CYBER SECURITY AT SEA

We've only just begun

If you think cyber security issues in shipping have been resolved, think again – or be prepared for a rude awakening.

JORDAN WYLIE
Founder and principle consultant,
JWC International

The maritime industry is in fact among the most vulnerable to cyber attack. Ironically, shipowners are among those least concerned with cyber risk, according to Jordan Wylie, founder and principle consultant at JWC International, a global cyber security advisor.

"The term 'cyber attack' means many things to many people," says Wylie. "While the protection of personal and financial data is critical, shipping companies face additional higher profile risks."

"As we increasingly turn to hyper-connectivity, where machines communicate with each other, we join every other sector that wants to conduct business faster, distribute goods cheaper and operate more efficiently," he says. "We are doing this with little to no understanding of the security implications related to internet connectivity, and therefore we place our vessels, crew, systems and operations under increasing risk by joining this connected network without segregation or separation."

Despite this dire, or at least dour warning, Jordan Wylie can see why many do not take this present danger seriously:

"Understandably, people and businesses are sceptical. This is probably one of the most misrepresented risks in history, and it is largely misunderstood by a majority of people and businesses alike." The problems, Wylie claims, are often considered to be over-dramatised by the cyber security industry in order to sell security technology products.

But if you don't consider cyber security an issue, he warns, then consider the many cyber-attacks on businesses in the past few years, particularly the hacking cases that affected Yahoo. Despite its significant cyber security resources and budget, this internet giant was the victim of a breach affecting over 1.5 billion personal accounts, demonstrating the vulnerability that every company faces when it comes to security.

—

While the protection of personal and financial data is critical, shipping companies face additional higher profile risks.

Wylie reports that thousands of new malicious software and viruses are being discovered every single day, along with new software vulnerabilities, meaning that managing a company's exposure to cyber risk has never been more demanding. Far from being a retired issue, Wylie warns: "I would certainly not consider the cyber problem to be resolved."

The new reality
As the reliance on smart and automated operational technology systems increases within both

the shipping and offshore industries, so do the vulnerabilities of these critical systems to cyber-attack as they become increasingly connected to the Internet.

Another problem seems to be one of attitude, rather than technology. Owners and operators tend to feel their ships and cargo are not of interest for hackers. So what can be done to change attitudes and help owners prepare for the reality of cyber attacks?

“Attitude is linked to understanding,” says Wylie. “Cyber space is largely misunderstood, yet it is the backbone of the modern economy. The Internet is one of the most powerful creations in human history, yet 99.9 per cent of us do not understand how it works and therefore we do not understand how to defend our very dependence on it.”

On the other hand, Wylie concedes that hackers are probably not after a ship’s cargo or interested in taking control of a vessel. There are significantly easier and less risky ways for cyber criminals to make money, he says, like a simple ransomware infection on a shipping company’s system, encrypting cargo manifests and allowing the attacker to hold information hostage. The ransom cost in these cases is compounded by the loss of productive time until the data is recovered.

In addition, many companies underestimate the value of employee personal information that can be sold by hackers on the black market. “For this reason, every person, company and organisation is considered a potential target to hackers who comb the Internet to find soft targets to breach,” he says. In addition to the financial impact of cyber extortion, or the safety and operational impact of operational systems being compromised, companies also face significant legal and reputational impact from a cyber breach.

Get serious

This is where Wylie’s message gets serious for management: “Education about the emerging cyber security risk is not only necessary for crew members and employees, but also at the executive management level.” The sooner the boardroom recognises information and cyber security as a top business risk, as opposed to being “just an IT issue”, the sooner appropriate planning, manpower and resources can be prioritised to mitigate this growing risk, he says.

He advises shipowners to identify their business-critical systems and sensitive information assets and conduct regular risk assessments to ensure adequate controls and resources are in place to protect these systems and assets as a priority. “It is essential that these controls and resources be clearly defined in a corporate information security policy which should be complied with across the company and supply chain,” Wylie maintains.

But, do owners and operators have any real hope of keeping pace with hackers and cyber terrorists?

Online is quickly becoming the new front line.

“The technological environment on which our industry has become increasingly dependent, is a dynamic one with security vulnerabilities being discovered on critical systems and software on a daily basis.” It then becomes a race for the vendors and security practitioners to develop fixes or ‘patches’ to eliminate the identified vulnerabilities before hackers can exploit those gaps in security to gain access to a company’s critical information and systems.

Stay smart

For all these technological weaknesses, the weakest link of all may be the people themselves. “One of the most common security vulnerabilities for all companies, including shipping and offshore organisations, is their employees,” Wylie says. “Uninformed employees can easily be exploited or tricked into downloading malicious software onto company networks or conned into providing passwords to accounts and systems, all of which will provide the attacker access to your critical information.”

The development of a strong security culture through regular training and awareness campaigns is Wylie’s recommendation as the most effective fix for this vulnerability. He is a champion of the maritime and offshore industry initiative “Be Cyber Aware At Sea” campaign, designed to provide shipping and offshore companies with the tools, advice and products to help develop a strong culture and equip crews with the knowledge to identify, report and manage common cyber security threats to the workplace.

Another pitfall Wylie warns against is the once-ubiquitous USB stick, which he says can be pre-loaded with near invisible viruses that open a computer to hackers without the user being the wiser. In other words, be as sure of what you are putting in your computer as you would of what you put in your mouth.

Even with adequate precaution, Wylie says the maritime community still needs to be prepared for the worst, and even for the not-so-bad:

“The most likely attack scenarios we can expect against the industry in the near future will continue to be the common indiscriminate activity of very simple ‘phishing’ or ‘water holing’ attacks, where a user is duped into visiting a malicious website,” he relates. “Whilst these are very easy to defend against with education and up-to-date anti-virus, they are still rising in occurrence.”

And as the maritime industry’s business and safety critical systems become more connected to the internet, so do maritime operations become more exposed to worst case attack scenarios such as the targeting of navigation, safety and communications systems in order to disrupt the systems or deny access to them.

“Online is quickly becoming the new front line,” Jordan Wylie concludes, but he has a lifeline to throw out in the churning cyber sea: “The reality is that fortune favours the prepared.”

Jordan Wylie brings the message home