BEWARE the invisible threat

As more and more essential systems become automated, ports and shipping companies need to be more cyber-aware. **Federica Ragonese** investigates

As the container industry rapidly becomes more and more reliant on IT and increasingly focused on automation, the need for its players to be fully aware of newer types of threat such as cyber-attacks is increasingly urgent.

Andrew Ginter, vice-president industrial security at cyber-security provider Waterfall Security Solutions, told ***CM*** that the risk of falling victim to cyber security attacks is increasing as vessels and ports deploy new kinds of automation.

"Remote monitoring, diagnostics and even remote control of some automation systems are becoming increasingly common, dramatically increasing cyber risks. Concern seems to be increasing, as stakeholders become increasingly aware of modern threats," he said.

Philip Tinsley, security manager at BIMCO, the largest international association representing ship-owners, agreed that as more automation is introduced, the risk of cyber-attacks increases.

Gerry Northwood, COO of security provider MAST, added that as the industry becomes more IT-reliant, there is always a risk that cyber criminals will be "one step ahead of the good guys". He elaborated: "There is always the risk that, as you put in place new systems and you are trying to improve the efficiency of ports and shipping through more reliance on IT management systems, your security might fall behind."

Peter Broadhurst, senior vice-president for safety and security at mobile satellite communications provider Inmarsat Maritime, said that the increased risk of falling victim to cyber attacks was attributable to shipping becoming part of the modern age. As pointed out by the International Maritime Organisation (IMO), vessels are now digitally connected, with electronic navigation and chart updates and internet access for crew members.

As Broadhurst explained, passing data from shore to ships to keep electronic charts up to date, which can be done by satellite connection or through the delivery of a DVD or USB stick, exposes vessels to viruses and malware. The introduction of internet access on board makes vessels a target for hackers.

CATEGORIES OF THREAT

According to Northwood, potential cyber threats can be broken down into four main categories: activists; criminals wanting to break into systems to perform illegal activities; opportunists looking to cause mischief or make some financial gain; and industrial or state-sponsored espionage, which can also include terrorist threat.

Emmanouil Vrentzos, senior consultant on cyber threat intelligence at security consultancy Control Risks, told ***CM*** that states aiming to gain an advantage in conflicts taking place in areas such as the South China Sea, the Gulf, the Eastern Mediterranean and the Black Sea are using cyberspace to collect vital intelligence and are building the ability to undermine the economies and critical infrastructure of rival nations with sophisticated malware.

"Key geopolitical players are likely to be using cyberspace to collect vital information such as cargo contents, or to exploit automated cargo handling systems to smuggle explosives, weapons or communications jamming devices on board a vessel," he said. "They are also likely to be developing malware capable of undermining the seaworthiness of rival states' merchant fleets."

According to Vrentzos, most cyber security experts are increasingly concerned about the growing reliance of vessels on computer-controlled navigation and propulsion systems. "They have emphasised the compulsory introduction of

> "No matter how good some companies are, there are always parts of the industry which are behind the curve in the cyber security world and that is where the main threat will stem from"

Electronic Chart Display and Information Systems (ECDIS) by the end of 2017, which is potentially vulnerable to cyber-attacks," he remarked.

Tinsley told ***CM*** that another major concern around cyber security lies in the vast differences in operational technology and training in the shipping sector across the different regions. "No matter how good some companies are, there are always parts of the industry which are behind the curve in the cyber security world and that is where the main threat will stem from," he elaborated.

He added that, while the whole industry is aiming for more automation on board ships and becomes increasingly reliant on information and operational technology, some ports – for example, in Africa and Southeast Asia – still do not fully understand cyber threats. According to Broadhurst, reliance on Information Communication Technology (ICT) to improve efficiency leaves ships vulnerable to cyber attacks, which could lead to service disruption and in some cases injuries to personnel.

Left: Andrew Ginter, vice-president of industrial security at Waterfall Security Solutions

Right: Peter Broadhurst, senior vice-president for safety and security at Inmarsat Maritime

Below: Philip Tinsley, security manager at BIMCO

He went on: "Unfortunately, when connected to the Internet, ICT systems are open to abuse and hackers, some of whom can just be malicious, while others are professionals who are trying to benefit financially."

According to Ginter, the most serious form of cyber attack is cyber sabotage. Sabotage of navigation systems could potentially lead to ships hitting underwater obstacles or running aground, while sabotage of container handling systems at ports could potentially result in safety hazards to port personnel.

"More general sabotage of navigational and control system computers can leave vessels and port facilities incapacitated for days or longer as replacements are delivered on an emergency basis," he added.

Vrentzos told ***CM*** that in the short term container shipping and port management companies are as exposed as the rest of the economy to cybercrime, including 'ransomware' attacks, where sensitive business information is encrypted and blocked by attackers and the victim must pay a ransom to recover it.

He added: "The same companies are also likely to fall victim to generic phishing campaigns or social engineering attacks, which aim to infect computer networks with malware. As well as the creation of botnets – infected computers remotely controlled to facilitate cybercriminal operations – these malware attacks aim to intercept sensitive information, such as the contents of containers on-board vessels."

A CONSERVATIVE INDUSTRY

According to Vrentzos, the most significant danger in the maritime and port management sectors is the absence of a cyber security culture. He said that key stakeholders fail to consider cyber security as a priority area, and employees are not adequately trained against cyber attacks or aware of the risks involved in the use of unauthorised USB sticks and smartphones.

Broadhurst pointed out that the industry does not always embrace new technology very well and its players usually look at the advantages of using ICT without being fully aware of what they are exposing themselves to.

He added: "Over the last year there has been more awareness, but we are still not seeing a lot of activity in terms of implementing any real best practice around how to protect data. That is something that Inmarsat is proactively pursuing." The company is currently developing a new cyber security product that will be available at the end of 2016.

According to Tinsley, the main underestimated threats to the container shipping industry are organised criminals infiltrating shipping manifests in order to identify containers

carrying high-value products or to insert illegal products into low-value containers.

"A sophisticated criminal might think that nobody is checking the manifest of containers carrying, for example, rice and may decide to put illegal products – drugs, cash or weapons – into those containers, which get processed very quickly," he explained.

According to Ginter, targeted, remote-controlled cyber attacks can routinely defeat even the most sophisticated IT cyber defences, which means that the shipping sector needs to start "deploying safety/reliability-centric cyber protections".

While IT defences such as firewalls are relatively effective at protecting data, he pointed out, they are not effective for industrial control systems like those used in the shipping sector. "The real problem is that automated equipment is increasingly connected to networks, and the networks are interconnected. Any connection between networks that allows commands, queries or any kind of message to enter from an external network enables attacks to get through as well."

Ginter observed that encryption systems can be used to encrypt attacks as easily as they encrypt data. He added that more players in the shipping industry need to start using unidirectional gateways to protect their networks: these ensure a one-way flow of information out of the industrial system, while physically blocking all communications and cyber attacks trying to enter it from the Internet.

"Unidirectional gateways permit monitoring of critical shipboard and portside automation systems, and can even be configured to provide disciplined remote control of some such systems, without the risks of remote control attacks that so bedevil IT-style protections," he added.

Broadhurst stressed that raising awareness and educating ships' crews on how to use ICT is also necessary. He said: "Education is part of Inmarsat's strategy: we have to make sure that everybody is aware of the cyber threat, has done some risk analysis and is taking prudent measures."

He added that the majority of shipping insurance policies do not cover vessels for a cyber breach. "Insurance companies are only just becoming aware of the need to cover vessels for this new area, which they are having to seriously consider. They can no longer sit on the fence waiting to see what will happen."

RAISING AWARENESS

According to Tinsley, BIMCO is trying to raise awareness on the different types of cyber threat. "We would encourage a more open reporting system, but unfortunately there is not a single source which the industry can report to. This is something BIMCO is looking at," he added.

In January BIMCO, together with other shipping organisations, published a set of guidelines to help the industry protect against issues that could result from a cyber incident on-board a ship. According to Tinsley, BIMCO's document, which was approved by the IMO, goes hand in hand with that organisation's recently published interim guidelines on maritime cyber risk management.

Tinsley stressed that cyber security can only be dealt with if senior management understands what the threats to its business are, adding that management must be made aware of the threat and must then take action by training staff and raising awareness.

Northwood pointed out that complacency within the industry is probably the biggest danger. "Not identifying the cyber threat in the first place and doing something about it is probably the biggest problem. Even addressing the issue in terms of very simple, low-level response plans and IT awareness does a lot to improve security."

He added that more attention should be paid to the International Ship and Port Facility Security (ISPS) Code, a set of measures to enhance the security of ships and ports. Also,

Above: BIMCO's cyber security circle awareness diagram

> targeted, remote-controlled cyber attacks can routinely defeat even the most sophisticated IT cyber defences, which means that the shipping sector needs to start "deploying safety/reliability-centric cyber protections"

he concluded: "Shipping companies have to perform their due diligence on the ports they are operating from and the people who are providing the cargo very thoroughly. They need to understand what protection measures are in place at the embarkation and disembarkation points."

Vrentzos explained that shipping companies are advised to improve their cyber security awareness by adopting BIMCO's guidelines, adding that Control Risks strongly recommends introducing a tailored cyber threat intelligence programme that covers the surface, deep and dark webs [parts of the internet inaccessible to search engines], including social media, to identify early warning signs of cyber threat.