patents, the following applies:

[0077] Embodiments of the invention may also product what is know as a risk inventory, which is an ordered list of the inherent risks of malicious attacks to the resources of the network.

The overall infringement contention is therefore that Balbix utilizes the method of acquiring data to feed a risk model that has risk, severity scores, impact and mitigation actions embodied within it, with relationships between threats and IT systems in dependence of threat activity, observed data including targets of threats.

Acquiring data and modelling according to predicted threat and impact scores to determine risk and the result of mitigation actions being implemented are at the core of the alleged infringement.

CORAX CYBER (IP Acquired by Creditor 2020)

US 10,277,620 Application 15/259,477;

US Application 15/338,192 (Dispatch for Issue)

US Application 15/338,192

This Corax application is nearly identical in specific, method, objective to those of Balbix, yet Balbix is not stated as prior art by either the inventors or the USPTO examiner.

The objective of the invention is to identify those nodes on a network that pose the highest risk of breach to said network. The method includes mitigation actions that are calculated to have an effect on the risk value attributed to a node, permitting determination of the effectiveness of said mitigation action.

The overall application via the specification indicates specifying relationships between assets, threats and mitigation actions, infringing Quantar 15/696,202 in relation to mitigation and for the specifying the relationships between assets, threats and values for the general Quantar portfolio.

[0036] "A control may correspond to a mitigation of a security breach associated with the respective asset.....Examples of a control may include, but are not limited to, a firewall, antivirus software installed on the asset, etc."

[0041] "...In general, each node may be assigned one or more vulnerabilities and a value or score for the likelihood of a successful security breach and another value or score for an impact of a successful security breach."

[0041] "...In some embodiments, the likelihood value or score may be based on a known frequency of use of the vulnerability, a known frequency or use of the vulnerability with the type of asset represented by the node, or another factor or characteristic associated with the vulnerability."

[0041] "...The impact value or score may be based on a known amount of damage or cost that the vulnerability may result in, the value or cost of the asset, the value or cost of the data stored at the asset or that may be retrieved from the asset, etc."

US 10,277,620 Application 15/259,477

This is very similar to the previous Corax application, with an additional component and focus upon secondary node/asset vulnerabilities arising from a relationship to a primary asset subject to a vulnerability.

In this form, both applications also use modelling of dependency of assets/nodes (IT systems) and vulnerabilities (threats) as per Quantar. In this particular application, the cited prior art by the examiner included reference to Raugas, Mark, and the CyberPoint International patent listed above. Given CyberPoint's application is founded upon Quantar's patents, it would appear to indicate Corax infringement in turn.

NEOPRIME LLC

US 9,680,855 Application 14/319,994;
Continuation Application 15/618,809

The Neo Prime applications are related directly to the financial quantification of cyber threats, predicting loss within current and future periods. They also include security perimeter system enhancement of false positives, as per Quantar 15/696,202 (see [0077] below).

They also include the mitigation action impact upon predicted loss for cost-benefit of said actions.

14/319,994 Abstract [0032] "...The described technology generally relates to risk modelling and computer networks, and more specifically, to modelling risk in order to forecast damages to an organization's assets and the related loss resulting from man-made cyber-attacks, or accidents and system failures."

[0066] "In one or more embodiments, the described technology **provides an accurate quantification of risk, financial loss** and assessment of network security control measures to minimize damage given the rate and type of attack by, for example, quantifying the likelihood of damage and loss due to the range of cyber threat vectors, both attack-based and accidental, that can bypass current security mechanisms and damage assets. **Calculating the likelihood of damage to assets as a function of time over forecasted time intervals** and knowing the cost to an organization of deploying traditional security appliances is useful to assess cost-benefit decisions"

[0067] "...This damage-forecast method can be used to forecast financial losses from cyber-attacks over time windows looking forward from past, present, and future times".

[0073] The event-time distributions themselves change in time due to time dependent variables, which include attacker attributes, vulnerabilities, exploits, system vulnerabilities and components, security control measures, and/or other variables.

[0074] The resulting event-time distributions of the loss events are used, in various embodiments, to calculate the time distributions of the damage within the forecast time window.

[0077] The described technology allows broad correlation and integration of security and attack-related data that can provide a method for detection of network compromise, **lower false alarm rates on the detection**, improve response time and effectiveness for security teams.

[0081] First, scenarios for **existing and future cyber-related behaviors are modelled**

[0082] The described technology described herein calculates the likelihood of **financial loss resulting from network attack** as a distribution in time.

[0085] The described technology **calculates** damage and **financial loss**, including both direct and indirect first- and third-party losses, **resulting from damage to** the integrity, **availability**, and confidentiality **of information, services, equipment, and property**.

[0087] Embodiments of the described technology can **use a combination of Monte Carlo techniques and propagation of analytic distributions in order to create a model of the likelihood of loss in a computer network**.

A key description of the Neo Prime model is at:

[00115] FIG. 3 is a diagram of data flow in an arrangement of components according to an embodiment of the described technology. The data that is specific to a particular site or sites 302 and data that is independent of any particular sites 304 are inputs to the forecasting input builder component 306, which creates the forecasting input 308. **The forecasting input 308 is input to the threat forecasting component 310, the damage forecasting model component 314, and the financial loss forecasting component 318.** In various embodiments, in **one of the first steps to forecasting, the threat forecasting model component 314 computes the attackers' characteristics and attackers' attack rates 312, which is input to the damage forecasting model component 314. The damage**

forecasting component 314 in some embodiments computes the asset damage 316, and inputs this information to the financial loss forecasting component 318

Further, the model takes inputs of historic threat data to forecast financial loss:

[00118] "...The site properties are, in some embodiments, **used to retrieve the appropriate information from the databases** and collections 506 a-506 n: (a) historical attacker attributes 504 a, attack rates 504 b,.....e) historical attacker action properties are retrieved from data collection 506 e; and/or (f) historical attack campaign information 504 **is retrieved from historical attack data 506 f and recent attack data 506 g**".

The retrieval of threat data for Quantar patents is applicable to all issued patents. The temporal component of Neo Prime applications is embodied with Claim 1 of Quantar 15/696,202.

Monte Carlo is used in the same manner as Quantar in sampling a variable to produce a distribution:

[00136] In some embodiments of the technology described in FIGS. 11-13, **inputs to the forecasting models can be sampled using Monte Carlo** or other sampling techniques **in order to forecast the probabilistic propagation of uncertain model input values**.

[00139] FIG. 15 is a block diagram 1500 of an embodiment of the described technology that **uses the Monte Carlo method by sampling from the input distributions and simulating outcomes from forecast components**. The block diagram 1500 depicts an embodiment of the described technology that uses the Monte Carlo method by probabilistic sampling distributions 1504 from one or more input distributions 1502 to provide the distributions 1506 of the dependent properties that are needed to simulate outcomes from the risk forecasting model component 1508.

The Neo Prime specification also focusses on modeling the probabilities of threats to nodes within time windows, which does not have applicability to Quantar patents. However, the model requires a threat forecasting model, which comprises:

[00241] Given a targeted organization "o," **the total rate of attack** at one of its entry points "e," is

$$Q(o,e,u,t)=\sum \alpha Q \alpha(o,a,e,u,t),$$

where the sum is over all attackers "a," and "u" is the **type of attack**. The "**Q's**" are either idealized instantaneous rates or **rates over some specific time** of interest. Instead of the sum being over individual attackers, the sum can be over attacker categories.

Although the application then utilizes an additional component of attacker motivation/resource/skill within the model, it still draws upon attack rates per period.

Further, the model incorporates increased detection through lowered alarm rates, as per Quantar 15/696,202:

[00280] FIG. 22 depicts a chart 2200 related to on-site security live or periodic data feed driven solutions as part of an organization's security posture to mitigate loss. Chart 2200 lists examples of embodiments of the described technology **including improved detection through lowered false alarm rates**, location of the network breach, forecasting of time to bring in breach-response teams, and forecast pathways of the attacker when responding and containing the attack.

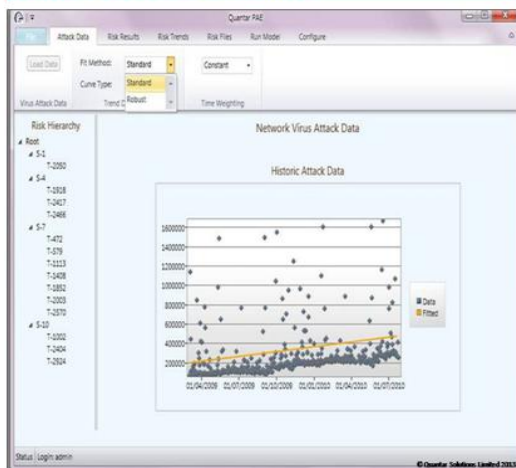
The Neo Prime method FIG.23 takes data feed of an organization, feeds the data to an Attacker Pathways & Probabilities Model 602, which inputs to the Detection Engine Model 602i, as per Quantar 15/696,202, which feeds back to the firewall to update rule sets and reduce false positives.

CASE USAGE

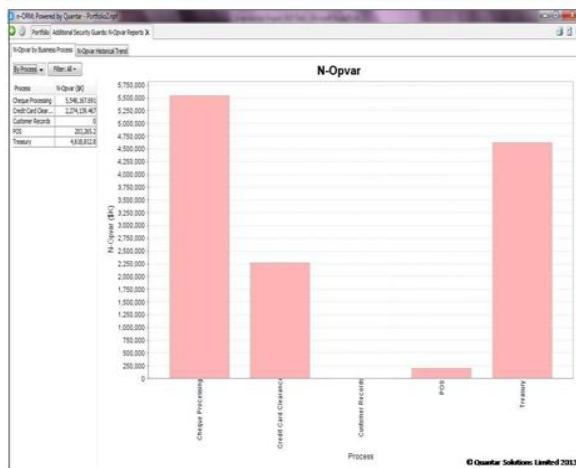
Use Case 1

Assess Prospective & Actual Vessel Cyber Risk

View cyber threats experienced by
The vessel over time



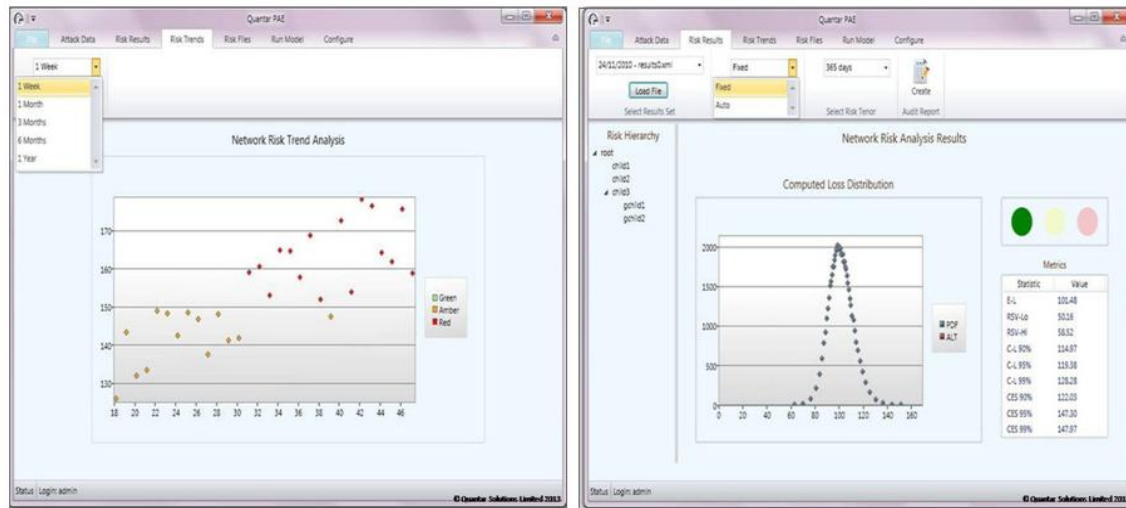
Analyse vessel risk across business
processes



Use Case 2

Assess cyber risks over time; value exposures; red/amber/green warning

Develop mitigation strategies ge based on stochastic simulations for a single or an aggregation of the fleet



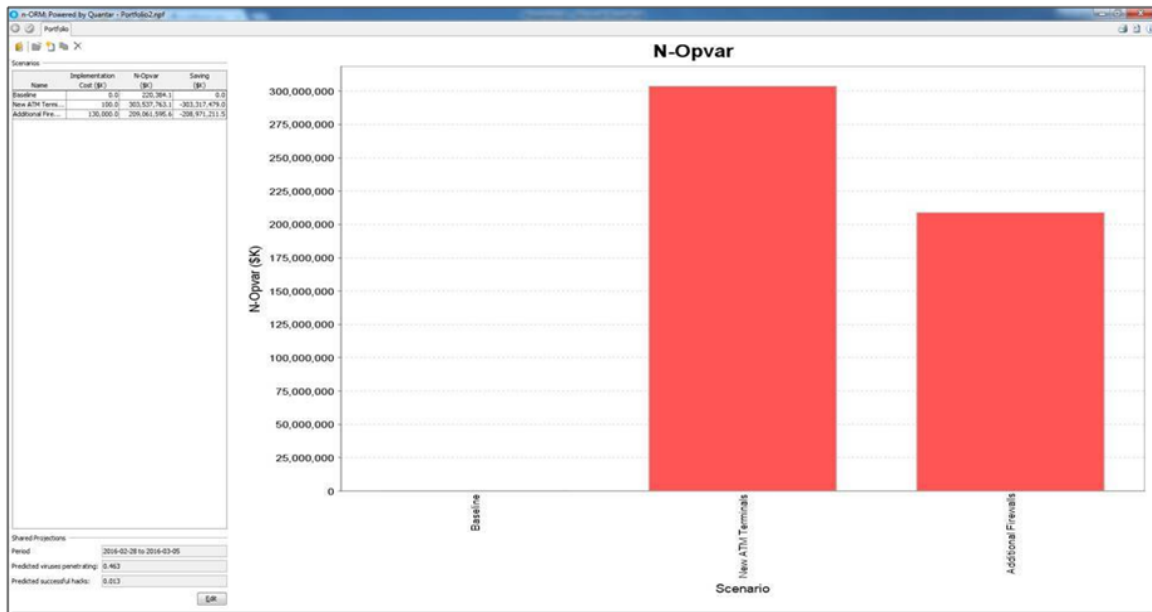
Use Case 3: Temporal Exposure Management

Risk and attack forecasting; Track risk exposure over time; Aggregate cyber risk portfolios for P&I Club cyber reinsurance

Attack Rate Forecasts				Risk Statistics			
Severity Id	12-Oct-2018	10-Jan-2019	14-Jul-2019	Statistic	12-Oct-2018	10-Jan-2019	14-Jul-2019
1	150824.42	154293.45	161424.24	Mean	217.30	217.18	217.38
4	420978.06	431058.55	451779.56	Variance	20481.48	20439.90	20475.09
7	1096786.81	1121879.86	1173460.02	RSV-Lo	9292.79	9275.45	9291.39
10	445144.37	455561.89	476975.69	RSV-Hi	11188.69	11164.45	11183.70
				CL 95%	443.76	442.94	443.08
				CL 99%	468.36	467.38	467.93
				CES 95%	504.79	543.03	534.72
				CES 99%	714.00	509.76	840.97

Use Case 4: Client Advisory & Regulatory Compliance

Calculate potential losses; Run “what-if” scenarios;
Allocate capital to mitigation actions; Regulatory reporting



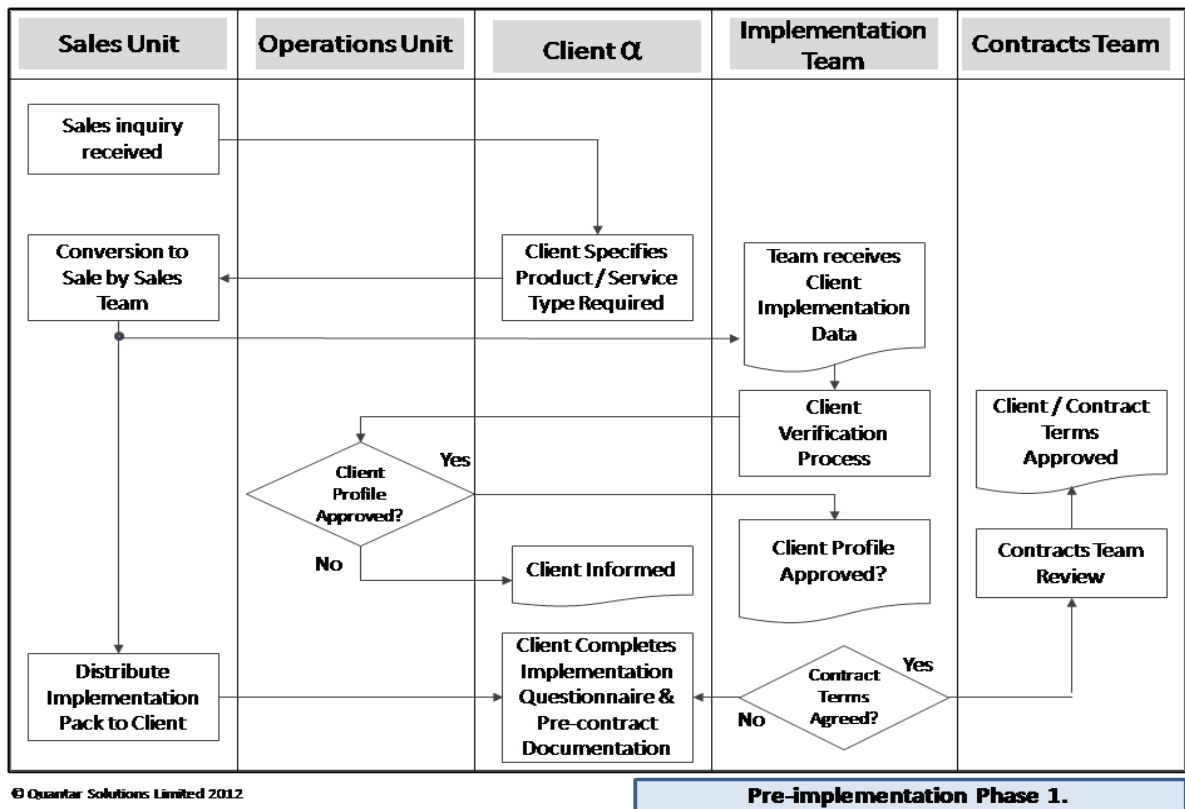
© Quantar Solutions Limited. All rights reserved. Do not distribute without permission. Page 4

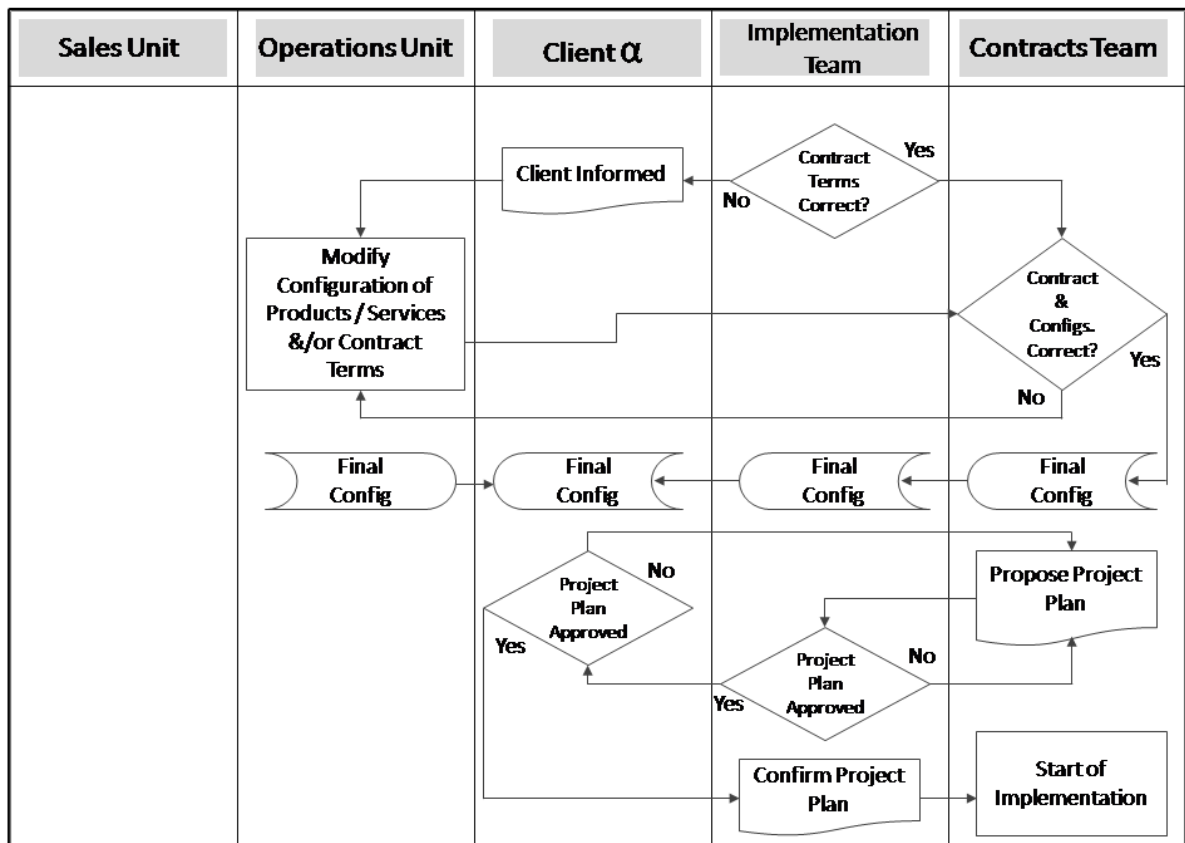
SELECTED COMPANY CITING QUANTAR PATENTS AS PRIOR ART

1. McAfee, Inc.
2. Raytheon
3. Bank Of America
4. Fireeye, Inc.
5. Cyberpoint International Llc
6. Amazon Technologies, Inc.
7. Isight Partners, Inc.
8. Alcatel Lucent
9. Cloudfare, Inc.
10. Hewlett-Packard
11. Guidewire Software, Inc
12. Cyence Inc.
13. Accenture Global Solutions

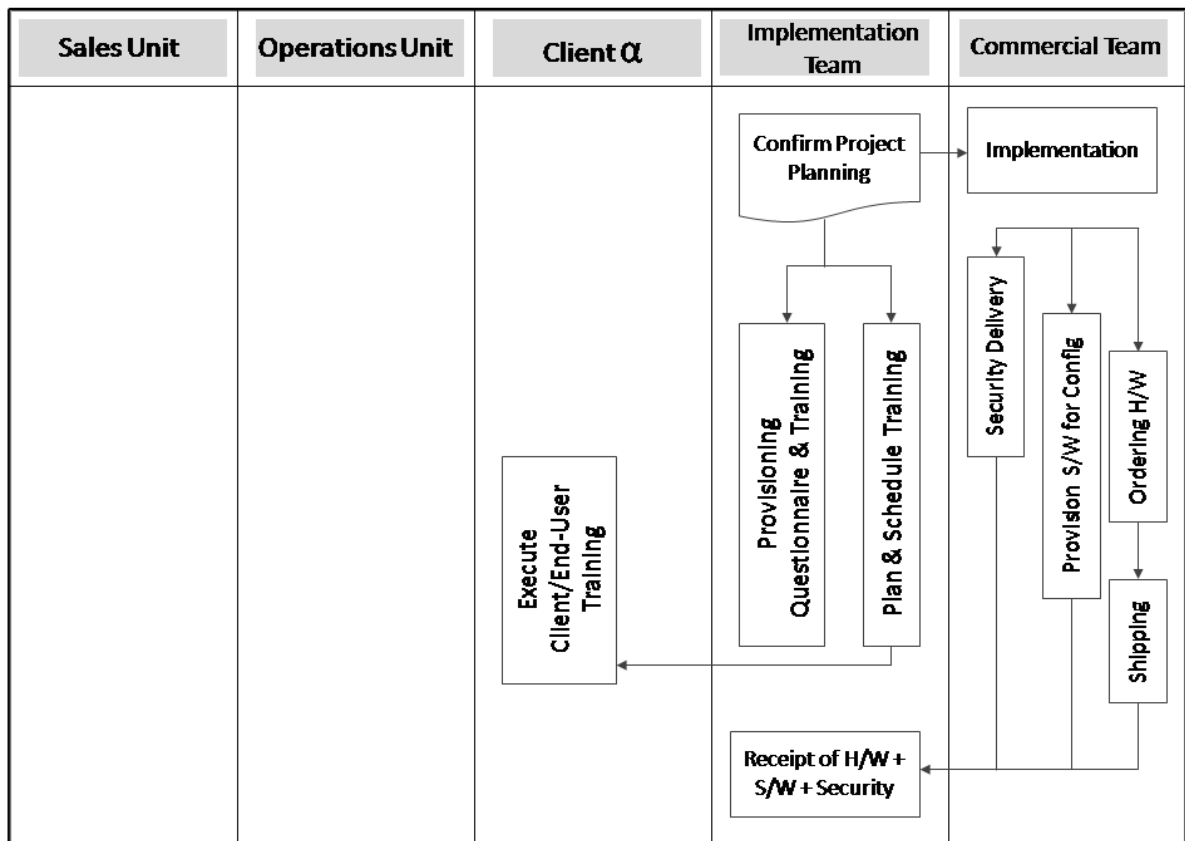
QUANTAR MARINE IMPLEMENTATION WORKFLOW MODEL

Existing software/hardware implementation workflow to be adapted for current Quantar/DMGT platform and local installation development:



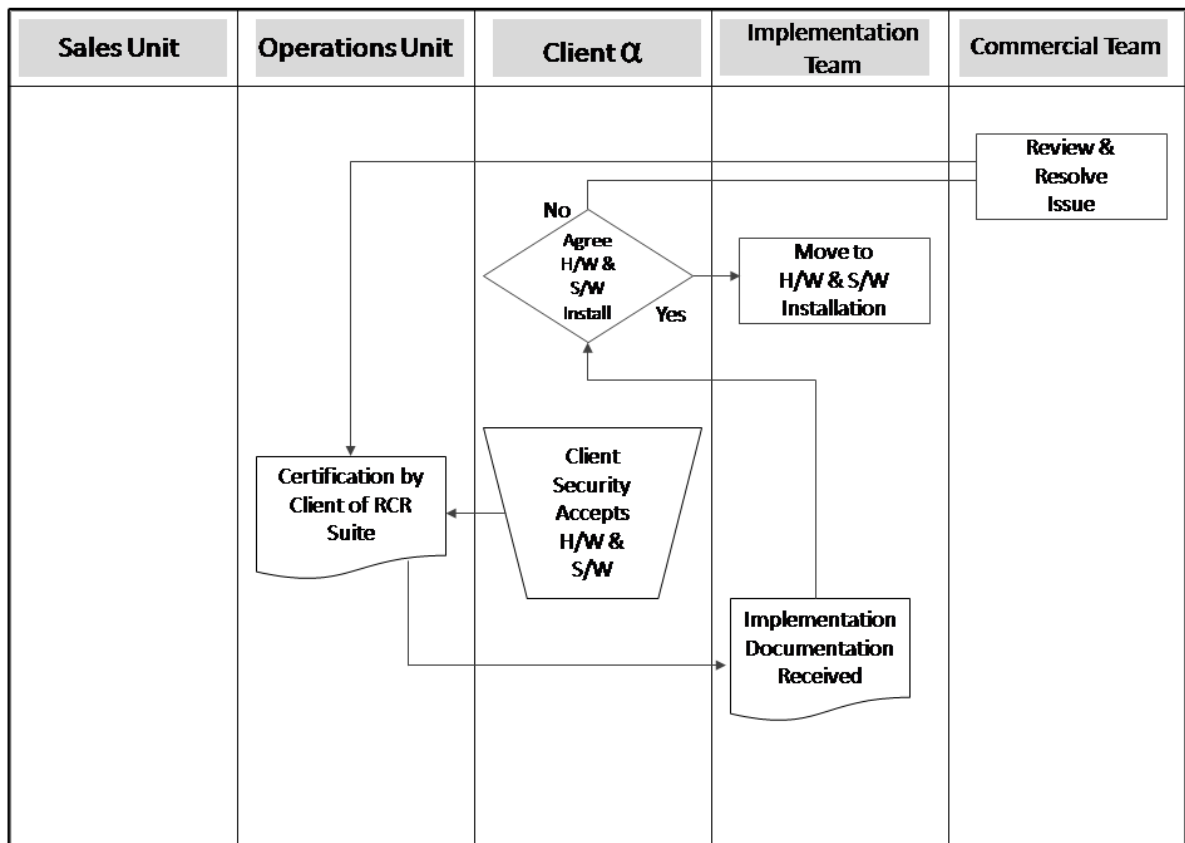


© Quantar Solutions Limited 2012

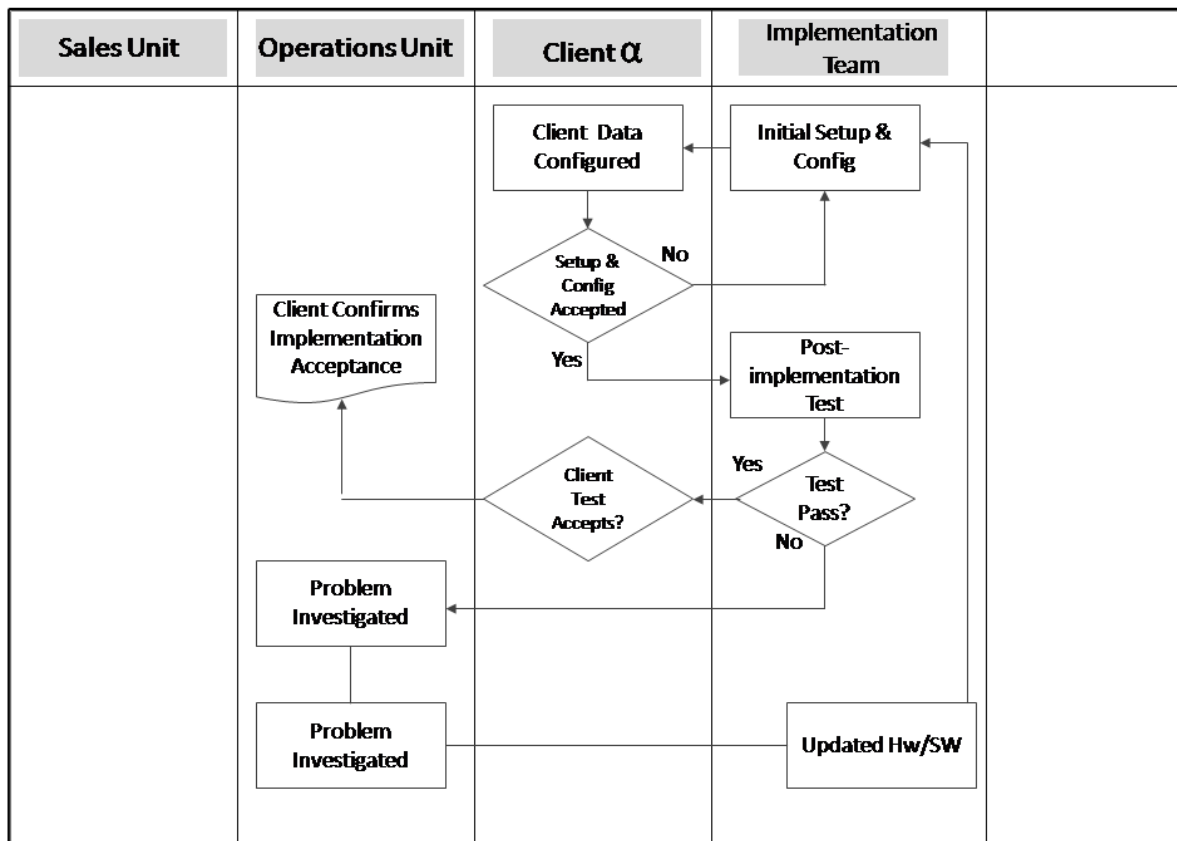
Pre-implementation Phase 2.

© Quantar Solutions Limited 2012

Implementation Phase 1.

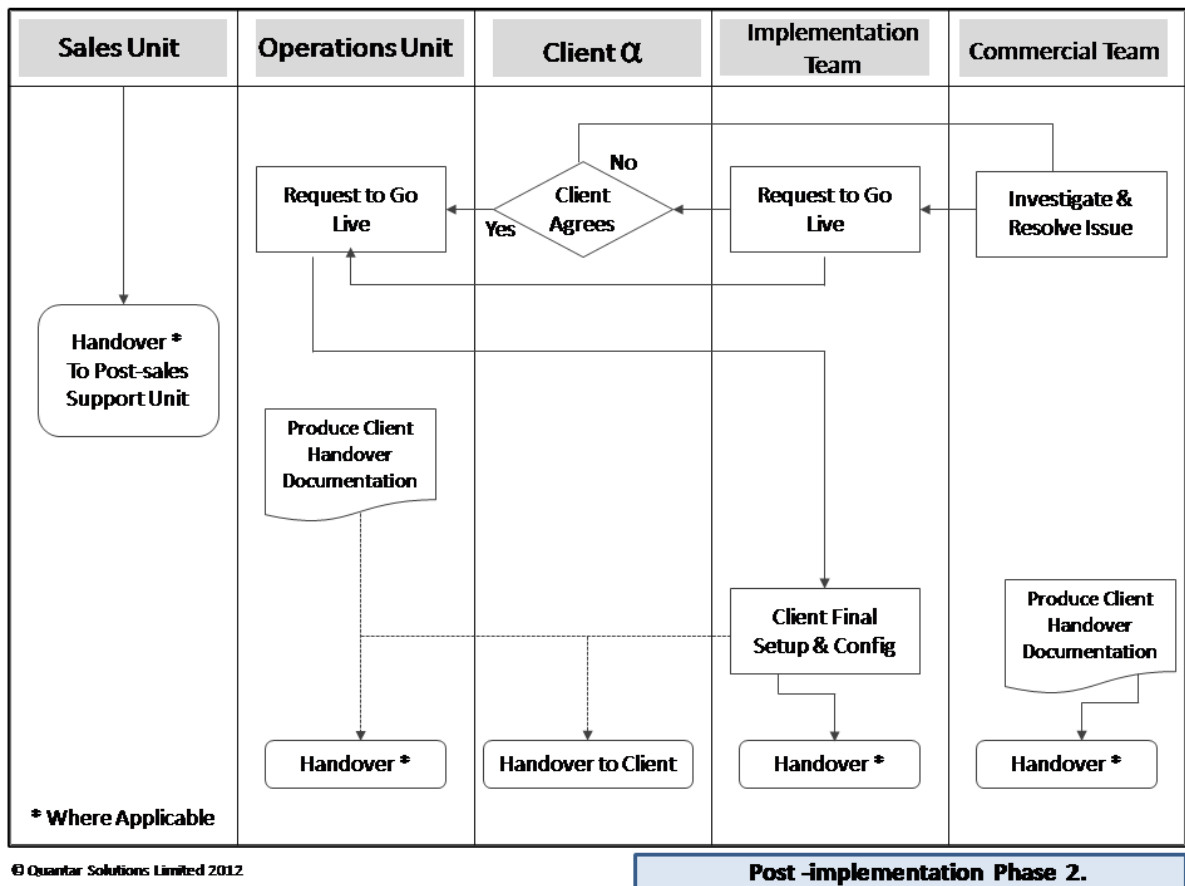


© Quantar Solutions Limited 2012

Implementation Phase 2.

© Quantar Solutions Limited 2012

Post-implementation Phase 1.



QUANTAR MARINE SOFTWARE PLATFORM SUPPORT MODEL

Introduction

The Quantar/DMGT marine cyber risk software platform is shortly due for release to its intended maritime and risk transfer customers. It is hoped that it will become an important tool to those companies; as such, they are likely to require an appropriate level of support. This support will range from answering simple questions about the configuration and operation of the software platform to detailed technical ones about the algorithms and diagnosing complicated issues.

This diverse support requirement will be most efficiently met using a widespread model, that of tiered support. Initial questions and requests will be assessed by a front-line support team. Simpler issues will be answered by them based on general PC knowledge, basic familiarity with the software via the platform and a database of frequently-asked questions (FAQs). More involved issues will be elevated to a second-tier team, who will investigate the problem and provide an answer. This will, if appropriate, be added to the FAQ database so that, if it presents itself again, the front-line team can provide the same answer more quickly and cheaply.

Where the new entity is unable to provide the front-line support team in an efficient manner using existing staff, so it shall be assumed that this will be supplied by a specialist third party. However, as creators of the software, the new entity itself will provide the second-line support. This document outlines the proposed terms for the terms of arrangement.

Considerations

The software platform provides regulatory compliance, cyber risk management and other allied capabilities. Additionally, the platform provides data for reinsurance and risk transfer. None of these activities are mission-critical in the manner I.T. security is, for example. It is therefore no necessary for support to be in real-time 24/7.

Quantar, DMGT have their offices in the UK and work within normal UK business hours. In particular, the offices are closed on weekends, bank holidays and between Christmas and the New Year. No support can be offered on those days by the new entity, but may be outsourced to third party suppliers. Office hours are 08:30 – 17:00 Monday – Thursday and 08:30 – 16:30 Friday. Support requests arriving outside those hours will be addressed on the following business day.

Support requests must be sent to in English. All responses to the issue will also be made in English.

Where possible, members of the original development team will be used to address support requests. To maintain a high level of service, other staff from the new entity's experienced engineering team will also be available, particularly for issues of a more general nature requiring less specialised knowledge of the application.

Priority Responses

The Support Pricing and Terms – August 2020 document, produced by Quantar, grades responses to the customer by service level (gold, silver and bronze) and impact level (critical, major and minor). The definitions of these levels may be found in the document. The new entity's response to the front-line service provider to be based on three priority levels: 1 (highest priority), 2 and 3. It is expected that the front-line support team assigns an issue to one of these levels based on the severity and customer expectation. A possible arrangement is shown in the table below, but it would be a decision for the new entity's management team and the front-line service team to make.

Table 1: Possible Priority Levels by Service Level and Impact Level

Impact Level	Bronze	Silver	Gold
Critical	2	1	1
Major	3	2	1
Minor	3	3	2

The new entity's response to a support request will depend on its assigned priority as detailed in the following table:

Table 2: Response Service by Priority Level

Area	Priority 3	Priority 2	Priority 1
How request is received from front-line support team	Email	Email	Email
Acknowledgement ¹	1 day	4 hours	4 hours
Assessment ²	2 days	1 day	4 hours

Start work to resolve ³	5 days	2 days	1 day
Telephone customer if required (normal UK business hours)	No	No	Yes
Interim status updates at least every 1-2 days	No	Yes	Yes
Generate custom hotfix for problem if appropriate	Yes	Yes	Yes

Notes:

1. Acknowledgement is reading of the support request email by an appropriate member of staff. The email system can in addition automatically send a receipt as soon as it receives a message. All times are measured in new entity business hours from the time its email system receives the request.
2. Assessment involves completing a preliminary diagnosis of the issue, deciding who should address it and, where appropriate, arranging for them to suspend work on their other project to make time available.
3. No guarantees can be given over resolution timescale as it will depend on the nature of the underlying problem, the quality of the diagnostic information supplied by the customer.

In the unlikely event that the new entity's team is unable to meet the timescale agreed for a particular priority, the price charged will be reduced to that of the priority actually achieved. For example, if it takes 6 hours to assess a Priority 1 request, all work on that support request would be charged at the Priority 2 rate.

Process

Customers will enter their support requests on a web portal. Initial triage on those requests will be performed by the front-line support team who will answer simpler, generic or frequently-asked questions directly. If the request is outside their remit, they will assess its importance, assign a priority and forward it to the relevant person within the new entity via email. It will save time if the notification includes all relevant configuration data such as operating system of the end user, client login details (without security passwords or other sensitive data), error log content and data files being used. Support requests will not be accepted without the front-line team's initial assessment.

The new entity's team will examine the forwarded request, if necessary liaising directly with the customer via email or telephone (priority 1 requests only). If the request is a question or a misunderstanding about the use of the platform, the team will provide a full explanation to the customer and also the front-line support team for inclusion in their FAQ database. This permits that team to answer the question directly if it arises again, providing a quicker service at reduced cost.

If the request requires a change to the platform and/or software source code to correct a problem, the team will instruct the external development team to make the change, test it and send the necessary update to the customer. An updated version will also be provided to the front-line support team, so they can give it to any other customers with the same issue, for distribution to the existing customer base and any future sales.

The sorts of request anticipated to be dealt with at each level include:

Table 3: Representative Support Requests by Tier

Front-line Team	Second-line (3rd Party)
Questions in the FAQ database	Error reports or crashes
Installation issues	Apparently incorrect calculation results
Configuration issues, file locations, etc.	Issues of very slow performance
Security access issue requests	
General PC questions (not platform related)	
Questions about the back-end of platform	

The team will maintain a log of all support requests, including the date and time of arrival, acknowledgement, assessment, starting and finishing work and total effort expended. This will be used for quality assurance and support service costing, and will be made available as a monthly aggregated report to the management team to review and make relevant changes to future support operations or in the cost of support for renewed pricing.

Commercial

The cost of responding to a support request will depend on the priority assigned to it. High-priority incidents will be afforded an expedited response even at the cost of disrupting other projects. Accordingly, the price of support will depend on the priority level. There will also be a cost of setting up the support arrangements and an ongoing administrative effort required. The price for these may be found in the table below:

Table 4: Prices for second-line platform and software application support⁵

Item	Price (ex. VAT)	Per
Initial set up of support system	£9008	One-off cost
Standing charge (covers administration, quality assurance and reporting)	£886	Month
Priority 1 support	£220	Hour. (chargeable in half-hour increments)
Priority 2 support	£180	
Priority 3 support	£120	

The standing charge covers the cost of administering the system, quality assurance and reporting. It is internally chargeable for each calendar month (or part month) in which the team receives support requests, whether, or not any requests are generated. This ensures that the cost averages out over an operational year, irrespective of volume request variances. The set-up charge has been included in the first year establishment costs within the financials.

⁵ Support costs 2020 have been estimated using third party support costs from a number of suppliers, including Canonical and AWS.

QUANTAR MARKET TESTING EXHIBITIONS

Business Continuity Management Conference (BCI): London, UK.



International Security & National Resilience Conference (ISNR): Abu Dhabi



©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

Risk & Insurance Management Conference (RIMS): Boston, USA



Indicative Patent Costs - Years 1-5

Maintenance Fees	
At 3.5 Years: \$800	\$4000
At 7.5 Years: \$1800	\$3600
At 11 Years: \$3700	
Issue Fees (2 continuations pending) \$600	
	\$1200
Filing Costs (assuming 5 new utility patents with PCT fees non-small entity)	
USPTO basic filing fee \$300	\$19466
USPTO search fee \$660	
USPTO examination fee \$760	
USPTO prioritised examination fee \$4000	
USPTO PCT basic national stage fee \$300	
USPTO national search submission of search documents \$240	
International transmittal fee \$240	
International search submission \$2080	
PCT fee to foreign offices:	
Filing fee \$1136	
EPO search fee \$1950	
Total Per Patent Filing: \$11666	

Prosecution Costs Request for continued examination (RCE 1) \$1600 assuming 5	\$8000
Total Patent Costs Year 1-5 * As at 09/09/2020	\$36266 £28008*

INDICATIVE INSURANCE COSTS FOR PERSONNEL SALARY PACKAGE

Key Man Insurance

Cost of Life Cover Only - 10 Year Policy Age 35 £7.10 Age 45 £12.66 Age 55 £26.78	Cost of Life and Critical Illness Cover - 10 Year Policy Age 35 £32.56 Age 45 £72.21 Age 55 £158.57
---	---

Key person insurance quotes calculated September 8th, 2020

Private Health Insurance Premiums*

PROVIDER	35 Year-Old P.A.	55 Year-Old P.A.
Bupa	£770	£1,972
VitalityHealth	£826	£2,921
Exeter Family Friendly	£844	£1,740
Aviva	£870	£1,226
Axa PPP	£893	£2,143

*Will vary according to health/medical history/London weighting required or not

Dental Insurance Premiums - based on 55-year old

PROVIDER	COST PER MONTH
Axa PPP	£20.65
Boots	£23.02
Simplyhealth	£28.87
WPA	£13.94
BUPA	£29.58

External Developer Software Support Costs

External support pricing is based upon known values from leading software suppliers. The level of service and terms will be determined within the contracts between the company and the software development company utilised.

As an indication of the levels and costs currently on the global market, Canonical's levels are included herein. Given the third party will not have the resources of Canonical, it is anticipated that support costs will be higher. However, in the case of the proposed development, the operation of it is not mission-critical in the same way that hardware and software in an enterprise environment is and this may reduce support burdens and therefore cost.

[Overview](#)
[Plans + Pricing](#)
[Reviews](#)

[GET IT NOW](#)

Pricing information
Starting at \$0.007/hour
+ Azure infrastructure costs

Categories
Compute
Security

Support
Support

Legal
License Agreement
Privacy Policy

The cost of running this product is a combination of the selected software plan charges plus the Azure infrastructure costs for the virtual machines on which you will be running this software. Your Azure infrastructure price might vary if you have enterprise agreements or other discounts.

To view pricing in a different currency, [change the billing country/region](#). Costs might vary by deployment region.

Software plan details

Ubuntu Pro 18.04 LTS

Ubuntu Pro is providing additional coverage for production environments running in the cloud

Starting at
\$0.007/hour

Pricing by virtual machine instance [Download table as CSV](#)

Show: ☒ Publisher recommendations ☐ All virtual machine instances

Region
West Europe

The publisher recommends the following 6 virtual machine instances for use with this software plan.

Plans and Pricing
This table provides the details about the plans and pricing

Virtual Machine		Configuration				Cost per hour		Total cost	
Instance	Category	Cores	RAM	Disk Space	Drive Type	Infrastructure Cost	Software Cost	Hourly	Monthly
DS11V2*	Memory Optimized	2	14GB	28GB	SSD	\$0.19	\$0.022	\$0.212	\$158.026
D2SV3*	General Purpose	2	8GB	16GB	SSD	\$0.12	\$0.022	\$0.142	\$105.946
D4SV3*	General Purpose	4	16GB	32GB	SSD	\$0.24	\$0.04	\$0.28	\$208.32
E2SV3*	Memory Optimized	2	16GB	32GB	SSD	\$0.16	\$0.022	\$0.182	\$135.706
DS1*	General Purpose	1	3.5GB	7GB	SSD	\$0.084	\$0.01	\$0.094	\$69.564
DS2*	General Purpose	2	7GB	14GB	SSD	\$0.168	\$0.022	\$0.19	\$141.658

Vessel Software Installation Guide & Server Pricing

IP-TAP nORM Monitoring System Installation and Operation Manual

Version 2 – July 2020

1	Introduction	137
2	Database and File Server Installation	137
2.1	Basic System Installation	137
2.1.1	Detailed Instructions	138
2.2	Create shared ssh keys	138
2.2.1	Detailed Instructions	139
2.3	NTP server setup	139
2.3.1	Detailed Instructions	139
2.4	Samba server setup + repository	139
2.4.1	Detailed Instructions	139
2.5	Database Configuration	140
2.5.1	Detailed Instructions	140
2.6	Cron setup + createXML configuration	141
2.7	Snort configuration directory + update checker cron	141
2.7.1	Detailed Instructions	141
2.8	Mappings file	141

4	Monitor Installation	141
4.1	Basic system installation	142
4.1.1	Detailed Instructions	142
4.2	NTP client to database server	142
4.3	Copy public key from database server	143
4.4	Snort installation	143
4.4.1	Detailed Instructions	143
4.5	Synchronise snort configuration	143
4.6	Monitor script installation	143
5	Operational Considerations	143
5.1	Mappings file	143
5.2	Snort Rules	144
6	Reference to Other Documentation	144

Introduction

This guide specifies the installation requirements for the two machines required for monitoring. The required CDs for the installation are:

- Ubuntu Server 20.04.1 LTS (support guaranteed until April 2025)
- FreeBSD Release 11.4 (June, 2020)
- Additional Software CD containing
 - MySQL Snort database initialisation script
 - XML creation script + library + sample mapping file
 - Initial snort configuration directory (including passive control alert)
 - Update Snort script
 - Monitor script + configuration file

The following sections describe the installation of, first, the Database and File Server and then the Monitor.

The IP address 10.0.0.1 will be used throughout this document to refer to the database server and 10.0.0.2 for the monitor. Replace these as required.

Where scripts are required to be configured, see the individual script for instructions.

Database and File Server Installation

For additional information, beyond this guide, see:

<http://help.ubuntu.com/6.06/ubuntu.serverguide/C/index.html>

Basic System Installation

©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.

Install the basic LAMP server from the • Ubuntu Server 20.04.1 LTS disk.

Special requirements:

- Needs 2 network ports configured
 - 1 external management address
 - 1 local IP address e.g. 10.0.0.1 (for connection to monitor)
- Additional package requirements
 - openssh-server (for remote management)
 - libhtml-parser-perl (for XML creation)
 - libdate-simple-perl (for date calculations)

For other package installation, see individual sections below.

Detailed Instructions

1. Turn on machine and insert CD (making sure the machine is set to boot from CD).
2. At the Ubuntu installation menu, choose "Install a LAMP server".
3. Choose the required language and keyboard options when prompted.
4. The basic components will then be installed.
5. If there is an available DHCP server, then the management port will be configured automatically. Otherwise, configure the network manually in the forms provided.
6. When prompted, choose an appropriate mirror of the Ubuntu archive (and give HTTP proxy information if required).
7. Select the required disk partitioning options; choosing to erase entire disk and accepting default partitioning should use the whole disk in one partition except for the swap.
8. Set clock to UTC.
9. Choose appropriate username and password.
10. The base system will then be installed (this may take some time).
11. When the installation is finished, reboot and remove the CD.
12. After the reboot, login and remove the CD option from /etc/apt/sources.list (i.e. comment out the line 'deb cdrom:...') and uncomment any other sources that have been commented.
13. Run: `sudo aptitude update && sudo aptitude dist-upgrade` to update the system.
14. Install the additional packages required using:
`sudo aptitude install openssh-server libhtml-parser-perl libdate-simple-perl`
15. Finally, add the second network configuration in /etc/network/interfaces

Create shared ssh keys

Create a pair of ssh keys with no password, for automated synchronisation between servers.

Detailed Instructions

Run the following command:

```
ssh-keygen -t dsa
```

(using the default file names and no password)

The public key will later be copied to the monitor.

NTP server setup

Setup an NTP server to keep the time of the monitor updated.

Detailed Instructions

Install the NTP server:

```
sudo aptitude install ntp-server
```

The change the default server in /etc/ntp.conf from ntp.ubuntu.com if required.

If the server (or any other settings) is changed, then restart NTP:

```
sudo /etc/init.d/ntp-server restart
```

Samba server setup + repository

Create a directory to store the XML files in.

Install a Samba Server to prove access to the directory.

Detailed Instructions

First make a directory for the XML files:

```
mkdir /mypath/xmlfiles
```

Then install Samba:

```
sudo aptitude install samba
```

Create a password for the current user:

```
smbpasswd
```

Edit the configuration file /etc/samba/smb.conf changing the workgroup to the required group, making sure the user is not in the invalid list and added the share point e.g.:

```
[share]
```

```
path = /mypath/xmlfiles  
comment = shared xml files  
browseable = yes  
writable = no
```

Comment out any other share definitions.

Finally, restart Samba:

```
sudo /etc/init.d/samba restart
```

Database Configuration

Setting up the database:

- Add remote access to connect from monitor
- Create snort user
- Create snort database and import structure
- Grant permissions for snort user on database

Detailed Instructions

Edit the MySQL configuration file `/etc/mysql/my.cnf` and remove the line:

```
bind-address = 127.0.0.1
```

Restart MySQL:

```
sudo /etc/init.d/mysql restart
```

Run MySQL:

```
mysql
```

Enter the following sequence of commands:

```
create user snort identified by 'password'; (replacing password)  
create database snort;  
use snort;  
source /pathto/create_mysql (The initialisation script on the CD)  
grant all on snort.* to snort@localhost identified by 'password';  
grant all on snort.* to snort@10.0.0.2 identified by 'password';
```

```
flush privileges;
```

Cron setup + createXML configuration

Copy the createXML.pl script and library file from the CD and edit the configuration options inside the script. Then add an item to cron, to run the script once a week.

Detailed Instructions

Edit the crontab:

```
crontab -e
```

And add the following line:

```
* * * * 1 cd createXMLpath && ./createXML.pl
```

This runs the createXML.pl script from its local directory every Monday.

Snort configuration directory + update checker cron

Copy the snort configuration directory from the CD provided (and edit the snort.conf output line, if necessary), also copy the update_snort.pl script (and edit the options as required). Add a line into the crontab to check for update requests at the desired interval.

Detailed Instructions

Edit the file snortconf/snort.conf and change the following line as required:

```
output database: alert, mysql, user=snort password=password  
dbname=snort host=10.0.0.1
```

Edit the crontab:

```
crontab -e
```

Add the following line (example for hourly checking):

```
0 * * * * cd updatesnortpath && ./update_snort.pl >/dev/null
```

Mappings file

In addition, it is necessary to enter the desired mappings from snort alerts to local target systems in the mappings file. See Operations below.

Monitor Installation

For additional information, beyond this guide, see: <http://www.freebsd.org/docs.html>

The monitor should ideally be configured to use RAID0 for the hard disk drives (to maximise disk write speed for capturing network traffic) before beginning this installation process.

Basic system installation

Install base system of FreeBSD Release 11.4 using Kern-developer with ports option.

Special requirements:

- 3 network ports
 - 1 active port with no IP (Intel NIC)
 - 1 local connection e.g. 10.0.0.2 (for communicating with database)
 - 1 external connection (for installation - can be disabled after initial installation)
- Additional packages
 - bash-3.1.10-1 (or equivalent)
- Change default shell to bash, for root user
- Permit SSH access as root

Detailed Instructions

1. Turn on the machine and insert FreeBSD installation disk.
2. Choose “Boot FreeBSD [default]” when prompted.
3. Next the machines hardware is automatically detected. This may take some time.
4. When prompted, choose the appropriate regional settings.
5. At the “sysinstall Main Menu” choose “Express” installation.
6. At the disk partitioning menu, use the default settings buy pressing 'A' then 'Q' on both pages. Also, choose the “BootMgr” option to install the FreeBSD Boot Manager.
7. Choose the “kern-developer” distribution and choose “yes” when prompted to install ports.
8. At “Installation Media”, select HTTP and then choose an appropriate site.
9. Configure the management network interface; this can be done automatically if DHCP if available.
10. The installation will now continue. This may take some time, depending on the network bandwidth and machine specification.
11. Select the following package: shells->bash_3.1.10-1 (or equivalent)
12. After giving a root password, check the sshd option to enable remote access.
13. The basic installation should now be complete. The computer will reboot. Remove the CD.
14. After the reboot, login as root and change the default shell to bash:
`chsh -s /usr/local/bin/bash root`
15. Edit /etc/ssh/sshd_config and uncomment the line #PermitRootLogin and change the 'no' to 'yes'. Then restart the ssh daemon: `/etc/rc.d/sshd restart`
16. Finally, configure the monitoring card in /etc/rc.conf

NTP client to database server

To configure the NTP client edit /etc/ntp.conf and put in the following lines:

©Copyright 2020. All Rights Reserved Dr. Phillip King-Wilson & Quantar Solutions Limited. Do not distribute without written permission. All information provided on a confidential basis & not for reuse.


```
server 10.0.0.1 primary
```

```
driftfile /var/db/ntp.drift
```

Restart the NTP daemon: `/etc/rc.d/ntpd restart`

Finally, add the following line to `/etc/rc.conf` to ensure NTP is started when the machine boots:

```
ntpd_enabled="YES"
```

Copy public key from database server

Copy the public key from the database server e.g.:

- `mkdir ~/.ssh`
- `scp user@10.0.0.1:~/.ssh/id_dsa.pub ~/.ssh/authorized_keys`

Snort installation

Compile snort from ports with MySQL support and install.

- Make log directory `/var/log/snort`

Detailed Instructions

1. Set the `http_proxy` environment variable if required.
2. `cd /usr/ports/security/snort`
3. `make` (check the MySQL option, when prompted)
4. Snort will now be compiled. There may be several messages saying that sources cannot be found; this is only a problem if the compilation fails.
5. `make install` (to install the build of snort)
6. `mkdir /var/log/snort`

Synchronise snort configuration

Type (all on one line):

- `rsync -ave ssh --delete user@10.0.0.1:/path/to/snortconf/ /usr/local/etc/snort`

Monitor script installation

Copy the monitor script (`gather.sh`) from the CD. The script can either be run manually or installed into the `rc.d` directory to be run automatically when the monitor is booted.

Operational Considerations

Mappings file

The file is a simple CSV file with one line per threat. Each line has five values:

- SID – the unique identification number assigned to this threat by SNORT1
- Alert – the name of the threat also provided by SNORT, but can be changed by the Administrator.
- Target – the `Target` attribute as needed by nORM's `Threat` tag and is provided manually by the administrator. The default value is "Unknown".
- Category – the `Category` attribute as required by nORM's `Threat` tag, again provided by the administrator. The default value is "Indiscriminate".
- Severity – the `SeverityScore` attribute as required by nORM's `Threat` tag. The default value automatically calculated from the SNORT priority value. The mapping from SNORT to nORM is 1 → 10, 2 → 7, 3 → 4, 4 → 1.

In order to determine appropriate values for this file please refer to the Mapping Targets document.

Snort Rules


To update snort rules:

1. Download the latest ruleset from <http://www.snort.org/>
2. Unpack the file
3. Copy the `rules` directory to `/path/to/snortconf` on the database machine
4. Execute the synchronisation command from section 0

Reference to Other Documentation

See also the Mapping Targets Documents

Back to Shop / Servers / Rack Servers / ProLiant DL20 Servers / HPE ProLiant DL20 Gen10 Server





HPE ProLiant DL20 Gen10 Server

Are you looking for a compact 1U server that supports workloads in a variety of environments?

The HPE ProLiant DL20 Gen10 server delivers a compact and versatile server...

[Show More](#) [QuickSpecs](#) ✓

Starting at £517.00 Exclude VAT ⓘ
As low as £13/mo 

Intel® Xeon® Scalable Processors [Compare](#) 


PowerEdge R240 Rack Server

Compute made simple

Increase performance, ability to scale, and simplify your IT with an entry-level 1U rack server designed for web hosting and multi-purpose applications.

Starting at £548.79

[View configurations](#)



Sample 50 Marine Reinsurers, Brokers & Underwriters

- | | |
|-----------------------|--|
| 1. Swiss Re | 26. Lockton |
| 2. Munich Re | 27. Samsung Fire & Marine |
| 3. AXA XL | 28. RSA Luxembourg |
| 4. Hannover Re | 29. Ed |
| 5. Lloyd's | 30. International Group |
| 6. Berkshire Hathaway | 31. Cefor |
| 7. RGA | 32. Beazley |
| 8. China RE | 33. QBE |
| 9. Korean Re | 34. Liberty Specialty Markets |
| 10. PartnerRe | 35. Zurich |
| 11. GIC Re | 36. Sedgwick |
| 12. Mapfre | 37. AFL Insurance Brokers |
| 13. Alleghany | 38. Ryan Specialty Group |
| 14. Everest Re | 39. Pioneer Underwriters |
| 15. Maiden Re | 40. Navigators |
| 16. Fairfax | 41. MS Amlin |
| 17. AXIS | 42. Novae Group |
| 18. Mitsui Sumitomo | 43. Allianz Global Corporate & Specialty |
| 19. Sampo | 44. Argo Group International Holdings |
| 20. Tokio Marine | 45. Barbican Insurance Group |
| 21. Marsh | 46. Ocean Marine |

- | | |
|-----------------------------|---------------|
| 22. Lampe & Schwartz | 47. Aviva |
| 23. Markel InternationalAon | 48. Gallagher |
| 24. Axa (Asia) | 49. GIC Re |
| 25. Ascot | 50. Mapfre |

Example Marine Software Solutions Providers

- | | |
|--------------------------|-----------------------|
| 1. Lloyds Register | 26. GT Maritime |
| 2. Spectec | 27. Hydrocomp |
| 3. Forecoast | 28. Marine Press |
| 4. ABB | 29. Oceaneering |
| 5. Siemens | 30. Marine Traffic |
| 6. ABS Management | 31. Actionseas |
| 7. Norcomms | 32. Anchorsoft |
| 8. DNV-GL | 33. Oceanis |
| 9. Thinkmarine | 34. Marine Digital |
| 10. Ocean Manager | 35. PortXchange |
| 11. SeaProc | 36. eYard |
| 12. Sertica | 37. Oceanbolt |
| 13. Marine Digital | 38. NavD |
| 14. Veson Nautical | 39. OrbitMi |
| 15. SBN Technologies | 40. OceanOps |
| 16. Big Ocean Data | 41. Boxport |
| 17. Bass | 42. Lexport |
| 18. Mariapps | 43. Traxens |
| 19. Q88 | 44. Freighthub |
| 20. Clear Lynx | 45. Rombit |
| 21. AXSmarine | 46. Nautilus Labs |
| 22. Napa | 47. MarCoPay |
| 23. Navis | 48. Marified |
| 24. Hanseatocsoft | 49. Arie Solutions |
| 25. Fortune Technologies | 50. Kongsberg Digital |

World Container Shippers and Number of Port Calls

(Calls in Europe: 35 Shippers out of 59)

1. AAL Shipping Agencies Asia, Australia 39	32. Mediterranean Shipping Company (MSC) Global 264
2. ACL Northern Europe , Eastern USA 16	33. MISC Berhad Asia, Australia, Europe , Middle East 67
3. Alaska Marine Lines Alaska 24	34. MOL Global 153
4. Alianca Asia, Americas, Northern Europe 58	35. Norasia Asia, Europe, Middle East 38
5. ANL Asia, Australia, Europe , Eastern USA 39	36. Nordo Link Sweden, Germany 2
6. Antillean Marine Shipping Corporation Caribbean 5	37. Norfolk Line Northern Europe 12
7. APL Global 150	38. Northland Services Alaska 23
8. Atlantic Cargo Northern Europe , Eastern USA 7	39. NSA Eastern and Southern USA 3
9. Atlantic Ro-Ro Carriers Northern Europe , Eastern USA 7	40. NSCSA Eastern USA, Middle East 16
10. Bermuda Container Line Bermuda, USA 2	41. NYK Global 129
11. Caribbean Feeder Services Caribbean 16	42. OOCL Asia, Australia, Europe , Middle East, North America 136
12. China Shipping Asia, Northern Europe , USA 35	43. OT Africa Line Europe , West Africa 54
13. Contenemar Spain, Northern Africa 11	44. PIL Global 122
14. COSCO Global 54	

15. Crowley Liner Services Caribbean 30 16. CSAV Global 114 17. Dole Ocean Cargo Express Europe , North America, South America 21 18. Eimskip Northern Europe , Eastern USA 15 19. Evergreen Marine Corp. Global 158 20. FESCO Asia, Northern Europe , USA 53 21. Hamburg Sud Global 115 22. Hanjin Global 88 23. Hapag-Lloyd Global 153 24. Islamic Republic of Iran Shipping Lines Asia, Europe , Middle East 40 25. K Line Global 122 26. Kent Line International Brazil, Eastern USA, Europe 22 27. King Ocean Services North America, South America 12 28. Libra Global 189 29. MACS Shipping Northern Europe , Southern Africa 30 30. Maersk Line Global 188 31. Matson Hawaii, Western USA 10	45. Regional Container Lines Asia, Australia, Middle East 63 46. Scotline Northern Europe 21 47. Seaboard Marine North America, South America 36 48. Senator Lines Asia, Europe , Middle East, South America 47 49. Star Shipping Northern Europe, Eastern USA 6 50. Totem Ocean Trailer Express Alaska 2 51. Tropical Shipping Caribbean 29 52. United Arab Shipping Company Asia, Europe , Middle East, North America 48 53. Wan Hai Lines, Ltd. Asia, Middle East, Western USA 53 54. WEC Lines Europe, East Africa, Middle East, Caribbean 57 55. West Coast Industrial Express North America, South America 18 56. Westwood Asia, Western USA 12 57. Wing Bridge Shipping Co. Caribbean 6 58. Yang Ming Asia, Europe , Middle East, North America 95 59. Zim Global 144
--	--

Initial Shipping Lines European Office Locations

MAERSK EUROPE	MSC EUROPE	CMA CGM EUROPE	HAPAG LLOYD EUROPE	HAMBURG SUD EUROPE
Albania	Albania	1. Austria	Albania	1. Austria
Algeria	Armenia	2. Belarus	1. Austria	Belarus
1. Austria	1. Austria	3. Belgium	2. Belgium	2. Belgium
Belarus	Azerbaijan	4. Bulgaria	3. Bulgaria	3. Bulgaria
2. Belgium	2. Belarus	5. Croatia	Bosnia /	4. Croatia
3. Bulgaria	3. Belgium	6. Czech Republic	Herzegovina	5. Cyprus
4. Croatia	Bosnia Herzegovina	7. Denmark	4. Croatia	6. Czech Republic
5. Cyprus	4. Bulgaria	8. Estonia	5. Cyprus	7. Denmark
6. Czech Republic	Cape Verde	9. Finland	6. Czech Rep.	8. Estonia
7. Denmark	5. Croatia	10. France	7. Denmark	9. Finland
Egypt	6. Cyprus	11. Germany	8. Estonia	10. France
8. Estonia	7. Czech Republic	12. Greece	9. Finland	11. Georgia
9. Finland	8. Denmark	13. Hungary	10. France	12. Germany
10. France	9. Estonia	14. Iceland	11. Germany	13. Greece
11. Georgia	10. Finland	15. Ireland	12. Greece	14. Hungary
12. Germany	11. France	16. Italy	13. Hungary	15. Iceland
13. Greece	12. Georgia	17. Latvia	14. Iceland	16. Ireland
14. Hungary	13. Germany	18. Lithuania	15. Ireland	17. Italy
15. Ireland	14. Greece	19. Malta	16. Italy	18. Latvia
Israel	15. Hungary	20. Montenegro	17. Latvia	19. Lithuania
16. Italy	16. Ireland	21. Netherlands	18. Lithuania	20. Malta
17. Latvia	17. Italy Le Navi	22. Norway	19. Malta	21. Netherlands
Lebanon	18. Italy Spadoni	23. Poland	20. Netherlands	22. Norway
Libya	Kazakhstan	24. Portugal	21. Norway	23. Poland
18. Lithuania	19. Latvia	25. Romania	22. Poland	24. Portugal
19. Malta	20. Lithuania	Russian Federation	23. Portugal	25. Romania
20. Montenegro	21. Luxembourg	26. Serbia	24. Romania	Russia
21. Morocco	22. Malta	27. Slovakia	25. Russian	26. Slovenia
22. Netherlands	23. Moldova	28. Slovenia	Federation	34. Spain
23. Norway	24. Montenegro	29. Spain	26. Serbia and	35. Sweden
24. Poland	25. Netherlands	30. Sweden	Montenegro	36. Switzerland
25. Portugal	26. North Macedonia	31. Switzerland	27. Slovenia	37. Turkey
26. Romania	27. Norway	32. Ukraine	28. Spain	38. Ukraine
27. Russia	28. Poland	33. United Kingdom	29. Sweden	39. United
28. Serbia	29. Portugal		30. Switzerland	Kingdom
29. Slovakia	30. Romania		31. Turkey	
30. Slovenia	Russia		32. Ukraine	
31. Spain	31. Serbia		33. United	
32. Sweden	32. Slovakia		Kingdom	
33. Switzerland	33. Slovenia			
Syria	34. Spain			
34. Tunisia	35. Sweden			
35. Turkey	36. Switzerland			
36. Ukraine	37. Turkey			
37. United Kingdom	38. Ukraine			
	39. United Kingdom			
	Uzbekistan			

Microsoft Power BI PRO Functionality at £7.50 Per User/Month

Feature/Capability	Power BI Pro
Create datasets and reports in Power BI Desktop	x
Publish datasets and reports to Power BI Service	x
Create dashboard(compilation of visuals from one or more reports)	x
Q&A natural language queries	x
Data alerts	x
E-mail subscriptions ("subscribe")	x
Export to CSV, Excel	x
Export to PowerPoint	x
Access to all data sources (unrestricted)	x
Scheduled data refresh via On-Premises Gateway in Personal Mode	Up to 8x/day
Scheduled data refresh via On-Premises Data Gateway	Up to 8x/day
DirectQuery and Analysis Services Live Connection via On-Premises Data Gateway	x
Use of streaming datasets	x
Use of custom visuals from Office Store	x
Publish to Web (public report distribution)	x
Power BI Mobile Apps	x
Cortana/Windows integration for report rendering	1GB per file
Maximum size of an imported dataset	10GB per user
Maximum data storage quota	x
Multi-tenant service	x
Third party SaaS Apps (from AppSource)	x
Integration with Azure Active Directory	x

Proof of Marine Market for Cyber Threat Quantification September 2020

Astaara adds Howard Potter as head of marine cyber

reinsurancene.ws/astaara-adds-howard-potter-as-head-of-marine-cyber/

September 14, 2020

Astaara, a newly launched insurer focusing on cyber threats in the maritime industry, has added Howard Potter as head of marine cyber.

Potter has over 25 years' industry experience and joins from RSA Group, where he served as global product director for marine.

In 2000, he moved to CNA Maritime as branch manager in Birmingham, and then to Canada in 2004 as head of marine for CNA Canada.

After three and a half years there he moved back to London, remaining with CNA until taking up his position at RSA.

'Howard is a fantastic addition to the team at Astaara. He has a wealth of industry experience both in the UK and overseas,' said Robert Dorey, CEO of Guernsey-based marine insurance and risk assessment specialists, Astaara.

Commenting on his appointment, Potter said, "This is the perfect time to be joining Astaara when risk is increasing exponentially, and solutions are needed. The company's approach to cyber solutions is refreshing and has an offering not seen elsewhere."



Newly launched Astaara gets investment from West of England P&I Club

reinsurancencn.ws/newly-launched-astaara-gets-investment-from-west-of-england-pi-club/

June 17, 2020

Astaara, a newly launched insurer focusing on cyber threats in the maritime industry, has received a significant investment from the West of England P&I Club.

Based in Guernsey, Astaara functions as an integrated insurance services and risk management advisory business, supported by a dedicated analytics capability.

Chief Executive Officer (CEO) Robert Dorey welcomed the investment from West of England P&I Club.



“This investment recognises the underlying demand for marine cyber specialist insurance services and validates the approach of Astaara in addressing the gaps in the existing marine and cyber insurance market,” he said.

Dorey continued: “The current market conditions are unparalleled in terms of health threats due to global pandemic – to ports, ships crews and head office operations. This has forced marine operators to be more reliant than ever on digitisation, and this is already against a backdrop of ever-increasing sophistication of cyber-attacks which disrupt supply chains, and stakeholders’ confidence in their investments.”

Tom Bowsher, CEO of West of England P&I Club, also commented: “The cyber solution provided by Astaara is second to none and the most comprehensive in the market – we are investing in a cyber product and a team that has a huge amount of experience.”

“Astaara clearly meets the demands of the shipowning and broader maritime community, of which we have a long and proud tradition of supporting,” Bowsher went on.

“We have full confidence in Robert and the team, and the Astaara product, which in our view is the only comprehensive and integrated cyber solution that properly aligns the service that owners need with genuine experience, expertise and commitment.”

ARTICLES OF ASSOCIATION QUANTAR SOLUTIONS LIMITED

The Companies Act 1985 (as amended)

PRIVATE COMPANY LIMITED BY SHARES

ARTICLES OF ASSOCIATION OF

OF

Quantar Solutions Limited

PRELIMINARY

1. (a) Subject as hereinafter provided, the Regulations contained in Table A of the Companies (Tables A to F) (Amendment) Regulations 1985 as amended by SI 2007/2541 and SI 2007/2826 (such Regulations hereinafter referred to as "Table A") shall apply to the Company.
- (b) Regulations 24, 35, 36, 40, 53, 62, 73 to 75 (inclusive), 77, 78, 79, 80, 81, 94 to 98 (inclusive), 111, 112 and 117 of Table A shall not apply to the Company.
- (c) "the 1985 Act" means the Companies Act 1985 including any statutory modification or re-enactment thereof for the time being in force.
- (d) "the 2006 Act" means the Companies Act 2006 and any provisions for the time being in force.
- (e) The expressions "relevant securities" and "equity securities", wheresoever appearing herein, shall bear the meanings ascribed to them by the 1985 Act.
- (f) "communication" means the same as in the Electronic Communications Act 2000.
- (g) "electronic communication" means the same as in the Electronic Communications Act 2000.
- (h) "executed" includes any mode of execution.

SHARES

2. (a) Subject to the provisions of the 1985 Act and the 2006 Act, and to the following provisions of these Articles, the Directors shall have authority to exercise any power of the Company to offer, allot or otherwise dispose of any shares in the Company, or any relevant securities, to such persons, at such times and generally on such terms and conditions as they think proper provided that insofar as the Company in General Meeting shall not have varied, renewed or revoked the said authority:
- (i) The Directors shall not be authorised to make any offer or allotment of shares in the Company, or grant any right to subscribe for, or to convert any securities into, shares in the Company if such allotment, or an allotment in pursuance of such offer or right, would or might result in the aggregate of the shares or stock in issue exceeding, in nominal value, the amount of the authorised share capital of the Company for the time being, and such limitation shall determine the maximum amount of the relevant securities which at any time remain to be allotted by the Directors hereunder.
- (ii) The period within which the said authority to allot relevant securities may be exercised shall be limited to five years, commencing upon the date of incorporation of the Company.
- (b) Any offer or agreement in respect of relevant securities, which is made prior to the expiration of such authority and in all other respects within the terms of such authority, shall be authorised to be made, notwithstanding that such offer or agreement would or might require relevant securities to be allotted after the expiration of such authority and, accordingly, the Directors may at any time allot any relevant securities in pursuance of such offer or agreement.
- (c) The authority conferred upon the Directors to allot relevant securities may at any time, by Ordinary Resolution of the Company in General Meeting, be revoked, varied or renewed (whether or not it has been previously renewed hereunder) for a further period not exceeding five years.

SHARE CAPITAL

- 3.1 The share capital of the Company at the date of adoption of these Articles is £2,000 divided into 1,000 Ordinary-A Management shares of £1.00 each and 1,000 Ordinary-B shares of £1.00 each
- 3.2 The 1,000 Ordinary-A Management shares ('A' shares) and 1,000 Ordinary-B shares ('B' shares) shall have the same rights and privileges and shall rank pari passu in all respects except as set out below.

3.3 As Regards Voting:

Each 'A' share is entitled to ten votes for each one share held. Each 'B' share is entitled to one vote for each one share held.

3.4 As Regards Income:

Should a dividend be declared by the company, the entitlement of the 'A' shareholders and the 'B' shareholders shall be consistent with the voting rights attributable to each class, such that for every £1 (or fraction of) paid to each 'A' shareholder the dividend shall be ten times greater than the dividend paid to each 'B' shareholder.

3.5 As Regards Capital:

On a winding up or on a reduction of capital involving a return of capital the assets of the Company shall be applied first in repaying to the holders of the 'A' shares and the 'B' shares the capital paid up or credited as paid up thereon and the balance of the assets of the Company shall belong to and be distributed among the holders of the 'A' shares and the 'B' shares rateably according to the ratio of 10:1 in favour of 'A' shares.

3.6 As Regards Variation of Class Rights:

The class rights of the 'A' shares cannot be varied without the consent of 75% of the 'A' shareholders at a separate class meeting and the class rights of the 'B' shares cannot be varied without the consent of 75% of the 'A' shareholders and 75% of the 'B' shareholders at a separate class meeting.

3.7 Restriction on Creation of Share Capital

No further share capital ranking in priority to the 'A' shares shall be created without the consent of a Special Resolution passed by the holders of 'A' shares passed at a separate class meeting or by the consent in writing of all the holders of 'A' shares. No further share capital ranking in priority to the 'B' shares shall be created without the consent of a Special Resolution passed by the holders of the 'A' and 'B' Shares passed at a separate class meeting or by the consent in writing of all the holders of the 'A' and 'B' shares.

3.8 Section 89(1) and Section 90(1) to (6) of the 1985 Act shall not apply to any allotment of equity securities by the Company. The shares comprised in the initial allotment by the Company shall be at the disposal of the Directors as they think proper but thereafter, unless otherwise determined by Special Resolution of the Company in General Meeting, any relevant securities shall, before they are allotted on any terms to any person, be first offered on the same or more favourable terms to each person who holds shares in the Company in the proportion which is, as nearly as practicable, equal to the proportion in nominal value held by him of the aggregate of such shares in issue.

Such offer shall be made by notice to the members specifying the number of shares offered and the period, being not less than twenty one days, within which the offer, if not accepted, will be deemed to have been declined. After the expiration of such period, or on receipt of

notice of the acceptance or refusal of every offer so made, the Directors may, subject to these Articles, dispose of such securities as have not been taken up in such manner as they think proper. The Directors may, in like manner, dispose of any such securities as aforesaid, which by reason of the proportion borne by them to the number of persons entitled to such offer as aforesaid or by reason of any other difficulty in apportioning the same, cannot in the opinion of the Directors be conveniently offered in the manner hereinbefore provided.

- 4
 - (a) No share shall be issued at a discount.
 - (b) The Company shall not have power to issue share warrants to bearer.
 - (c) Any invitation to the public to subscribe for any shares or debentures of the Company is prohibited.
5. Subject to the provisions of the 1985 Act and the 2006 Act:
 - (a) The Company may purchase any of its own shares, provided that the terms of any contract under which the Company will or may become entitled or obliged to purchase its own shares shall be authorised by Special Resolution of the Company in General Meeting before the Company enters into the contract.
 - (b) The Company shall be authorised, in respect of the redemption or purchase of any of its own shares, to give such financial assistance, or to make such payments out of capital as may be permissible in accordance with the 1985 Act and the 2006 Act, provided that any such assistance or payment shall first be approved by Special Resolution of the Company in General Meeting.
 - (c) The Company may by Special Resolution reduce its share capital and any capital redemption reserve or share premium account in any manner authorised by law.

LIEN

6. In Regulation 8 of Table A, the words "(not being a fully paid share)" shall be omitted. The Company shall have a first and paramount lien on all shares standing registered in the name of any person (whether he be the sole registered holder thereof or one of two or more joint holders) for all moneys presently payable by him or his estate to the Company.

TRANSFER OF SHARES

- 7 No 'B' share in the company or any interest therein shall be transferred or otherwise disposed of unless and until the procedures outlined in sub-Articles 7.1 to 7.4 below (inclusive) shall have been complied with
- 7.1 If at any time a member or any other person entitled to be registered in respect of a 'B' share or shares of the company (hereinafter referred to as "the proposed transferor") shall desire to transfer or otherwise dispose of any share or shares registered in his name or any interest therein, he shall first give notice (hereinafter called "the transfer notice") to the board of

directors of the company specifying the number of shares that he desires to sell or transfer ("the transfer shares").

- 7.2 Within one (1) month of receipt of the transfer notice the board of directors shall serve a copy of the transfer notice on all the 'A' shareholders (other than the proposed transferor) ("the eligible shareholders") and at the same time by written notice ("the offer notice") to all the eligible shareholders offer the transferred shares for purchase by them in the proportion to which their existing holding of 'A' shares bears in relation to all the issued shares in the company of that class. The offer notice shall specify the period (not being less than fourteen (14) days or more than twenty eight (28) days) during which the offer shall remain open for acceptance by the Eligible Shareholders ("the Availability Period"). In the event of competition for the Transfer Shares, the Transfer Shares shall be sold to the Eligible Shareholders who accept the offer (as nearly as may be and without increasing the number sold to any Eligible Shareholder beyond the number applied for by him) in proportion to their respective holdings of shares on the date when the Offer Notice is served and if, in the event of competition for the Transfer Shares and after application of the foregoing provisions of this sentence, there remain any unallocated Transfer Shares ("the Excess Shares"), the Excess Shares shall be sold to the Eligible Shareholders who accept the offer in respect of more than their proportional entitlement (as nearly as may be and without increasing the number sold to any Eligible Shareholder beyond the number applied for by him) in proportion to the respective holdings of shares of such Eligible Shareholders (calculated as aforesaid). To the extent that such offer is not accepted and there remain available any Transfer Shares such Transfer Shares shall, subject to sub-Articles 7.10 to 7.12 below, be disposed of as the Proposed Transferor sees fit.
- 7.3 Any acceptance of an offer pursuant to an Offer Notice shall be by notice in writing to the company (a "Shareholders Notice") within the availability Period and if the offer is not accepted within the Availability Period, it will be deemed to have been refused and the Proposed Transferor shall, subject to sub-Articles 7.10 to 7.12 below (inclusive), be entitled to dispose of the Transfer Shares as he sees fit.
- 7.4 If any Eligible Shareholder or Eligible Shareholders shall within the requisite periods as specified above serve a Shareholders Notice or Notices, the Board of Directors shall give notice thereof to the Proposed Transferor who shall thereupon become bound upon payment to him of the price calculated in accordance with sub-Article 7.8 below ("The Specified Price") to transfer to each purchaser those Transfer Shares which the Purchaser is entitled and bound to buy. Completion of a Transfer of Shares under this Article shall take place within fourteen (14) days after the Proposed Transferor has been notified that a Shareholders Notice has been served upon the Company in accordance with sub-Article 7.3 hereof.
- 7.5 A Transfer Notice and a Shareholders Notice once given shall be irrevocable
- 7.6 If the proposed Transferor is bound to transfer to a purchaser all or some of the Transfer Shares in accordance with the foregoing sub-Articles but makes default in transferring his shares, the company may receive the Specified Price and thereupon shall cause some person nominated by the board of Directors to transfer the shares to the purchaser on behalf of the Proposed Transferor (for which purpose any person so nominated is hereby irrevocably appointed the attorney of the Proposed Transferor) and shall cause the name of the

purchaser to be entered in the register of members as the holder of the shares and shall hold the specified Price in trust for the Proposed Transferor. The receipt of the company for the Specified Price shall be a good discharge to the purchaser and after the name of the purchaser has been entered in the register of members of the company in purported exercise of the aforesaid power the validity of the proceeding shall not be questioned by any person. The proposed Transferor shall in such case be entitled to receive the Specified Price for the shares without interest upon delivering up the certificates for the shares to the company.

- 7.7 If after service of a shareholders Notice a purchaser makes default in paying the Specified Price for the Shares on the day appointed for completion, the meeting at which completion is to take place shall be adjourned to the tenth business day thereafter at the same time and place. If the purchaser does not at the adjourned meeting pay the Specified Price for the shares, the Proposed Transferor (having being ready willing and able to complete) may, subject to sub-Articles 7.10 to 7.12 below (inclusive), dispose of the shares the subject of the Shareholders' Notice as he sees fit.
- 7.8 For the purposes of this Article 7, the Specified Price shall be Market Value which shall be such sum as is agreed between the Proposed Transferor and the Board of Directors as being a fair market value and in default of such agreement either the Proposed Transferor or the Board of Directors may refer the matter to the Auditors of the company for the time being for such auditors to prepare and issue a certificate as to the price for each of the Transfer Shares which are the subject of a Shareholders Notice such price to be calculated as a fair value of the business as a going concern on the basis of the asset value and profitability thereof as shown in the latest available audited accounts of the company and ignoring any discount which might otherwise arise by virtue of the Transfer Shares representing a minority of the shares of the Company in issue at that time and such price to be based upon a situation where there is a willing vendor and a willing purchaser and the price referred to in the said certificate shall be final and binding upon the Proposed Transferor and the Purchaser. In so certifying the said auditors shall be deemed to be acting as experts and not as arbitrators. The cost of obtaining the auditor's certificate shall be borne by (the company in any event)
- 7.9 Subject to sub-Articles 7.12 to 7.14 below (inclusive), the Directors shall not refuse to sanction or register the transfer of any share provided that the procedure outlined in sub-Articles 7.1 to 7.4 above (inclusive) has been complied with.
- 7.10 The Directors may refuse to register the transfer of a share on which the company has a lien.
- 7.11 The Directors may refuse to register a transfer unless
- (a) it is lodged at the office or at such other place as the directors may appoint and is accompanied by the certificate for the shares to which it relates and such other evidence as the directors may reasonably require to show the right of the transferor to make the transfer;
 - (b) it is in respect of only one class of shares; and
 - (c) it is in favour of not more than four transferees.
- 7.12 No share shall be transferred to any infant, bankrupt or person of unsound mind.

Reinsurance Annual Premium Workings

E.U. deadweight tonnage global share: 811 000 000 tons

Assume 80.745% of vessels are over 100 000 tons: 655 000 000 tons

E.U. Fleet: 13 407

80% : 10 725 vessels

U.S. 95.6% of E.U. fleet size: 5725

Tankers: 10.51% = 68.84 Mln tons @ \$0.5747

Container: 8.5% = 55.67 Mln tons @ \$0.3971

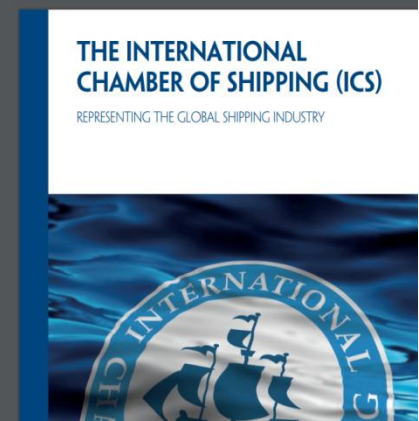
General Freight: 14.7% = 96.285 Mln tons @ \$0.3971

Bulk Carrier: 10.89% = 71.33 Mln tons @ \$0.3971

US Fleet By Country (Flags of Convenience)	Deadweight Tonnage in Millions
USA	11
Panama	320
Marshall Islands	253
Bahamas	66
World Total	1966
EU 28	811
US Total	650
US Share %	33.03%
EU Share %	41.25%
EU 28 - Total Number of Vessels	13407
EU - 28 Total Number of Vessels Container + Tanker + General + Bulk	5988
EU 28 - % of EU Total Vessels Container + Tanker + General + Bulk	44.66%
World Total Number of Vessels	94169
World Total Vessels Container + Tanker + General + Bulk	46322
Extrapolated Number of US Vessels Container + Tanker + General + Bulk	5725 (95.6% of E.U. Fleet Size)

Tonnage category	2020 rate per gt - in US cents	EU Fleet Tonnage	Reinsurance Premium PA (in cents)	\$USD (Millions) EU Fleet Annual Reinsurance	US Fleet	Reinsurance Premium PA (in cents)	\$USD (Millions) Annual Reinsurance Rate	US + EU Fleet Reinsurance Premiums P.A. \$ Mln
Persistent Oil tankers	57.47	68209000	3919971230	39.199	65214624	3747884441	37.478	
Clean Tankers	25.82	0	0	0	0	0	0	
Dry	39.71	223000000	8855330000	88.553	213210300	8466581013	84.665	
Passenger	321.61	0	0	0	0	0	0	
Chartered tankers	21.58	0	0	0	0	0	0	
Chartered dries	10.54	0	0	0	0	0	0	
Totals				127.752			122.143	249.895

MARITIME SECTOR - CYBER ASSESSMENT & CONTROLS



THE INTERNATIONAL CHAMBER OF SHIPPING (ICS)
REPRESENTING THE GLOBAL SHIPPING INDUSTRY

internet, since the devices connecting to it are unmanaged, their security status (antivirus, updates etc.) is unknown and their users could be acting maliciously, intentionally or unintentionally.

Monitoring data activity

It is important to monitor and manage systems to be aware of the networks' status and to detect unauthorised data traffic. Logging should be implemented in the firewall and ideally in all network attached devices so that in case of a breach, the responsible person can trace back the source and methodology of the attack. This will help to secure the network from any similar attacks in the future.

A network Intrusion Detection System (IDS) or Intrusion Protection System (IPS) can alert the system administrator in real-time of any attacks to the network systems. The IDS and IPS inspect data traffic entry points or both to identify known threats or to reject traffic, which does not comply with the security policy. An IPS should comply with the latest industry best practices and guidelines.

It is recommended to place a sensor on the internet-facing segment, because the public servers are a visible target to attackers. Another sensor should be placed behind the firewall, to monitor traffic between the internet and the internal network. An IDS/IPS sensor could also be placed by a remote access segment, for instance a Virtual Private Network (VPN).

Protection measures



Working together
for a safer world



Working together
For a safer world

Cyber-enabled ships

Deploying information and communications technology in shipping – Lloyd's Register's approach to assurance

First edition, February 2016

A Lloyd's Register Guidance Note



Cyber-enabled ships

ShipRight procedure assignment for cyber descriptive notes for autonomous & remote access ships

A Lloyd's Register guidance document

Version 2.0, December 2017



ShipRight

Linked Supporting Services

Procedure for the Assessment of Cyber Security for Ships and Ships Systems

September 2019

Notice No.1

Rules and Regulations for the Classification of Ships, July 2019

The status of this Rule set is amended as shown and is now to be read in conjunction with this and prior Notices. Any corrigenda included in the Notice are effective immediately.

Please note that corrigenda amends to paragraphs, Tables and Figures are not shown in their entirety.

Issue date: November 2019

Amendments to	Effective date	IACS/IMO implementation (if applicable)
Part 1, Chapter 2, Section 2	1 January 2020	N/A
Part 1, Chapter 3, Sections 2 & 11	1 January 2020	N/A

IHS MARKIT MARINE SOLUTIONS



MARITIME SOLUTIONS

Maritime Portal	5
Bespoke Data Solutions	6-8
Offline Data Solutions	9
Directories	10

TRADE SOLUTIONS

PIERS	12-13
Global Trade Atlas (GTA)	14
Global Trade Atlas Forecasting	15

ENERGY SOLUTIONS

Commodities at Sea - Crude	17
Commodities at Sea - Dry Bulk	18
Market Intelligence Network (MINT)	19

RISK SOLUTIONS

Risk & Security Capabilities	21
Trade Finance	22
Maritime Intelligence Risk Suite	23

RESEARCH & ANALYSIS CAPABILITIES

Data Analytics	25
----------------	----



Risk & Security Capabilities

Identifying and evaluating maritime risk is a challenging business for marine insurers, finance, ship owners, operators and security agencies. In today's ever-changing global landscape understanding risk implications of international events, factors affecting operations and supply chains and spotting growth opportunities is vital to business success.

IHS Markit is the leading provider of maritime & trade solutions to the insurance and security sectors, as well as many other organisations looking to assess risk, protect maritime assets and minimize supply chain disruption.

IHS Markit's maritime and trade information, intelligence and analysis helps our clients to:

- Minimise global risk by tracking all aspect of the world fleet
- Understand the global and local threats posed by the shipping fleet
- Identify and monitor any ships that represent potential threats
- Identify credentials on every ship including crew, cargo, operator and country of origin
- Build a risk profile for a single ship, owner or fleet
- Analyse current positions and historical movements to detect anomalies in trading patterns
- Improve operational efficiency and risk management
- Track ships and global maritime events

Maritime Intelligence Risk Suite

Whether your risk relates to operations, monitoring and surveillance, piracy, war or other risks that could potentially impact your business, IHS Markit Maritime Intelligence Risk Suite provides the insight you need to give your business a competitive advantage.

Powered by Sea-web™ and AISLive, the Maritime Intelligence Risk Suite integrates intelligence from IHS Markit's divisions such as Economics & Country Risk, Aerospace & Defence, and a newly developed Risk Events database. The suite provides the tools and intelligence needed to identify, evaluate, monitor and forecast potential risks to your business.

Utilize in-depth analysis to minimize global risk

- Search the risk events database for casualties, piracy and pollution events to identify high or low risk areas
- Forecast potential risks
- Forecast changes in trends that may affect future premiums and business opportunities
- Visualize, search and track real-time AIS ship positions of the global fleet when transitioning through high risk zones
- View port risk rating and evaluate port traffic
- Search details of the ship, who owns and operates it, detention history and images to construct a complete picture of any potential threat.

Understand operational risk to build situational awareness	Optimise operational efficiency to reduce costs and potential risks to operations and supply chains.
Forecast & Analyse Risk	Conduct research and gather detailed information on the global fleet, trading patterns and risk event analysis.
Identify Maritime Threats	Understand global and local threats posed by the shipping fleet and identify maritime risk events

SAMPLE GDPR / ISO DOCUMENTS

Master Document and Record List		Key:					
Doc Ref: ISF01							
Issue: 1							
Authorised By: [Name 1]							
Date: [dd/mm/yyyy]							
Document Ref	Document/Record Name	Issue	Release	Amended	Comments	Storage Location	Retention Period
ISO 27001:2013	Information technology. Security techniques. Information security management systems. Requirements	Current	2013	N/A	ISO/IEC Standard	C.	Whilst current
ISO 27002:2013	Information technology. Security techniques. Code of practice for information security controls	Current	2013	N/A	ISO/IEC Standard	C.	Whilst current
IS01	Statement of Applicability (SoA)		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS02	Acceptable Use Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS03	Access Control Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS04	Asset Management Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS05	Corporate Digital Records Preservation Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS06	Corporate Records Management Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS07	Encryption Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS08	ICT Security Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS09	Information Backup and Restore Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS10	Information Classification and Handling Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS11	Internet and Email Acceptable Use Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS12	iSMS Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS13	Operational Management		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS14	Password Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS15	Record Disposal Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS16	Scanning and Disposal Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS17	Secure Desk Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS18	Secure Email Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS19	Security Incident Management Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS20	Server Security Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS21	Supplier Security Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS22	Third Party Connection Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS23	Wireless Network Policy		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS24	Data Protection & Storage Media Handling Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS25	Desktop PC Security Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS26	Disposal of ICT Equipment Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS27	Document and Record Control Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS28	Business Continuity Policy Manual		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS29	Improvement Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS30	Incident Reporting and Management Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS31	Information Classification and Handling Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS32	Information Systems Development and Maintenance Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS33	iSMS Internal Audit Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS34	Laptop & Mobile Device Security Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS35	Malicious Software and Anti-Virus Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS36	Mobile Phone Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS37	Physical and Environmental Infrastructure Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS38	Records Appraisal Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS39	Risk Assessment and Treatment Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS40	Security Awareness Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS41	Teleworking and Mobile Working Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
IS42	Management Review Procedure		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF01	Master Document and Record List		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF02	Access Matrix (RASCI Table)		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF03	ICT Asset Inventory		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF04	Approved Hardware List		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF05	Approved Software List		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF06	Digital Preservation Risk Assessment and Action Plan		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF07	Record Management Action Plan		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF08	Nonconformity and Corrective Action Report Form		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF09	Nonconformity and Corrective Action Log		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF10	Data Restore Request Form		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF11	Backup Media Log		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF12	Disposal Log		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF13	Risk Assessment Template for The Scanning of Records and The Destruction of Their Paper Original		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF14	Disposal Authorisation Document		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF15	Security Incident Form		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF16	Mobile Device Request Form		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF17	Risk Analysis and Treatment plan		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF18	Training Matrix		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF19	Briefing Acknowledgement Form		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF20	Appraisal Record		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF21	Change Request Form		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF22	iSMS Objectives & Targets		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF23	Approved Supplier List		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF24	Supplier Questionnaire		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF25	Register of Legislation		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF26	Management Review Minutes		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]
ISF27	Internal Audit Schedule and Report		1 [dd/mm/yyyy]	N/A	Initial Release	C.	[Time]

Master Document and Record List						
			Key:			
Doc Ref:	GDPR_REC_2.8		<i>Italics: External Document</i>			
Issue:	1		Bold: Under Review			
Authorised By:	Name		Bold & Strikethrough: Deleted			
Date:	dd/mm/YYYY					
Document Ref	Document / Record Name		Issue	Release	Amended	Comments
GDPR_DOC_1.0	Data Protection Policy		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_1.1	GDPR Preparation Document		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_1.2	Data Protection Audit Guidance		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_2.0	Subject Access Request Procedure and Guidelines V1		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_2.1	Subject Access Request Procedure and Guidelines V2		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_2.2	Personal Data Breach Notification Procedure		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_2.3	Procedures for International Transfers of Personal Data		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_2.4	Data Protection Impact Assessment DPIA		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_2.5	Data Protection Impact Assessment Policy		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_2.6	Consent Procedure		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_2.7	GDPR Training Policy		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_2.8	Website Privacy and Cookies Notice		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_2.9	Information Security Policy		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_3.0	Business Continuity Plan		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_3.1	Retention and Disposal Policy		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_3.2	Retention of Records Policy		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_3.3	Risk Assessment Procedure		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_3.4	Collection of Evidence Procedure		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_3.5	Physical Entry Controls and Secure Areas Procedure		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_DOC_3.6	Responding to Information Security Reports		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_REC_1.0	Clauses for Personal Data Transfer Set 1 2001-497-ec		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_REC_1.1	Clauses for Personal Data Transfer Set 2 c2004-5721		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_REC_1.2	Clauses for Personal Data Transfer Processors c2010-593		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_REC_1.3	Rationale for a Data Protection Officer		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_REC_1.4	Data Protection Officer Job Description and Responsibilities		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_REC_1.5	Summary DPO Job Description		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_REC_1.6	ISACA GDPR Data Protection Impact Assessment Tool xls		Current	dd/mm/YYYY	N/A	Initial Release
GDPR_REC_1.7	Copyright and Reproduction Notices		Current	dd/mm/YYYY	N/A	Initial Release

Document Ref	Document / Record Name		Issue	Release	Amended	Comments	Storage Location	Retention Period
GDPR_DOC_1.0	Data Protection Policy		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_1.1	GDPR Preparation Document		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_1.2	Data Protection Audit Guidance		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_2.0	Subject Access Request Procedure and Guidelines V1		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_2.1	Subject Access Request Procedure and Guidelines V2		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_2.2	Personal Data Breach Notification Procedure		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_2.3	Procedures for International Transfers of Personal Data		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_2.4	Data Protection Impact Assessment DPIA		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_2.5	Data Protection Impact Assessment Policy		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_2.6	Consent Procedure		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_2.7	GDPR Training Policy		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_2.8	Website Privacy and Cookies Notice		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_2.9	Information Security Policy		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_3.0	Business Continuity Plan		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_3.1	Retention and Disposal Policy		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_3.2	Retention of Records Policy		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_3.3	Risk Assessment Procedure		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_3.4	Collection of Evidence Procedure		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_3.5	Physical Entry Controls and Secure Areas Procedure		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_DOC_3.6	Responding to Information Security Reports		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current

Document Ref	Document / Record Name		Issue	Release	Amended	Comments	Storage Location	Retention Period
GDPR_REC_1.0	Clauses for Personal Data Transfer Set 1 2001-497-ec		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_1.1	Clauses for Personal Data Transfer Set 2 c2004-5721		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_1.2	Clauses for Personal Data Transfer Processors c2010-593		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_1.3	Rationale for a Data Protection Officer		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_1.4	Data Protection Officer Job Description and Responsibilities		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_1.5	Summary DPO Job Description		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_1.6	ISACA GDPR Data Protection Impact Assessment Tool xls		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_1.7	Copyright and Reproduction Notices		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_1.8	Disposal Schedule		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_1.9	Example Risk Assessment Criteria for Inbound PID		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_2.0	Example Risk Assessment Criteria for Outbound PID		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_2.1	Privacy Statement Register		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_2.2	GDPR Website Legal Notices		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_2.3	Log of Information Assets for Disposal		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_2.4	User Deletion Request Form		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_2.5	Risk Assessment Process Template		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_2.6	Subject Access Request Record		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_2.7	Use of Email Notice		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_2.8	Master Document and Record List xls		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_2.9	RACI Chart V1 xls		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_3.0	RACI Chart V2 xls		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR_REC_3.1	Generic Risk Register Template xls		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current

GDPR Audit Checklists							
Cybersecurity Checklist		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
Data Controller Obligations Under the GDPR		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
Data Processor Obligations Under the GDPR		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
Data Protection Audit		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
Data Protection Impact Assessment Checklist		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
Data Retention Policy Checklist		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
DPIA Policy Annex Question Areas and Evidence		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
Example of personal Data Inventory		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
Examples of Personal Data Identifiers		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR Accountability Audit		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR Audit Checklist V2		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR Audit Checklist V1		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR Breach Response Checklist		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR Compliance Analysis Pareto Chart xls		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR Compliance Assessment Questionnaire		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR Compliance Checklist V3		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
GDPR Compliance Checklist V4		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
Information mapping Project Checklist Chart		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
Privacy Notice Checklist		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
Privacy Notice Checklist Under Articles 6 and 9		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
Privacy Policy Checklist		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current
Subject Access Request Checklist		Current	dd/mm/YYYY	N/A	Initial Release	C:	Whilst Current

LUEL RESEARCH - BACK-END SOFTWARE/HARDWARE EVALUATION & DEVELOPMENT

IP-TAP nORM Monitoring System Development

Final Report

M. S. Withall and I. W. Phillips
Computer Science
Loughborough University

Contents

1	Introduction	2
1.1	Project Goals	2
2	Hardware Used	2
2.1	Traffic Generator	2
2.2	Monitor I	3
2.3	Monitor II	3
2.4	Database and File Server	3
3	Operating System and Software Choices	3
3.1	Operating Systems	3
3.2	Software	4
4	Additional Software	6
4.1	Monitor	6
4.2	XML Output	6
4.3	Passive Control	7
5	Benchmarking	8
5.1	Test Data	8
5.2	Experimental Design	9
5.3	Hardware benchmarking	9
5.4	Software benchmarking	9
A	Test Machine Specifications	9
A.1	Traffic Generator and Monitor I	9
A.2	Monitor II	10
A.3	Database and File Server	10

1 Introduction

This report covers the development of the monitoring system to be used in conjunction with nORM. It includes details of the systems and software used and developed. In addition, some guidelines for benchmarking a system and some of the benchmarks from throughout the development process are included.

1.1 Project Goals

The goals of the project are as follows:

- To capture network traffic from an arbitrary source (at up to 1Gb/s).
- To detect and store information about attacks within the captured traffic.
- To create temporal profiles of the stored attacks.
- To export the temporal profiles in a predefined Extensible Markup Language (XML) file format for use with nORM.
- To make the XML files available via a web or file server.
- To provide documentation for the construction and configuration of the system.
- To provide hardware requirements and benchmarking information for the system.

2 Hardware Used

The following is a list of the development machines used during the project. It must be emphasised that these may not be the ‘ideal’ specification but give an idea of the performance for a given specification.

Three HP machines were used for the testing and development (one was later replaced with a higher specification machine).

2.1 Traffic Generator

One of the machines was taken as separate to the main system and used as a traffic generator. This acted as a substitute for real network data, such that we had ‘complete’ control of the traffic, for test purposes.

The machine used throughout the project was an Hewlett Packard (HP) DL140 Server (for the specification see Appendix A). In addition to the basic specification, an Intel 1000Pro (PCI-X133) Network Interface Card (NIC) was used to maximise the traffic sending capabilities of the machine *i.e.* to get as near

to 1Gb/s send rate as possible. The traffic generation is limited by the machine interrupt handling. As the bus can easily handle 1Gb/s of data, the number of packets must be the bottleneck (see benchmarks in Appendix B) therefore, for smaller packet sizes, and hence more packets per second, the performance (in terms of Gb/s) will degrade. The faster the machine the less the degradation.

2.2 Monitor I

One of the remaining machines was used as the main capture interface. The network traffic goes directly into this machine and in the final system the traffic is also analysed here.

This machine is the same (in terms of hardware specification) as the traffic generator. This includes the addition of an Intel 1000Pro NIC. The machine was later replaced with the machine described in the next subsection.

2.3 Monitor II

The replacement machine for the main capture interface was an HP DL360. The main differences were the addition of a second Central Processing Unit (CPU) and RAID0 on the hard disk drives (see Appendix A for the specification).

The addition of a second CPU allows both the capture and the analysis of the traffic on the same machine. This is still not as good as performing the tasks on separate machines, however, transferring the data between machines may be ‘impractical’; and the benefits would potentially be minimal (see benchmarks in Appendix B for more detail).

2.4 Database and File Server

The final machine was used as a database and file server; to store attack information and provide access to the XML files for nORM.

The machine was an HP ML380 (see Appendix A for the full specification).

3 Operating System and Software Choices

The following subsections describe the choices of operating systems and off-the-shelf software used in the development of the system.

3.1 Operating Systems

The initial choice of operating system was GNU/Linux (in this case Ubuntu Server version 6.06¹). The main reasons for the choice were that GNU/Linux is a proven stable platform, which supports a wide variety of hardware that is likely to be used; and the configuration and administration for the required

¹<http://www.ubuntu.com/server>

tasks is easy. GNU/Linux is also free, and Ubuntu 6.06 will be supported with security updates and fixes for 5 years from April 2006.

FreeBSD² is widely regarded as superior to GNU/Linux for high-speed network monitoring applications and, therefore, we decided to compare the performance. FreeBSD often performed better and is preferred in the final system (see the benchmarks in Appendix B). GNU/Linux was still used on the database and file server machine.

3.2 Software

This section covers the additional off-the-shelf software used within the system. All of it is free, open-source software that is in common, everyday use. None of the software has been modified in any way and none of the source code has been used in the development of additional code, therefore, there should be no licensing problems.

3.2.1 Snort

Snort³ is a simple, flexible Network Intrusion Detection System (NIDS), which fits well into the way we wanted to set the overall system up. It works in both Linux and FreeBSD; and has a large user base providing regular updates and additions to the rules for detecting attacks.

Occasionally, vulnerabilities will be found in Snort and reported on the snort website. Security patches should be applied (and other advice taken) as required.

The other serious options was Bro⁴. It is a more complicated, heavyweight NIDS, which would be harder to integrate into the overall system. Bro was not used as snort proved sufficient for the task.

3.2.2 MySQL

The MySQL database server⁵ is one of the databases supported by snort. It is easy to set up and does everything required for use with snort. The main advantage of MySQL is that it is automatically installed as part of Ubuntu Server's Linux, Apache, MySQL and PHP (LAMP) configuration, therefore, no additional administration work is required for this choice.

The other main option was PostgreSQL⁶. This would probably be better for very heavy usage (especially on multi-processor machines, as it makes better use of the extra power) or very large databases. If necessary, it can trivially replace MySQL (*i.e.* minimal adjustment to snort and the additional scripts).

²<http://www.freebsd.org/>

³<http://www.snort.org/>

⁴<http://bro-ids.org/>

⁵<http://www.mysql.com/>

⁶<http://www.postgresql.org/>

3.2.3 Bash

The Bash shell (and its associated scripting language) is used for simple scripts that glue together the larger components of the system, *e.g.* snort. It is a very lightweight, powerful scripting option, which is available in both GNU/Linux (the default shell) and FreeBSD (optional).

3.2.4 Perl

The Perl⁷ programming language was used for extracting the attack information from the database and producing the associated XML files. Perl has simple off-the-shelf libraries for accessing MySQL (and PostgreSQL) databases, and is very powerful for text processing tasks (such as creating XML). It is also installed by default in the Ubuntu LAMP configuration.

3.2.5 Apache

Apache⁸ could be used for the distribution of the XML files. Apache is one of the industry standard web servers, it is secure, stable and automatically installed as part of the Ubuntu LAMP server. As it only needs to provide access to the XML files, there will be minimal load on the system.

3.2.6 Samba

An alternative to Apache (and possible in preference to) is to use WindowsTM file sharing via Samba⁹. This will allow the machine running nORM to mount a shared directory on the file server as a local directory to access the XML files.

3.2.7 Miscellaneous tools

Other tools used are:

tcpdump — a simple program that allows network traffic to be captured from the NIC and written to a file on the hard disk¹⁰.

rsync — allows two directories to be synchronised over a network.

cron — allows commands to be run at a predefined time or at regular intervals.

ssh — allows secure remote access to a machine.

ntp — allows the time-of-day clock on each system to remain accurate and synchronised.

⁷<http://www.perl.org/>

⁸<http://httpd.apache.org/>

⁹<http://us4.samba.org/samba/>

¹⁰<http://www.tcpdump.org/>

4 Additional Software

In addition to the off-the-shelf software and tools, it was necessary to write several scripts to provide the missing functionality and to glue all of the tools together.

4.1 Monitor

A bash script was written for the monitor machine to capture, store and analyse the network traffic. This script is installed as `gather.sh`.

The first stage is to gather the network traffic using `tcpdump` for a specified number of seconds (or packets). This is done to minimise the loss of packets that would occur by having `snort` capture the traffic directly. If `snort` were capturing the packets, bursts of high traffic rate, in conjunction with the analysis of the packets, would cause more packets to be dropped. The packets are stored on the hard disk by `tcpdump`.

The file is then passed to `snort`, which detects the attacks within the traffic and store the information about them in the database. `Snort` is a separate process run using the ‘nice’ program, which gives priority to other processes. As it doesn’t need to work in ‘real-time’, this approach will minimise the impact on the `tcpdump` process.

This script can be placed in the `/etc/rc.d` directory, so that it runs automatically when the machine is booted or run manually, as required.

4.1.1 False-Positive Reduction

One major problem with NIDS, in general, is that there tends to be a large number of *false-positives* (alerts that are generated erroneously).

Two possible approaches to limiting the impact are:

1. to have a custom `snort` configuration that is finely tailored to the network being monitored;
2. to train an ‘expert system’ for the particular network being monitored, based on the actions of the network administrator.

Neither of these solutions are ideal, as they require a lot of work to set up, maintain and are not general purpose (*i.e.* won’t function correctly on a different network) and won’t completely eliminate false-positives.

Further research is required on this area, in the direction of unsupervised learning, in the interim option 1 would be recommended.

4.2 XML Output

On a weekly (or 4-weekly) basis, an XML file (conforming to the supplied schema) is generated from the `snort` alerts database. This is performed by a Perl script.

A list of alerts is extracted from the database from within a specified time window, with the count of each type of attack binned in one hour bins (this is the default value and can be configured based on the expected network traffic). Each alert is then mapped to a threat name, a category (directed or indiscriminate) and a severity. This information is provided by the administrator of the system and reflects the IT infrastructure being monitored. In the case where no mapping has been provided the threat is listed as “Unknown” and the Snort priority is assigned. The severity score (called ‘priority’ in snort) is converted from the Snort ratings of 1–4 (with 1 being the highest) to the nORM value range of 1–10 (with 10 being the highest).

This script is run at the desired interval, using cron, and the results stored in a known location on the file server. The file server directory is shared in a manner that can be mounted as a directory on the machine running nORM (*i.e.* using Samba (Windows file sharing)).

4.3 Passive Control

A passive control mechanism was used to update the snort configuration within the system.

The snort configuration is stored on the LAMP server and all adjustments are made here. This is synchronised with the monitor when a request is made to do so.

To synchronise the configuration, an Internet Control Message Protocol (ICMP) packet containing the predefined updated string (*e.g.* ‘updatesnort-now’) is sent anywhere on the monitored network, such that it is visible to the monitor. If using the ping tool to send the update request, the update string must be no longer than 16 characters.

An additional snort rule was written to detect this packet and when snort is run on the traffic an alert is stored in the database, with an unused priority value (13); this is ignored by the XML file generator.

The database is regularly polled to see if an update is required. This polling interval should be related to the snort frequency (as update requests are only detected when snort is run). If there is an update request newer than the previous logged, then the snort configuration is synchronised (using rsync) with the monitor and the new update time stored in the log.

This method is secure as a malicious attacker can only request an update from the monitored network, not specify what that update contains. As the update is processed only when the polling detects the requirement, it won’t be subject to a denial-of-service attack as only one update per polling interval will occur at most. The only way the monitoring system may be attacked is if the management network is compromised.

5 Benchmarking

This section covers the tests used to evaluate the performance of the hardware and software used for the NIDS.

5.1 Test Data

Consists of two sets of data from Defense Advanced Research Projects Agency (DARPA) and one each from two different honeypots. A honeypot is a machine especially placed on the Internet to attract malicious traffic.

5.1.1 1999 DARPA week 1, Monday (outside)

The DARPA traffic¹¹ was created using a simulation network, which gathered traffic for approximately twenty-two hours a day. The traffic from this first week is free from any attacks.

The first packet arrived at 08:00:02 on Monday, March 1 and the last packet arrived at 06:00:02 on Tuesday, March 2. There are a total of 1,362,869 packets and 302,026,432 bytes of data. This is an average packet size of approximately 222 bytes.

5.1.2 1999 DARPA week 2, Monday (outside)

The traffic from the second week contains attacks.

This first packet arrived at 08:00:01 on Tuesday, March 8 and the last packet arrived at 06:00:49 on Wednesday, March 9. There are a total of 1,337,777 packets and 307,917,628 bytes of data. This is an average packet size of approximately 230 bytes.

5.1.3 Small honeypot data set (12 IP addresses)

This data set is taken from traffic gathered by a honeypot emulating 12 Internet Protocol (IP) addresses. The traffic was captured on August 26 2006 (for the full 24 hour period). There are a total of 48,087 packets and 4,086,763 bytes of data. This is an average packet size of approximately 85 bytes. As this is a honeypot, there is no legitimate traffic and hence all traffic should be classified as malicious by the NIDS.

5.1.4 Large honeypot data set (1024 IP addresses)

This data set is taken from another honeypot, this time emulating 1024 IP addresses. The traffic was captured on October 10 2006. There are a total of 27,156,530 packets and 1,849,752,543 bytes of data. This is an average packet size of approximately 68 bytes.

¹¹http://www.ll.mit.edu/IST/ideval/data/1999/1999_data_index.html

5.2 Experimental Design

There are two aspects to the benchmarking. The first is to test the performance capabilities of the monitoring hardware (including the handling of the number of packets arriving per second and writing them to disk). The second is to test the performance of set of software tools running on the monitor.

5.3 Hardware benchmarking

There are two types of test. The first is using fixed size User Datagram Protocol (UDP) packets varying from 100 bytes to 1500 bytes (in 100 byte increments) at maximum send rate. This is used to test the effect of number of packets per second on the monitoring. The second test is to replay the four data sets described in Section 5.1 at varying data rates to test the effect of real data on the monitor. The varying of the data rate will show how dropped packets are affected. These tests can be set to capture to `/dev/null` (effectively discarding the packets when received) or capturing to file, which tests the effect of writing to the hard disk.

The information being gathered on the above tests are the number of packets captured, dropped and missing (*e.g.* lost in the network). From this we can infer the baseline capturing capabilities of the monitor hardware, before trying the monitoring system on top.

5.4 Software benchmarking

The hardware benchmarks give the maximum expected performance of the system. Essentially the same tests can be run with the full system and the difference will show the effect that the additional software has on performance. In addition to the previous defined measurements, the number of alerts can be gathered for each test set and their variance at different data rates. Also as the snort analysis is run ‘offline’ the time that this takes can be measured and compared to the capture window.

A Test Machine Specifications

The following are the specifications of the three different HP servers used in the development process.

A.1 Traffic Generator and Monitor I

- HP DL140
- 3.4GHz Xeon (1MB Cache)
- 3GB 400MHz RAM
- 2 x 80GB HDD

- Intel Pro 1000 PCI-X133 NIC

A.2 Monitor II

- HP DL360
- 2 x 3.2GHz Xeon (2MB Cache) Hyper-Threading
- 2GB 400MHz DDR2 PC3200 ECC RAM (as 2 DIMMS)
- 2 x 72.8GB Pluggable U320 SCSI 15000rpm HDD
- Hardware PCI-X RAID Controller
- 2 x Onboard Broadcom 1Gb/s Ethernet NIC
- Intel Pro 1000 PCI-X133 NIC

A.3 Database and File Server

- HP ML380
- 3GHz Xeon (2MB Cache)
- 3GB 400MHz RAM
- 3 x 140GB HDD

B Complete Benchmarks

The following tables show the results of various tests and benchmarks carried out during the development process.

Packet size	Sent	Captured	Dropped	Missing	Utilisation (%)	Received (%)	Dropped (%)	Packets per sec
1500	4,914,419	4,914,419	0	0	98.2884	100.0000	0.0000	81,906.98
1400	5,259,037	5,259,037	0	0	98.1687	100.0000	0.0000	87,650.62
1300	5,655,669	5,655,658	11	0	98.0316	99.9998	0.0002	94,261.15
1200	6,116,982	6,116,982	0	0	97.8717	100.0000	0.0000	101,949.70
1100	6,660,243	6,660,243	0	0	97.6836	100.0000	0.0000	111,004.05
1000	7,309,118	7,309,118	0	0	97.4549	100.0000	0.0000	121,818.63
900	8,098,733	8,098,201	532	0	97.1848	99.9934	0.0066	134,978.88
800	9,075,941	8,837,735	238,206	0	96.8100	97.3754	2.6246	151,265.68
700	9,378,176	7,448,368	1,929,808	0	87.5296	79.4224	20.5776	156,302.93
600	9,280,860	7,869,540	1,411,320	0	74.2469	84.7932	15.2068	154,681.00
500	9,612,737	6,648,734	2,964,003	0	64.0849	69.1659	30.8341	160,212.28
400	9,741,978	6,446,601	3,295,377	0	51.9572	66.1734	33.8266	162,366.30
300	9,886,648	6,048,300	3,838,348	0	39.5466	61.1764	38.8236	164,777.47
200	9,977,165	5,800,145	4,177,020	0	26.6058	58.1342	41.8658	166,286.08
100	10,262,223	5,346,792	4,915,431	0	13.6830	52.1017	47.8983	171,037.05
Random	8,448,457	8,447,063	1,394	0	Unknown	99.9835	0.0165	140,807.62

Table 1: The results from testing Monitor I (running Linux) with the Broadcom NIC. UDP packets of fixed size (in 100 byte steps) are sent for 60 seconds. The test highlights how the number of dropped packets is affected by the number of packets sent.

Packet size	Sent	Captured	Dropped	Missing	Utilisation (%)	Received (%)	Dropped (%)	Packets per sec
1500	4,914,805	4,914,149	0	656	98.2961	99.9867	0.0000	81,913.42
1400	5,259,120	5,259,120	0	0	98.1702	100.0000	0.0000	87,652.00
1300	5,655,759	5,655,734	25	0	98.0332	99.9996	0.0004	94,262.65
1200	6,117,050	6,117,033	17	0	97.8728	99.9997	0.0003	101,950.83
1100	6,660,345	6,660,241	104	0	97.6851	99.9984	0.0016	111,005.75
1000	7,309,488	7,308,843	645	0	97.4598	99.9912	0.0088	121,824.80
900	8,098,829	8,097,961	868	0	97.1859	99.9893	0.0107	134,980.48
800	8,901,336	8,899,296	2,040	0	94.9476	99.9771	0.0229	148,355.60
700	8,988,560	8,983,004	5,556	0	83.8932	99.9382	0.0618	149,809.33
600	9,034,764	9,031,550	3,214	0	72.2781	99.9644	0.0356	150,579.40
500	9,074,701	9,067,879	5,721	1101	60.4980	99.9248	0.0630	151,245.02
400	9,127,429	9,123,786	3,643	0	48.6796	99.9601	0.0399	152,123.82
300	9,303,912	9,294,603	9,309	0	37.2156	99.8999	0.1001	155,065.20
200	9,439,019	9,436,100	2,919	0	25.1707	99.9691	0.0309	157,316.98
100	9,740,239	9,740,239	0	0	12.9870	100.0000	0.0000	162,337.32
Random	8,039,863	8,037,675	2,188	0	Unknown	99.9728	0.0272	133,997.72

Table 2: The same test as Table 1 with the Intel NIC. Note the considerable reduction in dropped packets. The move from onboard networking to a dedicated PCI-X interface is likely to contribute to the improved performance.

Packet size	Sent	Captured	Dropped	Missing	Utilisation (%)	Received (%)	Dropped (%)	Packets per sec
1500	4,909,531	4,909,007	48	476	98.1906	99.9893	0.0010	81,825.52
1400	5,253,599	5,253,491	48	60	98.0672	99.9979	0.0009	87,559.98
1300	5,649,716	5,649,603	53	60	97.9284	99.9980	0.0009	94,161.93
1200	6,110,513	6,110,440	13	60	97.7682	99.9988	0.0002	101,841.88
1100	6,656,338	6,656,308	0	30	97.6263	99.9995	0.0000	110,938.97
1000	7,301,523	7,301,400	63	60	97.3536	99.9983	0.0009	121,692.05
900	8,089,953	8,089,836	57	60	97.0794	99.9986	0.0007	134,832.55
800	8,825,112	8,824,882	170	60	94.1345	99.9974	0.0019	147,085.20
700	8,996,501	8,996,196	245	60	83.9673	99.9966	0.0027	149,941.68
600	9,028,838	9,028,476	302	60	72.2307	99.9960	0.0033	150,480.63
500	9,040,150	9,039,771	319	60	60.2677	99.9958	0.0035	150,669.17
400	9,140,309	9,139,661	588	60	48.7483	99.9929	0.0064	152,338.48
300	9,286,948	9,286,467	451	30	37.1478	99.9948	0.0049	154,782.47
200	9,500,883	9,499,664	1,129	90	25.3357	99.9872	0.0119	158,348.05
100	9,744,643	9,742,751	1,808	84	12.9929	99.9806	0.0186	162,410.72
Random	8,108,416	8,108,160	196	60	Unknown	99.9968	0.0024	135,140.27

Table 3: The same test as in Table 2 but this time running FreeBSD. Another improvement in the packet capture, although some packets appear not to arrive at the NIC.

Packet size	Sent	Captured	Dropped	Missing	Utilisation (%)	Received (%)	Dropped (%)	Packets per sec
1500	4,914,698	4,912,760	1,556	382	98.2940	99.9606	0.0317	81,911.63
1400	5,259,157	5,257,431	1,726	0	98.1709	99.9672	0.0328	87,652.62
1300	5,655,746	5,653,585	2,161	0	98.0329	99.9618	0.0382	94,262.43
1200	6,117,062	6,114,764	2,298	0	97.8730	99.9624	0.0376	101,951.03
1100	6,660,325	6,657,823	2,502	0	97.6848	99.9624	0.0376	111,005.42
1000	7,309,481	7,306,581	2,900	0	97.4597	99.9603	0.0397	121,824.68
900	8,098,811	8,095,677	3,134	0	97.1857	99.9613	0.0387	134,980.18
800	8,775,403	8,771,954	3,449	0	93.6043	99.9607	0.0393	146,256.72
700	8,967,951	8,964,141	3,810	0	83.7009	99.9575	0.0425	149,465.85
600	9,003,134	8,999,472	3,662	0	72.0251	99.9593	0.0407	150,052.23
500	9,019,654	9,016,038	3,616	0	60.1310	99.9599	0.0401	150,327.57
400	9,078,017	9,074,312	3,705	0	48.4161	99.9592	0.0408	151,300.28
300	9,302,583	9,298,899	3,684	0	37.2103	99.9604	0.0396	155,043.05
200	9,512,069	9,508,432	3,637	0	25.3655	99.9618	0.0382	158,534.48
100	9,756,785	9,752,860	3,925	0	13.0090	99.9598	0.0402	162,613.08
Random	8,654,453	8,650,840	3,613	0	Unknown	99.9583	0.0417	144,240.88

Table 4: The same as the test from Table 3 but this time using Monitor II and writing the packets to the RAID0 hard disk drive. This causes a small percentage of dropped packets, mainly due to writing the packets to disk.

Packet size	Sent	Captured	Dropped	Missing	Utilisation (%)	Received (%)	Dropped (%)	Packets per sec
1500	8,684,714	8,680,073	4,647	-6	17.3694	99.9466	0.0535	144,745.23
1400	8,663,803	8,654,238	9,572	-7	16.1724	99.8896	0.1105	144,396.72
1300	8,951,364	8,942,417	8,950	-3	15.5157	99.9000	0.1000	149,189.40
1200	8,986,632	8,977,587	9,045	0	14.3786	99.8994	0.1006	149,777.20
1100	9,273,583	9,265,108	8,481	-6	13.6013	99.9086	0.0915	154,559.72
1000	9,351,104	9,342,316	8,788	0	12.4681	99.9060	0.0940	155,851.73
900	9,586,887	9,577,159	9,732	-4	11.5043	99.8985	0.1015	159,781.45
800	9,768,124	9,758,762	9,367	-5	10.4193	99.9042	0.0959	162,802.07
700	10,003,246	9,993,979	9,268	-1	9.3364	99.9074	0.0926	166,720.77
600	10,073,176	10,064,053	9,124	-1	8.0585	99.9094	0.0906	167,886.27
500	10,540,545	10,530,097	10,450	-2	7.0270	99.9009	0.0991	175,675.75
400	10,451,544	10,441,294	10,252	-2	5.5742	99.9019	0.0981	174,192.40
300	10,888,632	10,877,939	10,696	-3	4.3555	99.9018	0.0982	181,477.20
200	11,891,167	11,879,418	11,749	0	3.1710	99.9012	0.0988	198,186.12
100	12,555,234	12,542,940	12,296	-2	1.6740	99.9021	0.0979	209,253.90
Random	9,888,955	9,884,422	4,535	-2	Unknown	99.9542	0.0459	164,815.92

Table 5: This is a comparative test using a local test network running at 10Gb/s (the same tests as in Tables 1 to 4). The additional packets are due to the connection between the packet generator and the monitor not being a dedicated link.

Packet size	Sent	Captured	Dropped	Missing	Utilisation (%)	Received (%)	Dropped (%)	Packets per sec
1500	11,175,734	11,163,284	12,452	-2	22.3515	99.8886	0.1114	186,262.23
1400	11,254,669	11,242,905	11,765	-1	21.0087	99.8955	0.1045	187,577.82
1300	11,483,822	11,471,197	12,625	0	19.9053	99.8901	0.1099	191,397.03
1200	11,577,323	11,565,205	12,123	-5	18.5237	99.8953	0.1047	192,955.38
1100	11,842,060	11,829,190	12,873	-3	17.3684	99.8913	0.1087	197,367.67
1000	11,915,069	11,908,384	6,685	0	15.8868	99.9439	0.0561	198,584.48
900	12,221,138	12,214,575	6,568	-5	14.6654	99.9463	0.0537	203,685.63
800	12,208,432	12,195,260	13,175	-3	13.0223	99.8921	0.1079	203,473.87
700	12,650,376	12,636,883	13,496	-3	11.8070	99.8933	0.1067	210,839.60
600	12,588,886	12,575,527	13,359	0	10.0711	99.8939	0.1061	209,814.77
500	12,791,387	12,777,807	13,585	-5	8.5276	99.8938	0.1062	213,189.78
400	12,792,942	12,778,675	14,270	-3	6.8229	99.8885	0.1115	213,215.70
300	13,238,894	13,224,147	14,747	0	5.2956	99.8886	0.1114	220,648.23
200	15,611,530	15,595,035	16,500	-5	4.1631	99.8943	0.1057	260,192.17
100	16,116,974	16,099,969	17,008	-3	2.1489	99.8945	0.1055	268,616.23
Random	12,243,527	12,230,411	13,116	0	Unknown	99.8929	0.1071	204,058.78

Table 6: The same 10Gb/s test as Table 5 but this time with multiple sending threads to generate more traffic.

Packet size	Sent	Captured	Dropped	Missing	Utilisation (%)	Received (%)	Dropped (%)	Packets per sec
1500	4,914,435	1,183,587	3,730,856	-8	98.2887	24.0839	75.9163	81,907.25
1400	5,259,460	1,183,584	4,074,999	877	98.1766	22.5039	77.4794	87,657.67
1300	5,655,668	1,210,786	4,444,882	0	98.0316	21.4084	78.5916	94,261.13
1200	6,116,993	1,180,437	4,936,564	-8	97.8719	19.2977	80.7025	101,949.88
1100	6,660,238	1,109,064	5,551,174	0	97.6835	16.6520	83.3480	111,003.97
1000	7,309,342	1,060,172	6,249,170	0	97.4579	14.5043	85.4957	121,822.37
900	8,098,747	909,925	7,188,822	0	97.1850	11.2354	88.7646	134,979.12
800	9,077,315	741,392	8,335,925	-2	96.8247	8.1675	91.8325	151,288.58
700	9,382,818	684,165	8,698,653	0	87.5730	7.2917	92.7083	156,380.30
600	9,416,330	729,529	8,686,801	0	75.3306	7.7475	92.2525	156,938.83
500	9,656,619	740,301	8,916,318	0	64.3775	7.6663	92.3337	160,943.65
400	9,761,258	829,114	8,932,144	0	52.0600	8.4939	91.5061	162,687.63
300	9,895,393	947,826	8,947,573	-6	39.5816	9.5785	90.4216	164,923.22
200	10,017,294	1,126,363	8,890,990	-59	26.7128	11.2442	88.7564	166,954.90
100	10,244,853	1,534,397	8,710,515	-59	13.6598	14.9772	85.0233	170,747.55
Random	8,459,155	1,157,612	7,301,588	-45	Unknown	13.6847	86.3158	140,985.92

Table 7: The same traffic as generated in Tables 1 to 6 with Monitor I running Linux with the Broadcom NIC but this time capturing using Snort with a minimal set of rules, *e.g.* no flow reconstruction. There are a very large number of dropped packets at this packet rate.

Packet size	Sent	Captured	Dropped	Missing	Utilisation (%)	Received (%)	Dropped (%)	Packets per sec
1500	4,914,915	1,155,999	3,757,919	997	98.2983	23.5202	76.4595	81,915.25
1400	5,259,604	1,149,389	4,109,049	1166	98.1793	21.8531	78.1247	87,660.07
1300	5,655,672	1,189,793	4,465,879	0	98.0316	21.0372	78.9628	94,261.20
1200	6,116,996	1,193,605	4,923,391	0	97.8719	19.5129	80.4871	101,949.93
1100	6,660,242	1,133,845	5,526,397	0	97.6835	17.0241	82.9759	111,004.03
1000	7,309,124	1,074,553	6,234,571	0	97.4550	14.7015	85.2985	121,818.73
900	8,098,743	942,707	7,156,036	0	97.1849	11.6402	88.3598	134,979.05
800	9,077,479	782,668	8,294,811	0	96.8264	8.6221	91.3779	151,291.32
700	9,391,311	738,822	8,652,489	0	87.6522	7.8671	92.1329	156,521.85
600	9,378,321	813,630	8,564,691	0	75.0266	8.6756	91.3244	156,305.35
500	9,892,756	740,795	9,151,002	959	65.9517	7.4883	92.5020	164,879.27
400	9,950,680	853,007	9,097,673	0	53.0703	8.5723	91.4277	165,844.67
300	9,972,390	973,729	8,998,661	0	39.8896	9.7642	90.2358	166,206.50
200	10,197,816	966,356	9,231,525	-65	27.1942	9.4761	90.5245	169,963.60
100	10,299,655	1,242,492	9,057,229	-66	13.7329	12.0634	87.9372	171,660.92
Random	8,641,666	1,122,987	7,518,723	-44	Unknown	12.9950	87.0055	144,027.77

Table 8: The same test as Table 7 but with the full default Snort configuration, *i.e.* flow reconstruction, many signatures. This doesn't make much difference as there are no flows to reconstruct as all the traffic is UDP.

	Duration	Captured	Dropped	Missing	Utilisation (%)	Received (%)	Dropped (%)	Packets per sec
TCPDump	23.86	4,709,011	67,963	31,726	13.7025	97.9269	1.4133	201,538.14
Snort Simple	21.49	4,458,143	319,222	31,335	15.2136	92.7099	6.6384	223,764.54
Snort Full	18.11	274,822	4,504,431	29,447	18.0531	5.7151	93.6725	265,527.33
Snort Mysql	18.23	278,902	4,500,081	29,717	17.9342	5.7999	93.5821	263,779.48
Snort Mysql	38.50	479,673	1,197	0	0.8492	99.7511	0.2489	12,490.13
Snort Mysql	48.12	480,380	490	0	0.6794	99.8981	0.1019	9,993.14

Table 9: This tests different configurations of Snort with Monitor I and the Broadcom NIC, running Linux. This time real traffic is used from the Small Honeypot data set. The Honeypot data is repeated 100 times for the fast packet rates (4,808,700 packets sent and 408,676,300 bytes) and 10 times for the two slow tests (480,870 packets and 40,867,630 bytes). There is an average packet size of 84.99 bytes. This suggests that around 12,500 packets per second may be the limit of performance with this configuration.

	Duration	Captured	Dropped	Missing	Utilisation (%)	Received (%)	Dropped (%)	Packets per sec
TCPDump	30.44	4,808,700	0	0	10.7405	100.0000	0.0000	157,973.06
Snort Simple	30.38	4,566,658	242,042	0	10.7617	94.9666	5.0334	158,285.06
Snort Full	30.76	307,256	4,501,444	0	10.6288	6.3896	93.6104	156,329.65
Snort Mysql	30.38	313,957	4,494,743	0	10.7617	6.5289	93.4711	158,285.06
Snort Mysql	38.50	478,474	2,396	0	0.8492	99.5017	0.4983	12,490.13
Snort Mysql	48.12	478,689	2,181	0	0.6794	99.5464	0.4536	9,993.14

Table 10: This is the same test as Table 9 but this time with the Intel NIC. The performance is slightly worse than the Broadcom but without the missing packets.

	Duration	Captured	Dropped	Missing	Utilisation (%)	Received (%)	Dropped (%)	Packets per sec
TCPDump	30.41	4,808,113	560	27	10.7511	99.9878	0.0116	158,128.90
Snort Full	30.62	3,719,198	1,089,447	55	10.6774	77.3431	22.6557	157,044.42
Snort Mysql	30.42	3,483,423	1,325,241	36	10.7476	72.4400	27.5592	158,076.92
Snort Mysql	38.50	480,844	26	0	0.8492	99.9946	0.0054	12,490.13
Snort Mysql	48.11	480,870	0	0	0.6796	100.0000	0.0000	9,995.22

Table 11: This test is the same as in Table 10 but using FreeBSD rather than Linux. Also, the Snort Simple test has been omitted. Due to a bug the final three rows don't appear to have stored anything in the database but they are included for completeness.

	Duration	Captured	Dropped	Missing	Utilisation (%)	Received (%)	Dropped (%)	Packets per sec
TCPDump	30.40	4,804,979	3,721	0	10.7546	99.9226	0.0774	158,180.92
Snort Full	30.92	4,029,990	778,710	0	10.5738	83.8062	16.1938	155,520.70
Snort Mysql	30.95	1,632,676	3,176,024	0	10.5635	33.9525	66.0475	155,369.95
Snort Mysql	38.49	466,384	14,486	0	0.8494	96.9875	3.0125	12,493.37
Snort Mysql	48.12	468,228	12,642	0	0.6794	97.3710	2.6290	9,993.14

Table 12: The same test as Table 11 but this time with Monitor II and logging alerts to the database works in the final three rows. There is a significant improvement over the results for Linux.

Packet rate	Sent	Received	Dropped	Missing	Received (%)	Dropped (%)	Alerts	Logged	Alerts (%)
1000	1,337,777	1,337,536	0	241	99.9820	0.0000	3195	3209	100.0000
1000	1,337,777	1,337,536	0	241	99.9820	0.0000	3194	3208	99.9687
2500	1,337,777	1,337,465	71	241	99.9767	0.0053	3148	3185	98.5290
5000	1,337,777	1,337,179	357	241	99.9553	0.0267	3104	3599	97.1518
10000	1,337,777	1,336,342	1,203	232	99.8927	0.0899	3059	3400	95.7433
15000	1,337,777	1,332,432	5,173	172	99.6005	0.3867	3008	3427	94.1471
20000	1,337,777	1,306,014	31,609	154	97.6257	2.3628	2971	2988	92.9890
25000	1,337,777	1,255,682	81,959	136	93.8633	6.1265	2909	2914	91.0485
30000	1,337,777	1,170,096	167,578	103	87.4657	12.5266	2753	2758	86.1659
35000	1,337,777	1,081,690	255,969	118	80.8573	19.1339	2416	2420	75.6182
40000	1,337,777	1,012,426	325,254	97	75.6797	24.3130	2273	2780	71.1424
45000	1,337,777	933,216	404,458	103	69.7587	30.2336	2040	2045	63.8498
50000	1,337,777	863,093	474,650	34	64.5170	35.4805	1843	1861	57.6839

Table 13: This test uses the DARPA Week 2 data to show the effect of dropped packets on the number of alerts generated. Running the data set directly through Snort produces: 1,337,536 packets processed, 3169 alerts, 3169 logged.

PPS	Sent	Drops to /dev/null	Drops to file	Null drops (%)	File drops (%)
5000	1362869	0	0	0.0000	0.0000
10000	1362869	0	177	0.0000	0.0130
20000	1362869	4	1224	0.0003	0.0898
30000	1362869	36	5078	0.0026	0.3726
40000	1362869	246	12655	0.0181	0.9286
50000	1362869	298	20320	0.0219	1.4910
60000	1362869	395	29149	0.0290	2.1388
70000	1362869	613	34753	0.0450	2.5500
80000	1362869	971	46952	0.0712	3.4451
90000	1362869	976	58699	0.0716	4.3070
100000	1362869	586	60488	0.0430	4.4383
110000	1362869	1285	74951	0.0943	5.4995
120000	1362869	769	72815	0.0564	5.3428
130000	1362869	984	77980	0.0722	5.7218
140000	1362869	940	74141	0.0690	5.4401
150000	1362869	1181	80049	0.0867	5.8736

Table 14: This test compares the writing packets to disk and discarding packets on Monitor I running Linux using DARPA Week 1 traffic. Writing to disk has a significant impact on the performance.

PPS	Sent	Drops to /dev/null	Drops to file	Null drops (%)	File drops (%)
5000	1362869	0	0	0.0000	0.0000
10000	1362869	0	0	0.0000	0.0000
20000	1362869	269	505	0.0197	0.0371
30000	1362869	459	822	0.0337	0.0603
40000	1362869	633	876	0.0464	0.0643
50000	1362869	424	0	0.0311	0.0000
60000	1362869	314	433	0.0230	0.0318
70000	1362869	0	0	0.0000	0.0000
80000	1362869	212	0	0.0156	0.0000
90000	1362869	300	1059	0.0220	0.0777
100000	1362869	172	468	0.0126	0.0343
110000	1362869	922	478	0.0677	0.0351
120000	1362869	282	0	0.0207	0.0000
130000	1362869	0	0	0.0000	0.0000
140000	1362869	0	0	0.0000	0.0000
150000	1362869	0	0	0.0000	0.0000

Table 15: This is the same as Table 14 but using FreeBSD. The performance is much improved.

PPS	Sent	Drops to /dev/null	Drops to file	Null drops (%)	File drops (%)
5000	1362869	0	0	0.0000	0.0000
10000	1362869	0	0	0.0000	0.0000
20000	1362869	0	0	0.0000	0.0000
30000	1362869	0	0	0.0000	0.0000
40000	1362869	0	0	0.0000	0.0000
50000	1362869	90	0	0.0066	0.0000
60000	1362869	226	509	0.0166	0.0373
70000	1362869	614	0	0.0451	0.0000
80000	1362869	658	332	0.0483	0.0244
90000	1362869	639	817	0.0469	0.0599
100000	1362869	0	0	0.0000	0.0000
110000	1362869	0	0	0.0000	0.0000
120000	1362869	0	346	0.0000	0.0254
130000	1362869	0	381	0.0000	0.0280
140000	1362869	1921	0	0.1410	0.0000
150000	1362869	0	0	0.0000	0.0000

Table 16: This test is the same as Table 15 but this time using Monitor II with RAID0. Writing to the hard disk has a negligible effect now.

FINANCIAL STATEMENTS

PHASE 1 FINANCIAL PROJECTIONS

PERIOD 01/01/2021 – 31/12/2021

COMPANY

QUANTAR SOLUTIONS LIMITED

for

DMGT & DMG Ventures

MARINE CYBER ANALYTICS PROGRAM

12 Month Forecast to
31 Dec 2021
Investment

Expenditure				<i>BS Allocation</i>		Financed by		
Accountancy & audit fees			£ -	Cash		Founder non-cash equity A	£ 428,531	
0			£ 1,000			Founder non-cash equity B	£ 428,531	
Advertising - Including for Hiring Purposes			£ 110	Cash		DMGT equity:		
Bank charges			£ -	Cash		DMGT equity A	£ 90,000	
External Specialist Consultancy fees			£ 10,800	Cash		DMGT equity B	£ 90,000	
External Installation Contractor			£ 1,800	L&B		Shareholder C	£ -	
Intellectual Property Fees			£ -	Cash		Shareholder D	£ -	
Key Man Dental & Health Insurance			£ 2,500	Cash		Shareholder E	£ -	
Software & Hardware Development			£ 1,000	Cash		Shareholder loans	£ -	
Legal and professional fees			£ 34,992	Cash		Bank Loans	£ -	
Founder Consultancy Fees			£ -	Cash		Total		£ 1,037,062
Overseas Flights & Hotel Costs to Developer			£ 1,700	Cash			857062	
Induction Week + Review Point Hotel Costs			£ 800	L&B				
Printing and stationery - Including Marketing			£ 144	Cash				
St Johns Innovation Forwarding Postage			£ 631	Cash				
St Johns Innovation Centre Rent			£ 2,860	Cash		(Deficit)/Excess		940552
Meeting Rooms Costs			£ 225	Cash				
Microsoft Azure/Power BI Cloud Subscription			£ 240	Cash		Set (deficit)/excess to zero by		
Atlassian Cloud Subscriptions			£ 600	Cash		changing		
Mobile Telephone Fees & Data			£ 100	Cash				
Subsistence			£ 1,800	Cash				or
UK Travel to Marine Area London			£ 120	L&B				
Sundry Expenses			£ 12,500	Cash				or
Website & Self-Assessment Video/Forms Hosted			£ 6,250	Stock				
Vessel Hardware			£ 3,750	Other FA				
Office Hardware Installations			£ -	Other FA				
Port Hardware Installations			£ -	Other FA				
0			£ -	£ -				
0			£ -	£ -				
0			£ -	£ -				
Contingency		15%	£ 12,588	Cash				
Total			£ 96,510					

Opening Balance Sheet

[illegible]

[illegible]

	12 Month Forecast to 31 Dec 2021 VAT Workings														
VAT Assumptions															
Standard Vat Rate	19.00%														
Month			Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21	Nov-21	Dec-21	<u>Total</u>
Sales			£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Expenses															
Direct Costs	V	£	-	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Wages and salaries (net)															
Accountancy & audit fees	V	£	-	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Advertising - Including for Hiring Purposes	V	£	-	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	160
Bank charges															
External Specialist Consultancy fees	V	£	-	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
External Installation Contractor	V	£	-	£ -	£ 287	£ 575	£ -	£ 287	£ -	£ 287	£ -	£ 96	£ 96	£ 96	£ 1,724
Intellectual Property Fees	V	£	287	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	287
Key Man Dental & Health Insurance	V	£	-	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Software & Hardware Development	V	£	-	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	399
Legal and professional fees	V	£	-	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	160
Founder Consultancy Fees															
Overseas Flights & Hotel Costs to Developer	V	£	-	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Induction Week + Review Point Hotel Costs	V	£	-	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	271
Printing and stationery - Including Marketing	V	£	-	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	128
St Johns Innovation Forwarding Postage		£	-												
St Johns Innovation Centre Rent		£	-												
Meeting Rooms Costs	V	£	-	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	457
Microsoft Azure/Power BI Cloud Subscription	V	£	36	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	36
Atlassian Cloud Subscriptions	V	£	38	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	38
Mobile Telephone Fees & Data	V	£	-	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	96
Subsistence	V	£	-	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	16
UK Travel to Marine Area London															
Website & Self-Assessment Video/Forms Hosting															
Vessel Hardware	V	£	-	£ -	£ 399	£ 798	£ -	£ 399	£ -	£ 399	£ -	£ -	£ -	£ -	£ 1,996
Deductable		£	362	£ -	£ 687	£ 1,373	£ -	£ 687	£ -	£ 687	£ -	£ 96	£ 96	£ 96	£ 5,768
VAT PAYABLE					£ (1,048)			£ (2,060)			£ (687)			£ (287)	£ (4,082)

12 Month Forecast to
31 Dec 2021
Profit and Loss Account

		Margins
Sales	£ 78,000	
Cost of sales	£ (153,212)	
Gross Profit	£ (75,212)	-96%

Administrative Overheads		
Sales Ports	£ -	
Sales Vessels	£ -	
Sales Operator Office	£ -	
Wages and salaries (net)	£ (48,744)	
PAYE & NI	£ (24,000)	
Accountancy & audit fees	£ -	
Advertising - Including for Hiring Purposes	£ (840)	
Bank charges	£ (110)	
External Specialist Consultancy fees	£ -	
External Installation Contractor	£ (9,076)	
Intellectual Property Fees	£ (1,800)	
Key Man Dental & Health Insurance	£ -	
Software & Hardware Development	£ (2,101)	
Legal and professional fees	£ (840)	
Founder Consultancy Fees	£ (34,992)	
Overseas Flights & Hotel Costs to Developers	£ -	
Induction Week + Review Point Hotel Costs	£ (1,429)	
Printing and stationery - Including Marketing Materials	£ (672)	
St Johns Innovation Forwarding Postage	£ (144)	
St Johns Innovation Centre Rent	£ (631)	
Meeting Rooms Costs	£ (2,403)	
Microsoft Azure/Power BI Cloud Subscriptions	£ (189)	
Atlassian Cloud Subscriptions	£ (202)	
Mobile Telephone Fees & Data	£ (504)	
Subsistence	£ (100)	
UK Travel to Marine Area London	£ (1,800)	
Website & Self-Assessment Video/Forms Hosting	£ 120	
Vessel Hardware	£ (10,504)	
Depreciation	£ (12,250)	
Total expenses	£ (153,212)	
Net Profit before Interest and Tax	£ (75,212)	-96%
Loan interest	£ -	
Net Profit before Tax	£ (75,212)	
Corporation tax	£ -	
Net profit after tax	£ (75,212)	-96%

[illegible]

12 Month Forecast to 31 Dec 2021 Sensitivity Analysis						
Sales and Profit						
Forecast		Low		Medium		High
Sales	-10%	£ 70,200	N/A	£ 78,000	10%	£ 85,800
Cost of Sales	5%	£ (160,872)	N/A	£ (153,212)	-5%	£ (145,551)
Gross Profit		£ (90,672)		£ (75,212)		£ (59,751)
Salaries	5%	£ 76,381	N/A	£ 72,744	-5%	£ 69,107
Other overheads	5%	£ (237,253)	N/A	£ (225,956)	-5%	£ (214,658)
Net Profit before Tax		£ (251,544)		£ (228,423)		£ (205,302)
Cashflow						
Opening Cash Balance		£ -		£ -		£ -
Profit Before Tax		£ (251,544)		£ (228,423)		£ (205,302)
Add Back Depreciation		£ (12,250)		£ (12,250)		£ (12,250)
Corporation Tax		£ (3,750)		£ (3,750)		£ (3,750)
FA Purchases/Disposals		£ (24,500)		£ (24,500)		£ (24,500)
Loan Capital Repayments						
Movement in other Debtors		£ (12,000)		£ (12,000)		£ (12,000)
Movement in Other Creditors		£ (2,287)		£ (2,287)		£ (2,287)
Closing Cash Balance		£ (306,332)		£ (283,210)		£ (260,089)

PHASE 2 FINANCIAL PROJECTIONS

PERIOD 01/01/2022 – 31/12/2022

COMPANY

QUANTAR SOLUTIONS LIMITED

for

DMGT & DMG Ventures

MARINE CYBER ANALYTICS PROGRAM

12 Month Forecast to 31 Dec 2022 Business Details

Company or Business Name		Quantar	
Financial Year End		Day	31
		Month	12
		Year	2022
Historic financial data			
Fixed Assets			
Land & buildings		£	-
Other (depreciable)		£	-
			£ -
Current Assets			
Stock		£	-
Trade Debtors		£	-
Other Debtors		£	-
Cash		£	-
		£	-
Creditors < 1 year			
PAYE & NI		£	-
Corporation Tax		£	-
VAT		£	-
Other Creditors		£	-
		£	-
Creditors > 1 year		£	-
Net Assets/Liabilities			£ -
Capital and Reserves			
Share capital		£	-
Profit and Loss Account		£	-
Other reserves		£	0
Shareholders' Funds			£ -

12 Month Forecast to
31 Dec 2022
Investment

Expenditure				<i>BS Allocation</i>		Funding of Equity Stakes		<i>BS Allocation</i>
Accountancy & audit fees		£	2,400	Cash		Founder equity Ordinary Shares(non-cash: patents/software)	£ 428,603	Equity
N/A		£	-			Founder equity Preference Shares(non-cash: patents/software)	£ 428,602	Equity
Advertising - Including for Hiring Purposes		£	10,500	Cash		DMGT equity:	£ -	N/A
Bank charges		£	420	Cash		DMGT-V equity Ordinary Shares	£ 200,000	Equity
External Specialist Consultancy fees		£	7,500	Cash		DMGT-V equity Preference Shares	£ 200,000	Equity
External Installation Contractor		£	119,000	Cash		Employee Share Options	£ -	Equity
Intellectual Property Fees		£	2,700	Cash		Shareholder D	£ -	Equity
Key Man Insurance		£	930	Cash		Shareholder E	£ -	Equity
Software & Hardware Development		£	105,867	Cash		Shareholder loans	£ -	Long Loans
Legal and professional fees		£	5,000	Cash		Bank Loans	£ -	Long Loans
Zoom Video Conference Fee		£	175	Cash		Total	£ 1,257,205	
Overseas Flights & Hotel Costs to Developers		£	3,600	Cash				
Induction Weeks + Review Point Hotel Costs		£	12,000	Cash				
Printing and stationery - Including Marketing Materials		£	1,125	Cash				
St Johns Innovation Forwarding Postage		£	288	Cash				
St Johns Innovation Centre Rent		£	234	Cash		(Deficit)/Excess	706019	
Meeting Rooms Costs		£	6,240	Cash				
Microsoft Azure/Power BI Cloud Subscriptions		£	21,600	Cash		Set (deficit)/excess to zero by		
Atlassian Cloud Subscriptions		£	240	Cash		changing		
Mobile Telephone Fees & Data		£	1,500	Cash				
Employee Dental & Health Insurance		£	9,996	Cash			or	
UK Travel to Marine Area London		£	2,100	Cash				
Office Equipment (Laptops + Mobile Telephones etc)		£	10,937	Other FA			or	
Website & Self-Assessment Video/Forms Hosting		£	240	Cash				
Vessel Hardware		£	120,900	Other FA				
Office Hardware Installations		£	31,200	Other FA				
Port Hardware Installations		£	2,600	Other FA				
Contingency		15%	£ 71,894	Cash				
Total		£	551,186					

	12 Month Forecast to 31 Dec 2022 Sales and Direct Costs													
Month		Jan-22	Feb-22	Mar-22	Apr-22	May-22	Jun-22	Jul-22	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22	Total
Sales units and price	Price	Units	Units	Units	Units	Units	Units	Units	Units	Units	Units	Units	Units	Total units
Vessels Renewals from Phase 1	£ 3,000	0	0	2	4	0	2	0	2	0	0	0	0	10
Vessels - Standard Pricing	£ 4,500	0	5	5	5	5	10	10	10	10	10	11	12	93
Per-vessel Platform Access Standard Rate	£ 1,250	0	0	25	25	50	120	120	120	120	130	130	130	970
Per-vessel Platform Access Middle Rate	£ 100	0	0	0	0	0	0	0	0	0	0	0	0	0
Per-vessel Pricing for Platform Access Low Rate	£ 75	0	0	0	0	0	0	0	0	0	0	0	0	0
Operator Offices Renewals from Phase 1	£ 6,000	0	0	1	2	0	1	0	1	0	0	0	0	5
Operator Offices Standard Pricing	£ 7,800	4	4	2	0	3	2	0	2	3	1	2	2	24
Ports Renewals from Phase 1	£ 6,000	0	0	0	0	0	0	0	0	0	1	1	1	3
Ports Standard Pricing	£ 9,600	0	0	2	0	0	0	0	0	0	0	0	0	2
Risk Carriers Subsidised First Clients	£ 30,000	0	0	0	0	0	0	0	0	0	0	0	0	0
Risk Carriers Standard Pricing	£ 60,000	0	0	0	0	0	0	0	0	0	0	0	0	0
Marine Equipment Subsidised First Clients	£ 3,000	0	0	0	0	0	0	0	0	0	0	0	0	0
Marine Equipment Standard Pricing	£ 5,400	0	0	0	0	0	0	0	0	0	0	0	0	0
Total Hardware Installations Per Month		4	9	9	5	8	12	10	11	13	11	13	14	119
Sales														
Vessels Renewals from Phase 1	£ -	£ -	£ 6,000	£ 12,000	£ -	£ 6,000	£ -	£ 6,000	£ -	£ 6,000	£ -	£ -	£ -	£ 30,000
Vessels - Standard Pricing	£ -	£ 22,500	£ 22,500	£ 22,500	£ 31,250	£ 62,500	£ 45,000	£ 45,000	£ 45,000	£ 45,000	£ 45,000	£ 49,500	£ 54,000	£ 418,500
Per-vessel Platform Access Standard Rate	£ -	£ -	£ 31,250	£ 31,250	£ 62,500	£ 150,000	£ 150,000	£ 150,000	£ 150,000	£ 150,000	£ 162,500	£ 162,500	£ 162,500	£ 1,212,500
Per-vessel Platform Access Middle Rate	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Per-vessel Pricing for Platform Access Low Rate	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Operator Offices Renewals from Phase 1	£ -	£ -	£ 6,000	£ 12,000	£ -	£ 6,000	£ -	£ 6,000	£ -	£ 6,000	£ -	£ -	£ -	£ 30,000
Operator Offices Standard Pricing	£ 31,200	£ 31,200	£ 15,600	£ -	£ 23,400	£ 15,600	£ -	£ 7,800	£ 23,400	£ 7,800	£ 15,600	£ 15,600	£ 187,200	
Ports Renewals from Phase 1	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 6,000	£ 6,000	£ 6,000	£ 18,000
Ports Standard Pricing	£ -	£ -	£ 19,200	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 19,200
Risk Carriers Subsidised First Clients	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Risk Carriers Standard Pricing	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Marine Equipment Subsidised First Clients	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Marine Equipment Standard Pricing	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Total Sales		£ 31,200	£ 53,700	£ 100,550	£ 77,750	£ 108,400	£ 222,600	£ 195,000	£ 214,800	£ 218,400	£ 221,300	£ 233,600	£ 238,100	£ 1,915,400
Total Direct costs	CoGS %													
Vessels Renewals from Phase 1	1%	£ -	£ -	£ 72	£ 144	£ -	£ 72	£ -	£ 72	£ -	£ -	£ -	£ -	£ 360
Vessels - Standard Pricing	11%	£ -	£ 2,513	£ 2,513	£ 2,513	£ 2,513	£ 5,025	£ 5,025	£ 5,025	£ 5,025	£ 5,025	£ 5,528	£ 6,030	£ 46,735
Per-vessel Platform Access Standard Rate	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Per-vessel Platform Access Middle Rate	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Per-vessel Pricing for Platform Access Low Rate	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Operator Offices Renewals from Phase 1	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Operator Offices Standard Pricing	11%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Ports Renewals from Phase 1	1%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Ports Standard Pricing	1%	£ -	£ -	£ 66	£ 133	£ -	£ 66	£ -	£ 66	£ -	£ -	£ -	£ -	£ 332
Risk Carriers Subsidised First Clients	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Risk Carriers Standard Pricing	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Marine Equipment Subsidised First Clients	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Marine Equipment Standard Pricing	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Total Direct Costs		£ -	£ 2,513	£ 2,651	£ 2,790	£ 2,513	£ 5,164	£ 5,025	£ 5,164	£ 5,025	£ 5,025	£ 5,528	£ 6,030	£ 47,428
Workings														
Direct costs per Product	Labour	Materials	Other	Total	CoGS %	% Of Sales (excluding renewals)								
Vessels Renewals from Phase 1	£ 10,000	£ 13,000		£ 23,000	1%	Vessels	21.85	0.2185						
Vessels - Standard Pricing	£ 93,000	£ 120,900	£ -	£ 213,900	11%	Platform Access	63.30	0.6330						
Per-vessel Platform Access Standard Rate	£ -	£ -	£ -	£ -	0%	Carrier Offices	9.77	0.0977						
Per-vessel Platform Access Middle Rate	£ -	£ -	£ -	£ -	0%	Ports	1.00	0.0100						
Per-vessel Pricing for Platform Access Low Rate	£ -	£ -	£ -	£ -	0%		95.92							
Operator Offices Renewals from Phase 1	£ 5,000	£ 30,000	£ -	£ -	0%									
Operator Offices Standard Pricing	£ 24,000	£ 187,200	£ -	£ 211,200	11%									
Ports Renewals from Phase 1	£ 3,000	£ 18,000	£ -	£ 21,000	1%									
Ports Standard Pricing	£ 2,000	£ 19,200	£ -	£ 21,200	1%									
Risk Carriers Subsidised First Clients	£ -	£ -	£ -	£ -	0%									
Risk Carriers Standard Pricing	£ -	£ -	£ -	£ -	0%									
Marine Equipment Subsidised First Clients	£ -	£ -	£ -	£ -	0%									
Marine Equipment Standard Pricing	£ -	£ -	£ -	£ -	0%									

	12 Month Forecast to 31 Dec 2022 Employee Costs														
Tax Assumptions															
Effective PAYE rate	25%														
Employers NI rate	11.93%														
(Adjusted for NI Shreshold at £56212)															
Month			Jan-22	Feb-22	Mar-22	Apr-22	May-22	Jun-22	Jul-22	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22	Total
Employees	Salary	No.													
Founder	£ 3,300	12	£ 3,300	£ 3,300	£ 3,300	£ 3,300	£ 3,300	£ 3,300	£ 3,300	£ 3,300	£ 3,300	£ 3,300	£ 3,300	£ 3,300	£ 39,600
Finance	£ 5,000	12	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 60,000
Engineering	£ 5,000	12	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 5,000	£ 60,000
Analytics	£ 7,083	12	£ 7,083	£ 7,083	£ 7,083	£ 7,083	£ 7,083	£ 7,083	£ 7,083	£ 7,083	£ 7,083	£ 7,083	£ 7,083	£ 7,083	£ 84,996
Industry Engagement	£ 5,416	12	£ 4,500	£ 5,416	£ 5,416	£ 5,416	£ 5,416	£ 5,416	£ 5,416	£ 5,416	£ 5,416	£ 5,416	£ 5,416	£ 5,416	£ 64,076
Growth Officer	£ 6,000	12	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 6,000	£ 6,000	£ 6,000	£ 18,000
Operations Head	£ 4,500	12				£ 4,500	£ 4,500	£ 4,500	£ 4,500	£ 4,500	£ 4,500	£ 4,500	£ 4,500	£ 4,500	£ 40,500
Head of Installations	£ 3,500	0	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Office Administrator Part Time Pro Rata	£ 1,300	0	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Other	£ -	0	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Other	£ -	0	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Other	£ -	0	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Other	£ -	0	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Other	£ -	0	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Other	£ -	0	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Other	£ -	0	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Other	£ -	0	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Other	£ -	0	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Other	£ -	0	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Other	£ -	0	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Total Gross salaries			£ 24,883	£ 25,799	£ 25,799	£ 30,299	£ 30,299	£ 30,299	£ 30,299	£ 30,299	£ 30,299	£ 36,299	£ 36,299	£ 36,299	£ 367,172
Total Employers NI			£ 2,967	£ 3,077	£ 3,077	£ 3,613	£ 3,613	£ 3,613	£ 3,613	£ 3,613	£ 3,613	£ 4,329	£ 4,329	£ 4,329	£ 43,785
Total PAYE			£ 6,221	£ 6,450	£ 6,450	£ 7,575	£ 7,575	£ 7,575	£ 7,575	£ 7,575	£ 7,575	£ 9,075	£ 9,075	£ 9,075	£ 91,793
Total Salary Costs			£ 27,850	£ 28,876	£ 28,876	£ 33,912	£ 33,912	£ 33,912	£ 33,912	£ 33,912	£ 33,912	£ 40,628	£ 40,628	£ 40,628	£ 410,957
Net Salaries			£ 18,662	£ 19,349	£ 19,349	£ 22,724	£ 22,724	£ 22,724	£ 22,724	£ 22,724	£ 22,724	£ 27,224	£ 27,224	£ 27,224	£ 275,379
Total PAYE and NI			£ 9,188	£ 9,526	£ 9,526	£ 11,188	£ 11,188	£ 11,188	£ 11,188	£ 11,188	£ 11,188	£ 13,403	£ 13,403	£ 13,403	£ 135,578

	12 Month Forecast to														
	31 Dec 2022														
	VAT Workings														
VAT Assumptions															
Standard Vat Rate	19.00%														
Standard Rate If Sales Offshore	0.00%														
Month		Jan-22	Feb-22	Mar-22	Apr-22	May-22	Jun-22	Jul-22	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22	Total	
Sales		£ 31,200	£ 53,700	£ 100,550	£ 77,750	£ 108,400	£ 222,600	£ 195,000	£ 214,800	£ 218,400	£ 221,300	£ 233,600	£ 238,100	£ 1,915,400	
Expenses															
0		£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	
Wages and salaries (net)															
Accountancy & audit fees	V	£ 32	£ 32	£ 32	£ 32	£ 32	£ 32	£ 32	£ 32	£ 32	£ 32	£ 32	£ 32	£ 383	
Advertising - Including for Hiring Purposes	V	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 1,676	
Bank charges															
External Specialist Consultancy fees	V	£ -	£ 399	£ -	£ 399	£ -	£ -	£ -	£ 399	£ -	£ -	£ -	£ -	£ 1,197	
External Installation Contractor	V	£ 383	£ 862	£ 862	£ 479	£ 766	£ 1,150	£ 958	£ 1,054	£ 1,245	£ 1,054	£ 1,245	£ 1,341	£ 11,400	
Intellectual Property Fees	V	£ -	£ -	£ 287	£ -	£ -	£ -	£ -	£ -	£ 144	£ -	£ -	£ -	£ 431	
Key Man Insurance															
Software & Hardware Development	V	£ -	£ -	£ -	£ 5,634	£ -	£ -	£ 5,634	£ -	£ -	£ -	£ -	£ -	£ 16,903	
Legal and professional fees	V	£ 798	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 798	
Zoom Video Conference Fee															
Overseas Flights & Hotel Costs to Developers	V	£ 96	£ 96	£ 96	£ -	£ -	£ 96	£ 96	£ -	£ -	£ -	£ 96	£ -	£ 575	
Induction Weeks + Review Point Hotel Costs	V	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 1,916	
Printing and stationery - Including Marketing Materials	V	£ -	£ 140	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 180	
St Johns Innovation Forwarding Postage	V	£ -	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 46	
St Johns Innovation Centre Rent	V	£ -	£ 3	£ 3	£ 3	£ 3	£ 3	£ 3	£ 3	£ 3	£ 3	£ 3	£ 3	£ 37	
Meeting Rooms Costs	V	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 996	
Microsoft Azure/Power BI Cloud Subscriptions	V	£ 287	£ 287	£ 287	£ 287	£ 287	£ 287	£ 287	£ 287	£ 287	£ 287	£ 287	£ 287	£ 3,449	
Atlassian Cloud Subscriptions	V	£ 38	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 38	
Mobile Telephone Fees & Data	V	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 239	
Employee Dental & Health Insurance	V	£ -	£ 133	£ 133	£ 133	£ 133	£ 133	£ 133	£ 133	£ 133	£ 133	£ 133	£ 133	£ 1,596	
UK Travel to Marine Area London															
Office Equipment (Laptops + Mobile Telephones etc)															
Website & Self-Assessment Video/Forms Hosting	V	£ -	£ 3	£ 3	£ 3	£ 3	£ 3	£ 3	£ 3	£ 3	£ 3	£ 3	£ 3	£ 38	
Vessel Hardware	V	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	
Office Hardware Installations	V	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	
Port Hardware Installations	V	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	
Deductable		£ 1,635	£ 1,959	£ 1,708	£ 6,975	£ 1,229	£ 1,708	£ 7,151	£ 1,915	£ 1,852	£ 1,516	£ 1,804	£ 1,804	£ 41,901	
VAT PAYABLE IF UK VAT RATE				£ 1,910,098			£ 1,905,488			£ 1,904,482			£ 1,910,276	£ 1,873,499	
VAT PAYABLE IF OFFSHORE SALES				£ 5,302			£ 9,912			£ 10,918			£ 5,124	£ 31,255	

12 Month Forecast to 31 Dec 2022 Profit and Loss Account					
					Margins
Sales			£ 1,915,400		
Cost of sales			£ 960,957		
Gross Profit			£ 954,443		50%
Administrative Overheads					
Sales Ports Standard Pricing		£ -			
Sales Vessels Renewals From Phase 1		£ -			
Sales Operator Office Standard Pricing		£ -			
Wages and salaries (net)		£ (275,379)			
PAYE & NI		£ (135,578)			
Accountancy & audit fees		£ (2,400)			
Advertising - Including for Hiring Purposes		£ (8,824)			
Bank charges		£ (420)			
External Specialist Consultancy fees		£ (6,702)			
External Installation Contractor		£ (60,000)			
Intellectual Property Fees		£ (2,700)			
Key Man Insurance		£ (930)			
Software & Hardware Development		£ (88,964)			
Legal and professional fees		£ (4,202)			
Zoom Video Conference Fee		£ (175)			
Overseas Flights & Hotel Costs to Developers		£ (3,025)			
Induction Weeks + Review Point Hotel Costs		£ (10,084)			
Printing and stationery - Including Marketing Materials		£ (945)			
St Johns Innovation Forwarding Postage		£ (242)			
St Johns Innovation Centre Rent		£ (197)			
Meeting Rooms Costs		£ (5,244)			
Microsoft Azure/Power BI Cloud Subscriptions		£ (18,151)			
Atlassian Cloud Subscriptions		£ (202)			
Mobile Telephone Fees & Data		£ (1,261)			
Employee Dental & Health Insurance		£ (9,996)			
Patent & Software Amortisation @10% PA		£ (85,721)			
Office Equipment (Laptops + Mobile Telephones etc)		£ (10,937)			
Website & Self-Assessment Video/Forms Hosting		£ (202)			
Vessel Hardware		£ (116,212)			
Office Hardware Installations		£ (29,962)			
Port Hardware Installations		£ (2,462)			
Depreciation		£ (79,844)			
Total expenses			£ 960,957		
Net Profit before Interest and Tax			£ 954,443		49.83%
Loan interest			£ -		
Net Profit before Tax			£ 954,443		
Corporation tax			£ (149,887)		
Net profit after tax			£ 804,556		42%
Workings					
Corporation Tax					
Profits per accounts		£ 954,443			
Add back non deductible items:					
Depreciation	£ (79,844)				
UK Entertaining	£ (85,721)				
		£ (165,564)			
Profits chargeable to tax		£ 788,879			
Corporation Tax at	19%	£ 149,887			

12 Month Forecast to 31 Dec 2022 Closing Balance Sheet							
Fixed assets							
Land & buildings			£	-			
Other (depreciable)			£	159,687			
					£	159,687	
Current assets							
Stock		£	-				
Trade Debtors		£	471,700				
Other Debtors		£	-				
Cash		£	960,957				
				£	1,432,657		
Creditors < 1 Year							
PAYE & NI		£	(13,403)				
Corporation Tax		£	(149,887)				
VAT		£	(5,124)				
Other Creditors		£	-				
				£	(168,414)		
Net Current Assets					£	1,264,243	
Creditors > 1 Year							
Net Assets/(Liabilities)					£	1,264,243	
Capital and reserves							
Share capital				£	-		
Profit and loss account				£	-		
							Check balance
Shareholders' funds					£	1,264,243	0
Workings							
Fixed Assets - Land & Buildings				Creditors < 1 year			
Opening balance	£	-		PAYE & NI		£	(13,403)
Additions/(Disposals)	£	-		Corporation Tax		£	(149,887)
Closing balance	£	-		VAT		£	(5,124)
				Other Creditors		£	-
				Closing Balance		£	(168,414)
Other Fixed assets (Depreciable)							
Opening balance	£	-					
Additions/(Disposals)	£	159,687		Creditors > 1 year			
Sub-total	£	159,687		Opening balance		£	-
Depreciation at a				Less repayments			
rate of	50%	£	(79,844)	Closing balance		£	-
Closing Balance		£	79,844				
				Profit & loss account			
				Opening Balance		£	-
				This year		£	804,556
				Closing Balance		£	804,556

12 Month Forecast to
31 Dec 2022
Sensitivity Analysis

Sales and Profit						
Forecast		Low		Medium		High
Sales	-10%	£ 1,723,860	N/A	£ 1,915,400	10%	£ 2,106,940
Cost of Sales	5%	£ 1,009,005	N/A	£ 960,957	-5%	£ 912,909
Gross Profit		£ 2,732,865		£ 954,443		£ 3,019,849
Salaries	5%	£ 431,505	N/A	£ 410,957	-5%	£ 390,409
Other overheads	5%	£ 577,500	N/A	£ 550,000	-5%	£ 522,500
Net Profit before Tax		£ 3,741,870		£ 1,915,400		£ 3,932,759
Cashflow						
Opening Cash Balance		£ -		£ -		£ -
Profit Before Tax		£ 3,741,870		£ 1,915,400		£ 3,932,759
Add Back Depreciation		£ (79,844)		£ (79,844)		£ (79,844)
Corporation Tax		£ -		£ -		£ -
FA Purchases/Disposals		£ (159,687)		£ (159,687)		£ (159,687)
Loan Capital Repayments						
Movement in other Debtors		£ (471,700)		£ (471,700)		£ (471,700)
Movement in Other Creditors		£ (18,527)		£ (18,527)		£ (18,527)
Closing Cash Balance		£ 3,012,113		£ 1,185,643		£ 3,203,001

PHASE 2 FINANCIAL PROJECTIONS

PERIOD 01/01/2023 – 31/12/2023

COMPANY

QUANTAR SOLUTIONS LIMITED

for

DMGT & DMG Ventures

MARINE CYBER ANALYTICS PROGRAM

	12 Month Forecast to 31 Dec 2023 Expenses and Cashflow Forecast													
		Jan-23	Feb-23	Mar-23	Apr-23	May-23	Jun-23	Jul-23	Aug-23	Sep-23	Oct-23	Nov-23	Dec-23	Total
Month		Jan-23	Feb-23	Mar-23	Apr-23	May-23	Jun-23	Jul-23	Aug-23	Sep-23	Oct-23	Nov-23	Dec-23	Total
Sales Vessels Renewals From Phase 1		£ -	£ -	£ 6,000	£ 12,000	£ -	£ 6,000	£ -	£ 6,000	£ -	£ -	£ -	£ -	£ 30,000
Sales Vessels Standard Pricing		£ -	£ 22,500	£ 22,500	£ 22,500	£ 22,500	£ 45,000	£ 45,000	£ 45,000	£ 45,000	£ 45,000	£ 49,500	£ 54,000	£ 418,500
Sales Per-vessel Platform Access Standard Rate		£ -	£ -	£ 31,250	£ 31,250	£ 62,500	£ 150,000	£ 150,000	£ 150,000	£ 150,000	£ 162,500	£ 162,500	£ 162,500	£ 1,212,500
Sales Per-vessel Platform Access Middle Rate		£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Sales Per-vessel Pricing for Platform Access Low Rate		£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Sales Operator Offices Renewals from Phase 1		£ -	£ -	£ 6,000	£ 12,000	£ -	£ 6,000	£ -	£ 6,000	£ -	£ -	£ -	£ -	£ 30,000
Sales Operator Office Standard Pricing		£ 31,200	£ 31,200	£ 15,600	£ -	£ 23,400	£ 15,600	£ -	£ 7,800	£ 23,400	£ 7,800	£ 15,600	£ 15,600	£ 187,200
Sales Ports Renewals from Phase 1		£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 6,000	£ 6,000	£ 6,000	£ 18,000
Sales Ports Standard Pricing		£ -	£ -	£ 19,200	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 19,200
Sales Risk Carriers Subsidised First Clients														
Sales Risk Carrier Standard Pricing		£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Sales Marine Equipment Subsidised First Clients														
Sales Marine Equipment Standard Pricing		£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -		£ -	£ -	£ -
Total income		£ 31,200	£ 53,700	£ 100,550	£ 77,750	£ 108,400	£ 222,600	£ 195,000	£ 214,800	£ 218,400	£ 221,300	£ 233,600	£ 238,100	£ 1,915,400
		31,200												
Expenditure	Amount													
		£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Wages and salaries (net)	30,824.00	30,824.25	30,824.25	30,824.25	30,824.25	30,824.25	30,824.25	30,824.25	30,824.25	30,824.25	30,824.25	30,824.25	27,224.25	366,291
PAYE & NI	15,176	15,176	15,176	15,176	15,176	15,176	15,176	15,176	15,176	15,176	15,176	15,176	15,176	£ 182,110
Accountancy & audit fees	£ 300	£ 300	£ 300	£ 300	£ 300	£ 300	£ 300	£ 300	£ 300	£ 300	£ 300	£ 300	£ 300	£ 3,600
Advertising - Including for Hiring Purposes	£ -	£ 3,500	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 3,500
Bank charges	£ 75	£ 75	£ 75	£ 75	£ 75	£ 75	£ 75	£ 75	£ 75	£ 75	£ 75	£ 75	£ 75	£ 900
External Specialist Consultancy fees	£ -	£ -	£ 5,000	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 5,000
External Installation Contractor	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Intellectual Property Fees	£ -	£ -	£ -	£ 1,800	£ -	£ -	£ -	£ -	£ -	£ 900	£ -	£ -	£ -	£ 2,700
Key Man Insurance	£ 80	£ 80	£ 80	£ 80	£ 80	£ 80	£ 80	£ 80	£ 80	£ 80	£ 80	£ 80	£ 80	£ 960
Software & Hardware Development	£ -	£ -	£ -	£ 30,000	£ -	£ -	£ -	£ 30,000	£ -	£ -	£ -	£ -	£ -	£ 60,000
Legal and professional fees	£ -	£ 2,500	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 2,500
Zoom Video Conference Fee	£ -	£ 175	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 175
Overseas Flights & Hotel Costs to Developers	£ -	£ 600	£ 600	£ 600	£ -	£ -	£ 600	£ 600	£ -	£ -	£ -	£ 600		£ 3,600
Review Point Hotel Costs	£ -	£ -	£ -	£ 1,500	£ -	£ -	£ 1,500	£ -	£ -	£ 1,500	£ -	£ -	£ 1,500	£ 6,000
Printing and stationery - Including Marketing Materials	£ -	£ 800	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 800
St Johns Innovation Forwarding Postage	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 300
St Johns Innovation Centre Rent	£ 22	£ 22	£ 22	£ 22	£ 22	£ 22	£ 22	£ 22	£ 22	£ 22	£ 22	£ 22	£ 22	£ 264
Meeting Rooms Costs	£ -	£ -	£ -	£ 780	£ -	£ -	£ 780	£ -	£ -	£ 780	£ -	£ -	£ 780	£ 3,120
Microsoft Azure/Power BI Cloud Subscriptions	£ 2,500	£ 1,800	£ 2,500	£ 2,500	£ 2,500	£ 2,500	£ 2,500	£ 2,500	£ 2,500	£ 2,500	£ 2,500	£ 2,500	£ 2,500	£ 29,300
Atlassian Cloud Subscriptions	£ -	£ 240	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 240
Mobile Telephone Fees & Data	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 2,100
Employee Dental & Health Insurance	£ 852	£ 852	£ 852	£ 852	£ 852	£ 852	£ 852	£ 852	£ 852	£ 852	£ 852	£ 852	£ 852	£ 10,224
UK Travel to Marine Area London	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 175	£ 2,100
Office Equipment (Laptops + Mobile Telephones etc)	£ -	£ 4,000	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 4,000
Website & Self-Assessment Video/Forms Hosting	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 25	£ 300
Vessel Hardware	£ 1,250	£ -	£ 6,250	£ 6,250	£ 6,250	£ 6,250	£ 12,500	£ 12,500	£ 12,500	£ 12,500	£ 12,500	£ 13,750	£ 15,000	£ 116,250
Office Hardware Installations	£ 1,250	£ 5,000	£ 5,000	£ 2,500	£ -	£ 3,750	£ 2,500	£ -	£ 1,250	£ 3,750	£ 1,250	£ 2,500	£ 2,500	£ 30,000
Port Hardware Installations	£ 1,250	£ -	£ -	£ 2,500	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 2,500
Corporation tax		0	0	0	0		0	0	0	0	0	0	0	£ -
VAT Payable		1635	1959	1708	6975	1229	1708	7151	1915	1852	1516	1804	1804	£ 31,255
VAT Refunds		£ -	£ -	£ (5,302)	£ -	£ -	£ (9,912)	£ -	£ -	£ (10,918)	£ -	£ -	£ (5,124)	£ (31,255)
Total expenditure		£ 67,979	£ 69,038	£ 92,565	£ 63,454	£ 61,458	£ 59,905	£ 100,480	£ 65,894	£ 60,593	£ 65,495	£ 68,883	£ 63,089	£ 838,834
Marine Hardware Equipment Installed		£ 5,000	£ 11,250	£ 11,250	£ 6,250	£ 10,000	£ 15,000	£ 12,500	£ 13,750	£ 16,250	£ 13,750	£ 16,250	£ 17,500	£ 148,750
Other fixed assets - Office Equipment (Laptop: Mobile Telephone etc)		£ 4,000	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 4,000
Land & Buildings		£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Opening bank balance		£ -	£ (45,779)	£ (72,367)	£ (75,632)	£ (67,586)	£ (30,644)	£ 117,051	£ 199,071	£ 334,227	£ 475,783	£ 617,838	£ 766,305	£ -
Movement in month		£ (45,779)	£ (26,588)	£ (3,265)	£ 8,046	£ 36,942	£ 147,695	£ 82,020	£ 135,156	£ 141,557	£ 142,055	£ 148,467	£ 157,511	£ 923,816
Closing bank balance		£ (45,779)	£ (72,367)	£ (75,632)	£ (67,586)	£ (30,644)	£ 117,051	£ 199,071	£ 334,227	£ 475,783	£ 617,838	£ 766,305	£ 923,816	£ 923,816
Months with cashflow deficit		£ (45,779)	£ (72,367)	£ (75,632)	£ (67,586)	£ (30,644)								
Maximum cashflow deficit				£ (75,632)										

	12 Month Forecast to														
	31 Dec 2023														
	VAT Workings														
VAT Assumptions															
Standard Vat Rate	19.00%														
Standard Rate If Sales Offshore	0.00%														
Month			Jan-22	Feb-22	Mar-22	Apr-22	May-22	Jun-22	Jul-22	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22	Total
Sales			£ 146,150	£ 146,150	£ 136,400	£ 62,250	£ 110,800	£ 100,200	£ 92,750	£ 101,750	£ 109,550	£ 126,250	£ 96,250	£ 96,250	£ 1,324,750
Expenses															
0			£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -
Wages and salaries (net)															
Accountancy & audit fees	V	£ 48	£ 48	£ 48	£ 48	£ 48	£ 48	£ 48	£ 48	£ 48	£ 48	£ 48	£ 48	£ 48	£ 575
Advertising - Including for Hiring Purposes	V	£ 559	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 559
Bank charges															
External Specialist Consultancy fees	V	£ -	£ 798	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 798
External Installation Contractor	V	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Intellectual Property Fees	V	£ -	£ -	£ 287	£ -	£ -	£ -	£ -	£ -	£ -	£ 144	£ -	£ -	£ -	£ 431
Key Man Insurance															
Software & Hardware Development	V	£ -	£ -	£ 4,790	£ -	£ -	£ -	£ -	£ 4,790	£ -	£ -	£ -	£ -	£ -	£ 9,580
Legal and professional fees	V	£ 399	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 399
Zoom Video Conference Fee															
Overseas Flights & Hotel Costs to Developers	V	£ 96	£ 96	£ 96	£ -	£ -	£ 96	£ 96	£ 96	£ -	£ -	£ -	£ 96	£ -	£ 575
Induction Weeks + Review Point Hotel Costs	V	£ -	£ -	£ 239	£ -	£ -	£ 239	£ -	£ -	£ -	£ 239	£ -	£ -	£ 239	£ 958
Printing and stationery - Including Marketing Materials	V	£ 128	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 128
St Johns Innovation Forwarding Postage	V	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 48
St Johns Innovation Centre Rent	V	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 42
Meeting Rooms Costs	V	£ -	£ -	£ 125	£ -	£ -	£ 125	£ -	£ -	£ -	£ 125	£ -	£ -	£ 125	£ 498
Microsoft Azure/Power BI Cloud Subscriptions	V	£ 287	£ 399	£ 399	£ 399	£ 399	£ 399	£ 399	£ 399	£ 399	£ 399	£ 399	£ 399	£ 399	£ 4,678
Atlassian Cloud Subscriptions	V	£ 38	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 38
Mobile Telephone Fees & Data	V	£ 28	£ 28	£ 28	£ 28	£ 28	£ 28	£ 28	£ 28	£ 28	£ 28	£ 28	£ 28	£ 28	£ 335
Employee Dental & Health Insurance	V	£ 136	£ 136	£ 136	£ 136	£ 136	£ 136	£ 136	£ 136	£ 136	£ 136	£ 136	£ 136	£ 136	£ 1,632
UK Travel to Marine Area London															
Office Equipment (Laptops + Mobile Telephones etc)															
Website & Self-Assessment Video/Forms Hosting	V	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 4	£ 48
Vessel Hardware	V	£ -	£ 998	£ 998	£ 998	£ 998	£ 998	£ 1,996	£ 1,996	£ 1,996	£ 1,996	£ 1,996	£ 2,195	£ 2,395	£ 18,561
Office Hardware Installations	V	£ 798	£ 798	£ 399	£ -	£ 599	£ 399	£ -	£ 200	£ 599	£ 200	£ 399	£ 399	£ 399	£ 4,790
Port Hardware Installations	V	£ -	£ -	£ 399	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ 399
Deductable		£ 2,529	£ 1,517	£ 6,160	£ 623	£ 623	£ 1,082	£ 5,508	£ 623	£ 1,130	£ 623	£ 718	£ 987	£ 21,323	
VAT PAYABLE IF UK VAT RATE					£ 1,314,545			£ 1,322,423			£ 1,317,489			£ 1,322,423	£ 1,303,427
VAT PAYABLE IF OFFSHORE SALES					£ 10,205			£ 2,327			£ 7,261			£ 2,327	£ 22,121

12 Month Forecast to 31 Dec 2022 Profit and Loss Account					
					Margins
Sales			£ 1,324,750		
Cost of sales			£ 230,510		
Gross Profit			£ 1,094,240		83%
Administrative Overheads					
Sales Ports Standard Pricing		£ -			
Sales Vessels Renewals From Phase 1		£ -			
Sales Operator Office Standard Pricing		£ -			
Wages and salaries (net)		£ 366,291			
PAYE & NI		£ (182,110)			
Accountancy & audit fees		£ (3,600)			
Advertising - Including for Hiring Purposes		£ (1,824)			
Bank charges		£ (900)			
External Specialist Consultancy fees		£ (4,202)			
External Installation Contractor		£ 11,400			
Intellectual Property Fees		£ (2,700)			
Key Man Insurance		£ (960)			
Software & Hardware Development		£ (43,097)			
Legal and professional fees		£ (1,702)			
Zoom Video Conference Fee		£ (175)			
Overseas Flights & Hotel Costs to Developers		£ (3,025)			
Induction Weeks + Review Point Hotel Costs		£ (4,084)			
Printing and stationery - Including Marketing Materials		£ (620)			
St Johns Innovation Forwarding Postage		£ (254)			
St Johns Innovation Centre Rent		£ (227)			
Meeting Rooms Costs		£ (2,124)			
Microsoft Azure/Power BI Cloud Subscriptions		£ (25,851)			
Atlassian Cloud Subscriptions		£ (202)			
Mobile Telephone Fees & Data		£ (1,861)			
Employee Dental & Health Insurance		£ (10,224)			
Patent & Software Amortisation @10% PA		£ (85,721)			
Office Equipment (Laptops + Mobile Telephones etc)		£ (4,000)			
Website & Self-Assessment Video/Forms Hosting		£ (262)			
Vessel Hardware		£ (116,212)			
Office Hardware Installations		£ (29,962)			
Port Hardware Installations		£ (2,462)			
Depreciation		£ (79,844)			
Total expenses			£ 230,510		
Net Profit before Interest and Tax			£ 1,094,240		82.60%
Loan interest			£ -		
Net Profit before Tax			£ 1,094,240		
Corporation tax			£ (176,449)		
Net profit after tax			£ 917,792		69%
Workings					
Corporation Tax					
Profits per accounts		£ 1,094,240			
Add back non deductible items:					
Depreciation	£ (79,844)				
UK Entertaining	£ (85,721)				
		£ (165,564)			
Profits chargeable to tax		£ 928,676			
Corporation Tax at 19%		£ 176,449			

PHASE 2 SALES PROJECTIONS

PERIOD 01/01/2024 – 31/12/2024

COMPANY

QUANTAR SOLUTIONS LIMITED

for

DMGT & DMG Ventures

MARINE CYBER ANALYTICS PROGRAM

	12 Month Forecast to													
	31 Dec 2024													
	Sales and Direct Costs													
Month		Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Jul-24	Aug-24	Sep-24	Oct-24	Nov-24	Dec-24	Total
Sales units and price	Price	Units	Units	Units	Units	Units	Units	Units	Units	Units	Units	Units	Units	Total units
Vessels Renewals from Phase 1	£ 3,000	0	0	0	0	0	0	0	0	0	0	0	0	0
Vessels - Standard Pricing	£ 4,500	5	5	5	5	5	5	5	5	5	5	5	5	60
Per-vessel Platform Access Standard Rate - New Clients	£ 1,250	5	5	5	5	5	5	10	10	10	5	5	5	75
Per-vessel Platform Access Middle Rate - Existing Clients	£ 100	0	0	15	15	10	0	0	0	0	0	0	0	5
Per-vessel Pricing for Platform Access Low Rate - Existing Clients	£ 75	0	0	10	10	40	120	120	120	120	130	130	130	930
Operator Offices Renewals from Phase 1	£ 6,000	0	0	0	0	0	0	0	0	0	0	0	0	0
Operator Offices Standard Pricing	£ 7,800	8	8	4	0	6	4	0	5	6	5	5	5	56
Ports Renewals from Phase 1	£ 6,000	0	0	0	0	0	0	0	0	0	0	0	0	0
Ports Standard Pricing	£ 9,600	2	1	2	0	1	1	0	0	0	0	0	1	8
Risk Carriers Subsidised First Clients	£ 30,000	1	1	1	1	1	1	0	0	0	0	0	0	6
Risk Carriers Standard Pricing - Existing & New Clients	£ 60,000	1	1	1	0	0	0	2	1	1	2	1	0	10
Marine Equipment Subsidised First Clients	£ 3,000	0	0	0	0	0	0	0	0	0	0	0	0	0
Marine Equipment Standard Pricing	£ 5,400	0	0	0	0	0	0	0	0	0	0	0	0	0
Total Hardware Installations Per Month		15	14	11	5	12	10	5	10	11	10	10	11	124
Sales														
Vessels Renewals from Phase 1	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Vessels - Standard Pricing	£ 22,500	£ 22,500	£ 22,500	£ 22,500	£ 22,500	£ 22,500	£ 22,500	£ 22,500	£ 22,500	£ 22,500	£ 22,500	£ 22,500	£ 22,500	270,000
Per-vessel Platform Access Standard Rate - New Clients	£ 6,250	£ 6,250	£ 6,250	£ 6,250	£ 6,250	£ 6,250	£ 6,250	£ 12,500	£ 12,500	£ 12,500	£ 6,250	£ 6,250	£ 6,250	93,750
Per-vessel Platform Access Middle Rate - Existing Clients	£ -	£ -	£ 1,500	£ 1,500	£ 1,000	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	4,000
Per-vessel Pricing for Platform Access Low Rate - Existing Clients	£ -	£ -	£ 750	£ 750	£ 3,000	£ 9,000	£ 9,000	£ 9,000	£ 9,000	£ 9,750	£ 9,750	£ 9,750	£ 9,750	69,750
Operator Offices Renewals from Phase 1	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Operator Offices Standard Pricing	£ 62,400	£ 62,400	£ 31,200	£ -	£ 46,800	£ 31,200	£ -	£ 39,000	£ 46,800	£ 39,000	£ 39,000	£ 39,000	£ 39,000	436,800
Ports Renewals from Phase 1	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Ports Standard Pricing	£ 19,200	£ 9,600	£ 19,200	£ -	£ 9,600	£ 9,600	£ -	£ -	£ -	£ -	£ -	£ -	£ 9,600	76,800
Risk Carriers Subsidised First Clients	£ 19,200	£ 9,600		£ -	£ 9,600	£ 9,600	£ -	£ -	£ -	£ -	£ -	£ -	£ 9,600	-
Risk Carriers Standard Pricing - Existing & New Clients	£ 30,000	£ 30,000	£ 30,000	£ 30,000	£ 30,000	£ 30,000	£ -	£ -	£ -	£ -	£ -	£ -	£ -	180,000
Marine Equipment Subsidised First Clients	£ 60,000	£ 60,000	£ 60,000	£ -	£ -	£ -	£ 120,000	£ 60,000	£ 60,000	£ 120,000	£ 60,000	£ -	£ -	600,000
Marine Equipment Standard Pricing	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Total Sales	£ 219,550	£ 200,350	£ 171,400	£ 61,000	£ 128,750	£ 118,150	£ 164,000	£ 143,000	£ 150,800	£ 197,500	£ 137,500	£ 96,700	£ 1,731,100	
Total Direct costs	CoGS %													
Vessels Renewals from Phase 1	1%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Vessels - Standard Pricing	12%	£ 2,780	£ 2,780	£ 2,780	£ 2,780	£ 2,780	£ 2,780	£ 2,780	£ 2,780	£ 2,780	£ 2,780	£ 2,780	£ 2,780	33,362
Per-vessel Platform Access Standard Rate - New Clients	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Per-vessel Platform Access Middle Rate - Existing Clients	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Per-vessel Pricing for Platform Access Low Rate - Existing Clients	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Operator Offices Renewals from Phase 1	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Operator Offices Standard Pricing	12%	£ -	£ -	£ 183	£ 183	£ 122	£ -	£ -	£ -	£ -	£ -	£ -	£ -	488
Ports Renewals from Phase 1	1%	£ -	£ -	£ 9	£ 9	£ 36	£ 109	£ 109	£ 109	£ 109	£ 118	£ 118	£ 118	846
Ports Standard Pricing	1%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Risk Carriers Subsidised First Clients	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Risk Carriers Standard Pricing - Existing & New Clients	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Marine Equipment Subsidised First Clients	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Marine Equipment Standard Pricing	0%	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	£ -	-
Total Direct Costs		£ 2,780	£ 2,780	£ 2,972	£ 2,972	£ 2,939	£ 2,889	£ 2,889	£ 2,889	£ 2,889	£ 2,898	£ 2,898	£ 2,898	34,696
Workings														
Direct costs per Product	Labour	Materials	Other	Total	CoGS %		% Of Sales (excluding renewals)							
Vessels Renewals from Phase 1	£ 10,000	£ 13,000		£ 23,000	1%		Vessels	21.85	0.2185					
Vessels - Standard Pricing	£ 93,000	£ 120,900	£ -	£ 213,900	12%		Platform Access	63.30	0.6330					
Per-vessel Platform Access Standard Rate - New Clients	£ -	£ -	£ -	£ -	0%		Carrier Offices	9.77	0.0977					
Per-vessel Platform Access Middle Rate - Existing Clients	£ -	£ -	£ -	£ -	0%		Ports	1.00	0.0100					
Per-vessel Pricing for Platform Access Low Rate	£ -	£ -	£ -	£ -	0%			95.92						
Operator Offices Renewals from Phase 1	£ 5,000	£ 30,000	£ -	£ -	0%									
Operator Offices Standard Pricing	£ 24,000	£ 187,200	£ -	£ 211,200	12%									
Ports Renewals from Phase 1	£ 3,000	£ 18,000	£ -	£ 21,000	1%									
Ports Standard Pricing	£ 2,000	£ 19,200	£ -	£ 21,200	1%									
Risk Carriers Subsidised First Clients	£ -	£ -	£ -	£ -	0%									
Risk Carriers Standard Pricing - Existing & New Clients	£ -	£ -	£ -	£ -	0%									
Marine Equipment Subsidised First Clients	£ -	£ -	£ -	£ -	0%									
Marine Equipment Standard Pricing	£ -	£ -	£ -	£ -	0%									

END NOTES

1. The financial projections contained herein are based upon penetration into the E.U. marine sector, followed by commencement of operations within the US marine sector. The Asian and E.U. shipping sectors are the two largest in the world and as such the projections should be extrapolated based upon the volume offered by the Asian marine sector, which has its global offices based in London.
2. The patent portfolio and software entered into the Founder equity funding is based upon values as at September 2020.
3. Opening balance sheet values are based upon a new entity being established for the sole purpose of launching a joint venture between DMGT / DMG Ventures and the Founder, with no previous trading recorded. Any values attributed from Phase 1 operations are via internal invoicing or relevant methods.
4. All information provided is based upon good faith and represents only data publicly available and no representation is made as to its validity and, or accuracy as at September 2020.
5. No offer is explicitly or implicitly made by reference to the documentation, whether to DMGT, DMG Ventures and or any other party.
6. Taxation and tax structures are based upon available information from the HMRC and other bodies, plus data provided under a consultancy agreement by Nauta Dutilh, Brussels.
7. All information, diagrams, illustrations, xls models, screendumps illustrating functionality and features, logos provided are the copyright of Dr. Phillip King-Wilson and Quantar Solutions Limited, all rights reserved 2020©. CyCalc© and Quantar© are registered trademarks.

Quantar Solutions Limited



Business Case Presentation

MARINE CYBER RISK ANALYTICS COMPANY

for

Daily Mail and General Trust plc

DMGT

&

dmg :: ventures

27th September 2020

END