Challenge of keeping up with technology

BIMCO's Phil Tinsley explains how increased cyber awareness brings both opportunities and threats

Phil Tinsley

Shipping companies need to be able to understand cyber threats

Credit: Yuri Samoilov

Some new buzzwords have entered the shipping industry's vocabulary, words that until recently had not been heard on board ships, in ports, in shipping company offices or in broking houses. These words – IoT (the Internet of Things), big data, cyber space and cyber hygiene – are now routinely slipped into conversations when discussing current and future threats to the shipping industry.

Topic: Cyber security

Keywords: IoT, big data, risk

Background: Vulnerabilities need to be exposed if the industry is going to capitalise on the opportunities offered by technological advances

Such threats, however, should not be taken in isolation, giving the impression that the industry is doomed. Future developments within the cyber world have the potential to bring efficiencies and improvements with cost and labour saving measures, greater safety and environmentally aware procedures, and more secure operations throughout the whole of the shipping industry.

The current reality is far from certain. Companies are reluctant to share information regarding cyber attacks on board ships for fear of reputational damage and, in some cases, the need to protect their brand integrity. This results in challenges for organisations like BIMCO, who are keen to assist the industry as a whole and ensure that preventative measures and adequate training are implemented to mitigate cyber security risks. It is a real challenge to identify the scale and type of threat unless the industry willingly shares its experiences. Even with the offer of full confidentiality there is still widespread reluctance to share incident information even to an impartial body such as BIMCO. Understanding the actual threat, how to deal with further attacks and prevent re-occurrence are a common theme throughout the guidelines published so far.

Cyber awareness from a security and a safety perspective can be developed through a stepped process as depicted in the diagram. Any one of the fins could be a starting point for a ship to begin their awareness campaign, even if it is due to an incident which requires a response. Learning from an incident and ensuring preventative measures are put in place reduces the risk from that threat re-occurring.

The *'Guidelines for Cyber Security Onboard Ships'* is a publication produced by BIMCO and partners, including the International Chamber of Shipping, Intertanko, Intercargo and CLIA. This document has been in circulation since the beginning of 2016 and has received support from many areas within the industry. Those companies that have studied the guidelines and put procedures in place have taken the first step towards protecting their assets against what is perceived as a growing threat. This protection starts at the very top and unless cyber security is addressed thoroughly at board level with time and money set aside for training personnel, ensuring operating systems are secure, measuring risk appetite and developing cyber resilience, the threat will not diminish.

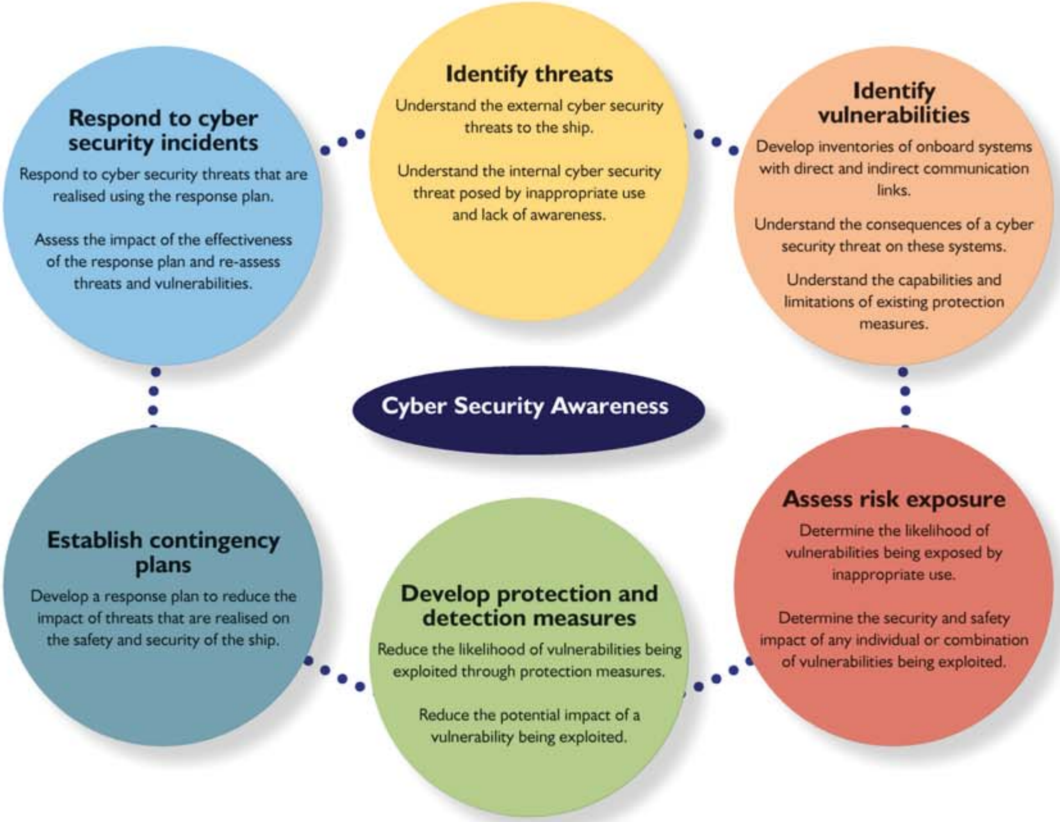
Full disclosure

When chartering ships to third party operators it is important to audit the operating systems that will be introduced on board; and the connections to shore establishments to ensure secure communications are maintained and to avoid infection by software bugs (malware) which may remain embedded in the ships operating system once the charter is over.

Marine insurers are now very much aware that cyber threats must be taken seriously. Cyber Attack Exclusion Clause 380 is currently a common agenda item in the boardrooms of shipowners and operators. This clause states a requirement for shipping companies to consider losses arising from computer use, computer systems or computer software. Failure to provide proof of mitigation and lack of cyber threat consideration could lead to insurance cover being voided in respect of future cover and subsequent claims.

The attitude that cyber criminals are only interested in big companies to extract the maximum possible payout is pure myth. Whether the criminals are activists, including disgruntled employees, criminals, opportunists or terrorists, their motive and objectives may differ considerably. The challenge for a hacker to attempt to gain control of a ship's operational system may be seen as just that - a challenge. He or she may not have any motive other than to prove it can be done.

How can cyber protection be enforced? Only by finding out what the vulnerabilities are through a third party penetration test, audit or an independent review, can a shipping company understand their vulnerabilities. Yes, this is an extra cost but is likely to save further financial losses in the future not to mention the reputational damage a serious cyber attack could have on a


Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and lack of awareness.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communication links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protection measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish contingency plans
Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.
Respond to cyber security incidents
Respond to cyber security threats that are realised using the response plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.
Cyber Security Awareness

company or shipping line. The question should be asked "Can we afford to do nothing?"

The future operational objective for ships and ports is to move into a more digitised arena with the development of paperless ships and fully automated systems. There will no doubt be development issues but there is an interesting lead from Danish shipping which has moved to digital certification of ships, transitioning from the traditional paper based system to using electronic certificates from June 24, 2016. This follows 100 Maersk Line boxships going paperless in late 2015 and will be an interesting keyhole to the challenges ahead.

Complete connectivity

Shipping companies looking at future employment trends realise the traditional remote and unconnected life of seafarers will be overtaken by a requirement for shorter periods at sea and full connectivity at all times. The thought of being "unconnected" is a prospect that many within the younger generation would not contemplate within their job searches. The challenge for the future is to detach the operational technology from the information technology with separate secure systems and guaranteed communications.

The progress in navigational systems in conjunction with electronic charts, which will become mandatory in line with the requirements set out below, is recognition of the accuracy of and dependency on modern navigation systems.

Sceptics will argue that more electronic dependency increases the risk of cyber security breaches. The opposing argument is that this is a natural development within the industry which creates endless opportunities to be more efficient with resulting cost savings. As cyber awareness develops in the industry, measures must be put in place to develop security measures at the same pace that technological advances are made.

There are no short cuts to building up resilience, but with a clear review of procedures, equipment and the increased knowledge and awareness of personnel, these should be seen as important first steps. It matters not if readers are from an agency, brokering, chartering, insurance, or ship management background – the approach and measures should be exactly the same. If the industry as a whole can act together on cyber security and take unified action it will hopefully save organisations from suffering some of the financial losses, reputational damage, and loss of customer faith that a number of well-established businesses throughout the world have suffered as a consequence of cyber crime. **SN**

Phil Tinsley assists BIMCO members with all aspects of maritime security, including piracy, drug smuggling, stowaways, mixed mass migration and cyber security. Prior to pursuing a career in maritime security, Phil was an officer in the Royal Marine Commandos, attaining the rank of Major after 31 years of military service.

"Even with the offer of full confidentiality there is still widespread reluctance to share incident information even to an impartial body such as BIMCO"

A total of 100 Maersk Line boxships went paperless in late 2015