Cyber risks creep up on the unwary

31 Jan 2019

John Bensalhia finds out why bulk terminals are just as vulnerable to attack as container hubs

Ports have found that there's a price to pay for modern technological marvels: cyberattacks pose a great threat to ports. The last 12 months have seen cyberattacks aimed at the Port of San Diego, where a cyber security threat disrupted the port’s information technology systems; the Port of Barcelona, where an attack affected some of the port's servers and systems; and a Cosco Shipping-affiliated terminal at the Port of Long Beach, which suffered a ransomware attack.

Such attacks can have a serious effect on all terminals in a port, not just on the more public facing container terminals. Ahead of last year's Association of Bulk Terminal Operators' annual conference, Ian Adams, chief executive, said that both physical and cyber security remain a particular weak spot for the ship-to-shore interface. “Ports and terminals are not only at risk from breaches in their own security but also their customers’. If hackers attack terminals it can result not only in the loss of sensitive information, but also loss of power, loss of system availability, port congestion and reputational damage. Terminal operators do need to have a robust business continuity plan in place.”

Talking to Port Strategy, Mr Adams says that the risks to bulk terminals are the same as for any other business: “There could be attacks from activists wanting to impact the reputation of the terminal; criminals seeking to gain financially; or opportunists who hack for the fun of it and then find that they can gain financially. There is also the threat of terrorist- or state-sponsored cyberattacks with the intention to gain knowledge or cause disruption to the economy.”

Hindering business flows

Business interruption is singled out as a key cyber risk by Michael Yarwood, senior loss prevention executive at TT Club. As well as this, there are risks associated with denial of service malware – “perpetrators restricting access to your systems in lieu of a ransom payment”, he says. This is where, for example, automated operations which rely on operational technology (OT) could be extremely exposed.

An instant response to a damaging cyber breach should be to report it to the appropriate authorities. Yet some businesses remain concerned that the disclosure of cyberattacks may put people off using their services. They believe that if word gets out that cyber threats or attacks have affected business, their reputation could be damaged along with future business prospects. However, non-disclosure could cause repeat attacks, resulting in greater harm.

With that in mind, countries such as Canada require reports of security breaches by law. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) requires private sector organisations and companies to report data security breaches to a Privacy Commissioner and inform customers if there is any risk stemming from the breach.

Mandatory reporting of significant IT disruptions apply to the 170 companies which are in the Port of Rotterdam and its industrial areas. From June 2018, any major incidents have to be reported to the Port Cyber Hotline. These include online issues that can greatly affect vessel arrival and departure, and security of the port and freight transhipment.

Global imbalances

On a general level, a major challenge is to address current mindsets in locations that are not as technologically advanced. Last year's Africa Cyber Security Conference addressed the threats posed by cyber criminals, noting that geography isn't an issue when it comes to online crime. One of the speakers, Auguste Diop, managing director of Talentys, acknowledged that “digital security is in its infancy” in Africa (although Kenya and South Africa are more sophisticated in this department).

Boukary Ouedraogo, managing director of Atos Afrique de l'Ouest, said that the challenge is to change mindsets and to bring the culture of security to business, while Mr Diop said that even though Africa wasn't as advanced in this field, it could still learn from mistakes made in other locations. “As a latecomer to digital technology, Africa can turn its handicap into an advantage by avoiding the errors made in cyber security by Europe and America.”

In order to prevent possible cyberattacks causing significant damage, bulk terminals can take a number of precautions. “Up-to-date security software and sound procedures to prevent access to the systems will help ports to combat this problem,” says Mr Adams.

“Bulk terminals should ensure that all software – especially legacy systems – are kept up to date and install any available patches,” adds Mr Yarwood.

“They should implement layers of defence, starting with the outermost layer of physical security, followed by management-level procedures and policies, as well as firewalls and architecture.”

Other precautions include implementing specifically targeted policies, account management, security updates and antivirus solutions, as well as employing network hardening measures “to ensure that patch management is adequate and proactively reviewed”.

“A sound removable device policy should also be employed, with provisions to ensure all USBs are encrypted and tested for viruses prior to being used with other devices,” says Mr Yarwood. “And finally, another action is the vetting of third-party providers to ensure that their cyber security procedures meet your expectations.”

Further support

Outside projects are also available to help tackle the risks posed by cyberattacks. Valenciaport Foundation's Sauron Project, for example, uses modern visualisation techniques such as cyber 3D models and immersive interfaces as a means of detecting and dealing with outside threats. Sauron can also evaluate possible outcomes of a cyber threat, thanks to its Hybrid Situation Awareness application. In the event of a serious risk to the port, this application can notify the appropriate security teams, who can then tackle the problem more quickly, preventing severe disruption.
Founded by technology group Wärtsilä and cyber security company Templar Executives, the International Maritime Cyber Centre of Excellence boasts a cyber academy and MCERT (Maritime Cyber Emergency Response Team). The team is available 24 hours a day to tackle emergencies, providing real-time help for members with cyber-related attacks, threats and incidents. The services of MCERT are available to ports around the globe, who can also call the team for advice and support on cyber security. Meanwhile, the Cyber Academy provides a good source of education about cyber-related subjects at all levels, including security coaching for senior management and cyber awareness for all organisational levels in the maritime industry.

But the challenges surrounding bulk terminals' cyber security present opportunities for ports to prepare for such risks. “The main opportunity for those who have not yet fallen victim to such an attack is to risk assess and prepare,” says Mr Yarwood. “Comprehensive threat assessments should be conducted to determine the threat landscape and to understand the potential attack surface faced by ports and terminals.”

Cyber resilience can also be built in other ways. Mr Yarwood says that personnel awareness and training can be improved through frequent briefings. Regular reviews of bring your own device and password policies should be introduced as a means of building up resistance to potential cyber threats. As well as this, bulk terminals should also envisage worst case scenarios. “Consider business continuity,” explains Mr Yarwood. “How would the day-to-day operation of your business be affected if you lost all IT and OT systems for 48 hours?”

MCERT director, Chris Gibbons, adds: “As the maritime world becomes more complex, interconnected and reliant on technology, we are faced with an enormous challenge: either we work together to improve our ability to defend ourselves by confronting and defeating the malicious acts so we are not vulnerable targets or collateral damage, or we fragment and fail.”

---

**CYBERATTACK KNOWLEDGE IS POWER**

As a result of potential cyber risks, bulk terminals face a number of challenges. TT Club’s Michael Yarwood cites a number of examples, including information and operational technology infrastructures, as well as IT/OT interaction and interoperability with other businesses. A key challenge is to get the terminal personnel fully aware and trained – as Mr Yarwood puts it: “Vulnerability to attack will always lie in human error.”

A range of training courses in cyber security are available. Cyberkeel's support for the maritime industry is designed to improve cyber security and reduce outside risks. One of its services is training, which is specifically pitched at various levels in accordance with each client's requirements, whether single or multi-company. A system administrator technical training course, for example, includes sections on Windows Internals and Attacks (including detailed views of vulnerabilities and exploits in modern software); Privilege Escalation and Lateral Movement; Endpoint Defences (including antivirus strengths and weaknesses, and detailed anti-hacking technologies); and Persistence and Network Defences.

Lloyd's Maritime Academy also offers an online course that grants a certificate in maritime cybersecurity. Port managers, harbour masters and ship managers can take a 12-week course that offers a greater understanding of the cyber risks posed. It looks at monitoring of cyber incident investigations, emergency response mechanisms, how to tackle extant threats and reducing the impact of potential attacks.