UK P&I CLUB

NYA

TT CLUB

# Risk Focus: Cyber

Considering threats in the maritime supply chain

UK P&I CLUB
IS MANAGED
BY **THOMAS**
**MILLER**

**CONTENTS**


| | |
|---|---|
| Summary | 3 |
| Introduction | 4 |
| Impact on maritime supply chain | 5 |
| Onshore | 6 |
| At sea | 8 |
| Call to action | 12 |
| Response | 13 |
| Conclusions | 13 |
| Glossary of terms | 14 |
| About us | 15 |

# Increasing use of automated and digital systems is exposing the sector to a greater risk of cyber crime

- The IMO Resolution MSC.428(98) prompts the shipping community to understand cyber vulnerabilities and how they could affect operations
- A number of leading actors including BIMCO and the US Coast Guard have contributed to industry guidelines
- Regional directives and legislation such as the Directive on Security of Network and Information Systems (NIS Directive) and EU General Data Protection Regulation (GDPR) are indicative of the growing importance of cyber security
- Cyber incidents have varied from unsophisticated mandate fraud scams and ransomware viruses to Global Navigation Satellite System (GNSS) and Automatic Identification System (AIS) jamming and spoofing
- Cyber-crime-as-a-service, or the purchase of attack methods on the dark web, has made it easier for those with limited technical capability to conduct sophisticated attacks
- The overwhelming majority of incidents are not targeted attacks
- Inadequate training and a lack of awareness around cyber security both onboard ships and onshore elevates the likelihood of incidents caused by human error

## Introduction

On 27 June 2017 the shipping giant A.P. Moller Maersk fell victim to a global malware attack known as 'NotPetya' also referred to as 'ExPetr'. Online cargo booking was consequently impacted, forcing staff to use personal email accounts to respond to critical emails. As key processes relied predominantly on IT systems, personnel were forced to resort to manual processes. It took almost one week for all services to resume and for the shipping firm to regain total control of its systems.

Maersk has since revealed the attack caused congestion in as many as 80 ports operated by APM Terminals and cost the company as much as USD 300 million. Estimates suggest the global ransomware attack resulted in losses of at least USD 850 million, with predictions of future attacks to be in the billions as economies increasingly rely on IT infrastructure.

This untargeted incident highlights the shipping and logistics industry's vulnerability and perhaps more importantly, the need to adopt appropriate response protocols. In early 2017, SeaIntel revealed 44% of the top 50 carriers have weak or inadequate cyber security policies and processes, including weak passwords, delayed installation of security patches and the use of unencrypted web browsers. Given this current state and increasing automation in the maritime and logistics industry, it is inevitable companies will require a robust information security management system.

### The move towards automation

The shipping and logistics industry has increasingly moved towards better integrated and automated systems. The International Maritime Organization's (IMO) e-navigation concept, first introduced in 2006 to enhance navigation safety, is one example of the demand for more integrated systems to improve efficiency and reduce risk. E-navigation essentially collects, integrates and analyses data from ships at sea and at shore using electronic systems. The main motivation behind this move has been to mitigate the rising number of marine accidents, the majority of which are caused as a direct result of human error.

With the expansion of digitalised systems, training and staff/crew awareness are crucial. In a survey conducted by BIMCO and Fairplay in 2016, 21% of respondents from the maritime sector admitted to being victims of a cyber attack. However, the actual number of victims is likely to be higher for two reasons. Firstly, not all victims are likely to admit to the security breach particularly to avoid potential reputational damage. Secondly, it is highly likely that more victims are being targeted but effective security measures already in place are either mitigating the impact of the attack or preventing successful breaches.

With approximately 90% of world trade transported by sea, the maritime sector is an attractive and lucrative target to perpetrators of cyber crime. As a direct result of greater

interconnectivity and digitisation, particularly relating to the ship bridge, a cyber attack at sea or at the ship/port interface has become a question of when rather than if it will occur.

**New industry standards and guidance**

On 1 June 2016 the IMO released new regulation guidelines on cyber risk management to raise awareness of threats and vulnerabilities to the maritime sector. The guideline was issued in response to the increased threat of cyber related incidents reported in the maritime sector and seeks to address cyber risks under the International Safety Management (ISM) Code enforced on all ships. Resolution MSC.428(98), introduced on 7 June 2017, requires administrations to take the necessary steps to incorporate cyber threat considerations appropriately through safety management systems and address this by the first annual verification after 1 January 2021. However, it is recommended that action is taken now to identify and mitigate these risks.

The latest cyber security guideline distributed by BIMCO also advises of cyber risk management controls to be in place alongside the existing ISM and International Ship and Port Facility Security (ISPS) codes. The comprehensive guideline recommends plans to consider "ship to shore" connections including internet, radio, telecommunication, computer, network and other related systems. Cyber security as part of ship safety management systems should include measures to prevent, detect and respond in the event of a cyber incident.

Similarly, the US Coast Guard issued a draft Navigation and Vessel Inspection Circular (NVIC) 05-17 titled 'Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities'. The circular currently under review requires incorporation of personnel training, drills and exercises to test capabilities, security measures for access control, handling cargo, delivery of stores, procedures for interfacing with ships and security systems and equipment maintenance. The guideline also recommends controls in place to protect, detect, respond and recover to cyber-related breaches.

Further still, the maritime and logistics sector needs to be alert to the requirements set out in the EU General Data Protection Regulation (GDPR) adopted in 2016 will be enforced from 25 May 2018. While fundamentally concerning rights in relation to data, the same vulnerabilities in relation to cyber activity apply. The regulation will apply to all organisations regardless of their physical location, so long as the data they hold or process belongs to any individual residing in the EU – giving the GDPR extensive jurisdiction far beyond the previous Data Protection Directive of 1995. Penalties for non-compliance may be very significant; violations considered to be serious could result in a fine of up to EUR 20 million fine (approximately USD 25 million at the time of writing) or 4% of the total global turnover of the company, whichever is the higher. The new regulation has a number of mandatory requirements including consent, right to access, right to be forgotten, data portability, privacy by design, breach notification and accountable data protection officers. The maritime and logistics sector is inherently global and regularly transmits and stores information that falls in the scope of this regulation; it is therefore necessary to take steps to prepare for the implications of the GDPR.

Also of relevance is the EU Directive on Security of Network and Information Systems (NIS Directive), which is aimed at enhancing and strengthening cyber security in order to minimise the impact on the provision of critical services. The NIS Directive applies to sectors and businesses that operate in critical industries including transportation which extends to maritime carriers and ports. The extent of the impact will depend on individual member states who will set individual guidelines and penalties for non-compliance. For example, in the UK, organisations deemed as non-compliant can be fined a maximum of GBP 17 million (approximately USD 24 million). In order to avoid this, UK organisations will need to be audited against 14 principles issued by the National Cyber Security Centre (NCSC).

Thus, while some of the recent regulatory guidance provided are specific to the maritime and supply chain domain, others are indicative of the general direction of travel and highlight cyber security as even more pertinent than before.

**The threat in context**

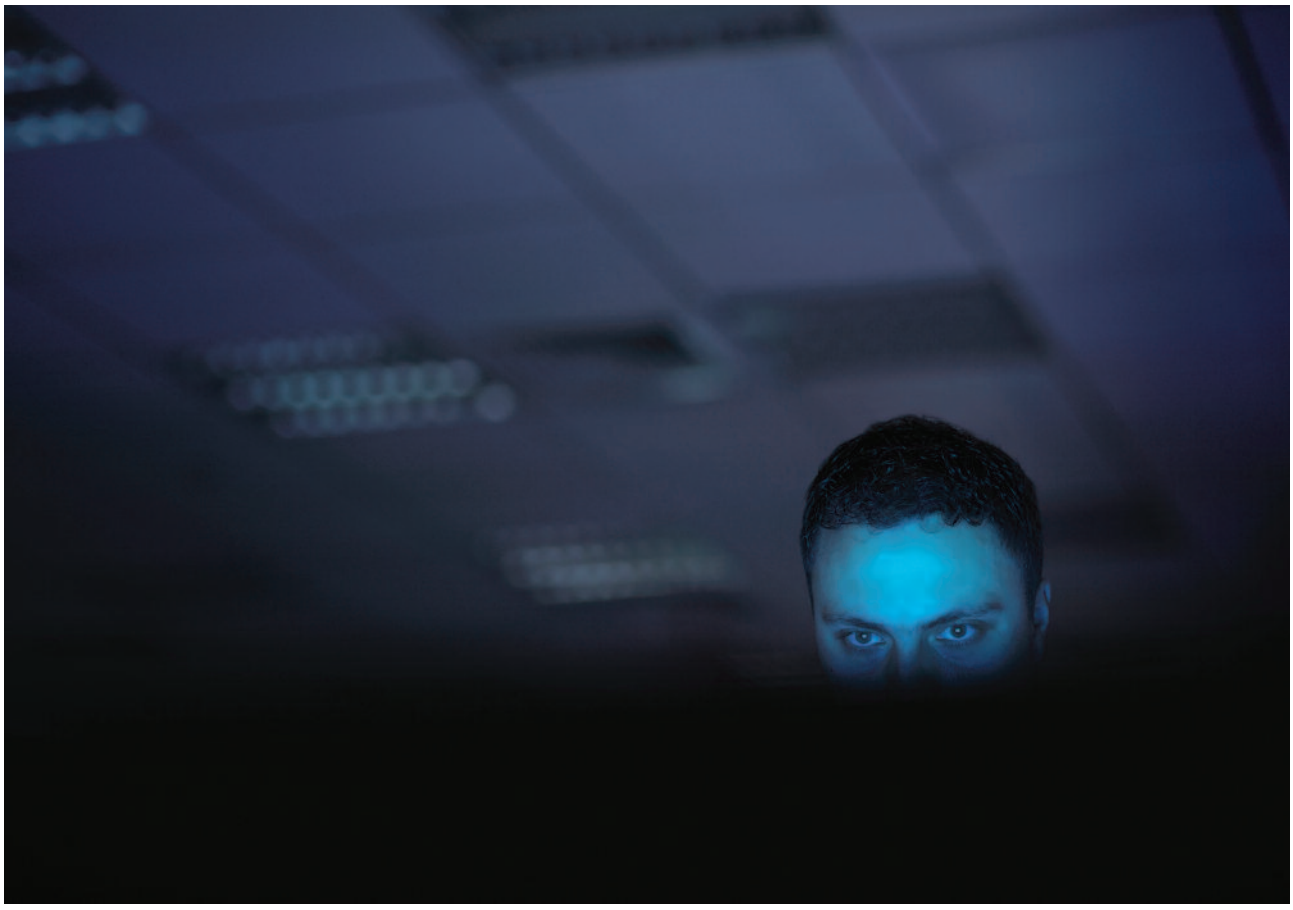
A cyber attack is the illegitimate breach by hackers to access IT systems and/or data. This can be achieved both locally via physical access and remotely by connecting to related IT networks. It is the deliberate exploitation of computer systems and networks that threaten data confidentiality, integrity and availability (CIA) – three core elements of information security. Once the flow of data is disrupted, it can result in a halt or slowing of business operations and possibly reputational damage.

In the maritime domain, a cyber attack can be the modification or destruction of any data including radio frequency (RF) domains, therefore meaning both GNSS and AIS jamming and spoofing are viable attack methods. Consequently, there are significant implications of a cyber attack that can feasibly impact navigational systems. Similarly, Terminal Operating Systems used as part of port infrastructure, for example cargo handling equipment, are equally vulnerable to potential breaches.

Cyber threats continue to evolve and remain innovative, constantly presenting new threats and exposing vulnerabilities. Reports by AV-TEST indicate an average of 4.2 new files of malware code were being generated every second in 2017. Whilst zero-day exploits, vulnerabilities that are unknown to the vendor and therefore no security patches have been created to mitigate against its vulnerability, have steadily increased in the last five years.

While patches and updates become available, cyber criminals still seek to find new vulnerabilities to exploit, thereby posing an enduring and adaptable threat. Further still, the increased sale of DDoS-as-a-service or malware-as-a-service on the dark web means that with limited technical capability, individuals can purchase malicious software and execute complex cyber attacks – undoubtedly contributing to a rise in attacks.

Ultimately, despite evolving cyber threats, the main vulnerability of attack lies in human error. While humans are largely the cause they too are ultimately the answer to managing cyber risks. Within the shipping and logistics sector, personnel have been notably targeted in social engineering attacks. Such



incidents involve the manipulation of people into sharing confidential information or performing specific actions, including transferring payments into different accounts.

## Impact on maritime supply chain

Cyber attacks reported in the maritime and logistics sector have impacted or targeted the following:

- Company online services, including cargo or consignment tracking systems
- Email correspondence by distributing links to malicious websites or files
- Removable media by spreading malicious malware
- Websites by redirecting users to fraudulent sites to encourage personnel to disclose user information
- Navigation systems (to a lesser extent)

The extent to which an attacker can breach a company operating system depends on the size of the vulnerability being exploited and the chosen method of attack. Depending on the significance of the breach, a perpetrator may be able to affect the system's operation, gain access to commercially sensitive data and/or gain full control of systems.

The motives, objectives and capabilities of the attacker will determine the effect they have on company systems and data. An attacker may explore systems, expand access and ensure they are able to return to the system in order to access commercially sensitive or confidential data, and/or disrupt operations of the company systems.

At the time of writing, there have been no publicly known major incidents resulting from a targeted cyber attack against a ship. Despite the lack of reported incidents, the growing attack surface and sophistication of attacks could result in significant economic losses.

### Man-in-the-middle attacks

Man-in-the-middle attacks have targeted the shipping and logistics industry and have resulted in payment scams similar to those faced by other industries. Such incidents are executed via phishing scams (e.g., fraudulent emails) and CEO fraud (impersonating management). In some cases, spyware has been used by cyber criminals to infiltrate victim devices and monitor email correspondence while remaining undetected on the system.

In many cases shipping companies have had their email correspondence with suppliers monitored. Cyber criminals have used the emails to pose as the legitimate supplier asking for payments to be made to a criminal account. These incidents have caused a significant financial impact, with one Malaysian bunker company losing USD 1.1 million to the scam. In this case the bunker company made two separate payments, the first on 31 May 2017 and a second on 2 June 2017. The payments were issued following receipt of a genuine looking invoice that sought to channel payments to new banking account details.

### Perpetrators

There are several key motivations and numerous actors involved in committing cyber crimes. Perpetrators can be categorised as activists, criminals, opportunists and state-sponsored actors, and while their motivations can vary, consequently so do their objectives.

**Perpetrators: Motivation and objectives**

| Group | Motivation | Objective |
|---|---|---|
| **Activists (including disgruntled employees)** | ▪ Reputational damage<br>▪ Disruption of operations | ▪ Destruction of data<br>▪ Publication of sensitive data<br>▪ Media attention<br>▪ Denial of access to the service of system targeted |
| **Criminals** | ▪ Financial gain<br>▪ Commercial espionage<br>▪ Industrial espionage | ▪ Selling stolen data<br>▪ Ransoming stolen data<br>▪ Ransoming system operability<br>▪ Arranging fraudulent transportation of cargo<br>▪ Gathering intelligence for more sophisticated crime, exact cargo location, off ship transportation and handling plans etc. |
| **Opportunists** | ▪ The challenge | ▪ Getting through cyber security defences<br>▪ Financial gain |
| **States**<br>**State-sponsored organisations**<br>**Terrorists** | ▪ Political gain<br>▪ Espionage | ▪ Gaining knowledge<br>▪ Disruption to economies and critical national infrastructure |

Source: BIMCO Guidelines on Cyber Security Onboard Ships

### IT and OT systems

Broadly speaking there are two main systems upon which the maritime and logistics industry relies heavily: Information Technology (IT) and Operational Technology (OT). Both systems are used extensively and are susceptible to cyber attacks, though the impact of an incident on either system can vary. In the case of the former, the main concern is largely reputational and financial risk, however the latter faces additional threats to physical assets.

IT systems refer to the technology used for information processing that include software, hardware and communications software. OT systems however refer to hardware and software used to detect or cause a change through monitoring and control of physical devices and processes. This is found in cyber-physical systems including motors, pumps, RF communications, navigation systems, cargo handling systems and terminal operating systems.

The convergence of IT and OT systems is considered to be relatively recent, and has also introduced the new challenge of ensuring security without disrupting critical services. Of the vulnerabilities evident in OT systems, critically is the presence of legacy systems. An entity with out-of-date software faces an elevated threat from cyber attack; while IT systems require extensive maintenance and updates, OT systems typically do not. OT systems have been designed and developed to be robust and durable, allowing them to be in place for at least 10-20 years, however this increases the likelihood of legacy systems being present. The increased convergence of the two systems, the use of software and linked networks compounds the cyber security threat as they are not updated regularly.

OT systems are comprised of both hardware and software systems that are used to monitor and control processes and at times physical equipment. Industrial Control Systems (ICS) use OT and refer to systems used to operate and automate industrial processes.

## Onshore

### Inter-connecting sites of operations

Shipping operations can be divided into three sites of operations. Firstly, operations that relate to port office facilities, information systems, communication system and machinery. Secondly, relevant onshore offices relating to the shipowner, ship management and cargo interest. The majority of communications between these two relies heavily on IT systems with the exception of machinery at ports that rely increasingly on OT systems. And finally, the ship itself which uses a combination of both IT and OT systems (see 'At sea' section).

Similar to ICS, Industrial Automation Control Systems (IACS) employed at terminals face a growing cyber threat as convergence with IT systems are cemented. IACS are made up of four components including Terminal Operating System (TOS), Terminal Logistics System (TLS), Control System (CS) and Container Handling Equipment (CHE). Such systems comprise complex networks of sensors and actuators used to guide the movement of containers and cargo.

IACS systems that are physically separated from other networks, while posing a limited cyber security threat, remain dangerous in the case of unauthorised access or software

upgrades often overlooked during maintenance works. Implementation of a sound cyber security policy used to establish a formal governance framework is effective in ensuring commitment from top-level management and can limit the impact of a security breach.

When dealing with ICS and IACS alike, it is paramount to recognise such industrial assets have longer operational lifespans than typically employed in IT systems. Hence, the requirement to separate and/or isolate systems when possible. Most importantly network hardening measures, effective patch management and continued assessment and evaluation must be employed to protect systems. In addition, IACS are likely to have legacy systems in place contributing to a more vulnerable environment, therefore requiring a detailed understanding of how systems are interconnected, and limiting the exposure of legacy systems to networks.

TOS used to control the movement and storage of cargo both at ports and terminals have been designed to optimise the process flow of transhipment. However, TOS also face a threat of being targeted. TOS can cause significant physical damage if targeted, that would naturally have financial implications. While such systems are not typically targeted, they remain vulnerable due to their increased reliance on IT infrastructure. In the 2013 cyber-physical attack at Port Antwerp, port authorities eventually installed a firewall but this was again bypassed by the perpetrators by installing wireless devices used to record keystrokes. TOS relies on several systems including mobile computers and wireless Local Areas Networks (LANs), all of which can be exploited by cyber criminals.

Additionally, disruptions at ports and terminals have further repercussions. Third party logistics companies are also inadvertently affected in such instances, resulting in further chaos, confusion and ultimately financial losses. For example, in the recent Maersk cyber attack, at least 17 terminals were significantly affected and resulted in significant losses for A.P. Moller's logistics unit, Damco, who reported losses of USD 8

**Significant incidents**

| Date | Victim | Consequences |
|---|---|---|
| **Nov 2017** | Clarksons | Perpetrators gained unauthorised access to computer systems, accessing confidential information and threatening to release information unless ransom payment is made. Company share prices decreased by 2.71% |
| **Jun 2017** | Ships in Novorossiysk, Russia | At least 20 ships in the Black Sea were reporting false data was being transmitted, indicating the ships were 32km inland of their actual position. It is now believed to have been as a result of a GNSS spoofing attack |
| **Jun 2017** | A.P. Moller Maersk | NotPetya also known as ExPetr ransomware led to outages on A.P. Moller Maersk computer systems impacting both oil and gas production and port operations. Following the incident, Maersk claimed to have changed its IT systems to prevent similar incidents from occurring in the future. The incident resulted in an estimated USD 300 million of losses |
| **Apr 2016** | South Korea | 280 ships were forced to return to port due to problems on their navigation systems. The issue was largely blamed on North Korea however this remains unconfirmed |
| **2012-14** | Danish Port Authority | An email virus spread through the port network that was likely initiated through an infected pdf document. The virus spread and successfully reached other Danish government institutions |
| **2012** | Australian Customs and Border Protection Service agency | Cargo systems controlled by customs and border protection were hacked in order to determine which shipping containers were suspected by authorities |
| **2011-13** | Port of Antwerp | The port had been a victim of an APT attack since 2011 commissioned by a drug cartel. The attack targeted terminal systems which were subsequently compromised by hackers and used to release containers without port authorities becoming aware. Illicit drugs and contraband worth approximately USD 365 million, firearms and approximately USD 1.5 million were seized when authorities finally became aware |
| **Aug 2011** | Iranian Shipping Line (IRISL) | The servers were hacked resulting in damage to data relating to rates, loading, delivery and location. Consequently, the location of many cargo containers remained unidentified and an undisclosed amount of financial losses were incurred as a result |

Source: NYA

million compared to profits of USD 12 million for the same period the previous year.

Other threats affecting port and terminal operations include disclosure of cargo information. Container release codes are often easily found and identifiable. Such key information regarding the cargo can be tempting to opportunistic criminals and can be of use to perpetrators in more targeted attacks.

The use of electronic command and control systems compounded with the increased reliance on internet-based services at ports heightens the threat of being targeted by cyber criminals. IT and OT computer security have been identified by port management as requiring particular protection. However, the process of securing ports has evolved in line with the growing cyber threat and consequently security to date has remained at least one step behind perpetrators.

**Key shoreside vulnerabilities**

Port facilities are comprised of four main asset types including buildings, linear infrastructure, plant and machinery and lastly, information and communication systems. Cyber incidents affecting ports threaten efficiency and safety of operations that could target one or a combination of asset types.

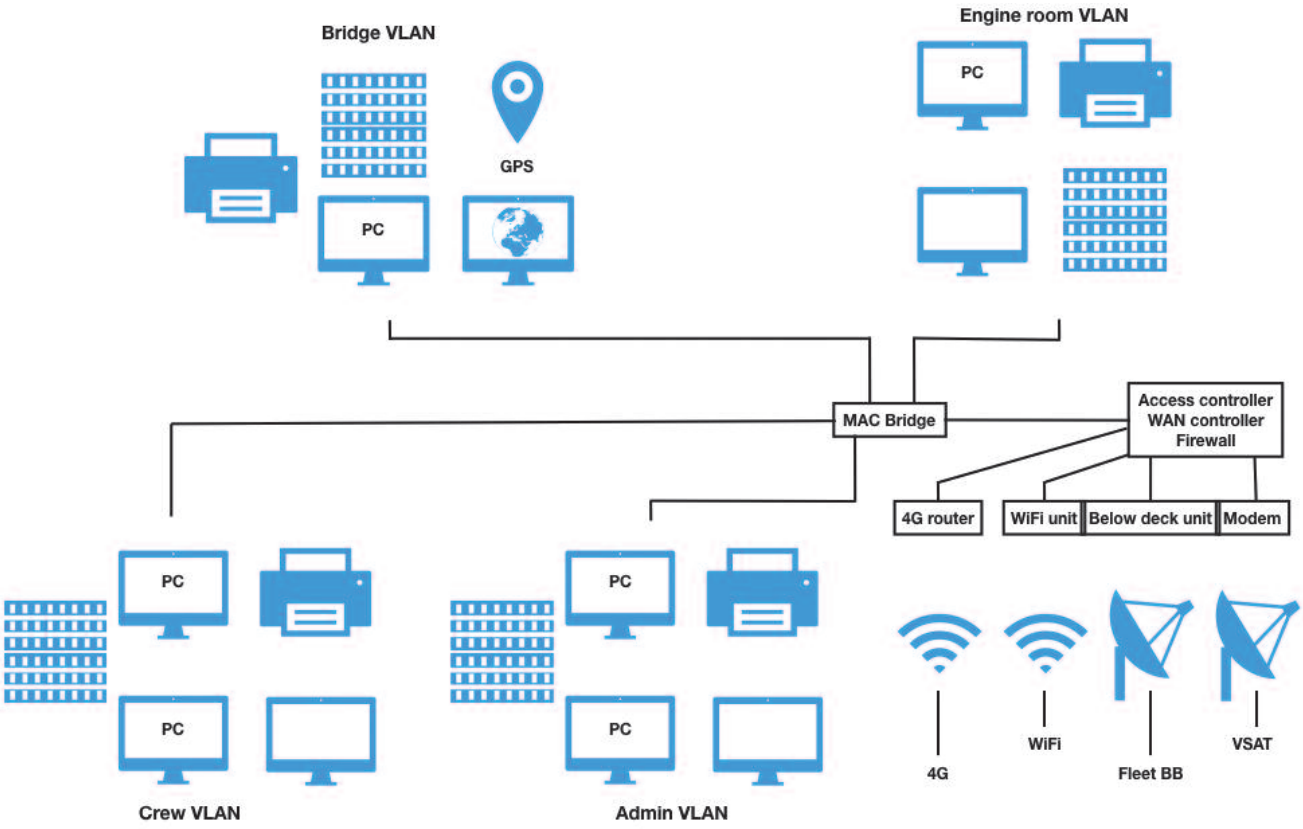
**Buildings** related to ports include maritime control centres, terminals, data centres, maintenance sheds, storage accommodation and administrative accommodation for port staff and government services. Most buildings utilise IT-based management systems.

Advanced Persistent Threat (APT) attacks can have siginifcant financial implications for ports and terminals. In 2011 Port Antwerp was targeted in a cyber-physical attack that went undetected until 2013. The attack began through an email campaign commissioned by drug traffickers to target staff at the port with malicious software. The data accessed by the perpetrators was used to identify and intercept the containers known to be holding drugs. The breach was only detected after a number of containers went missing with no known explanation. The software was later discovered and removed, after which the perpetrators broke into the port offices and locally intercepted staff keyboard inputs and took screenshots of workstations. Illicit drugs and contraband worth approximately USD 365 million, firearms and approximately USD 1.5 million were seized when authorities finally became aware. This notable attack is indicative of the vulnerability present in the maritime supply chain.

**Linear infrastructures** often include control systems and include cargo handling systems, conveyer systems and dockside linear infrastructure.

**Plant and machinery** used at ports can include tidal locks, automatic barriers or gates, cranes and conveyer systems, non-fixed cranes, gauges, pumps and valves. Most systems are controlled by OT systems with the majority connected to the port's enterprise network.

**Typical shipboard IT system configuration**




Source: NYA

**Information and communication systems** are often managed by IT systems, particularly for cargo operations. Data includes scheduling of land-side container arrival, cargo information, data about delivery, driver, container number, size and arrival time, tracking of container locations, planning and scheduling of loading containers to ships, information for customs authorities including payment and customs clearance. This is all typically organised with a centralised asset management system dependent on IT systems.

## At sea

As the shipping industry seeks continuing convergence between systems into more centralised control mechanisms, it needs to recognise the threat of expanding the potential attack surface from cyber activity. While connections between technology onboard ships are integral to operational efficiency so too is the connection between offshore and onshore. Technology is used to increase the connectivity between ships and onshore offices, and there is a growing demand for this to be the case. Data related to ship operations including key information such as fuel consumption and container tracking are increasingly demanded by onshore offices and are essential for efficiency.

### Ship-to-shore connections

- Very-small-aperture terminal (VSAT)
- Wireless Networking (WIFI)
- Fleet Broadband (FBB)
- Fourth generation broadband cellular (4G)
- Very High Frequency (VHF)
- Global Navigation Satellite System (GNSS)
- Automatic Identification System (AIS)

Ships are typically connected to the shore via satellite, 4G and Wi-Fi. Of these connections, satellite connections are wrongly believed to be the most secure, since intercepting the connection is believed to require specialist knowledge on the part of the perpetrator or hacker. However, it is important to note that none of the systems remain completely secure. Further still, 4G and Wi-Fi systems use standard security protocols that are well-known and understood by perpetrators making them likely targets. TCP/IP rules that govern the connection to the internet have known vulnerabilities that are commonly exploited by cyber criminals.

Most ships use computers to connect to the internet to transmit commercial traffic, asset tracking and general communication with the shore. The general architecture of on board systems relies increasingly on computers to operate, however they are not often interconnected. Maintaining security of standalone systems is considered to be far easier – and containment of a cyber incident more likely – than that of connected systems. However, even stand-alone systems are susceptible to human error. This could involve the use of an

infected removable device being attached to critical systems as is often used for installing updates, or social engineering attacks targeting personnel encouraging them to open a compromised link that could, in turn, install malicious content.

**OT systems on ships**

OT utilised in the shipping industry incorporates a variety of systems including Electronic Chart Display and Information System (ECDIS), GNSS, data loggers and programmable logic controllers (PLCs). Other systems include Industrial Control Systems (ICS) used for a number of key operations in the maritime sector, including Supervisory Control and Data Acquisition (SCADA) equipment that is used increasingly in maritime and shipping operations.

*OT display onboard ship – Source: NYA*

Commercial merchant ships rely on ICS for implementing a number of tasks and systems, including navigation and communications systems, fire protection on board and managing of cargo. Vessel traffic management systems also include integrated ICS.

The increased reliance on digital systems used to monitor and control onboard machinery further increases the threat as said systems are susceptible to intrusion threats both internally and externally. For example, SCADA deployed on ships controls the distribution of onboard electric power and generates data about the power consumption, which is used by the shipping company for administrative purposes. Systems can be intruded and the compromise remain undetected for extended periods of time. In this manner, hackers can infect a system, monitor the traffic, observe all activity and identify the most critical time to strike to have the greatest impact on operations, disrupting anything from access control systems and physical security of the ship and cargo, to steering and propulsion. Further still, part of ship equipment can often be controlled remotely.

ICS are exposed to several attack vectors including external hacks, denial of service attacks, and virus and worm infiltrations. Increasingly, ICS are being integrated into software applications, internet-enabled devices and other non-proprietary IT offerings; this has increased the vulnerability of such systems to malicious attacks and equipment failures. Given the nature of these systems, disruptions or failures can result in great losses including fatalities and damage to property.

While OT systems are considered less vulnerable as they are not IT based, these have also previously been targeted. The Stuxnet attack known as the Operation Olympic Games targeted Iranian centrifuges in a highly sophisticated multi-state-sponsored attack. The joint US-Israel operation was responsible for destroying approximately a fifth of Iran's nuclear centrifuges. The virus was administered in stages, with the initial attack remaining undetected on the system. The virus was designed to map out the blueprint to the Natanz nuclear plant to understand how computers controlled the centrifuges. Once understood, the worm administered into the Natanz plant gradually added pressure on spinning centrifuges without it triggering an alert to the central control system as it replayed recordings of the plant taken during the reconnaissance stage of the operation. This attack accounted for the destruction of up to 10,000 centrifuges between November 2009 and January 2010. The incident is significant as it demonstrated, for the first time, the tangible damage cyber attacks could cause on ICS.

The growing convergence of IT and OT systems used in the maritime sector has increased the threat. Central command systems used to synchronise and centralise individual PLCs are used extensively on ships. Systems such as Kongsberg Maritime C20 Marine Automation are commonly used. These systems can remain secure by running on bespoke languages not widely known by hackers or by maintaining a segmented system to decrease further the likelihood of a cyber infection. Further vulnerabilities lie in outsourcing of ICS to third party vendors.

**Vulnerabilities to ships**

**GNSS jamming**

Ships rely on GNSS for positioning navigation and timing (PNT) therefore its vulnerabilities can have serious implications for safety and navigation. Jamming can be caused by natural, accidental and indeed deliberate means. Criminals can easily purchase jammers online for as low as USD 100, with the potential to cause serious harm to ships worth significantly more. This easy access to jamming units online means perpetrators with limited technical capability can interfere with signals resulting in erroneous data being reported on other integrated ship systems.

The impact of GNSS jamming was demonstrated in a number of experiments conducted by the UK General Lighthouse Authorities (GLA). Of note, the Flamborough Head trail[1] showed the ECDIS, AIS and ship radar all presented incorrect data as a direct result of GNSS jamming. These systems are relied upon to provide key navigational and situational awareness to the ship as well as to inform other ships in the vicinity of their location and velocity. Therefore, incorrect data resulting from a jamming attack can have wider security implications.

[1] Grant, A., (2008) Research and Radionavigation General Lighthouse Authorities, 'GPS Jamming Trial'

Recommendations made by the GLA include use of Enhanced Loran (eLoran) systems[2], which similar to GNSS, is a navigation and timing system. eLoran is considered a viable backup in the case of GNSS disruption caused by natural disasters or corruption as a result of malicious and/or criminal intent.

**GNSS spoofing**

In 2013, a study by the students of the University of Texas[3] exposed a key vulnerability in GNSS systems that can be exploited by cyber criminals. The study proved hackers can feasibly intercept the satellite signal similar to a "man-in-the-middle" attack and can feed false information to the ground service. By transmitting signals to a targeted ship and increasing the strength and frequency of the signal in increments, the ship begins to trust the signal. This allows the perpetrator to feed false information to the ship and veer the ship off course while remaining undetected by both the crew and onshore offices. While in this instance the crew were aware, as this was an experiment, the test proved the potential vulnerability could be exploited and remain undetected by crew.

However, it should be noted that the majority of ships have more than one GNSS unit that are integrated in multiple systems. The connection between these systems is not always understood and therefore in the case of a jamming or spoofing incident, multiple alarms can go off on the bridge, adding to the already stressful situation. Often there are limited, if any, contingency plans in place with crew often not trained adequately to respond to GNSS receivers failing.

Further still, by compromising the confidentiality, integrity and availability (CIA) of GNSS, AIS data is also vulnerable, as positioning data transmitted by AIS relies on GNSS coordinates. On 22 June 2017 reports emerged of what is now widely believed to have been a mass GNSS spoofing attack in the Black Sea. The master of a ship in Novorossiysk, Russia, realised his GNSS coordinates placed him 32km inland. He then contacted other ships in the vicinity and at least 20 other ships claimed to be experiencing the same issue. Navigation experts claim the spoofing sent false signals and resulted in the receiver providing false information. There is speculation that this incident could have been a Russian state-sponsored attack with over 250,000 cell towers reportedly equipped with GNSS jamming devices in Russia, however at present this incident remains unconfirmed.

GNSS spoofing previously was believed to require specialist knowledge, but commercial hardware and software can now easily be found and accessed online increasing the threat of similar incidents in the future. However, spoofing incidents can be detected by crew members and therefore more covert spoofing remains harder to accomplish and, therefore, less likely.

In a report published by the London Economics title 'The economic impact on the UK of a disruption to GNSS'[4], the economic benefits attributed to GNNS used in the maritime sector in the UK is estimated at USD 587 million per annum. This includes USD 457 million saved in time and fuel as a result of navigational tools supported by GNSS, USD 91 million in fishing benefits and a further USD 11.7 million attributed to

[2] Grant, A., (2010) Research and Radionavigation General Lighthouse Authorities, 'Observed impact of GPS Jamming and the benefits of eLoran
[3] University Texas News, 'UT Austin Researchers Successfully Spoof an $80million Yacht at Sea', 29 July 2013
[4] London Economics, 'The economic impact on the UK of a disruption to GNSS', 2017

Cospas-Sarsat distress alerts used to locate and assist in search and rescue operations. The report concludes that a five-day loss in GNSS would cost the UK USD 149 million. The financial implications to the UK alone indicate the reliance of the maritime sector on GNSS systems and further highlights the impact of shipping on the economy. However, despite the significant implications of GNSS loss, mitigation measures are rarely considered and often remain unprotected, making it possible for opportunist cyber criminals to exploit this key vulnerability.

**AIS**

AIS is utilised for tracking of ships but also for maritime security, situational awareness, search and rescue operations. AIS messages are exchanged by radio frequency (VHF) and rely on GNSS coordinates to report to nearby stations via VHF. AIS is a two-way system relaying information from ship to ship and from ship to shore.

The main vulnerabilities of AIS are owed to a lack of:

**Validity checks:** AIS can be sent from any location without geographical validity checks being carried out

**Timing checks:** The absence of a timestamp means it is possible to replay AIS data no longer current

**Authentication:** No authentication protocols are used in the transmission of AIS information making it possible to create fraudulent AIS packets to impersonate another ship

**Integrity checks:** AIS messages are entirely unencrypted, increasing the threat of messages being intercepted and modified

AIS, similar to GNSS, is considered a soft target for cyber-attacks as these systems are not provided with an in-built mechanism to encrypt or authenticate signals. This makes these systems particularly vulnerable to attacks such as blocking (prevents the locking of a position) and jamming or spoofing (which feeds the receiver false information). Jammers can be used on land or at sea and can have a radius of over 30km.

Such attacks can have great repercussions and have the potential to cause significant losses. Spoofing the AIS or the closest point of approach could involve faking a possible collision with a target ship. Software defined radio transceivers could be used to transmit ship AIS or vessel traffic system (VTS). If visibility is reduced, ships rely on GNSS signals to identify other ships in the vicinity and communicate their positions. If the GNSS signal is wrong, the potential for accidents in transit routes rises substantially. Furthermore, if a ship transiting a key canal was to be targeted in a cyber attack, this could have a significant economic impact on the coastal state.

While it is evident that vulnerabilities exist, AIS has not yet been the main target of cyber criminals despite publicly available material indicating how an attack could be carried out.

**Legacy systems**
Legacy systems pose as much a significant threat offshore as they do onshore. All information, cargo handling and administrative systems and operating systems present on ships require updating. Vulnerabilities found in legacy systems can easily be exploited by organised crime groups, further contributing to destabilising regions involved in or susceptible to illicit drug trades. This was the case at Port Antwerp in 2011 when an Advanced Persistent Threat (APT) went undetected for two years. The attack was commissioned by an organised drug cartel and was used to transit illicit narcotics.

Older legacy ICS often operate in more independent modes and tend to have unsophisticated password policies and security administration. Manuals and training videos are publicly available and many hacker tools can now be downloaded online and applied with limited system knowledge, increasing the threat and highlighting the necessity to airgap critical networks. However, the threat of legacy systems being exploited onshore is considered to be higher than onboard ships.

**Antivirus**
Offshore systems should be maintained to ensure antivirus software installed is updated and preventative measures must be taken to ensure scans are carried out for new vulnerabilities previously undetected by the software. Shipboard computer networks in particular face a significant threat owing to the absence of boundary protection measures. In addition, the multitude of actors involved in the operation and chartering of ships may result in a lack of accountability and the increased chance of human error. While the threat of an attack resulting from the absence of adequate antivirus is considered to be high, ships are not necessarily being targeted. However, simple preventative measures such as this could help avoid greater repercussions.

**ECDIS**
Like computer systems, bridge systems such as ECDIS can be targeted in a cyber attack. The threat can arise through viruses uploaded from a USB stick, from opening a link received via email; an internet-based intrusion by a hacker or from an insider threat. Despite ECDIS being run on computer systems, adequate safety measures required to protect the systems are often overlooked as it is considered a stand-alone system and therefore not treated as a PC. At present, it is considered unlikely for a targeted attack on systems running ECDIS.

*ECDIS onboard ship – Source: NYA*

**BYOD**
The rise in Bring Your Own Device (BYOD) policies has allowed for devices to connect to networks without being adequately configured, further exposing the network to contracting malicious content. In addition, companies providing wireless to guests and clients may expose cyber vulnerabilities if they are connected to networks linked to critical systems relating to the operations of the company.

## Call to action

The three key areas of consideration in a comprehensive security risk management include considerations to people, procedures and technology.

**People, procedures, technology**

Cyber security criminals often exploit the people factor through the use of common hacking tool kits readily available in the public domain. Consequently, a mandatory awareness programme should be taken by all employees to explain the risk from cyber security attacks and set up preventive measures. It is important to establish an appropriate cyber security incident response team – either consisting of internal employees, outsourced to a third party or both - along with an assigned contact point.

Further to this, many elements of operations are likely to be outsourced to third-party vendors. It remains the responsibility of the company to ensure sufficient due diligence has been taken to avoid a cyber incident resulting from the action or inaction of third parties. For example, ensuring information security management standards such as ISO 27001 are complied with by the third party can reduce the risk substantially.

To tackle cyber security incidents in an effective and consistent manner, it is essential to develop an appropriate strategic approach and a formal cyber security incident response process which should include:

- Identifying cyber security incidents
- Investigating the situation
- Taking appropriate action
- Recovering systems, data and connectivity

Many organisations have vastly insufficient logging, archiving, correlation and simulation capabilities. Effective logging saves both time and money in the case of a cyber security incident and can be used as part of a defence or prosecution in a court case.

Ultimately, the crew and especially the ship master is responsible for safety and security at sea – crew training is imperative to make the right decisions in the event of a cyber security incident.

### Prevention

The following are a number of key preventative measures that should be taken to strengthen the security posture onshore at ports, terminals and onboard ships:

- Implementing layers of defence, starting with the outermost layer of physical security, followed by management-level procedures and policies, firewalls and architecture, computer policies, account management, security updates and finally antivirus solutions
- Operating a least-privileged principle, where information and access is limited to a need-to-know basis
- Employing network hardening measures, ensuring patch management is adequate and proactively reviewed
- Segregation and protocol-aware filtering techniques protect against cyber threats from impacting critical systems, such as engine and propulsion control or semi/fully automated processes
- Employing a sound removable device policy with provisions to ensure all USBs are encrypted and tested for viruses prior to being used with other devices, also known as 'sheep-dipping'
- Frequent awareness briefings and training programmes to educate all employees on best practice. These can cover installation and maintenance software while avoiding infection and propagation, safeguarding user information and the treatment of cyber physical threats such as the presence of any third-party
- Conduct comprehensive threat assessments to determine the threat landscape and understand the potential attack surface faced by ports, terminals and ships
- Vulnerability assessments of ships, ports and terminals to identify critical systems, understand the potential exposures faced by each and the impact on overall business continuity in the event of a cyber attack
- Risk assessment and risk treatment options can then be reviewed and implemented to ensure a robust system is in place to prevent incidents where possible and equip employees to detect and respond in cases which could not be prevented
- Vetting of third party providers to ensure cyber security precautions are taken

Relying on a reactionary approach to security has resulted in significant financial loss at a number of ports and border agencies as demonstrated in recent incidents (see table – page 7). The myriad of functions reliant on OT means it is imperative to have intrusion protection and detection systems employed that are regularly updated to best protect core shipping operations at ports.

## Response

It is critical for the shipping and logistics industry to recognise that cyber attacks will occur, and thus information needs to be given in advance to establishing appropriate response procedures.

### Detection and identification

The first stage of the cyber incident management process following an attack consists of the gathering of evidence. By analysing log files, error messages as well as other resources such as Intrusion Detection Systems (IDS) and firewalls, you will be able to determine whether you are dealing with an event or an incident.

The early part of an investigation consists of classifying cyber security incidents by the potential impact they may have; prioritising these incidents and assigning response to incidents to the appropriate personnel.

### Containment

The containment phase encompasses three essential steps to effectively mitigate the damage and prevent the destruction of any evidence. The initial step, short-term containment, aims to limit the incident's impact before it escalates. This can be as straightforward as isolating a network segment of infected workstations or switching all traffic to failover servers.

System Back-Up is the second step and involves taking a forensic image of the affected systems as they were during the incident. This image can be used as evidence if the incident is a result of a criminal act. The last step focuses on long-term containment in which the affected systems are temporarily mended, by removing accounts and/or backdoors left by attackers on affected systems and installing security patches on both affected and neighbouring systems.

### Eradication

The eradication phase consists in the removal of malicious content and the full restoration of affected systems. In order to prevent reinfection, the phase usually involves the complete reimaging of the infected system's hard drives. This phase also involves steps taken to ensure the systems will not be compromised again by identifying where the defences failed (for example by installing patches to fix vulnerabilities that were previously exploited by the perpetrator).

### Recovery

The purpose of this phase is to test, monitor and validate the systems that are being put back into production to ensure that they will not be re-infected by malware or compromised by other means.

## Conclusions

The industry continues to demand greater interconnectedness with initiatives such as the introduction of the IMO E-navigation. Incidents recorded to date have led to significant quantifiable financial losses, however, it is harder to identify losses resulting from reputational damage, where recovery can be complex or difficult. Further still, significant attacks targeting port facilities and onshore offices can lead to extensive disruption to operational continuity. As the industry embraces technology, the exposure and threat continues to grow and therefore with every process in the shipping industry that is automated and digitised, risk assessments need to be carried out to mitigate against potential new threats and vulnerabilities posed by these evolving cyber threats.

With the impending regulation around maritime cyber security, adopting maritime cyber risk management into the ISM code, while not currently clear, is likely to rest on 'reasonableness' and the notion of 'duty of care'. This could require establishing a comprehensive training and awareness program, conducting threat and risk assessments, and performing vulnerability assessments of individual ships to ascertain main vulnerabilities since installations and the connection of systems vary from ship to ship.

Critical systems integral to the operation of ships include a manual override to prevent disastrous outcomes of relying heavily on automated and centralised systems, however it is not known how prepared crew would be in the case of an emergency requiring a manual override. While it is entirely feasible for a ship to be remotely hacked, or targeted to adversely affect control systems, or for it to be spoofed to veer off its transit route without it being traced, the likelihood is currently assessed as being low. There are currently no confirmed incidents of a cyber attack directly targeting a ship.

Arguably, ports and terminals are far more exposed to the threats described, representing the confluence of physical and communications activity in the international supply chain. The interfaces are complex, and the drive towards interconnected control systems and efficient processes inexorable. Most of all, at the ship/port interface there is much opportunity to cause loss and damage, far beyond the persistent exposure to criminal activity.

National and regional initiatives, such as by the NIS Directive, EU GDPR and the US Coast Guard circular, in relation to ports and terminals, together with the broader supply chain, are likely to align closely with the principles adopted in the maritime environment.

Ultimately, the main threat continues to derive from human error – downloading malicious content, opening an unsecured web browser or falling victim to social engineering attacks and phishing scams. This remains the most common cause of cyber incidents in all sectors, and the maritime supply chain is no exception. As the feasibility of a more damaging attack increases, all stakeholders – in particular ports and terminals, and shipowners and operators alike – must prepare for the inevitable. Appropriate plans and processes need to be established and enforced to mitigate against this growing threat.

## Glossary of terms

**Advanced Persistent Threat (APT)**
A network attack that remains undetected for an extended period of time, often with a motive to use, copy or steal data and IP

**Antivirus**
Software used to detect and destroy computer viruses

**CEO Fraud**
Email scam targeting company email accounts that impersonate company executives with the aim of getting unsuspecting accounts and/or HR departments to transfer money or send sensitive information

**Confidentiality Integrity Availability (CIA)**
Key information security principle that guides policies. Confidentiality seeks to limit access to information, integrity is the assurance that the information has not been tampered and availability is the assurance that secure access to the information is provided to authorised personnel

**Cyber-crime-as-a-service**
The purchase of cyber attack tools and services on the dark web

**Decryption**
Process of converting encrypted data into a human-readable format

**Denial of Service (DoS)**
A cyber attack that prevents legitimate users from accessing a service by flooding the network or server with excessive requests that have invalid return addresses

**Distributed Denial of Service (DDoS)**
A type of DoS attack where multiple compromised systems (botnets) are used to target a single system with the aim of taking the service offline

**Encryption**
Process of converting data into code to prevent unauthorised access

**Firewall**
System that can be implemented in hardware and software and is used to prevent unauthorised access to and from a private network

**Hardware**
Physical components of a computer and electronic systems

**Least Privilege**
Adopting a policy that limits user profile privileges to minimal based on the end user's job necessities

**Legacy System**
Outdated technology often open to security vulnerabilities

**Man-in-the-middle**
Attack whereby the perpetrator secretly relays and/or modifies communications between two legitimate users without the users knowing that their communications have been compromised

**Malware**
Software designed to disrupt, damage or gain unauthorised access to a computer system

**Phishing**
Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. Such an email may also request that an individual visits a fake website using a hyperlink included in the email

**Ransomware**
Malware which encrypts data on systems until such time as the distributor decrypts the information. Decryption keys are often provided after a Bitcoin payment by the victim.

**Scanning**
Attacking large portions of the internet at random

**Sheep-dipping**
A process to test files on removable devices in isolation before being connected to company devices and/or networks

**Social engineering**
A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media

**Software**
Computer program and instructions that run a computer

**Spear-phishing**
Similar to phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software

**Spoofing**
An attack in which a person or computer program impersonates another by falsifying data and gaining illegitimate access to systems or information

**Spyware**
Software that enables users to steal data and information from a target device by transmitting data covertly from the hard drive

**Targeted attacks**
Where a company or a ship's systems and data are the intended target

**TCP/IP**
Rules that govern and allow for the connection of a computer system to the internet

**Untargeted attacks**
Where a company or a ship's systems and data are one of many potential targets

**Virus**
Computer code that relies on spreading an infected host file, it can copy itself and is intended to corrupt the computer system or destroy data

**Worm**
Standalone malware program that copies itself in order to spread to other devices

## About us

**NYA**
Since 1990 we have been committed to helping clients understand the threats to their people, information, property and reputation. Our global team provides you with the expertise to mitigate and manage security risks so that you can focus on opportunities and meet objectives. NYA is retained by some of the world's largest insurers for crisis response and prevention services. Such insurance provides indemnification of all costs and immediate, guaranteed access to our team of crisis response consultants. We have responded to 80-100 cases each year since 1990, so our experience of incident types is broad. Regardless of the type of incident, the operating environment or complexity, we are committed to advising and supporting you through to resolution – anywhere in the world.

www.nyarisk.com

**UK P&I Club**
UK P&I Club is a leading provider of P&I insurance and other services to the international shipping community. Established in 1865, the UK P&I Club insures over 240 million tonnes of owned and chartered shipping through its international offices and claims network. 'A (Stable)' rated by Standard & Poor's with free reserves and hybrid capital of $597m, the UK P&I Club is renowned for its specialist skills and expertise that ensure 'best in class' underwriting, claims handling and loss prevention services.

www.ukpandi.com

**TT Club**
TT Club is the international transport and logistics industry's leading provider of insurance and related risk management services. Established in 1968, the Club's membership comprises ship operators, ports and terminals, road, rail and airfreight operators, logistics companies and container lessors. As a mutual insurer, the Club exists to provide its policyholders with benefits, which include specialist underwriting expertise, a worldwide office network providing claims management services, and first class risk management and loss prevention advice.

www.ttclub.com

**Thomas Miller**
UK P&I Club and TT Club are managed by Thomas Miller, an independent and international provider of market leading insurance services. Most of the businesses we currently own or manage are acknowledged leaders in their chosen market. Our portfolio includes mutual organisations and, increasingly, specialist insurance services businesses.

www.thomasmiller.com

www.ukpandi.com
www.ttclub.com