Cyber attacks are real and coming to a port near you, warns Dave MacIntyre

If the ports and terminal industry thought it was immune from the cyber attacks that are increasingly sweeping through the business world, the WannaCry and Petya/Not Petya attacks served a brutal wake-up call.

There are IT security lessons for port executives from both attacks, most significantly for the latter which affected APM Terminals and the Maersk shipping empire. Another area of concern is the potential for legal liability caused by vessel delays and subsequent cargo claims.

The Petya and Not Petya attacks crippled a number of APMT's global ports in June, with transactions having to be done on paper or by alternative email addresses. It was back to basics for an industry which prides itself on supply chain data connectivity.

The reality that the attacks hammered home is that ports are increasingly at risk from hackers and cyber viruses. Before these attacks, the oft-wheeled out example of the vulnerability of ports to cyber attack was the case of the Port of Antwerp, where hackers working for drug smugglers infiltrated cargo-tracking systems to aid the import of drugs hidden in containers. The hackers first gained access by sending malware to port staff and afterwards employed key-logging devices in a two-year period to June 2013.

Another old example saw crime syndicates penetrated systems used by Australian Customs and Border Protection in 2012, allowing them to see which shipping containers were being regarded as suspicious by authorities.

What is most disturbing for ports in these recent attacks is that unlike the Antwerp or Australian examples, which involved specific targets, the WannaCry and Petya attacks were random. Ports were simply collateral damage and their IT systems were exposed as vulnerable.

Which begs the question – what do ports need to do now, to protect themselves?

Post-mortem

The Moller-Maersk Group has promised a full post-mortem and will engage closely with customers and partners to share lessons from this incident. Meanwhile, experts in the cyber security industry say there are already some clear pointers for ports.

Ian Hirst, cyber security consultant at UK-based security organisation Maritime Asset Security and Training (MAST) Ltd, is blunt in his assessment that the attacks proved that there is a fundamental lack of understanding and knowledge in cyber security protection: “Both attacks could have been avoided with the application of some simple vulnerability management.”

That would have entailed the correct application of vendor patching, the latest antivirus software and by closing unwanted and unused communication ports on information systems.

“Moreover, the attacks could have been evaded if a governance and assurance programme was in place. Businesses should have vulnerability management policies in place and maintain

compliance standards with recognised industry bodies such as BIMCO and ISO, coupled with training and awareness policies, to mitigate any future risks.”

Mr Hirst says that where there are people and information systems there will always be vulnerabilities. Industrial Control Systems (ICS) tend to be operated by engineers and field personnel who may not be aware of the dangers and vulnerabilities of such systems.

“Much of the technology tends to be legacy and poorly secured with field devices often using default passwords or passwords selected by the operators with no minimum requirements enforced. There are many experts that are generally of the opinion that GPS, AIS and ECDIS are considered 'soft targets' due to their vulnerabilities and lack of encryption.

“Businesses must also account for human error when planning security responses as they can often be the weak link in any information system. It is important all employees at any level within a business are trained to meet the standards needed, and that there is a culture of security and compliance within the business to ensure any chinks in an organisation’s armour are adequately protected.”

Mr Hirst says ports need to move from reactive to proactive governance and assurance.

“Audits should be carried out both internally and externally and so should tests on all procedures. Finally, a business should ensure that training and awareness in cyber security issues is carried out and work towards certification in order to provide continual improvement and assurance.”

**Hacking tests**

Denmark-based CyberKeel brings a defensive as well as offensive approach to cyber security. It provides a comprehensive penetration test of a company's cyber security defences.

The better the hacker who does the test, the more holes you find, and therefore the more holes you will close off.

Chief executive Lars Jensen says the single greatest cyber security threat is the one sitting in a chair in front of the screen providing information, not out of malice but simply because most people are unaware of how hackers manipulate them.

“Even a skilled and well-trained IT administrator often does not know exactly what the attackers do - what are the tricks the hackers use. Without that knowledge they leave gaps in security without knowing it.”

His key lesson for ports and terminals is to configure their systems for defence-in-depth based on the assumption that at some point the outer defences will be breached, and have a contingency plan for the scenario where “you literally have to start everything from scratch - and that it is a plan you can execute.”

Mr Jensen says a high level of cyber security is about the painstaking discipline of constantly keeping maybe thousands of computers updated and patched, and configuring the network to deliver the required performance.

“Get a hacker in at regular intervals to spot the new holes and get them plugged. From the side of the attackers, there are constantly new tricks which they find, and what was effectively an impenetrable outer wall yesterday may suddenly be like Swiss cheese tomorrow.”

Legal liability

Ports and terminals also need to consider potential legal liabilities for delays and cargo damage.

Toby Stephens, Singapore-based partner of maritime law specialist HFW, says spoilage to reefer cargo is a prime example. “Reefer is time-sensitive, so if your system is down and you can't find the boxes or there has been a corruption of data affecting the maintenance of those containers, there is potential liability exposure.

“There will be contracts with lines using the terminals. It very much depends on the specific contract terminology between the counterparties and the legal obligations those contracts carry, as to the extent of any liability.

“The question of digitisation and the greater conductivity through the supply chain leads to further legal issues. Each of those links has a contractual relationship. Each link in the chain needs to know who is responsible for preventing the spread of malware when data is shared.

“Cyber attacks have only just hit the headlines in the last 12 months therefore there is a good chance that many contracts will be silent on what happens in response to a cyber breach. Ports need to think of the implications and clarify what could be their liability for any loss.”

FINES LOOM FOR DATA BREACHES

The European General Data Protection Regulation (GDPR) comes into force in May next year, carrying large fines for breach of data.

“If you hold data belonging to a third party, such as the nature of cargoes being shipped, then you have a duty to keep that data secure,” says HFW’s Toby Stephens. “The warning is clear: if someone hacks into your system there will be a fine. The question is how much? Liability could be exacerbated if it can be shown that sufficient protections were not in place.”

While these will initially apply in Europe, the international nature of trade suggests they will be a benchmark for other jurisdictions.

The onus is therefore on ports to not only show they have system protections in place but a crisis management plan that covers cyber breaches.

“It is important to have a contingency plan in place for a computer system or network which is breached. Those systems must include personnel being trained on the procedures they need to follow to protect the system, and what to do when a breach occurs.”

Mr Stephens says it is up to the ports industry to grasp the nettle in terms of cyber security: “We have gone through a period of increased awareness and improved maritime security with the ISPS Code. It is up to ports now to lead the way towards the next version of ISPS.”