Commodities

July
2016

CYBER PACK

holman fenwick willan hfw

IBM's CEO calls cyber crime *"the greatest threat to every company in the world"*[1] and Forbes projects the cost of cyber crime to reach US$2 trillion by 2019[2]. Furthermore, the 2015 Fortune 500 CEO survey found that cyber security came second when CEOs were asked about their companies' biggest challenges[3].

Cyber security as an economic, reputational and legal risk is the responsibility of the Board. Specific responsibility to protect the business, reputation, assets and interests of stakeholders, including trading partners, should be specifically allocated and monitored by a Board executive or Board committee which is held accountable for it[4].

This dedicated cyber pack looks in some detail at how exposed the commodity and shipping industry is and what basic steps can be taken to start to address the issue. We conclude the pack with providing you with our Product Suite which is a list of solutions, services and offers (some of which have been specifically negotiated by HFW) and are broadly speaking either inexpensive or complimentary, which we hope you can take advantage of.

What is cyber risk?

The risk posed by cyber events is defined by the Institute of Risk Management as *"any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems"*[5]. In reality, it is much more than just a failure of an organisation's IT systems, but also includes intentional infiltration or corruption of those technology systems by (criminal) third parties and weaknesses in an organisation's people and practices.

What are the implications of a cyber event?

Particular risks include:

- **Loss of intellectual property:** both your own and that of third parties.
- **Financial loss:** such as diversion, interception and redirection of payments through email infiltration and impersonation.
- **Business disruption:** as a result of a cyber event in October 2015, telecoms company TalkTalk lost 101,000 customers and suffered costs of £60m[6].
- **Reputational loss:** it can be highly embarrassing to tell your clients that you have lost their data!
- **Costs:** legal, regulatory (see our note on the EU Data Protection Regulation further in this Pack) and IT to manage and repair the damage.

Examples of cyber events in the commodities and maritime industry

- A European port had their IT systems breached for over two years before they were alerted – during this time, criminals had been using their systems to smuggle illegal goods[7].
- Criminals extracting release codes and documents for delivery of containers from terminal facilities.
- A hacker caused a floating oil-platform located off the coast of Africa to tilt to one side, thus forcing it to temporarily shut down[8].

1 http://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#5758f9993548

2 http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#7ad450033bb0

3 World Economic Forum, The Global Risks Report 2016, 11th edn, page 77

4 To this regard, please see the "Board Cyber Check-List" on page 6 of The City UK's "Cyber and the City" publication (May 2016) https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20and%20the%20city.pdf

5 http://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/

6 https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave

7 http://www.bbc.co.uk/news/world-europe-24539417

8 http://www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140423

- Cyber attackers used booby-trapped emails to steal logins that gave them access to a German steel mill's control systems, which led to parts of the plant failing and meant a blast furnace could not be shut down as normal, causing "massive damage"[9].
- Diverted freight, hire and sale contract payments.

Focus on the EU Data Protection Regulation

As matters currently stand (with the UK still being part of the EU), from 25 May 2018 a new EU Data Protection Regulation[10] (the GDPR) will apply across the EU, with extra-territorial reach[11].

Despite the Brexit vote, it is likely that either the UK will adopt something very similar to the GDPR or the GDPR will come into force whilst the UK is still in the EU and the UK will therefore have to comply until it actually leaves the EU. Even if the post-Brexit UK does not adopt the GDPR, it will have to have "equivalency" with the EU legislation in relation to future UK data protection legislation. To this regard please note the Information Commissioner's Office's "12 steps to take now" page on preparing for the GDPR[12].

The GDPR requires data controllers to implement "appropriate" technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

The GDPR introduces a **mandatory** obligation to report any personal data breaches within 72 hours, unless a party can demonstrate the breach is unlikely to result in a risk to the rights and freedoms of individuals. In which case, individuals must be notified without "undue delay" so they can take any necessary precautions. A breach of the GDPR can result in a fine of up to the greater of 4% of global turnover or €20 million.

Note also that even though an entity is domiciled outside the EU, the GDPR bites if the entity offers goods or services to data subjects within the EU. Therefore, many may need

to appoint a representative in the EU, although this is not currently the case.

Focus on commodities - is a cyber event a force majeure event?

Spotlight: Agri contracts

Most GAFTA and FOSFA contracts define a force majeure event by reference to a list of specified events which may prevent the seller from performing its loading obligations (when selling FOB or CIF). Both contracts widen a force majeure event to include *"any other [cause – FOSFA] [event – GAFTA] comprehended in the term Force Majeure"*. Arguably, this catch-all provision does not extend beyond physical or legal events related to the port, vessel or cargo, which may not include a cyber event (depending on how it manifests itself). To put the matter beyond doubt, we recommend parties include an express clause in their contracts stating that a cyber event **is** a force majeure event.

Spotlight: Coal

The SCoTA version 8 force majeure event is broadly defined[13]. The definition may capture a cyber event provided it is not related to a payment obligation.

Spotlight: Sugar

In addition to a number of specific events which prevent the seller supplying or delivering sugar at the load port, the RSA force majeure clause contains a broad catch-all provision[14]. The clause may capture a cyber event which prevents the seller supplying or delivering sugar at the load port. However, a cyber event which only affects the performance of a payment obligation will not be caught.

9 http://www.bbc.co.uk/news/technology-30575104

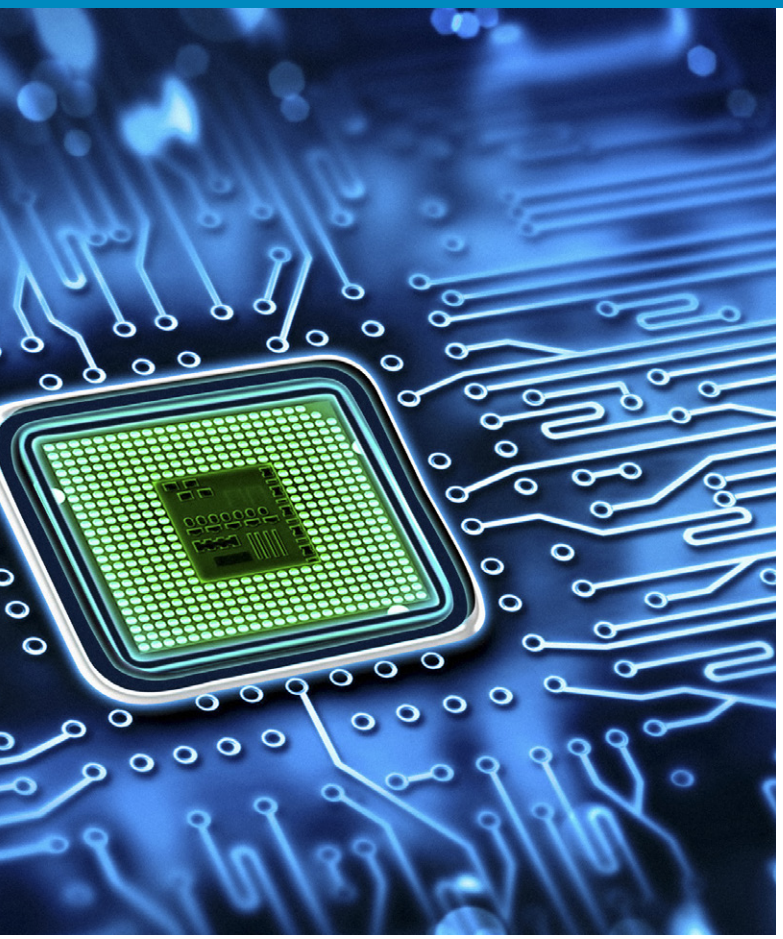
10 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

11 The implications will need to considered as part of the leaving process.

12 Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now, ICO: https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

13 A force majeure event is defined as *"any event or circumstance... (a) beyond the reasonable control of either Buyer or Seller which wholly or partly prevents or delays such Party from performing its obligations arising under this Agreement (apart from an obligation to make any payment under this Agreement); and (b) which cannot reasonably be overcome or avoided by such Party exercising all reasonable skill, care and diligence."*

14 See clause 11: *"... any other cause of force majeure (whether or not of like kind to those before mentioned) beyond the Seller's control..."*



Spotlight: Oil

The BP GTCs[15] state that a party can rely on a force majeure event to excuse a failure to perform an obligation if they prove such failure was due to an event beyond their control (although it excludes a failure to perform an accrued payment obligation). A non-exhaustive list of specific events is included in the BP GTCs for guidance[16]. Therefore a cyber event may well be held to be a force majeure event under the BP GTCs, provided it is not related to a payment obligation.

Conclusion

Clearly a cyber event does not automatically equate to a force majeure event. To avoid any doubt, parties should consider expressly amending their sale contracts to state whether a cyber event is a force majeure event, and/or whether a party should have any relief for failing to pay in the event of a cyber event.

Focus on commodities – limitation of liability

Parties should consider whether to expressly exclude a cyber event from their contracts or to include an express limitation of liability in relation to a cyber event.

SCoTA version 8 and the BP GTCs contain express limitation of liability provisions. These limit a party's liability for certain types of losses including, amongst others, loss of profit, indirect, and consequential losses. SCoTA also contains an aggregate liability cap for losses arising out of the contract which is equivalent to the contract price of the coal. The SCoTA limitation of liability provisions do not apply to any liability arising as a result of intentional or reckless default or gross negligence. In contrast, the BP GTCs limitation of liability provisions apply to liability arising out of a negligent act or omission.

Parties should consider whether they are satisfied with how their contract's limitation of liability provisions respond to losses arising from a cyber event.

Derivatives and Exchanges

The current LME Clear Rules and Regulations do not expressly refer to cyber events, but do contain a widely drafted force majeure clause. It refers to the *"closure, suspension or disruption of the operations of, or any default by"* a wide range of defined entities (including the settlement bank, operator, warehouse or transaction platform). This may well apply in the event of a cyber event.

The LME Clear Rules and Regulations also contain broad limitation of liability provisions, which exclude the exchange's liability for any *"losses, damages, claims, liabilities, costs or expenses"* arising from a force majeure event and so may well exclude liability for any losses arising from a cyber event.

The 2002 ISDA Master Agreement force majeure provisions refer to events which affect a party's ability to perform or receive payment or delivery, or otherwise comply with material terms of a transaction or under a credit support document. These provisions may apply in the event of a cyber event. Parties should consider whether they wish to rely on the default force majeure provisions or amend the provisions to make it explicit that they apply if a cyber event occurs.

15 The BP Oil International Limited General Terms & Conditions for the Sale and Purchase of Crude Oil and Petroleum Products – 2015 Edition – see clause 65.2.1.
16 Ibid.

Focus on shipping electronic bills of lading

EssDOCS state that the CargoDocs electronic bills of lading (E-BoL) are used in 73 countries by over 3,800 customers across all shipping modes[17] and that cyber security *"is a core element...developed through years of methodical testing and industry input[18]"*. The integrity and security of the E-BoL system is critical, but so is your preparation for and response to a cyber event in your contracts, insurance and internal policies.

Since their introduction in the 1980s, the use of E-BoL, has increased. As the use of E-BoLs increases, so must the risk of a cyber event disrupting trade, or even leading to the redirection or misappropriation of goods. It is not hard to imagine situations where fraudulent E-BoLs are issued or distributed or the E-BoL system is hacked.

As for insurance, the risk posed by cyber events is often described by insurers as a "non-marine" risk and so may require separate insurance (as we will go on to discuss), even if it is in relation to E-BoLs[19].

Focus on shipping – effect of cyber events on charterparties

Off-hire

Most time charters (almost without exception) include a clause providing that the vessel will be off-hire if the vessel is prevented from performing the charter. The off-hire clause in the NYPE 1946 form provides that in the event of the loss of time from *"breakdown or damages to hull, machinery or equipment… or by any other cause preventing the full working of the vessel, the payment of hire shall cease for the time thereby lost"*. *"Any other cause"* actually means any other cause like the ones in the preceding list – so, depending on the way in which a cyber event manifests itself, and the way in which it prevents the full working of the vessel, a cyber event **may** be an off-hire event.

However, it would be far better to include specific reference to cyber events, for example:

*In the event of the loss of time from deficiency of men or stores, fire, breakdown or damages to hull, machinery or equipment, grounding, detention by average accidents to ship or cargo, drydocking for the purpose of examination or painting bottom, **Cyber Event**, or by any other cause preventing the full working of the vessel, the payment of hire shall cease for the time thereby lost.*

"Cyber Event" means any act by a third party which affects the vessel's on-board computers, computer systems or computer software through or by the use of code, computer virus, process or any other electronic means whatsoever, without the consent of the owners.

Further, as underlined by the recent Supreme Court decision of The Global Santosh, it is clear that there is no substitute for proper drafting to appropriately allocate risk in your charterparties.

Payment of hire

Most charterparties require hire to be paid by an electronic transfer of funds – and that hire is only considered paid when it is received in the owner's bank account. If the charterer makes a payment, but that does not reach the

17 http://www.essdocs.com/edocs/electronic-bills-of-lading

18 http://www.essdocs.com/resources/security

19 Skuld FAQs, 20 October 2015: https://www.skuld.com/Documents/Topics/Circulars/IG_FAQs_Electronic_BLs_20151020.pdf?epslanguage=en

owner's bank account within the payment date (or at all), then the charterer will be in breach.

Consider the example we have seen time and again – the charterer receives an invoice and pays to the bank account therein provided, only to discover later that the invoice was not sent by the owner but by some imposter. These imposters can be quite convincing – using email addresses almost identical to the owner's.

An anti-technicality clause, depending on its breadth, may allow a charterer more time to pay, but pay (again) they must, or the owner will be at liberty to withdraw the vessel[20].

Whilst a charterer might not be able to avoid payment, contractual provisions which allow more time to pay, and an alternative payment method might be useful for example:

If a Cyber Event prevents payment of hire by charterers in accordance with this Charterparty, charterers shall have the option to make payment by any reasonable alternative means within 3 Banking Days of the expiry of any time allowed to make payment, with owners consent (such consent not to be unreasonably withheld). Any such payment shall stand as punctual.

"Cyber Event" means any act by a third party which affects the charterer's or owner's (or their respective banks' and/or agents') computers, computer systems or computer software through or by the use of code, computer virus, process or any other electronic means whatsoever, without the consent of the affected party.

Interruption to laytime and demurrage

Laytime and demurrage runs continuously and without interruption unless an exceptions clause applies or there is a delay caused by the owner. Most common laytime exception clauses are narrow in their construction and relate only to the vessel itself. Such an exception clause may well respond to a cyber event which affects the vessel directly, but will probably not include a situation where it is the port or terminal that is suffering from a cyber event.

Seaworthiness[21]

The common law obligation on an owner to provide a seaworthy vessel can be broken down into two requirements: firstly, the vessel, crew and equipment must be sound and able to withstand the ordinarily perils of the sea that would be encountered during the contemplated voyage. Secondly, the ship must be suitable to carry the contractual cargo.[22] The obligation extends beyond the mere physical state of the vessel and includes proper systems, manning and the ship's documents.[23]

A modern vessel cannot operate safely (or sometimes at all) without electronic navigational and communication equipment. Failing to protect the vessel against a cyber event could be a failure to exercise due diligence to make the vessel seaworthy.[24] This may also be a breach of Articles 3(1) and 4(1) of the Hague/Hague-Visby Rules and could lead to a claim under a bill of lading.

Regard must also be had for the ISM Code, which sets out the expected standards for the safe management of

20 Whether a failure to pay hire is a breach of condition and therefore repudiatory remains unclear. There is conflicting case law and the issue is currently being considered by the Court of Appeal. In *The Astra* [2013] 2 Lloyd's Rep 69 the High Court held obiter that payment of hire was a condition. A contrary decision was reached in *Spar Shipping AS v. Grand China Logistics Holding (Group) Co. Ltd* [2015] EWHC 718 (Comm) which is being appealed.

21 Please note the article on Tradewinds drafted by HFW and Quadrant Chambers: *"Owners must be diligent and proactive to prevent liability in cyber security"* (21 July 2016) http://www.tradewindsnews.com/weekly/769645/owners-must-be-diligent-and-proactive-to-prevent-liability-in-cyber-security

22 See *The Aquacharm* [1982] 1 Lloyd's Rep 7.

23 See *Seagate Shipping Ltd v Glencore International AG (The "Silver Constellation")* [2008] EWHC 1904 in which the requirement to obtain and maintain a Rightship approval was held not to be part of the Owner's obligation to make the vessel seaworthy.

24 In *Union of India v. Reederij Amsterdam* [1963] 2 Lloyd's Rep. 223 the House of Lords held that the obligation to exercise due diligence means that (1) inspections, repairs and other preparations must be completed to the level of a skilled and prudent shipowner and (2) any work carried out must be done with reasonable care, skill and competence.

a vessel. Neither the ISM nor the ISPS Codes specifically address cyber events. It is a similar position for SIRE and Rightship[25]. BIMCO has proposed the ISM and ISPS Codes use their fast roll-out procedures to address risk posed by cyber events[26]. In January 2016 BIMCO published guidelines to improve cyber security on ships [27]. Parties should review these guidelines and keep a close eye on future developments that address cyber security.

Safe ports

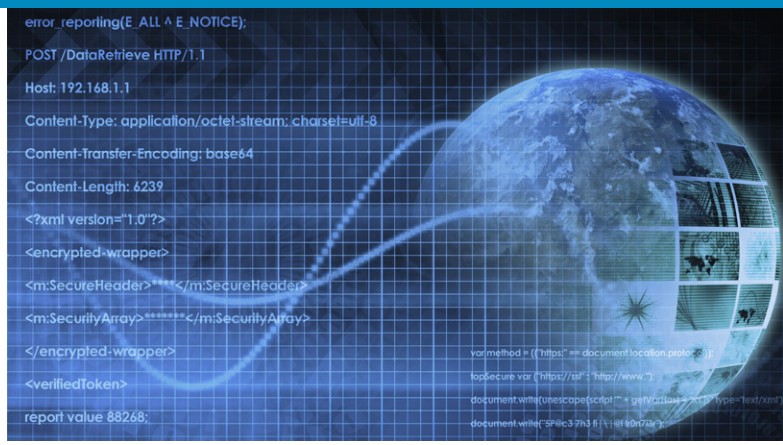
The classic definition of safety focuses on physical dangers such as shallows, reefs or protruding objects[28]. Safety has developed to cover political risks (such as requisitions, rebellions or wars), legal risk (such as arrests) and health risks (such as quarantines or epidemics). It is unclear if a cyber event would render a port unsafe. Arguably, a port might be unsafe if it suffers repeated cyber events due to poor cyber security[29]. Future developments should be closely watched.

Focus on cyber insurance

Insurance should be part of a cyber risk management strategy but, not a replacement for it.

With so much international trade still conducted through marine transportation of various kinds, the safety of vessels, crews, passengers, employees, ports, terminals, cargo and the inter-connected supply chain are critical to the efficient transaction of day to day business. Insurance seeks to develop products which address not only the traditional risks but also the modern activities and associated risks associated with the new ways of doing business.

There are now over 60 companies in the UK who market specific cyber insurance policies and over 70 in the USA. However, whilst there may be certain commonality in the name of the policy and some of the risks covered, it is important to bear in mind, as always, that the devil is in the detail. Not all insurance providers offer the same things and many wordings are inaptly put together. Policyholders and their advisors should also investigate whether some or all cyber risks (and associated costs) are covered under their



traditional property, "all risks", or liability policies. It is unlikely, unless expressly and clearly stipulated, but it is worth checking.

At the present time, in general terms, standalone cyber insurance policies are unlikely to insure property damage. In contrast, most standard form property and terrorism insurances are unlikely to insure (and expressly exclude) loss due to malicious cyber events. A very common exclusion in the marine and other specialists markets is the CL380 endorsement (or equivalent) known as the Institute Cyber Attack Exclusion Clause. However, attempts are being made to modify this in various policies due to market pressure.

Many players in the cyber insurance market focus upon providing policyholders with relief and support from the consequences of a cyber event. This is very helpful to SMEs and smaller operations who may not be well resourced enough to co-ordinate a breach response effectively. Such products are likely to cover first party losses such as:

- Data breach notification costs
- Forensic investigation costs to detect and seal the breach and preserve evidence
- Data recovery costs
- Public relations advice
- Credit monitoring expenses
- Identity theft

25 Currently Rightship and SIRE do not ask questions about a vessel's cyber security as part of their assessments. This is under review and likely to change in the future.

26 The IMO Maritime Safety Committee has proposed a series of measures to enhance maritime cyber security on ships. These out are set out in MSC 96/4/5.

27 These can be found at: https://www.bimco.org/News/2016/01/04_Cyber_security_guidelines.aspx

28 See *The Eastern City* [1958] 2 Lloyd's Rep. 127.

29 See *Gard Marine & Energy Ltd v China National Chartering Co Ltd (Rev 1) (The "Ocean Victory")* [2015] EWCA Civ 16 which is the subject of an appeal to the Supreme Court. The Court of Appeal has held that when determining if an event is an abnormal occurrence, evidence relating to the frequency or regularity of an event occurring must be considered. A port can have one or more prevailing characteristics such as high winds or a swell and if these characteristics occur together in a rare combination they will be considered an abnormal occurrence.

Some providers are offering insurance against reputation damage - however the parties must be clear at the outset about how such damage is to be quantified. Third party risks are intended to protect the insured mainly against liability to third parties in respect of losses resulting from unauthorised access to or dissemination of private and confidential or sensitive commercial information. The costs of defending the action and representation in connection with regulatory inquiries are also common. Specialist insurers are continually seeking to distinguish themselves from competitors by including new add-ons but, careful negotiation and consideration of applicable policy wordings is essential, along with appropriate professional advice.

Hot Topics with cyber insurance

At present, there are two hot issues in the specialist cyber insurance markets.

One issue is to what extent (if any) are fines and penalties associated with cyber events covered by the relevant insurance. Many insurers will provide cover "to the extent allowed under applicable law". Specific discussion on this is recommended to make sure that all parties understand what is covered and what is not, under current legislation.

The second issue is the physical damage arising from non-physical damage triggers.

Since most businesses now use computer generated commands to drive processes or business functions, it is obvious that a transmission of a virus through malware, a corruption of data, a DDOS (distributed denial of service attack) or other non-physical damage may cause significant loss and/or business interruption to a third party recipient via a computer network generated message. Traditional property and business interruption insurances require the proximate cause of loss to be some form of physical damage. Accordingly, insurers generally would not indemnify for a business interruption loss on the basis that no pre-requisite physical loss "proximately caused" by an insured peril had occurred. Causation/attribution issues in complex cyber claims can cause major difficulties and tensions.

Last year, Lloyd's acknowledged that "uncertainty" and "ambiguity" exists when policies are silent in relation to coverage for property damage and business interruption losses when a cyber event causes the physical damage and business interruption.

What if a computer message to an incident command system results in a fire which then causes damage to premises and property owned by a third party so that it has to curtail and shutdown its business for a while? In a similar scenario, if the computer message transmits a Trojan worm embedded in an email by a hacker which is sent to all supplier/clients of an entity with a promotional message which causes a shutdown of all computers of recipients as soon as the email is opened or forwarded. Are losses covered or not?

The language in specific policy wordings, together with the specific factual situation considered in relation to each loss, as well as the particular applicable law, is critical in determining whether a cyber breach event (as defined in the relevant policy and as interpreted under current case law), constitutes physical damage sufficient to trigger business interruption coverage.

Conclusions on cyber insurance

Of course, if no risk mapping or careful analysis of risk exposures by the business has taken place, together with live scenario-testing in preparing for an effective breach response, it is less likely that cover for the loss will be available.

In considering insurance as a risk management tool, businesses of all shapes and sizes should bear in mind that about half of all data breaches in all businesses come from within the work force, that 65% of large firms detected at least one cyber security breach in the last year; that the time from unauthorised intrusion to detection can range from 170-270 days (depending upon which survey you read); and that the cost of poor response to a foreseeable data breach can have significant economic and reputational consequences to the business and its stakeholders.

Don't think it can't or won't happen to you (it may already have done): it is a question of "when" not "if": it is best to be prepared - make sure your business is not "the weakest link" in its supply chain. Insurance can help, however worthwhile cover from a highly regarded insurer is unlikely to be available unless self-help and prudent self-management of the business institution can be demonstrated.

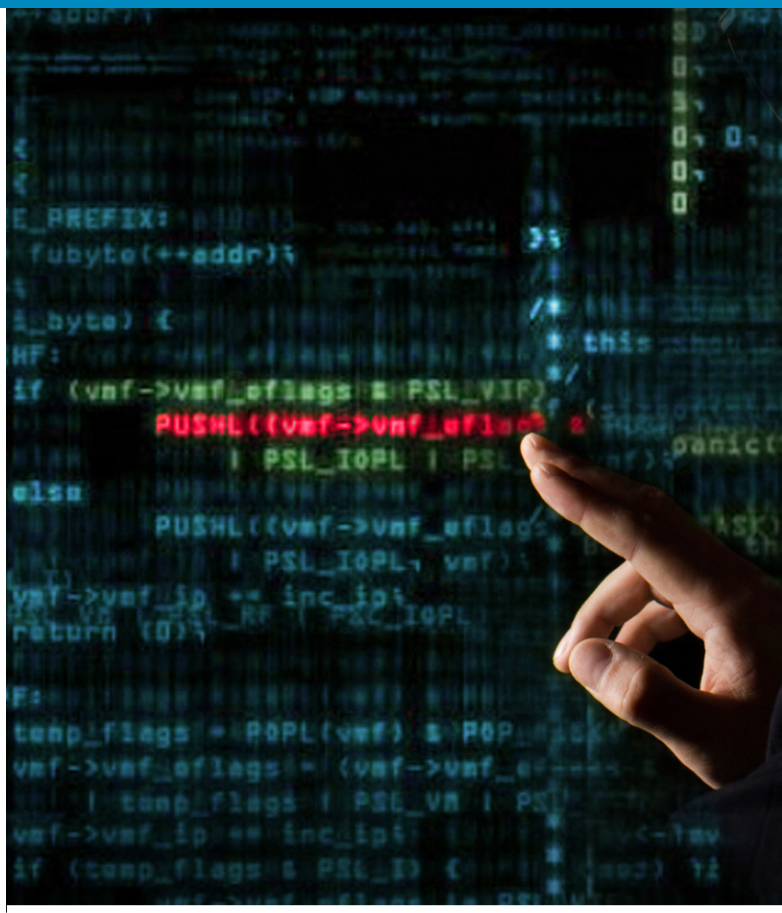
Focus on the US's approach to tackling cyber events in the maritime sector[30]

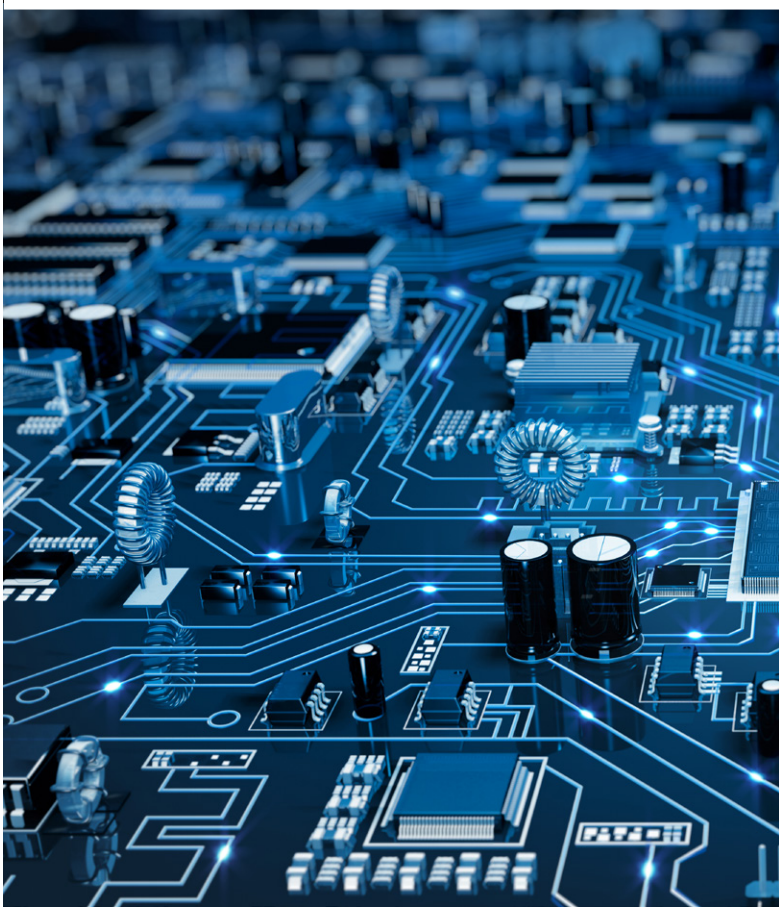
The US Coast Guard (USCG) is the lead agency in the US dealing with cyber security. The provisions establishing that role are beyond the scope of this pack. The Maritime Transportation Security Act of 2002 (MTSA) focuses on the prevention of "transportation security incidents" (or TSIs) and assigns the USCG responsibility for addressing the same.

Interestingly, the MTSA does not expressly address cyber security. However, the USCG has observed a cyber incident could cause a TSI. When the USCG published its "Cyber Strategy" in June 2015, it emphasised the need to protect *"maritime critical infrastructure"* from cyber events. Instead of mandating measures, the USCG has taken a guidance-based approach.

For example, the National Institute of Standards and Technology has published a "Cyber Security Framework" which describes a process for: identifying at risk assets, evaluating how to protect those assets and assessing how to detect, respond to, and recover from cyber events. Using that Framework, the USCG has issued guidance that while *"it is NOT a requirement, the USCG strongly encourages [regulated persons] to voluntarily review the [Framework] to determine how it might help them improve their cyber security posture*[31]*".* However, MTSA regulated persons are required to *"report suspicious activity, breaches of security, and TSIs in accordance with the provisions of 33 C.F.R. 101.305."*

Participants are therefore encouraged (or indeed required) by US authorities to understand and implement certain standards of cyber security.





30 We are indebted to Edward W. Floyd – Partner, Eaton & Van Winkle LLP for his contribution to this Pack.

31 ALCOAST Message 122/14.

Conclusions

Prevention is better than cure

- Assess your existing processes and procedures - what information/assets need to be protected? What are the potential risks? How can you improve your cyber security?
- Allocate the risk posed by cyber events in your contracts appropriately.
- Regularly update your anti-virus software, firewalls and other software and ensure your security policies respond to new threats and developments.
- Carry out due diligence of the risks posed by cyber events - review your supply chain to see who is the weakest link. It is a truism that hackers target the weakest link to infiltrate an organisation. That link can exist through the supply chain. How do you know that your supply chain has the same standard of cyber hygiene and resilience as your own entity? It can be embarrassing to ask, however, it can be more embarrassing not to ask.
- Set up a strategy to respond to a cyber event – Who should be involved? What are the priorities following a cyber event? How regularly is this strategy reviewed?
- Consider cyber insurance.
- Be aware of the possibility of insider assistance – both intentional and unintentional. 50% of all cyber breaches come from within an organisation - through deliberate or inadvertent acts or omissions of employees. A thorough top-down educational risk management programme is recommended, updated periodically, to ensure that employees at all levels are cyber-aware to phishing, whaling, memory stick cleaning, proper passwords, encryption, duties of confidence, how to handle commercially sensitive data/information etc.

Spotlight: Payment fraud and diverted payments

- Always check the details of an invoice and the email address attaching the invoice. **Be very careful!** HFW have dealt with cases where a single letter of an email address was changed, the payment request went undisputed and a payment was diverted.
- When paying a party for the first time, verify their details before making a payment – use a new email chain.
- When paying a party you have paid before, check the details match the last payment – if they do not, query why. Request all changes to payment terms be signed off/authorised by a director(s).
- Set up and maintain a “trusted payee” list/database.
- If you are unsure then pick up the phone **before** making the payment!
- If a payment is diverted, your next steps could include considering whether a freezing order would be appropriate or possibly an action against the bank for security/data protection failures.

HFW product suite

HFW cyber "fire drill"

It is very important that your business goes through realistic disaster scenarios in relation to different types of cyber events which may impact your business. Imagine having to admit that there has been no fire drill or fire equipment! We would suggest running your business, initially, through a smaller, containable event and then a medium range event which involves a consideration of potential reputation and third party claim ramifications. Finally, we can run your business through a "catastrophe event" (which may also involve considering a sizeable business interruption loss, cross jurisdictional regulatory problems and potential litigation).

HFW cyber disaster response team

It is now essential for each business entity to have an internal cyber breach disaster response group – pre-identified, trained and practiced, to liaise with your trusted HFW cyber team as your external advisory team. HFW can assist with training your business' internal team to prepare for, practice and execute these business critical functions. HFW can also provide you with a "breach counsel" to investigate, assess and advise upon the legal and regulatory issues. Your other external arsenal can also include forensic detectives to identify and isolate the causes of the cyber event, prevent a repeat attack and preserve evidence in relation to third party claims. Skilled public relations advice may also be needed for consistent internal and external messaging. Credit monitoring agents, social media watch and breach notification letter preparation and mailing facilities should also be engaged in advance.

HFW cyber contract and insurance review

HFW's cyber team can review your contracts and your insurance contracts to ensure that the risk and liabilities bought about by cyber events are appropriately covered as the parties wish for them to be.

HFW cyber bulletins/events

This is the first of a series of cyber packs. Please let us know if you would like to be added to our dedicated cyber email group which will keep you up-to-date with HFW's latest cyber events and packs.

PGI PROTECTION GROUP INTERNATIONAL

PGI Cyber Essentials Scheme

The UK Government Departments and public bodies are not permitted to trade with or outsource to third parties who cannot demonstrate an objective standard of cyber hygiene. The UK Government is promoting such a standard as a minimum foundational level through the "Cyber Essentials Scheme". This is a point by point check on specific fundamental key areas of cyber hygiene. When "cleared", an independently authorised body (CERT) issues a certificate which the entity can disclose and market. Our good contacts at PGI Group will give the Cyber Essentials Assessment and Training to you and get you through the test for a fee of £400 so that an appropriate certificate of compliance can be issued.

MOORE STEPHENS

Moore Stephens (MS) "healthcheck"

We are pleased to announce that HFW has entered into a facility with MS, a business advisory company headquartered in London, to provide a **complimentary healthcheck** of your cyber security. This healthcheck will be a quick way of highlighting areas where your business could immediately improve its cyber security. The healthcheck aims to highlight not only strengths but areas that you may want to consider to improve. This will involve a thorough face to face interview between MS' experts and your senior management. A report will then be produced outlining MS' observations and suggested improvements that your organisation may want to consider. MS' experts will follow-up each report with a face to face meeting to explain the content and areas for improvement.

For the avoidance of doubt, the above comments do not amount to legal advice and represent commentary only. Should you require legal advice please feel free to contact your usual HFW contact who (subject to conflicts) will be able to assist.

KEY CONTACTS

For more information, please contact:

Brian Perrott
Partner, London
T: +44 (0)20 7264 8184
E: brian.perrott@hfw.com

Anthony Woolich
Partner, London
T: +44 (0)20 7264 8033
E: anthony.woolich@hfw.com

Peter Schwartz
Consultant, London
T: +44 (0)20 7264 8171
E: peter.schwartz@hfw.com

Prashant Kukadia
Asssociate, London
T: +44 (0)20 7264 8070
E: prashant.kukadia@hfw.com

Simeon Newman
Associate, London
T: +44 (0)20 7264 8535
E: simeon.newman@hfw.com

Lawyers for international commerce hfw.com

Houston São Paulo London Paris Brussels Geneva Piraeus Beirut Riyadh Kuwait Dubai
Singapore Hong Kong Shanghai Perth Melbourne Sydney