Breaking Down Technology Threats

The word tsunami might have its roots in 19th-century Japan, but its meaning bears a striking modern-day relevance to the technology-based issues crashing down on the titanic and project cargo industry today.

The Meltdown Nature-induced maritime phenomenon can have devastating effects on individuals, communities, infrastructure and business; cyber incidents threaten to do the same from a technology standpoint. Cyber breaches are rising rapidly around the world affecting almost industrial sectors at different speeds, and the breakbulk industry is no exception. Jerry Loo, AML Shipping senior IT manager, put it plainly: “We should not imagine that, as a niche shipping segment, the multipurpose sector is any less prone to cyber attack.”

Gao pointed to a recent UK government survey of 1,000 businesses – most of which had no e-commerce interests – which indicated that 16 percent had had at least one cyber security attack in the past year, and concluded that 74 percent of businesses agreed that cyber security was a high priority for their senior management. And that is just a fraction of global businesses that face new daily threats of cyber attack.

RISING TIDE

The breakbulk industry is increasingly at risk from an exponential rise in cyber security threats, especially through specialist vessels and ports.

“EPCs, freight forwarders, ship’s crew, ports and associated industries may have recently experienced one form or another of cyber attack,” said Christian Vincente, vice president of media communications at Navireo, a maritime communications and connectivity company. “Many more may not be aware of the threats posed and may only have a little awareness and even less risk management in place to mitigate issues from cyber attacks. Historically, ships had no real need for IT networks, and there were only a few low-cost options for advanced IT networks.” However, times have changed and most ships now have an IT network of some type.

The high-profile cyber attack on the Port of Antwerp from 2011 to 2012 created a groundswell of concern around maritime-related cyber threats, leading to several maritime industry initiatives. One such initiative was HIMCO’s guidelines for cyber security so vessels that provide guidance and best practice for its members. The International Maritime Organization also plans to create cyber security certification for vessels. And from May 25, 2016, the EU General Data Protection Regulation will affect every organization that processes the personal data of EU residents this includes multipurpose vessel operators which process data for crew and staff.

With international bodies ramping up cyber security awareness, a global manufacturer is also leading up a cyber risk reporting initiative, the CSO Alliance. “A concern is that the International Maritime Bureau states at least 30 percent of all maritime crime is still unreported, so there is work to be done,” said Director Mark Smith. He added that CSO’s database has logged 1,060 maritime crimes since 2003, but none were noted as cyber crimes. The plan is to enter all of these crimes in CSO’s database for the future.

WARNING SIGNS

Warning signs of cyber attacks are now better known and can be recognized and mitigated by well-equipped vessels. The 2016 Maritime Security Survey by BHS Fairplay, in association with HIMCO, found that 74 percent of responses were clear that computer systems were the most common form of maritime cyber attack at 77 percent. Phishing: The fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers, in second, at 17 percent. Denial of service, an interruption in an unauthorized user’s access to a computer network, was ranked third at 18 percent. As the numbers of attackers are translated into the real world, new forms of attacks such as ransomware – a crypтовiral attack that holds the victim’s data hostage – are also evolving.

Jordan Wylie, campaign director for the Cyber Aware at Sea, said that a company’s biggest vulnerability is its people, and that identifying warning signs of a cyber attack is the first step in mitigating losses. False alarms can be costly in terms of time and manpower, but so can ignoring an ongoing attack and willful blindness where companies avoid action for fear of repercussions on the board or wider liabilities.

“Ports and ships are reluctant to report cyber crime for fear of being branded whistleblowers, tarnishing reputations and insurance issues, but people will report cyber crime anonymously,” pointed out Christopher Ham, an external partner with the CSO Alliance. “Anonymous reporting appears to be the only way to gather data at the moment.”

CRITICAL INFRASTRUCTURE

The motivations of cyber attackers are hidden and can vary from financial gain or international terrorism to monopoly or industrial espionage. Reports indicate that attacks are as diverse as phishing attacks and from nation states to disgruntled individuals.
employees. Breakbulk cargo specifically destined for a project could be the objective of a cyber attack for industrial espionage with the motivation attack of a vessel by a competitor or an insider.

Geopolitical conflicts are another source of threat for cyber attacks on project cargo. In 2016, South Korea reported about 280 vessels had to return to port after experiencing problems with their navigation systems, claiming North Korea was behind the disruption.

"Ships have no means of response to cyber attacks once they are more than 300 kilometers out to sea and are often helpless," Henny explained. But it is not just vessels at sea that are vulnerable. Henny added: "In one case on a roll-on, roll-off ship an email attachment was opened by a crewmember which enabled downloading of ransomware on to the crew list for a charter for military supplies. Consequently, the ship was stuck in port for three days causing US$30,000 of losses."

One reason cyber crime is rising is that it is lucrative and the probability of being caught is lower than traditional piracy. Project cargo is particularly vulnerable as it involves high-value assets. Protecting critical infrastructure in ports or on vessels is a complex task, and identifying the critical infrastructure of a vessel or port that is most vulnerable, and which offers the highest probability of successful attack and therefore the highest profit to attackers, is the first step a chief security officer should take.

According to Navarino's Vakarelis: "Communications at sea is increasing exponentially, with more and more data being transferred as vessels become extensions of the office making vessels more difficult to secure." Increasingly, ships are using networks for everything from engine monitoring to form filing for entering new waters as well as crew's bank accounts. Vakarelis said that one ship that was hacked saw the hackers get into the port's infrastructure and identify valuable contents in specific locations.

Sharif Gardner, cyber unit training manager of Novae, an insurance underwriting company headquartered in London, saw the main losses from cyber attacks as cost of damage to data which meant potential loss of hire risks, causing business interruption.

According to the IHS Study, of those respondents who acknowledged that their systems had been compromised, 67 percent experienced IT downtime; 48 percent lost corporate data, such as email, personal data, payroll, or human resource information; and 21 percent endured some form of financial loss.

"In one case on a roll-on, roll-off ship an email attachment was opened by a crewmember which enabled downloading of ransomware on to the crew list for a charter for military supplies. Consequently, the ship was stuck in port for three days."

- Christopher Henny, CSO Alliance

In terms of cost, half of those attacked faced costs of less than US$5,000, but a quarter lost up to US$50,000 and in two cases costs were more than US$500,000.

FINDING A SOLUTION

Breakbulk cargo handler Virginia Port Authority, or VPA, said it had implemented several cyber security strategies to mitigate cyber threats and associated losses. These include a defense and depth strategy; defense against phishing; and the 'principle of least privilege'. This last strategy means that individual employees are given minimal access to systems which they need to do a job and no others. "For example, if an employee is only in charge of breakbulk cargo then they are only given access to breakbulk modules," said Darich Runyan, senior director for information security at VPA.

"We have been pretty lucky so far as the marine terminal industry is still manually driven so there is not that much incentive for cyber attacks," he continued. "However, we face lots of reconnaissance attacks, almost everyday, and phishing, too."

At VPA, the breakbulk operating systems are separate from VPA’s primary terminal operating system, or TOS, although, the authority is in the process of migrating off an older mainframe system to a more modern cargo module provided by its TOS vendor.

"This will give us the ability to better defend our breakbulk program since it will be integrated within the TOS," Runyan said.

MARITIME CYBER AWARENESS

Creating awareness of cyber security threats and associated risks involves educating staff at all levels. "If you are thinking about cyber security for breakbulk and project cargo, either on vessels or in ports, then you need awareness. Knowing about threats and assessing the risks is just not enough to mitigate losses," said CSO Alliance’s Sutcliffe.

CSO Alliance intends to mobilize a global community of 400 company security officers, or CSOs, in more than 40 countries to more effectively counter maritime crime in a secure portal accessible via tablet and mobile. This will allow CSOs to connect, inform each other of the risks they face and, through structured information exchange with key stakeholders and the military, get support for their security planning and actions.

"The key issue in cyber crime is to ensure there is a clear boardroom understanding and awareness," said Sutcliffe. "There are at least two levels of cyber security awareness campaigns that you can implement; a global one, involving international agencies, and local one involving in-company awareness. Linking these two together will make your cargo even more resilient against losses from cyber attacks."

Jonathan Di Rollo is a freelance writer and cyber security awareness trainer based in Malaysia.