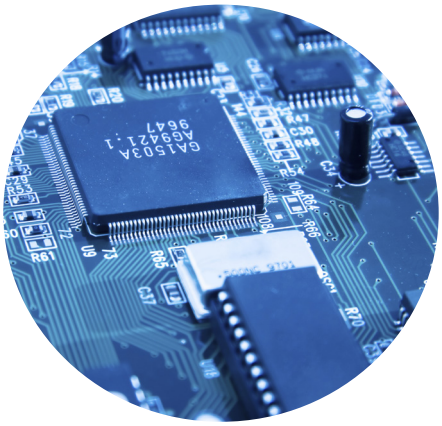
Risk insights

PORTS AND TERMINALS



The growing threat of cyber risks

With all the publicity surrounding the recent cyber attacks on Sony and Microsoft, it would be easy to assume that cyber criminals only target big-name brands. In reality; 'ordinary' businesses everywhere are being attacked by malicious individuals and groups who are attempting to steal data, shut down services or manipulate operations to their own ends.

Because of large-scale under-reporting by businesses worried about damage to their reputations, total losses resulting from cyber crime are difficult to quantify. McAfee, a leading global internet security provider, estimated the global figure to be USD445bn in 2014, up from USD300bn in 2013.

In the UK, large businesses do not always report online crimes, mostly for commercial reasons and particularly if they feel there is little chance that the perpetrators will be caught, according to a new report from the City of London Police. "In these cases, businesses are effectively absorbing the cost of the crime as a running expense," the report said.

How are UK ports at risk?

Matt Haworth, a Cyber and Information Assurance Specialist with cyber advice service provider Templar Executives believes that cyber security is now one of the most complex threats faced by the maritime industry and its critical infrastructure. "Ports and terminals are under attack from cyber criminals, organised crime and terrorist groups looking to disrupt national infrastructure and hostile governments," he says.

Information technology is not only integral to most aspects of a port's own operations - from the handling of cargo to storage and gate activities - but also in the exchange of data with third-parties such as; shipping lines, carriers' agents, freight forwarders, road haulage, train operating companies, and inspection and customs authorities. UK ports are vulnerable to cyber attack on two main fronts; attacks that target data and those aimed at physical assets and/or operations. A UK port has to consider both the strength of their defence systems and the systems of any third-parties they work with.

A cyber attack which targeted the Belgian port of Antwerp over a two-year period from June 2011 demonstrates the ability of determined criminals to break through a port's cyber defences. The audacious attack involved drug-traffickers recruiting hackers to breach IT systems at the port that controlled the movement and location of containers.

A gang based in the Netherlands hid cocaine and heroin among legitimate cargoes, including containers of timber and bananas shipped from South America. They then used hackers based in Belgium to infiltrate computer networks in at least two companies operating in the port of Antwerp. The hackers 'secure' data giving them the location and security details of containers, allowing the traffickers to send in lorry drivers to steal the cargo before the legitimate owner arrived.

The hackers gained access initially by mailing malicious software to staff, allowing the organised crime group to access data remotely. Even when the original breach was discovered and a firewall installed to prevent further attacks, the hackers

continued...

> "Many businesses outside the retail sector underestimate the risk of a cyber attack and the potential financial consequences of an attack on their trade"

...continued

physically broke into the premises and fitted key-logging devices onto computers.

Data-loss is expensive

Cyber criminals are often intent on obtaining data because it has value in itself or because they can potentially benefit financially from corrupting it to make it unusable, or inaccessible, for reasons of extortion.

New cases of hackers stealing the financial records of customers or employees regularly hit the headlines. The biggest settlement recently involved the US retail chain Target, which has agreed to pay USD10m in a proposed settlement of a class-action lawsuit related to a huge 2013 data-breach. At least 40 million credit cards were compromised in the breach during the 2013 holiday shopping season which may have resulted in the theft of as many as 110 million individual customer records, including information such as email addresses and phone numbers.

Tom Quy, a cyber risk broking specialist at Miller, says that laws relating to notification are not as stringent in the UK as they are in the US - but that is no reason to relax. "Rules and penalties are expected to change over the next couple of years as the EU starts to introduce new data-protection laws aimed at creating a more unified approach to data-breaches," he says. "In any case, data-loss for businesses like ports or terminals goes beyond consumer protection; the loss of business information can be very costly."

It is not only client data that is at risk from cyber criminals, data-breaches frequently target employees with the aim of obtaining confidential data relating to bank accounts, National Insurance numbers or medical records, for example. Employers have a duty of care to protect this information.

"Many businesses outside the retail sector underestimate the risk of a cyber attack and the potential financial consequences of an attack on their trade", Quy says. "It is not just about their obligations to notify customers and employees. The cost of recreating and restoring data and repairing systems can be huge and very disruptive," he explains. "Forensic IT costs to locate and fix a security problem can be particularly expensive and are comparable with what you might expect from a law firm, maybe in the region of GBP500 per hour for every expert on the case."

Operations at risk

Data security is probably the paramount concern, but UK port and terminal operations are targets for a number of reasons, not least the paralysing effect an attack could have on port movements, says David Rider, editor at CSO Alliance, the online resource for chief security officers in the maritime industry. "At a recent seminar on maritime cyber security in the US, Captain David Moskoff of the US Merchant Marine Academy suggested that a simple GPS jammer, widely available to buy online, could 'paralyse ship traffic and operations at US ports, and that would cause just one port an economic loss of USD1bn per day'," Mr Rider says.

A recent example of an attack made on a German steel mill's operations should resonate with any terminal operator that relies on sophisticated computer controlled crane equipment.

According to details of the incident that were revealed in the annual report of the German Federal Office for Information Security (BSI), a blast furnace at the steel mill suffered 'massive damage' following a targeted cyber attack on the plant's network.

Attackers used email and social media accounts to steal logins from employees that gave them access to the steel mill's automated control systems. This led to parts of the plant failing and meant a blast furnace could not be shut down as normal. The subsequent unscheduled shutdown of the furnace caused the damage, said the report.

Ports and terminals need to take the necessary steps to mitigate risk by developing resilience against the cyber threats faced, to protect themselves and their clients, Matt Haworth says. "Aside from disruption to services, there are inherent safety risks associated with poor cyber security, such as the compromise of navigation and monitoring systems which could be catastrophic," he warns.

Loss of confidence

Damage to reputation is a huge risk for ports and terminals operating in a competitive market. "The other likely outcome of an organised cyber attack against

a port would be the loss of confidence in the ability of the port to safely and securely conduct its business, resulting in reduced port operations and an impact on revenue," Matt Haworth adds.

A comprehensive set of measures to enhance the security of ships and port facilities; the International Ship and Port Facility Security Code (ISPS Code), was developed in response to the perceived physical threats to ships and port facilities in the wake of the 9/11 attacks in the US. Some experts think cyber security measures are still lagging behind however.

"The shipping and port industries are catching up in terms of adding enhanced security, and while the ISPS Code has done a great deal to bolster physical security in ports, the threat of cyber attack, although currently not widespread, remains," David Rider says. "We have seen hackers alter Automatic Identification System (AIS) transmissions from merchant ships at sea, for example. Through CSO Alliance, we are working with cyber security companies to help consolidate attack and incident data to benefit the entire maritime industry, but it is clear that more needs to be done to ensure robust systems are in place to check any potential cyber threats."

Cyber risks are a new threat for a shipping sector which is highly interconnected and increasingly reliant on automation, according to Allianz Global Corporate & Specialty's (AGCS) third annual Safety and Shipping Review 2015. "Cyber risk may be in its infancy in the sector today, but ships and ports could become enticing targets for hackers in future. Companies must simulate potential scenarios and identify appropriate mitigation strategies," Captain Rahul Khanna, Global Head of Marine Risk Consulting, AGCS said in the report. Scenarios highlighted in the Allianz report include cyber criminals targeting a major port, closing terminals, or interfering with containers or confidential data. "Such attacks could also result in significant business interruption costs, notwithstanding liability or reputational losses," the report said.

If exposed businesses are only just coming to terms with the threat posed by cyber crime, so are insurance companies. The growing realisation among insurers is that cyber risk is potentially a double-edged sword and needs to be carefully managed.

As ratings agency Fitch noted in a report; cyber risk is an area of significant potential growth for the insurance industry, but the unknown nature of the risk means that they are increasingly cautious about including cover in their property and liability policies.

"The peril has the potential to cause substantial losses due mainly to risk aggregation and the increasing sophistication of cyber attacks, as can be seen in the recent Sony hacking incident," Fitch said in a report published in March.

The cyber attack on Sony Pictures cost the company USD15m to investigate and repair. A cyber attack that targeted its PlayStation network in 2011 cost Sony USD170m in damages and repair work.

In its report, The Rise of Cyber Insurance, Fitch noted that the potential quantum of losses associated with cyber risk means that governments may even have to play a role in the prevention and indemnification of global cyber attacks.

Coverage questions

Tom Quy says a big question mark has been raised over insurers' exposure to cyber risk in standard policies that has implications for policyholders in the future.

"It means that there is a move among insurers to exclude the [cyber] exposure or charge for it as they get a better understanding of the risk aggregation in their portfolios," he says. "For policyholders, it means they might not be as well covered in the future against cyber threats as they think they are now under standard property, general liability or terrorism policies."

Quy believes forward-thinking businesses are purchasing 'standalone' data-breach and network security insurance to make sure that they have the cover in place to address all their first and third-party liabilities. The important elements of cover include privacy liability and employee liability, which will respond to legal actions filed against an organisation following the

continued...

...continued

unauthorised disclosure of private and confidential information, including that of the firm's own employees.

There is also protection providing defence and reimbursement for mandatory fines and penalties that follow regulatory action due to a privacy breach, as long as they are insurable by law.

When addressing notification related costs; cover is also available for customer support, credit file monitoring, legal services and public relations. Costs to recover, reinstate and recreate intangible assets destroyed during an attack are insurable as is a cyber extortion threat.

Business interruption is another important risk element that can be insured with reimbursement of net income that would have been earned had computer systems not been suspended or data-assets lost.

Advice on cyber risk management

Insurance is an important addition to a business' overall risk management portfolio but it is not a substitute for good cyber security. UK port and terminal operators looking to benchmark their security arrangements would do well to make use of the Government-backed Cyber Essentials Scheme, launched last year.

The scheme was designed to guide businesses in protecting themselves against the most common cyber threats by making advice available to download at no cost. Organisations successfully assessed by an independent Certification Body can then achieve a Cyber Essentials award to demonstrate that they meet the government endorsed set of basic controls on cyber security.

Calling on insurers to raise awareness of their cyber insurance offering and make sure that firms understand the extent of their coverage against cyber attack, Francis Maude, Minister for the Cabinet Office and Paymaster General said; "insurers can help guide and incentivise significant improvements in cyber security practice across industry by asking the right questions of their customers on how they handle cyber threats."

For more information on the issues raised in this article please contact:

Stephen Clarke
T +44 20 7031 2604
stephen.clarke@miller-insurance.com

Tour of Lloyd's

Would you like to visit Lloyd's and see the insurance market in action? We are happy to take visitors onto the trading floor and guide them around the historic parts of the building including the Adam Room, Nelson Collection and Old Library.

For more information or to arrange a visit, please contact:

Stephen Clarke
T +44 20 7031 2604
stephen.clarke@miller-insurance.com

Miller moves to new flagship office

On Monday 2 March, Miller moved into its new London flagship office at:
70 Mark Lane, London, EC3R 7NQ, United Kingdom

We look forward to welcoming clients, markets and business partners to our new headquarters. Our move to Mark Lane demonstrates Miller's growth and ambitions for the future and the new building provides a platform for closer working relationships between our specialists in London and internationally. It also allows us to further embrace technological initiatives which will add significant value to the service our clients receive. All Miller's London-based employees are now based in the new premises. The switchboard number, direct dial numbers and email addresses remain the same.