Cyber activity, a daily operational risk which needs to be addressed urgently

Photos: Rawpixel

# The norm, not the exception

by **Mike Yarwood**, *Claims Executive, TT Club*

**TT CLUB**
**established expertise**

TT Club specialises in the insurance of intermodal operators, non vessel owning common carriers, freight forwarders, logistics operators, marine terminals, stevedores, port authorities and ship operators. The company also deals with claims, underwriting, risk management as well as actively works on increasing safety through the transport & logistics field. For more info please visit www.ttclub.com

**Many in the marine supply chain business have operations characterised by widespread office networks and a reliance on multiple third party suppliers. Often IT systems are of an in-house, legacy nature, which may be poorly protected by security software. Specifically, ports and terminals are exposed to threats as they are at the confluence of physical and communications activity. Unfortunately, according to the data we've gathered, supply chain operators are vulnerable to disruptive cyber activity, from criminals or other perpetrators, impacting operations and putting commercially sensitive or confidential data at risk.**

The data interfaces are complex and the drive towards interconnected control systems and efficient processes, exacerbates the opportunities for outside malicious interference. Most of all, at the ship-port interface there's much opportunity to cause loss and damage, far beyond the persistent exposure to criminal activity (Tab. 1).

### At the core

The problem is intensifying. At a global level reports by AV-TEST, a German independent research institute for IT security, indicate that on average 4.2 new files of malware code were generated every second in 2017. From a maritime supply chain perspective an example of a serious IT incursion in 2017 was the spoofing attack on over 20 ships in Novorossiysk. Navigation experts claim the spoofing sent false signals and resulted in ship-board equipment providing false information as to the

***Tab. 1. Perpetrators: motivation and objectives***

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

*Source: BIMCO Guidelines on Cyber Security Onboard Ships*

***Tab. 2. Significant maritime cyber attack incidents***

| Date | Victim | Consequences |
|---|---|---|
| 11/17 | 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% |
| 06/17 | Ships in Novorossiysk | At least 20 ships in the Black Sea were reporting false data was being transmitted, indicating the ships were 32 km inland of their actual position. It is now believed to have been as a result of a Global Navigation Satellite Systems spoofing attack |
| 06/17 | A.P. Møller-Mærsk | NotPetya, also known as ExPetr, ransomware led to outages on the company's computer systems, impacting both oil & 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 $300m of losses |
| 04/16 | South Korea | Some 280 ships were forced to return to port due to problems with their navigation systems. The issue was largely blamed on North Korea, however, this remains unconfirmed |
| 2012-14 | Danish Maritime Authority | An e-mail 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 the authorities |
| 2011-13 | Port of Antwerp | The port had been a victim of an advanced persistent threat 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 approx. $365m, firearms and approximately $1.5m were seized when authorities finally became aware |
| 08/11 | 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*

location of the ships. There is speculation that this incident could have been a state-sponsored attack. A second incident, the NotPetya strike, impacted many in the supply chain, including A.P. Møller-Mærsk, resulting in large scale disruption and substantial costs for those immediately impacted and their partners (Tab. 2).

As to the extent of attacks, research that is available reveals a worrying situation. A BIMCO survey in 2016 suggested that more than 20% of respondents admitted to cyber attacks and in 2017 a SeaIntel Maritime Analysis report estimated that 44% of the top 50 container carriers had weak or inadequate cyber security policies and processes.

The US Coast Guard issued a draft Navigation and Vessel Inspection Circular (NAVIC) 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.

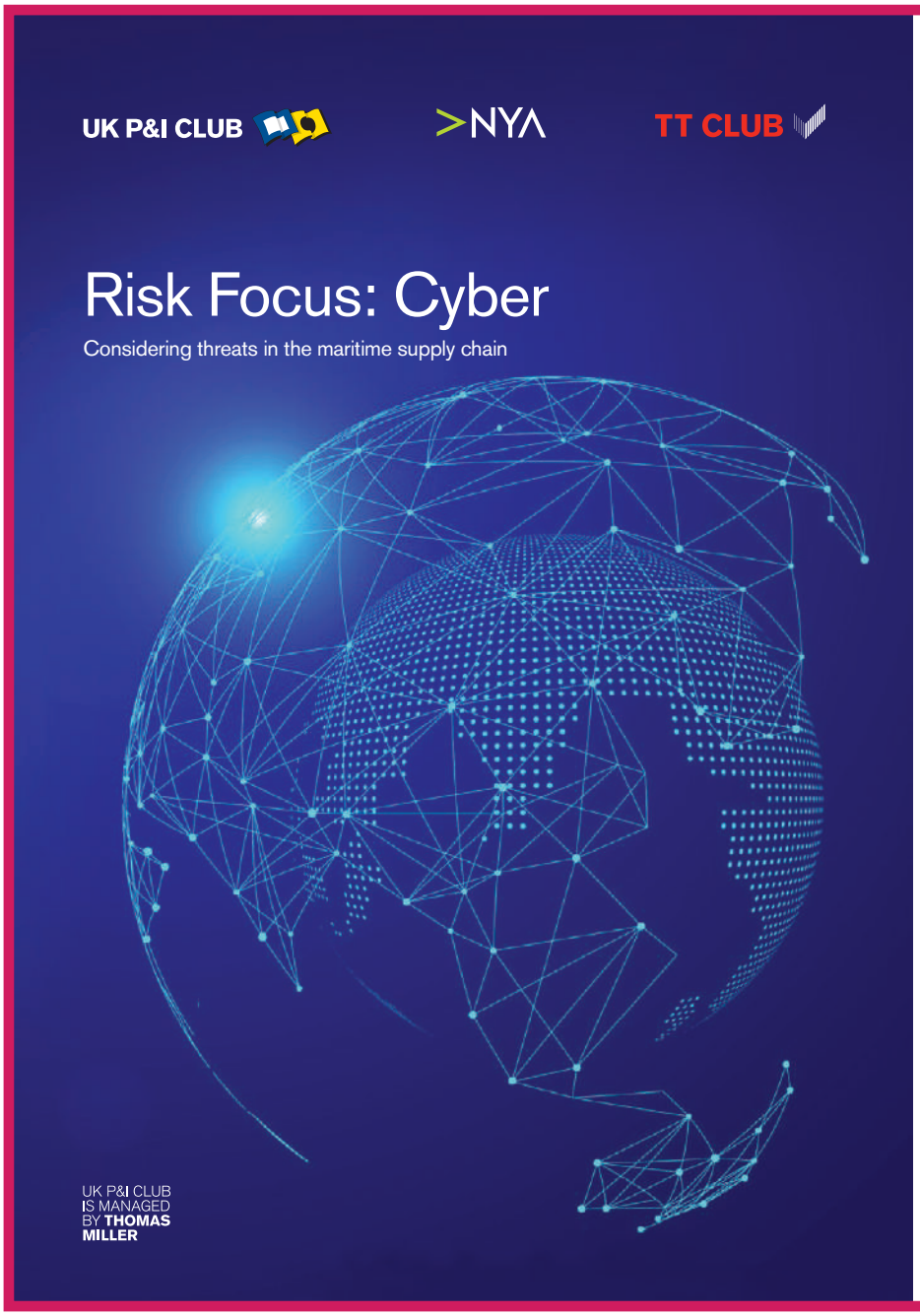
Additional national and regional initiatives, exemplified in the European Union by the Directive on Security of Network and Information Systems (NIS Directive) and General Data Protection Regulation (GDPR), are indicative of the development of regulatory expectations. While the latter does not directly address it, cyber protection is intrinsically at the core of data protection. Such initiatives,

together with known vulnerabilities, highlight that cyber security is ever more pertinent for ports and terminals, as well as the broader supply chain community.

**Cyber corporate culture**

As an insurance mutual, TT Club has always been dedicated to minimising risk through its loss prevention efforts. By publishing *Risk Focus: Cyber – Considering Threats in the Maritime Supply Chain*, jointly with the UK P&I Club and the cyber security consultants NYA, we hope to generate more awareness of the risks to help combat the situation. "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," the authors of *Risk Focus* underlined.

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. As such, awareness of the nature of potential attacks and the need for protection is clearly a crucial initial step towards a thorough risk assessment and mitigation – and this needs to become part of corporate culture. ■




**The maritime industry's reliance on computers and its increasing interconnectivity within the sector makes it highly vulnerable to cyber incidents. While digitalising one's operations can result in great performance gains, both on- and offshore, venturing into the cyber realm also poses a threat to all parts of the shipping sector.**

**With the number of cyber attacks targeting the shipping industry on the rise, TT Club and the UK P&I Club, together with the cyber experts from NYA, specialised in crisis response and management, have put together the *Risk Focus: Cyber. Considering threats in the maritime supply chain* white paper. The publication is meant to function as a guide on how to prevent losses and disruption due to malicious cyber activity.**

**Scan the QR code to directly access the white paper in which you'll find, among many, insights into the different cyber threats to IT and OT systems as well as the vulnerabilities of at sea and land-based operations which cyber criminals pick as their targets; characteristics of the perpetrators; what's the potential impact of a cyber attack on the seaborne part of the supply chain; what are the industry standards and international regulations in the field of maritime cyber security; cyber countermeasures; and a glossary of terms.**