SHORELINE

INTEGRATED CRIME CYBER INSURANCE

FOR THE MARINE TRANSPORT INDUSTRY

Developed in collaboration with

AXA XL, a division of AXA

Integrated Crime Cyber Insurance

When DNV GL writes about cyber security management, they use the expression "cybercrime" readily. So do the public and media and the P & I clubs alike: Standard Club defined it as "the intentional infiltration of a technology system by a third party without consent".

Depending upon the manifestation of the perpetrators' attack, and were insurance to have been arranged, the financial losses suffered by the policyholder might fall into one of two categories of risk, covered hitherto by two separate sets of underwriters:

Commercial Crime	an established class for the risks of fraud or theft, including activities that use the internet and including employee fraud or fidelity
Cyber	a developing market striving to deliver innovative covers in the face of new exposures, such as a computer system being infected or with criminal or malicious purpose

Our experience suggests that neither of these covers has been arranged habitually in the Marine Transport Industry. Equally, Shoreline recognises that the insurances for these new exposures have to be considered in the context of any company's risk management programme which now also has to consider the impact of an attack of this nature.

New-age pirates, however, who seek to disrupt or exploit businesses, do not recognise such a distinction and their methods increasingly blur the demarcation between the two insurance disciplines.

Given the overlap between the two lines of insurance, it is predictable, in event of claims, that the adjusters will question which policy provides cover. Consequently the **key design feature of our Integrated Crime Cyber Insurance is to offer the scope of cover hinted at by the expression Cybercrime.**

Action	Blend the two coverages into a combined All Risks policy wording. Unify General Conditions, Definitions, Exclusions.
Result	The widest conditions – all from a single source: One policy from which to recover claims One policy covering operations at sea or ashore One policy to turn to for service

Dependence on cyber systems itself creates vulnerabilities

DNV GL categorise exposures as follows:

Information Technology (IT)
- IT networks
- E-Mail
- Admin / Accounts / Crewing
- Planned maintenance / spares management and sourcing
- Charter Parties / bills of lading / notices of readiness
- Cargo Manifest systems

Operational Technology (OT)
- GPS
- AIS
- ECDIS
- SCADA
- Cargo Control
- Remote support for machinery

The concerns as to the quality of built in protection justify the description of VULNERABLE to potential attack: the “virtual pirate” will take advantage of opportunities to exploit weaknesses found in inter-connected IT systems and operational technology on board ship and ashore.

A lack of cyber security awareness and training is further exemplified by the ill-disciplined use of USB sticks brought on board by visitors being one of the biggest sources of “infection”.

Attacks can be specifically targeted or indiscriminate. Irrespective, the impact of Cybercrime on participants in Maritime Industries can be summarised as:

IT
- Ability to perform to expectations
- Financial results
- Property

OT
- Life
- Property
- Environment

Is your company prepared?

Marine transport is by no means immune from the activities of virtual pirates: be they cyber criminals, activists, terrorists or from an organized crime gang.

Attacks can take many forms: denial of service or data breaches, phishing, malware, ransomware or extortion, jamming, employee fraud, the actions of a disgruntled team member or even a nation state.

Would your company have been prepared for the impact of financial losses that arose or could arise as a consequence of:

- NotPetya ransomware attack costing shipping giant Maersk $300m[1]
- WannaCry: largest ransomware attack recorded to date. 200,000 victims in 150 countries[2]

Ransomware is lucrative for criminals because so many victims pay rather than face false accusations or because they desperately need their files to resume operations[3]

- Gangs using LinkedIn to impersonate company directors and demand cash transfers having falsified an e-mail account[4]
- Google and Facebook both being tricked by an individual, who purported to be a frequently used supplier, into sending him more than US$ 100 million[5]

Examples of "Diversionary Payment Fraud" or the new phenomenon of "Social Engineering"

- Hackers introducing a virus that changes destination bank details contained in e-mail instructions[6]

Or would it be prudent to buy insurance to provide you cover for such an increasingly frequent eventuality?

---

[1] *www.zdnet.com*

[2] *DNV GL*

[3] *www.bbc.co.uk/news/technology-35091714*

[4] *The Times 28/8/2017*

[5] *Fortune Magazine 2017*

[6] *HFW Circular*

Getting Smarter about Cyber Security
Regulation and commercial pressures

IMO Resolution MSC.428(98) will make cyber-security a regulatory imperative.

IMO member states are encouraged to ensure that cyber risks are addressed in Safety Management Systems no later than the first annual verification after 1st January 2021 of a company's Document of Compliance which will then have to include a chapter on cyber security.

Questions worth asking

- Are there designated officers within the company responsible for Information Technology and Security, with a remit for cyber security?
- How vulnerable are you to attack?
- What threats might affect you most acutely?
- How stringent are your "IT Hygiene" disciplines?
- How well trained is your treasury department?
- Is risk management a priority over risk transfer?
- Are you getting value from cyber security investment?

Links for guidance

DNV-GL points out that the ship management industry already addresses risk by looking at three key areas: people, process and technology. Countering cyber risk can adopt a similar approach. The society publishes a Cyber security ISM audit checklist and Recommended Practice for cyber security resilience management: **dnvgl.com**

BIMCO gives key steps for cyber risk management that should be incorporated into ship management systems: **bimco.org**

Risk management programmes will have to evolve accordingly.
Insurance for new risks such as cyber threats should be considered for those contingencies that cannot be eliminated at reasonable cost.

Other considerations:

- EU's General Data Protection Regulation (**GDPR**) enters into force 25th May 2018
- Tanker Management and Self Assessment No. 3 (**TMSA 3**) will operate from 1st January 2018, with new Element 13 - Marine Security, which requires security plans to have been put in place, which, inter alia, address cyber security risks, covering shored-based locations, vessels and personnel.

What Cover is being offered?

The cover focuses on offering Insureds indemnity for the financial losses they suffer because of a cyber-attack or a crime committed against their enterprise.

Financial losses include costs incurred in reinstating the Insured's business following an attack and business interruption on an enterprise-wide basis which is now delivered without the need for any of the company's property to have suffered physical damage.

Coverage is summarised per table below and will be offered subject to a combined single limit any one loss across all coverage and an annual aggregate limit so that insurers can manage their exposures.

The cover excludes any physical damage claims, all of which can be arranged in the traditional underwriting markets.

Key loss triggers:

- **Theft** of financial assets
- **Social Engineering**[1] meaning methods used to obtain access, data or money through fraud (also known as Mandate and Diversionary Payment Fraud.)
- **Extortion Demands and the use of ransomware**
- **Network Compromise** meaning any unauthorised access to, use or misuse of, modification to a computer or communication system, and/or denial of computer system resources by attacks perpetuated through any and all malware etc.
- **Data Breach** meaning any unauthorised acquisition of data by a third party (including an employee), disclosure or loss of data, that compromises the security, confidentiality and/or integrity of personal data or confidential business information
- **Costs incurred on Defence and in Mitigation of loss**

---

[1] *Such attacks have been successful through the centuries because they prey on human nature – for example, the desire to provide help to someone asking for assistance or letting one's guard down due to flattery or amiable conversation and personal charm.*

Although fraudsters frequently adapt their techniques and change targets, impersonation is the prevalent form of social engineering attacks that are costing businesses a lot of money. Successful infiltration of your or a third-party supplier's computer systems may allow a fraudster to give or manipulate payment instructions by email, so they appear to come from an authorised person, such as someone in a supplier's accounts department that you may have dealt with previously.

More sophisticated is the fraudster deploying the hacker's toolkit to enable access to and control over e-mail accounts. Hackers are looking to gain access to your computers and data, capture keyboard strokes (potentially compromising passwords on other systems) or intercept network traffic.

Summary of Cover

Head of Cover	Summarised cover	Type of Cover
Owned Asset and First Party Costs Protection		
Theft	Dishonest appropriation of assets by employees or third parties, with or without the threat of violence	Crime
Social Engineering	A plausible instruction from a seemingly legitimate source to deliver funds, resulting in a loss of assets	Crime
Loss of or Damage to Electronic Data	Replacing or updating data that has been destroyed, lost or corrupted	Crime and Cyber
Costs of Privacy Notification and Crisis Management	Costs of notifying those effected by a data breach, associated legal fees, cost of operating a call centre, PR expenses incurred to minimise reputational harm	Crime and Cyber
Computer Forensic Investigation Costs	Costs incurred in determining the existence, cause and scope of a network compromise or data breach	Cyber
Corporate Identity Fraud	Costs incurred in correcting public records or in applying for the dismissal of court proceedings	Crime
Business Interruption, Regulatory Investigations and Extortion Demands Due		
Business Interruption	Enterprise-wide loss of profits and/or operational expenses following a network compromise or data breach during the period of restoration. Physical damage *not* a pre-requisite and not to be confused with vessel specific loss of hire	Cyber
Regulatory Investigations	Costs of defence and regulatory fines (where insurable)	Cyber
Extortion Demands	Amounts demanded against the Insured by a third party threatening to commit a denial of service or data breach i.e. by ransomware	Cyber
Third Party Clauses		
Third Party Liability	To pay all losses and defence costs that the Insured becomes legally liable to pay in respect of breach of privacy or confidentiality, committing or failing to prevent a network compromise or data breach and loss or theft of documents or data	Cyber
Mitigation Costs and Emergency Costs		
Loss Mitigation	Costs incurred by the Insured with their approved Cyber Service Provider	Crime and Cyber
Emergency Costs	For those costs incurred in emergency and without having obtained prior consent of insurers	Crime and Cyber

Claims

In event of an attack, policyholders will be able to access Crawfords Cyber 24hr Hotline where staff will be able to supplement the company's crisis management procedures with access to proven experts.

All quotations will be issued accompanied by a Crime Cyber Claims Roadmap entitled **"Your company discovers a crime or cyber security breach... now what?"**

Crawfords commits to help formulate your response plan within an hour of your call. Typical questions that might need answering:

- Engaging pre-approved expert attorneys
- Engaging computer forensics to determine the existence, cause and scope of the breach
- Advice on the need to hire a public relations agency or crisis communications firm
- Advice on the need to notify and who needs notification
- Is a call centre required?
- Is credit or identity monitoring required?

Upon which build and execute a response plan with Crawford's support.

Who can buy Integrated Crime Cyber Insurance?

- Shipowners
- Ship operators
- Crew / Technical Managers
- Multi-modal / Logistics companies
- Port and Terminal Operators

And any marine enterprise that operates across these classifications.

Challenges overcome by Shoreline

Issue	Solution
Standard Cyber or Crime wordings are not fit for Marine purposes	Create a policy wording and Proposal Form specifically for participants in **Maritime Industries**
Two insurance product lines requires two policy forms	Merge/blend key components to form an **integrated** all embracing policy wording
Marine operations are international and as much land based as at sea	Policy forms will recognise enterprise wide activites be they **on board ship** or **shore based operations**
P & I club entries provide some cover	Policy is drafted to be **contingent** to recoveries from club entries, which do not provide cover for operations on shore
Style of cover	"All Risks" as opposed to named perils

Where can the cover be bought?

For more information on this product please contact:

Shoreline Ltd
PO Box HM 1354, Hamilton HM FX, Bermuda

T: +1 441 296 2324
F: +1 441 295 8504
E: shore@shoreline.bm
www.shoreline.bm

All policy wordings, proposal forms and support documents will shortly be available on the Shoreline website.

SHORELINE

INTEGRATED CRIME CYBER INSURANCE

Developed in collaboration with

AXA XL, a division of AXA