SUBSCRIBE:www.harboursreview.com

no. 2/2019 (26) april

# Harbours review

# Cyber

ISSN 2449-6022

## featured articles

Photo: Rawpixel

LOGISTICS
makes it
happen

Photo: All free download

## Dublin-Rotterdam ro-ro capacity goes up

**CLdN** has deployed the company's newbuild *Celine* on the route in question, increasing the frequency by one to a total of four sailings per week in each direction. The 235 m-long *Celine* offers 8,000 lane metres of cargo capacity. She also serves the **Dublin-Zeebrugge** link. The enhanced Dublin-**Rotterdam** connection comprises three ro-ro sailings (departing from Rotterdam on every Tuesday, Thursday and Saturday, and from Dublin on Thursdays, Saturdays, and Mondays) supplemented by a round trip taken care of with the help of a container carrier (sailing ex-Rotterdam on Saturdays and ex-Dublin on Tuesdays).

## Piraeus-NASPA New Maritime Silk Road MoU

The **Piraeus Port Authority** (PPA), controlled by the Chinese **COSCO**, has signed an agreement with the **North Adriatic Sea Port Authority** (NASPA). The deal is aimed at strengthening cargo flows between Piraeus and NASPA's **Venice** and **Chioggia**. As such, the parties will jointly work on coordinating the development of their ports, incl. infrastructure and services, in order to facilitate freight flows between Europe, the Mediterranean, and the Far East. Also, they'll exchange best practices and know-how in port management, particularly in the fields of IT, communications, and attracting investments. **Pino Musolino**, President, NASPA, commented, "In an upcoming scenario which foresees a powerful increase of trades between Asia and Europe along the new maritime Silk Road, it is necessary to put all our efforts on the rationalization of the logistics chains, starting from the ports and from the road connections with the inner markets, in order to shorten distances, to lower transports costs, to remove trucks from roads and improve the environmental sustainability of trades." He furthered, "Through this agreement, which is coupled with the other recently signed with COSCO Shipping for a weekly connection Piraeus-Venice, we want to clearly show that the development of trades primarily requires commercial agreements, optimization of services and targeted infrastructure interventions. This is the right path to create value for our economy and for our territory." **Capt. Fu Chengqiu**, CEO, PPA, added to this, "The Port of Piraeus, the largest port of Greece and the Eastern Mediterranean, is an ideal hub between Asia and Central & Eastern Europe. It is the first deep-sea EU port after crossing Suez Canal and offers combined transport solutions with efficient value-added services for cargoes, which can be re-distributed by road, rail, and sea. The establishment of our cooperation with the North Adriatic Sea Port Authority is targeting to strengthen the trade links between Asia and Mediterranean and to enhance the role of ports as engines for the European economy."

## DP World's bid to buy P&O Ferries and P&O Ferrymasters

The Dubai-based terminal operator has put on the table £322m with the aim of purchasing the holding company that owns the ferry operator and the logistics service provider. The transaction is subject to customary completion conditions. **DP World** expects to close the deal in the first half of 2019. The Dover-headquartered **P&O Ferries** currently has at its disposal a fleet of 21 vessels that altogether call to 11 ports in the North and Irish Seas. **P&O Ferrymasters** provides supply chain solutions in 19 European locations. Both companies were already part of DP World when the terminal operator bought the **P&O Group** in 2006. They were soon afterwards taken over by **Dubai World**. "We are pleased to announce the return of P&O Ferries back into the DP World family. P&O Ferries is a strong, recognisable brand and adds a best-in-class integrated logistics provider into our global portfolio. Importantly, P&O Ferries provides efficient European freight connectivity building on last year's acquisition of Unifeeder," **Sultan Ahmed Bin Sulayem**, Group Chairman and CEO, DP World, said.

## LNG-retrofitted *Nápoles* enters traffic

At the expense of around €12.5m **Baleària**'s ferry was equipped with dual-fuel engines by the **Gibdock** shipyard in **Gibraltar**, along with a 200t-big liquefied natural gas (LNG) storage tank. The 186 m-long ship, offering room for up to 950 passengers and 2,040 lane metres of cargo capacity, has replaced the *Martín i Soler* ferry on the service between **Huelva** and the **Canary Islands**. *Nápoles* is the first in a series of six ferries Baleària is planning to LNG-retrofit over the next two years in an EU-supported project. Meanwhile, the company's first brand-new LNG-run ferry, the 186.5 m-long *Hypatia de Alejandría* (800 pax, and 2,194 lm), was put into operation at the end of January. Her sister ship, *Marie Curie*, currently under construction at the **Cantiere Navale Visentini** shipyard in **Venice**, will soon join her. The company has invested €200m to construct the newbuilds. In addition, the **Armon de Gijón** shipbuilding yard is working on Baleària's €80m-worth *Eleanor Roosevelt*, a dual-fuel high-speed passenger-cargo craft (125 m-long, 28 m-wide, 1,200 pax, 500 lm).

## KMOU and MMU students to train on Kongsberg Digital's simulators

The Norwegian provider of next-generation software and digital solutions will furnish the South Korean *Segero* and *Hannara* sister training ships with real-time training simulators. Specifically, K-Sim Navigation, K-Sim Engine, and K-Sim Cargo simulators will be installed on-board the vessels belonging to the **Korea Maritime and Ocean University** (KMOU) and **Mokpo National Maritime University** (MMU). The K-Sim Navigation bridge, for instance, will be set up in a room behind the vessels' real bridges and will be configured to project either simulated sailing areas based on new Korean database models or the real view from the actual bridge, via on-board CCTV cameras, with data from real on-board sensors. By these means, students on the simulator bridge will have access to the exact same view as students on the real bridge, so that real-time situations can be discussed back and forth, and performance indicators can be compared. "The onboard simulators on these vessels introduce a whole new degree of realism. Instructors will be able to make clear, informed assessments and fine-tune simulator exercises as they see fit, while students will be able to access real-time vessel data and apply it to training routines in the virtual realm before moving forward to the main bridge and restaging operations with the actual ship," **Mark Stuart Treen**, Vice President Sales, **Kongsberg Digital**, explained. He also said, "Combining simulator technology with real in-situ assets represents an exciting new venture for Kongsberg, and reflects our purpose as a company in supporting customers in new territories, stimulating economic growth and tirelessly pushing the envelope with innovative applications for our technology leading simulators."

## Stena Bulk invests in scrubbers to comply with the 0.5% sulphur cap

At the expense of $55m, the Gothenburg-headquartered shipping line will have 16 of its vessels equipped with sulphur air pollution control devices. The installation will encompass 10 IMOIIMAXes, five Suezmaxes, and one medium range ship. The investment includes not only the equipment but also installation and time out of service. **Stena Bulk** has decided to invest in open loop scrubbers with water cleaning, meaning that apart from excess sulphur also particle matter will be taken from the exhaust gases. In addition, the devices will be 'hybrid-ready' to enable switching to closed loop operations in the future. According to the company, the payback time of investment will be between one and a half and two and a half years, which has already been secured by hedging the fuel spread. "We evaluated the different options and came to the conclusion that for our business by installing scrubbers we will secure greater availability of fuel for our vessels and by so limit our exposure to not finding the right fuel around the world and by that stay flexible in our trading," **Erik Hånell**, President and CEO, Stena Bulk, commented. He also said, "Even doing so we know it will require some changes and probably massive challenges in the planning logistically. We will, however, prepare ourselves best possible so that we can secure at least the same level of support to our customers as today."

## NCP chooses Navis N4

The terminal operating system (TOS) will be installed at **North Carolina Ports'** (NCP) **Wilmington** and **Morehead City** port facilities as well as the inland terminal in Charlotte, NC. In Wilmington, for instance, the investment will form part of a terminal enhancement project, including also redesigning the truck gate complex and expanding the container yard, aimed at supporting future growth and, eventually, automating the NCP's facilities. Thanks to the upgrade, the Port of Wilmington's annual container handling capacity will double up to 1.2m TEUs. The N4 TOS implementation will begin in spring 2019, and full implementation will coincide with the new container gate complex in late 2021. As part of the agreement, Navis will also provide a variety of professional services and training support to NCP. "Navis' technology produces the best opportunity for North Carolina Ports to use a single platform for all cargo handled at our terminals. Our ambitions reach well beyond the terminal operating systems and N4 gives us the foundation we need to increase velocity, safety and volume. We will achieve this via a series of automation projects connecting our technology with operations, our customers and the entire port constituency," **Bill Corcoran**, CIO, NCP, commented. **Susan Gardner**, Vice President and General Manager, Americas, Navis, added to this, "North Carolina Ports has a strong pedigree and successful track record supporting and enhancing the economy of North Carolina with its streamlined operations. As it looks to raise the bar on its terminal operations, customer service and safety initiatives, we are proud that N4 stood out as the only TOS solution that would help it realize its vision. We are eager to see what can be achieved together." **Paul J. Cozza**, Executive Director, NCP, summed up, "North Carolina Ports is excited to partner with Navis as we continue to invest in our future. Choosing a world-class terminal operating system further fulfils North Carolina Ports' commitment to sustainable growth and best-in-class levels of performance for our customers."

## FRS will put a new ship across the Melilla-Motril route

The **Tarifa**/**Cádiz**-based ro-ro & ferry line will introduce the refurbished ro-pax *Golden Bridge* on the service in question as of May. The 186 m-long and 24 m-wide ferry will offer room for up to 1,500 passengers (across 130 cabins) and space for 500 vehicles. She'll cross the **Melilla-Motril** stretch in five hours, down by two compared to the current crossing time. "We have listened to the requests of the people of Melilla, and we are going to operate a vessel that meets the needs of this route. As we say, we set out to gain the confidence of the Melilla's people with facts," **Ronny Moriana**, Managing Director, **FRS Iberia**, commented. He also underlined, "We are also grateful for the efforts and collaboration that the Melilla and Motril Port Authorities have shown us throughout this whole complex process of introducing a new vessel."

## Rotterdam gears up for Brexit

The **Port of Rotterdam**, the **Rotterdam** and **Vlaardingen municipalities**, and the Dutch **Directorate-General for Public Works and Water Management (Rijkswaterstaat)** are creating five new buffer parking sites for the trucks that may run into customs clearance problems if the UK decides to leave the EU without a trade deal. Up to 700 lorries will be able to wait there temporarily if their customs documents have not been properly prepared for maritime crossings to the UK post-Brexit. The aim of the coordinated action is to minimise any extra delays resulting from additional customs formalities at the ferry and short sea terminals – as required in trade with third countries – so as to ensure freight traffic to the UK runs as smoothly as possible. Additionally, more intensive passport checks and inspections made by the **Netherlands Food and Consumer Product Safety Authority** could mean longer processing times at terminals. On the northern bank in **Hoek van Holland**, the Municipality of Rotterdam has allocated the 200 trucks-big **Oranjeheuvel** site, close to the ferry terminal. In **Maasdijk**, in the **Municipality of Westland**, Rijkswaterstaat has created a buffer site for around 50 trucks. In the Municipality of Vlaardingen, a site is being created on **Waterleidingstraat** for around 80 trucks. On the southern bank, in turn, buffer parking sites are being created on **Moezelweg** and **Seattleweg** by the Port of Rotterdam Authority. The former site, located in the vicinity of the ferry and short sea terminals that operate out of the **Europoort** area, will provide space for approximately 290 trucks. The Seattleweg site will provide space for approximately 80 trucks. The buffer parking sites will be only accessible to trucks that have not been given access to the ferry terminals in the Port of Rotterdam because the Portbase system has not received prior notification of their cargo. Truck drivers can use these locations to liaise with their client or transport planner and make sure the necessary formalities can yet be completed. Exporters, hauliers, and shippers are advised to use Portbase to provide digital notification of their cargo that is destined for the UK. "Using this Dutch supply chain solution for Brexit, cargo can pass quickly and without unnecessary delay through customs to and from the UK, even after Brexit," a press release from the Port of Rotterdam read. In preparation for Brexit, the Port of Rotterdam Authority and the port's ferry terminals have jointly carried out a simulation on the possible impact Brexit might have on Rotterdam's UK-bound wheeled freight traffic. Based on historical data, it has been assumed that approximately 400 trucks will not have their formalities in order. This, in result, allowed estimating the required number of temporary buffer parking places for heavy goods vehicles to be prepared in advance. Of the roughly 54mt traded annually between the UK and Netherlands, around 40mt passes through the Port of Rotterdam. The bulk of the volume uses ferry and short sea crossings.

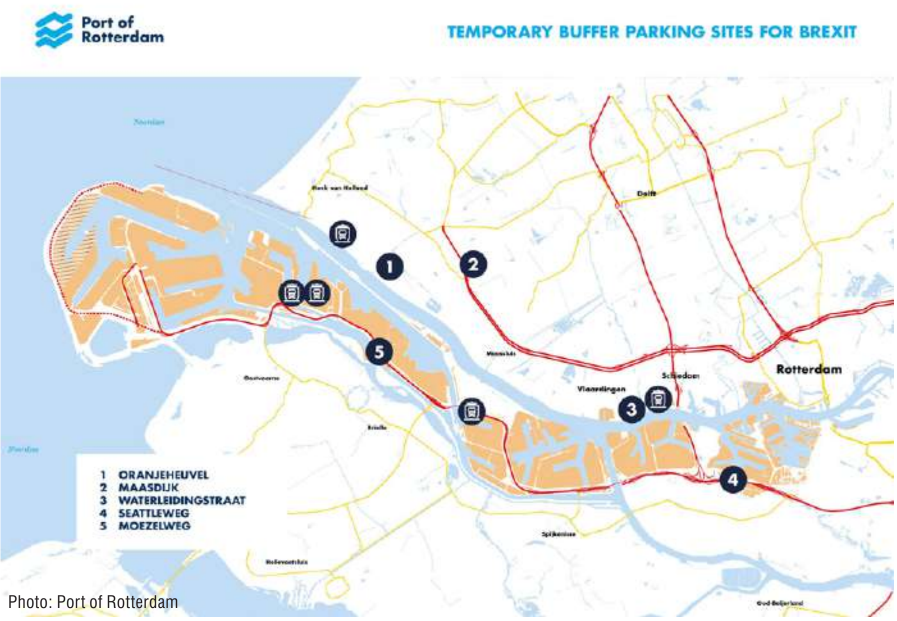


Photo: Port of Rotterdam

## FSG delivers the sixth ro-ro ship to SIEM

The 210 m-long and 26 m-wide *Maria Grazia Onorato*, offering 4,076 lane metres of cargo space, has been hired out to **Moby Lines**, part of the Italian **Onorato Armatori** group. The newbuild, the operations of which will be managed by **Tirrenia Compagnia Italiana di Navigazione**, will be deployed in the Mediterranean to serve traffic between **Genoa, Livorno, Catania**, and **La Valletta**. **FSG** will supply **SIEM** with two other ro-ro vessels of the same series, scheduled for delivery in 2019 and 2020, respectively.

## MSC contracts Fincantieri to build four luxury cruisers

The order, worth over €2b, will see the delivery of the GT 64k-big ships, each offering 481 guest suites, by 2026. The first vessel will be delivered by spring 2023, while the remaining three will come into service one per year over the following three years through 2026. "With this now firm order, MSC is entering a new segment that bears significant potential globally. While we already serve the premium market with the MSC Yacht Club featured on MSC Cruises' fleet, our new true luxury brand will deliver to this separate and fast-growing segment with super-yacht vessels and an experience to match that. Additionally, we are proud to partner again with Fincantieri for the development and construction of yet again another highly-innovative and exclusive class of ships," **Pierfrancesco Vago**, Executive Chairman, **MSC**'s Cruises Division, commented. **Giuseppe Bono**, CEO, **Fincantieri**, added, "Today's' announcement confirms our Group's ability and strength to convert the soft backlog into backlog. We are proud to have achieved this important goal in less than five months from the preliminary agreement. Fincantieri's reputation in a complex market such as the cruise one is at an all-time high. Our leadership in the luxury segment, among the most active ones, grows even stronger with these four ships, alongside our relationship with MSC and its growth plans."

## Sustainable marine biofuel oil put to the test

On 19 March, a **CMA CGM** container carrier was bunkered in the **Port of Rotterdam** with second generation biofuel derived from forest residues and waste cooking oil. The bunkering was a result of a co-op struck between **IKEA Transport & Logistics Services**, CMA CGM, the **GoodShipping Program**, and the Rotterdam port – the aim of which is to demonstrate the scalability, sustainability, and technical compliance of sustainable marine biofuel oil, and thereby spur the wider continued development of realistic options to curb greenhouse gas and sulphur oxide emissions from shipping. "This announcement comes at a time when the shipping sector is at a crossroads, with owners and operators required to switch to low sulphur fuels by 2020. The industry also faces impending International Maritime Organization (IMO) Greenhouse Gas (GHG) reduction requirements, including an objective to reduce average carbon intensity from shipping – the amount of carbon emitted for each unit of transport – by at least 40% by 2030, and 70% by 2050," a joint press release stated. The testing is being facilitated by the GoodShipping Program, a sustainable initiative dedicated to decarbonising ocean freight and is the latest step in the scaling of low carbon marine biofuel oils for wider commercial use within the maritime industry. The sustainable marine biofuel oil has been developed by **GoodFuels** following three years of intensive testing with marine engine manufacturers. According to the company, the second generation biofuel oil is expected to deliver 80-90% well-to-propeller $CO_2$ reduction vs. fossil equivalents. In addition, GoodFuels says, its product virtually eliminates sulphur oxide ($SO_x$) emissions – and does it without any requirement for engine modifications. "Through our pilot, we want to show that the means for decarbonisation in terms of alternative fuels are available. We have a responsibility to do our part to reduce the impact of our ocean freight. Through our participation, we send a signal to our customers and the ocean industry on our commitment to decarbonise. Only through collaboration can we achieve rapid, necessary change. With a successful pilot completed, our intention is to put the equivalent of at least all our containers out of Rotterdam on biofuel," **Elisabeth Munck af Rosenschöld**, Head of Sustainability, IKEA Global Transport & Logistics Services, said. **Dirk Kronemeijer**, CEO, The GoodShipping Program, added, "The aim of our program has always been not only to reduce carbon emissions from shipping but to show that the means to accelerate the energy transition are already available for the sector to grasp. Together we send a very clear message: sustainable biofuels are ready today, and we can meet the pathways laid out by the IMO in a manner that is attractive to major cargo owners such as IKEA." **Xavier Leclercq**, Vice President, CMA CGM, also commented, "Having an HFO-equivalent solution in bio-fuel oil available with no engineering or operational changes required to our vessel offers a safe, manageable and innovative opportunity to facilitate shipping's wider transition to new fuel solutions." **Allard Castelein**, CEO, the Port of Rotterdam, summed up by saying, "The Port of Rotterdam considers this initiative by IKEA, CMA CGM and GoodShipping to be a strong rallying cry to the shipping industry. This bunkering shows that decarbonisation of sea trade is well achievable. It's clear that shippers play an important role in decarbonising the industry. In Rotterdam the necessary infrastructure is available. Besides that, to support these kind of initiatives, we have just started a four year period during which we have €5 million to spend on stimulating specific projects to reduce carbon dioxide emissions from the global shipping industry."

# market sms

Photo: Pexels

## THE PORT OF ALGECIRAS:

### 4,773,079 TEUs handled in 2018 (+8.7% yoy)

In terms of tonnage, containerised freight traffic totalled 60.59mt last year, marking an uptick by 5.2% on the 2017 result.

***The Port of Algeciras' volumes***

| | 2018 | 2018/2017 |
|---|---|---|
| General cargo | 69,062.43kt | +5.5% |
| Liquids | 31,763.06kt | +10.4% |
| Local traffic | 2,274.35mt | -4.9% |
| Supplies (bunker) | 2,541.87kt | -10.3% |
| Dry bulk | 1,718.44kt | -18.3% |
| Fishing | 878.0kt | -13.4% |
| **Total** | **107,361.03kt** | **+5.7%** |
| **Unitised freight traffic** | | |
| TEUs | 4,773,079 | +8.7% |
| Ro-ro cargo units | 338,587 | +5.4% |
| **Passenger traffic** | | |
| Ferry | 5,952,840 | +7.5% |
| Pax cars | 1,213,451 | +1.6% |

## THE PORT OF TRIESTE:

### 62.68mt handled in 2018 (+1.2% yoy)

With 43.23mt (-1.2% year-on-year), the turnover of liquids accounted for the bulk of the Italian seaport's 2018 cargo traffic.

***The Port of Trieste's volumes***

| | 2018 | 2018/2017 |
|---|---|---|
| Liquids | 43,234.7kt | -1.2% |
| General cargo | 17,776.3kt | +7.4% |
| Dry bulk | 1,665.5kt | +1.6% |
| **Total** | **62,676.5kt** | **+1.2%** |
| **Unitised freight traffic** | | |
| TEUs | 725,426 | +17.7% |
| Ro-ro cargo units | 299,343 | -1.0% |
| New vehicles | 9,955 | -16.8% |
| **Passenger traffic** | | |
| Cruise | 42,724 | +56.3% |
| Ferry | 68,815 | -38.7% |
| **Total** | **111,539** | **-20.1%** |

## THE PORT OF DUBLIN:

### 37.99mt handled in 2018 (+4.3% yoy)

"Every year from 1993 to 2007 was a record year in Dublin Port. In the past four years we have seen this pattern re-emerge, with 2018 the fourth year in a row for record growth," Eamonn O'Reilly, Chief Executive, Dublin Port Company, commented. He continued, "Dublin Port's multi-million euro infrastructure investment programme continued with capital expenditure of 93m during 2018. Our investment in infrastructure is matched by our customers' continuing investments in new ships with huge freight capacity. Even as the €149m 2,800 lane metre W.B. Yeats enters service in Dublin Port, we are preparing for a second new Irish Ferries' ship with 5,610 lane metres and also for Stena Line's 3,100 lane metre E-Flexer, both due to enter service on the Dublin-Holyhead route during 2020. "While BREXIT brings uncertainties and challenges to our business, the combination of investments by our customers and by Dublin Port is underpinned by shared confidence in the future. Whether we are faced with a hard BREXIT or not on 29th March, it will become clearer in the coming days and weeks. If we are, Dublin Port will have significant additional border inspection post capacity available for State agencies in time. Coping with the challenges of a hard BREXIT is a challenge not only for us but also for State agencies and our customers. We will be as prepared as it is possible to be," O'Reilly underlined.

***The Port of Dublin's volumes***

| | 2018 | 2018/2017 |
|---|---|---|
| **Cargo traffic by destination (thousand tonnes)** | | |
| Imports | 22,741 | +5.5% |
| Exports | 15,253 | +2.5% |
| **Cargo traffic by freight type (thousand tonnes)** | | |
| Wheeled (ro-ro) | 24,050 | +2.7% |
| Containerised | 6,924 | +3.8% |
| Liquids | 4,621 | +7.8% |
| Dry bulk | 2,375 | +16.8% |
| Break-bulk | 24.0 | +7.2% |
| **Total** | **37,994** | **+4.3%** |
| **Unitised freight traffic** | | |
| Ro-ro cargo units | 1,031,897 | +4.0% |
| TEUs | 726,212 | +4.0% |
| Vehicles | 103,443 | +4.1% |
| **Passenger traffic** | | |
| Ferry | 1,827,674 | -1.0% |
| Cruise | 177,641 | +23.4% |
| **Total** | **2,005,315** | **+0.7%** |
| Pax cars in ferry traffic | 508,960 | -1.2% |

## THE PORT OF THESSALONIKI:

12.89mt handled in 2018 (-17.3% yoy)

The overall decrease was mainly driven by the 42.8% year-on-year slump noted in export traffic, which at the end of 2018 totalled 3.38mt. At the same time, imports lost 1.7% yoy and amounted to 9.51mt. Out of the total figure, the turnover of liquids reached the level of 6.63mt (-14% yoy), dry bulk – 3.41mt (+7% yoy), while general cargo – 2.85mt (-39.1% yoy). Thessaloniki's container traffic advanced by 5.6% yoy to a total of 424,500 TEUs. On the other hand, fewer passengers went through the quays of the Greek port – down by 11.7% yoy to 44,474, out of which 1,502 came on-board cruise ships (-38% yoy).

## THE PORT OF AARHUS:

540,363 TEUs handled in 2018 (+5.7% yoy)

In result, the Danish seaport broke its container handling record from the previous year. Altogether, just over 8.80mt went through Aarhus' quays last year, an increase by 2% on the result from 2017.

## THE PORT OF HAMINAKOTKA:

16.17mt handled in international & transit traffic in 2018 (+10.3% yoy)

Exports rose by 3.4% year-on-year to 11.23mt while imports by 30% yoy to a total of 4.94mt. The Finnish ports also took care of 792.3kt in coastal traffic -, down by 21.8% on the result from 2017. With 653,443 TEUs at end-2018, HaminaKotka's container traffic noted a downtick by 5.3% yoy.

## THE PORT OF OSLO'S FERRY TRAFFIC:

213,007 ro-ro cargo units handled in 2018 (-16.5% yoy)

As regards tonnage, wheeled ferry cargo traffic amounted to 587.5kt last year, noting a decrease by 3.4% year-on-year. Passenger ferry traffic contracted as well, by 1.0% yoy to a total of 2,344,007 travellers.

## HHLA'S SEA CONTAINER TERMINALS:

7,336k TEUs handled in 2018 (+1.9% yoy)

At the same time, the company's intermodal unit, road and rail, took care of 1,480k TEUs, the same level as in 2017.

## THE PORT OF HIRTSHALS:

148k ro-ro cargo units handled in 2018 (+4.2% yoy)

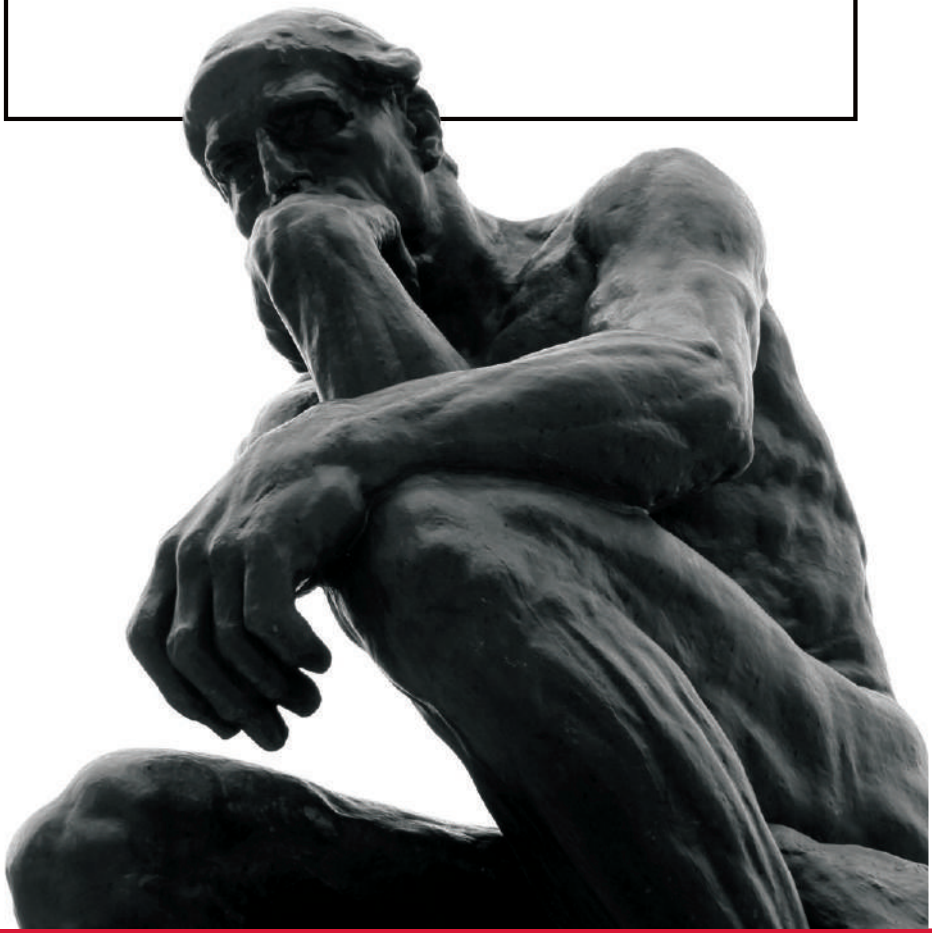
Hirtshals' ro-ro and ferry cargo traffic grew for the 10th consecutive year. Overall, the Danish seaport handled 1.9mt last year, more or less the same volume as in 2017. The handlings of stone and gravel came to a halt in 2018, but the increase noted in ro-ro traffic managed to fill in the missing turnover.

## THE PORT OF TRELLEBORG:

1,161,462 ro-ro cargo units handled in 2018 (+3.2% yoy)

The Swedish port also served a record number of passengers last year, up by 4.2% year-on-year to a total of 1,831,290 guests.

Photo: Port of Trelleborg



# Short Stories

Photo: Pixabay

## 3rd edition of the *Guidelines on Cyber Security Onboard Ships* – published

THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

Produced and supported by
BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL

BIMCO
CLIA
International Chamber of Shipping
Shaping the Future of Shipping
INTERCARGO
International Association of Dry Cargo Shipowners
InterManager
INTERTANKO
IUMI
International Union of Marine Insurance
OCIMF
WORLD SHIPPING COUNCIL
PARTNERS IN TRADE
v3

*Scan the QR code to get your own copy of the latest edition of the* Guidelines on Cyber Security Onboard Ships

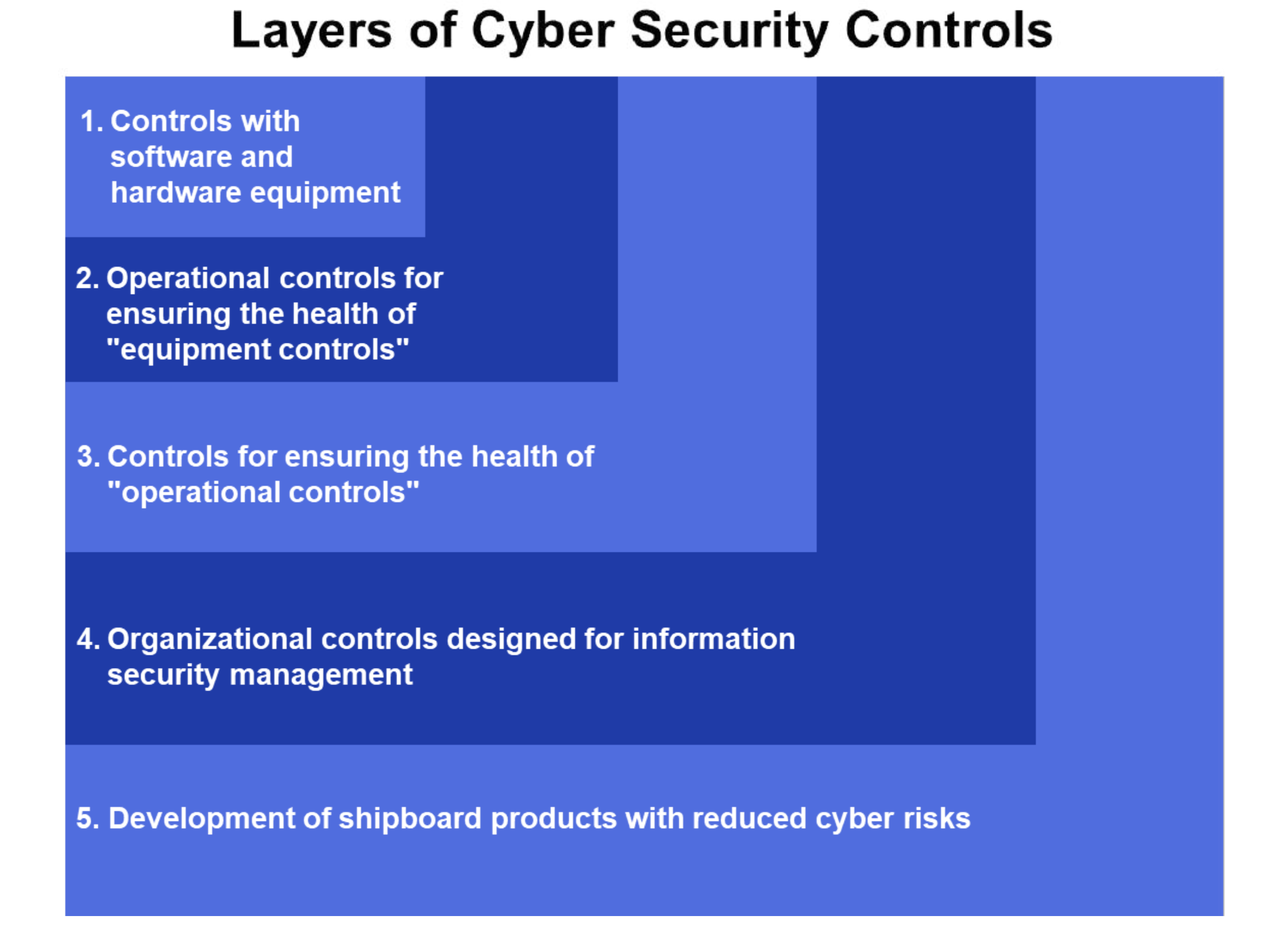
The revised version, published in December 2018, was expanded in several areas. First, it addresses the requirement of incorporating cyber risks in the ship's safety management system, as has been decided by the **International Maritime Organization**. Second, it contains guidelines around operational technology (OT) which is increasingly intertwined with information technology (IT). "[…] the risks associated with OT are different from IT systems. For example, malfunctioning IT may cause a significant delay of a ship's unloading or clearance, but with malfunctioning or inoperative OT there can be a real risk of harm to people, the ship or the marine environment," **Lars Lange**, Secretary General, **International Union of Marine Insurance** (IUMI), explained. Third, it provides more guidance for dealing with the cyber risks arising from parties in the supply chain. Specifically, the advice includes evaluating the security of service providers; defining a minimum set of requirements to manage the supply chain or third-party risks; making sure that agreements on cyber risks are formal and written; and also the need for ships to be able to disconnect quickly and effectively from shore-based networks, if required. Additionally, the 3rd edition of the ***Guidelines on Cyber Security Onboard Ships*** comprises a number of (anonymised) examples of actual incidents to demonstrate some of the real-world situations shipowners and operators face. The newest guidelines were prepared by a cyber security working group, with expert input from the **Baltic and International Maritime Council** (BIMCO), **InterManager** (an association representing ship managers), the **International Association of Dry Cargo Shipowners** (INTERCARGO), the **International Association of Independent Tanker Owners** (INTERTANKO), the **International Chamber of Shipping** (ICS), the **Oil Companies International Marine Forum** (OCIMF), the **World Shipping Council** (WSC), and IUMI.

## Naval Dome to cyber-protect Totem Plus

The Israeli provider of automation and navigation systems has signed a licence agreement with **Naval Dome**, also a company from Israel, for the use of the latter's maritime cyber security software. Under the agreement, **Totem Plus** is licensed to integrate the Naval Dome software with the hard drives across several hundred systems in the Totem Plus portfolio, providing, according to both parties, the highest level of cyber protection at the system build stage, prior to shipment to end-users. The Naval Dome software is encapsulated in existing maritime original equipment manufacturer (OEM) vendor software and hard disks. As such, it requires no change to the original software, nor does it change the operation of the OEM's software or systems. In result, the Totem Plus systems will leave the factory fully cyber-protected by Naval Dome. In addition, upon request, Totem Plus can supply the Naval Dome Dashboard, which provides ship and shore personnel with an exact picture of the security status of the critical equipment on-board ships across the entire fleet. "It is crucial for our customers to be supplied with systems that are protected at the very highest level. It is especially important for Totem ECDIS [Electronic Chart Display and Information System], the only ECDIS in the world offering Collision Avoidance DST [Decision Support Tool]. The Naval Dome system is the only dedicated maritime cyber security system to have so far achieved Security Level 4 under DNV GL CP-0231. There are currently no other OEMs supplying equipment embedded with this level of protection," **Capt. Azriel Rahav**, Chief Executive Officer, Totem Plus, commented. **Asaf Shefi**, CTO, Naval Dome, added, "I am delighted that Israeli-developed technologies are now at the very forefront of maritime cyber security. As the first original equipment manufacturer (OEM) licensed to integrate the Naval Dome software with its hardware, Totem Plus leads the way in the provision of equipment optimised for safeguarding against unauthorised penetration." Capt. Rahav also said in this context, "Supplying equipment already installed with the Naval Dome technology not only delivers confidence to customers that our products are type approved to deliver the highest level of security, but they only need to have one point of contact: the OEM." The two companies began working together in 2017 when the Naval Dome solution was used to protect a wide range of Totem Plus' installations on-board a 5,000 TEUs-big container ship, including ECDIS; Integrated Monitoring, Alarm & Control; Voyage Data Recorder; and Bridge Alert Management.

## ClassNK approaches cyber security, too

The Japanese classification society has released the ***ClassNK Cyber Security Approach***, in which it has outlined, based on related trends in international institutions and maritime bodies, its basic approach to ensuring on-board cyber security


Layers of Cyber Security Controls
1. Controls with software and hardware equipment
2. Operational controls for ensuring the health of "equipment controls"
3. Controls for ensuring the health of "operational controls"
4. Organizational controls designed for information security management
5. Development of shipboard products with reduced cyber risks

## ClassNK Cyber Security Series

### Guidelines for Designing Cyber Security Onboard Ships

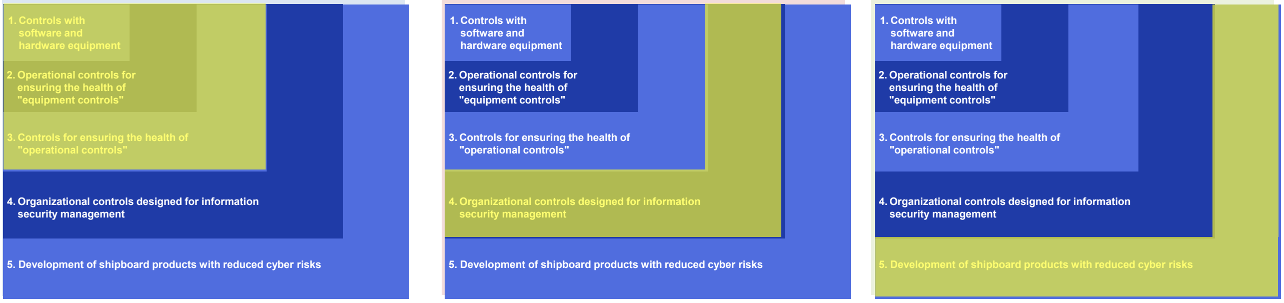
- ■ Target: Shipyards and shipowners
- ■ Extract controls applicable to ships from NIST SP800-53 using NIST SP800-82 as a reference
- ■ Examine the IACS Recommendations

### Cyber Security Management System for Ships

- ■ Target: Ship management companies and ships
- ■ Management system aimed at compatibility with the ISM Code system using the basic structures of ISO 27001 and ISO 27002

### Software Security Guidelines

- ■ Target: Shipboard equipment manufacturers
- ■ Verify development process and functional requirements based on guidelines with elements required for ships extracted from relevant ISO/IEC standards



1. Controls with software and hardware equipment
2. Operational controls for ensuring the health of "equipment controls"
3. Controls for ensuring the health of "operational controls"
4. Organizational controls designed for information security management
5. Development of shipboard products with reduced cyber risks
1. Controls with software and hardware equipment
2. Operational controls for ensuring the health of "equipment controls"
3. Controls for ensuring the health of "operational controls"
4. Organizational controls designed for information security management
5. Development of shipboard products with reduced cyber risks
1. Controls with software and hardware equipment
2. Operational controls for ensuring the health of "equipment controls"
3. Controls for ensuring the health of "operational controls"
4. Organizational controls designed for information security management
5. Development of shipboard products with reduced cyber risks

for ships, with the aim of helping stakeholders take appropriate measures. Ensuring navigational safety is regarded by **ClassNK** as the most important goal of on-board cyber security. The society will propose a set of physical, technical, and organizational measures (e.g., designing ships and on-board equipment with security by design), which cover both operational and information technologies, to achieve that goal. ClassNK will also classify cyber security controls into different layers and advise stakeholder what they can do within their scope of responsibilities. Based on these concepts, ClassNK will continually publish guidelines and standards that specify the parties responsible for implementing cyber security controls and the details thereof as part of the ***ClassNK Cyber Security Series***, along with the ***Cyber Security Management System for Ships and Software Security Guidelines*** that target ship management and future software, respectively. At the same time, ClassNK has released its ***Guidelines for Designing Cyber Security Onboard Ships*** for the shipbuilding industry. The guidelines include the security measures (SP800-53) developed by the ***National Institute of Standards and Technology*** (***Recommended Security Controls for Federal Information Systems***) as well as the latest recommendations of the **International Association of Classification Societies**. The guidelines and the *Cyber Security Approach* are publicly available through ClassNK's website for those registered to the My Page service (which is also free of charge).

## ClassNK and TÜV Rheinland enter into a cyber-security services co-op

The Japanese classification society and the German provider of testing, inspection, and certification services (incl. digital ones for safety, cyber security, and privacy) have agreed to jointly work on developing and delivering a cyber security certification scheme for the maritime industry. The collaboration will kick off by working on guidelines that target on-board software currently being developed by the society. This partnership will also bring pragmatic cyber security certification services to meet the maritime sector's needs. "Digital transformation is changing the way that business is conducted and offering more opportunities, while cybersecurity is an essential factor to its promotion and adoption in the maritime industry. Through the new partnership, we will do everything possible to overcome the cybersecurity challenges of the industry by combining TÜV Rheinland's abundant expertise and our society's accumulated knowledge and experience on management systems for ship operations as well as the structure, machinery and other components of ships themselves," **Koichi Fujiwara**, President and CEO, **ClassNK**, commented. To this **Dr. Michael Fübi**, Chairman, **TÜV Rheinland**, added, "Combining our expertise and experience in Industrial Services and Information Technology (IT), Operational Technology (OT) and cybersecurity, we are one of the few organizations developing deep capabilities to offer this level of cybersecurity expertise to the maritime industry which is concerned with the safety on-board vessel, compliance with regulatory requirements for cybersecurity, risk assessment and certification. The priority for TÜV Rheinland is to continue delivering its mature cybersecurity services to maritime sector across the globe to protect shareholder investment from cyber-attacks and strengthen the confidence of regulators and governments."

# info-nuggets

Photo: Rawpixel

## Survey Methodology And Respondent Profiles

Cyber Security Hub fielded an email survey to subscribers in October 2018 to identify enterprise cyber security trends. Cyber Security Hub received 286 survey completions. Responses were further narrowed to only those describing themselves as cyber security project owners with direct responsibility and cyber security organizational influencers, which resulted in 189 survey completions from qualifying subscribers.

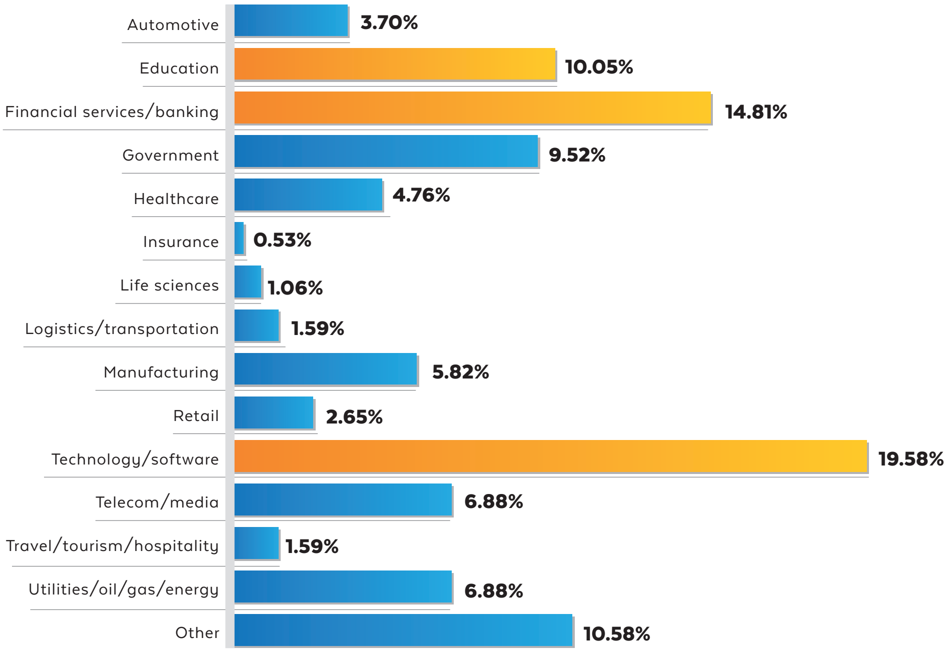
Nearly half of respondents' organizations conduct business in North America. Europe, Asia-Pacific (excluding South Asia), and the Middle East are also popular operating regions of survey respondents. (Figure 2)

**RESPONDENTS FROM THE TOP 3 SECTORS (Figure 1)**

Technology/Software, Financial Services/Banking, and Education -- represent over 44% of the industries in our survey. Approximately 89% of respondents associated with one of the 14 identified industries.

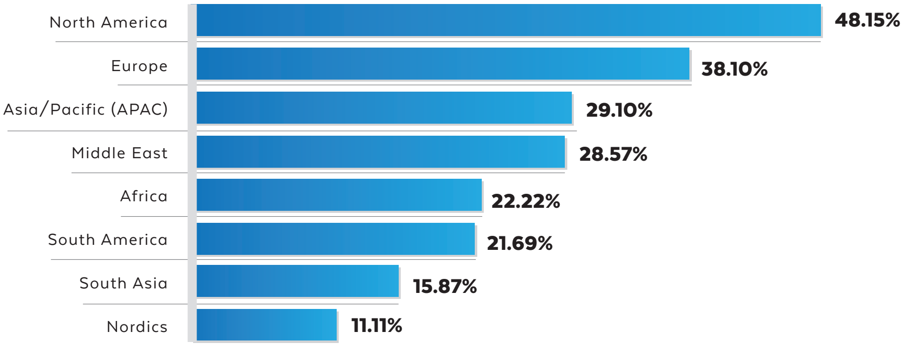
### INDUSTRY ORGANIZATION SECTOR

FIGURE 1: **Which industry vertical best describes where your organization sits?**



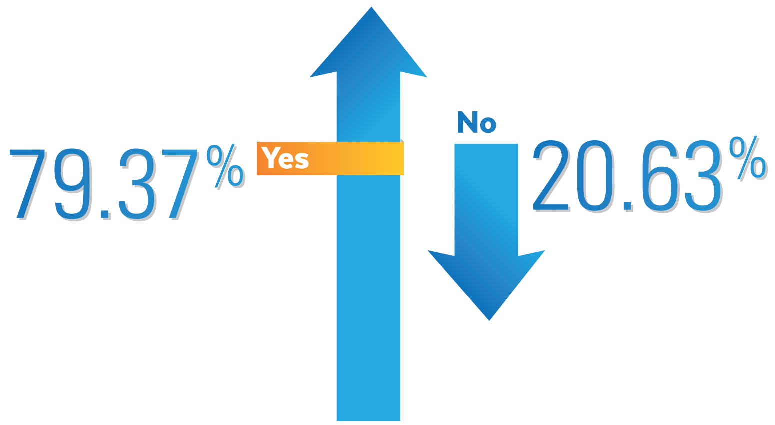
### Respondent Business Operating Region

FIGURE 2: **What world regions does your organization operate in?**



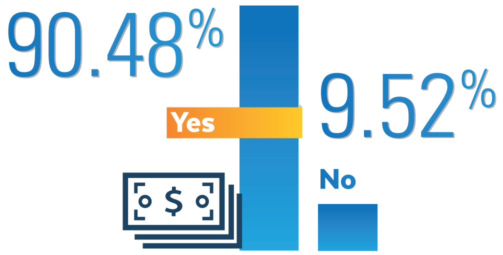
## The State Of Enterprise Cyber Security

**FIGURE 3: Do you feel as though the overall state of cyber security, meaning resiliency, compliance, awareness, etc., is improving?**



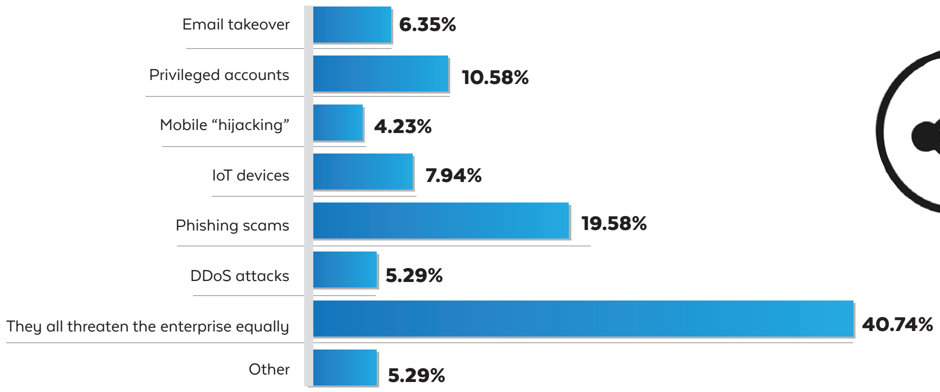
## Cyber Awareness Driving Business Growth

**FIGURE 4: Do you believe that cyber awareness can drive holistic business growth?**



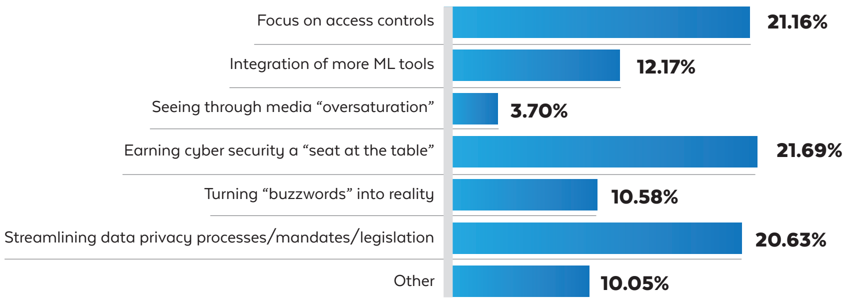
## Phishing Scams And Privileged Accounts Top Most Dangerous Threat Vectors

**FIGURE 5: What is the most dangerous threat vector, in your opinion?**



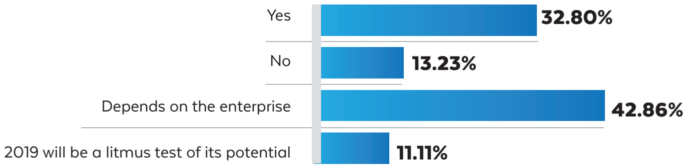
## Cyber Security Areas Needing Change In 2019

**FIGURE 6: What is one area of cyber security you believe needs to change the most in 2019?**



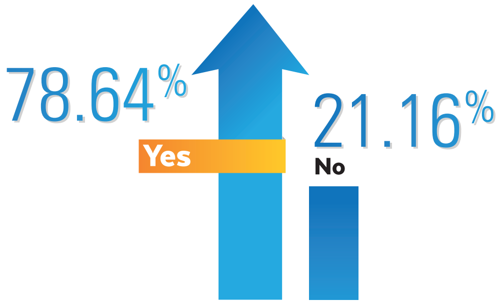
## Will Cyber Security Automation Observe Seismic Shifts In 2019?

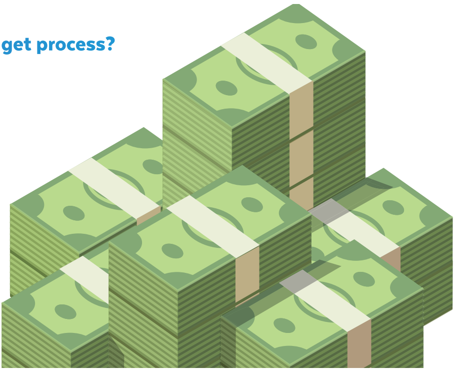
FIGURE 7: **Do you see seismic shifts toward automation in cyber security?**



## Cyber-spend In The Budgeting Process

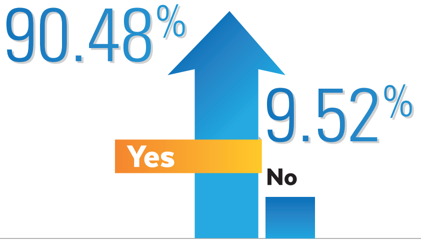
FIGURE 8: **Is "cyber-spend" still an enigmatic part of the budget process?**





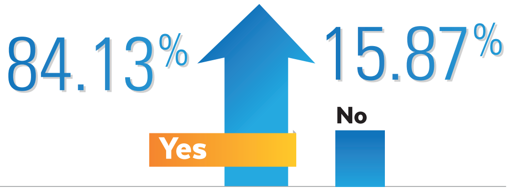
## Mobile Devices: A Growing Threat In 2019

FIGURE 9: **Will mobile devices pose even more of a threat in 2019?**



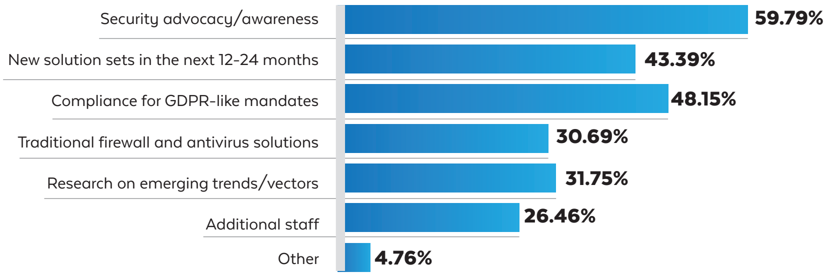
## Comprehensive, Single Vendor Endpoint Security Suites Remain Elusive

FIGURE 10: **Have endpoints confounded today's security professionals – piling on to other security/connectivity concerns?**



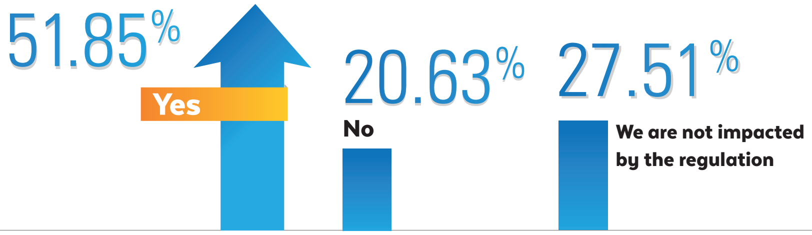
## Predicting 2019 Cyber Dollar Allocations

FIGURE 11: **With some enterprises combating limited resources, where do you see cyber-dollars being allocated in 2019?**



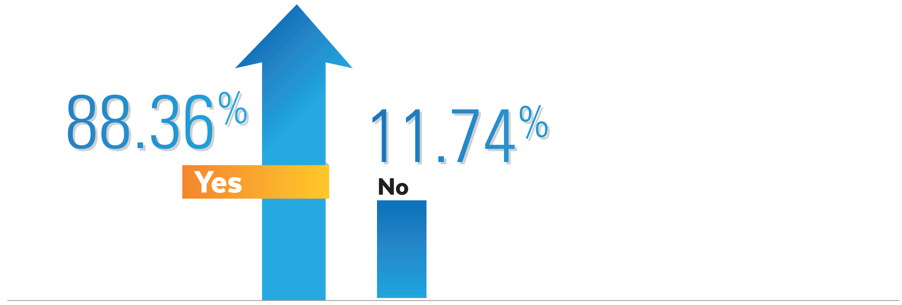
## GDPR Is Only The First Enterprise Challenge In Data Privacy Regulation

FIGURE 12: **Does GDPR remain a challenge for your enterprise?**



## The Growing Pipeline For Data Privacy Legislation

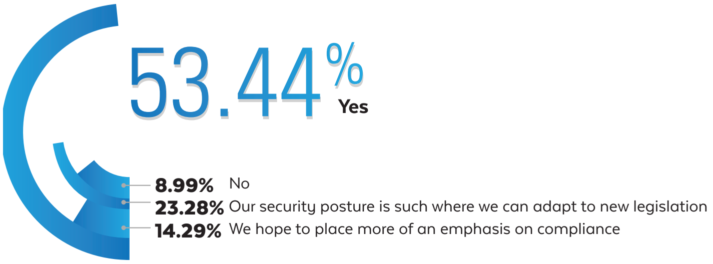
FIGURE 13: **Do you see the data privacy legislation pipeline growing in 2019?**



*[1] Forbes. Ezrati, Milton. "Cybersecurity: A Major Concern And A Great Business Opportunity". Forbes. 5 Sep. 2018: https://www.forbes.com/sites/miltonezrati/2018/09/05/cyber-security-a-major-concern-and-a-great-business-opportunity/#643018033e26*

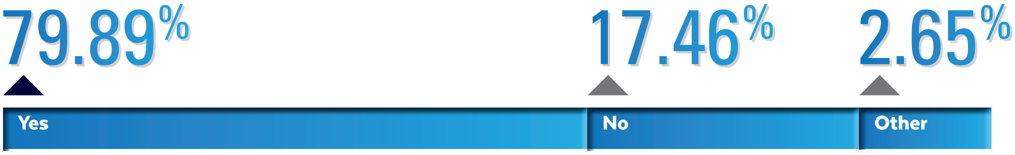
## Will That "Pipeline" Prove To Be A Challenge For Security Teams?

FIGURE 14: **Do you see the data privacy legislation pipeline growing in 2019?**



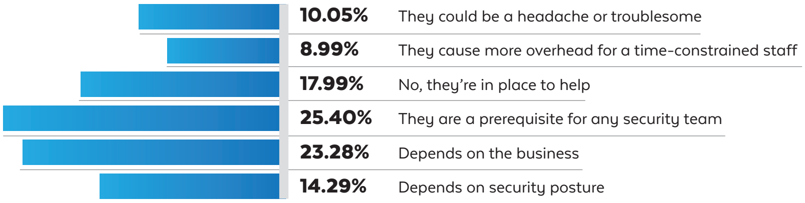
## Concern About Enterprise Security Being Bolted-on vs. Bolted-in

FIGURE 15: **Is security viewed as a bolted-on afterthought or incorporated into the development/ deployment stage?**



## Data Privacy Officers: Asset Or Headache?

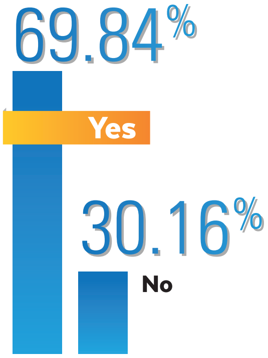
FIGURE 16: **Do you see Data Privacy Officers (DPO) or "security champions" in lines of business or development as an asset or a headache for the enterprise?**



## The Security Talent Crisis Continues In 2019

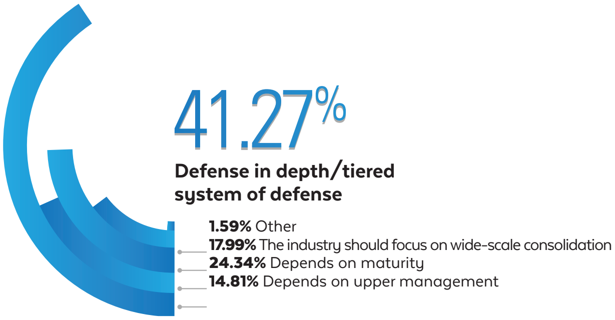
FIGURE 17: **Is the talent crisis an ongoing "pain point" for your security team?**

**Yes 69.84%**
**No 30.16%**



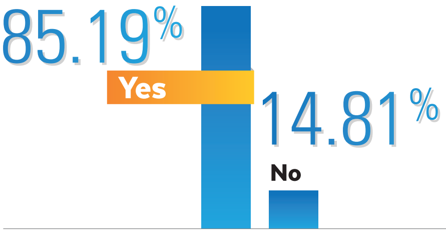
## Defense-in-Depth Tiered Strategies Trump Broad Industry Solution Consolidation

FIGURE 18: **Is "defense in depth" the answer or do enterprises desire more consolidation across their "point solutions"?**



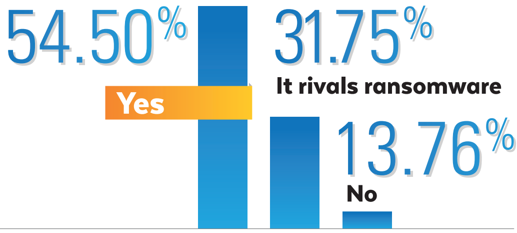
## Ransomware To Keep Practitioners "Up At Night" In 2019

**FIGURE 19: Will ransomware continue to keep security practitioners "up at night" in 2019 and beyond?**



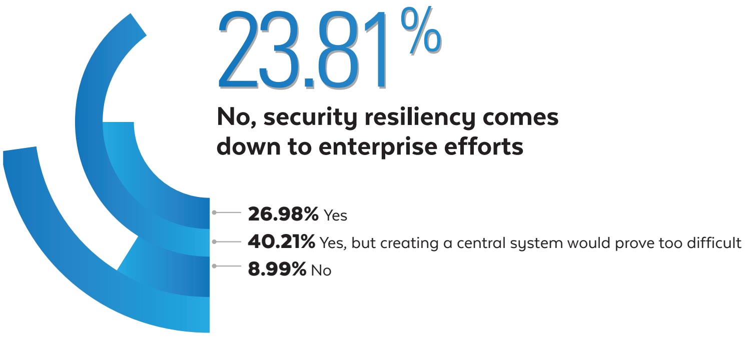
## Incidents Of Crypto-jacking Bigger Than Ransomware

**FIGURE 20: Is crypto-jacking even more of a threat than ransomware - due to its subtlety and potential financial impact?**



## Lack Of Centralized Government Regulation

**FIGURE 21: Do you believe the industry is lacking because major world powers do not have centralized cyber security regulatory frameworks?**



*[2] Morgan, Steve. "Cybersecurity Jobs Report 2018-2021". Cybersecurity Ventures. 31 May 2017: https://cybersecurityventures.com/j*

## Hacker Sophistication & Overall Cyber Security Sentiment

**FIGURE 22: Do you foresee hacker sophistication growing in 2019, or somewhat stabilizing with defense efforts?**

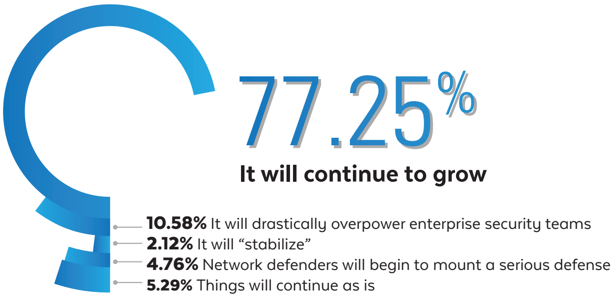
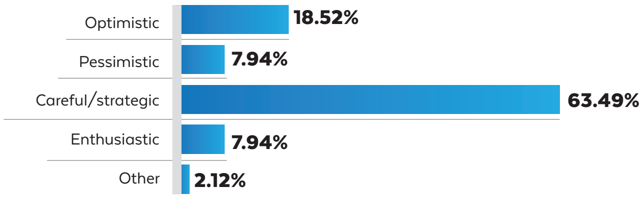


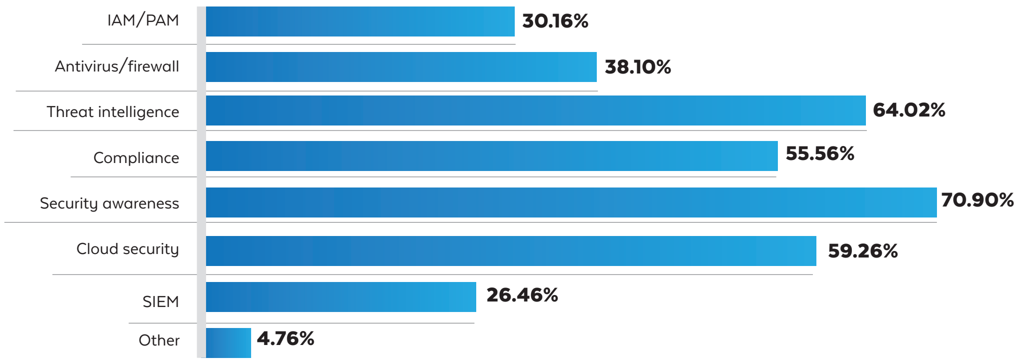
**FIGURE 23: Overall, my take on the cyber security space is:**



*[3] Trend Micro. "Unseen Threats, Imminent Losses; 2018 Midyear Security Roundup". Trend Micro. 28 Aug. 2018: https://documents.trendmicro.com/assets/rpt/rpt-2018-Midyear-Security-Roundup-unseen-threats-imminent-losses.pdf*

## Cyber Security Priority Solutions For 2019

FIGURE 24: **What solutions will be a priority for you in 2019?**



*[4] U.S. Department of Homeland Security. "Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing". U.S. Department of Homeland Security. 31 Aug. 2015: https://www.dhs.gov/publication/executive-order-13691-promoting-private-sector-cybersecurity-information-sharing*

- **Cyber Security is Strategically Important to the Enterprise:** Cyber must be integrated into the corporate culture and be operationalized in all facets of the organization. Don't treat Security and Data Privacy as a business unit or a department.

- **Awareness and Education Across the Organization:** "Security awareness doesn't have a user manual," writes LogMeIn product marketing manager Leah Bachmann. There is no magic recipe to get fellow employees smarter on security, though every day is a good day to keep your company and its data more secure using themes, memes, and compassion for human behavior.

- **Staffing and Skills Training:** "By 2021, there will be more unfilled cyber security jobs than the total population of Iowa, and there are currently more job openings for CISSP certification holders than CISSPs," observes Kayne McGladrey, Director of Security and IT for Pensar Development. However, the biggest issue around staffing in cyber security may be finding people who truly have the passion and skills to be in the specialization.

- **Insider Threats:** Threat actors are already using stolen insider credentials, with 53% of organizations confirming "insider attacks against their organization in the previous 12 months," according to Veratio. These risks are accelerating, not decreasing. The best defense is a "defense-in-depth," where overlapping layers of defense support one another, and where a compromise of one defense does not lead to a complete compromise.

- **Hackers:** External threat actors remain the single largest concern for enterprise cyber leaders. With increased access to data and automation in the workplace, the sophistication of hacker tools has also continued to grow. The profile of a hacker is also evolving from a "who" to a "what" as software bots and the scale of distributed digital attacks.

- **Unmanaged Mobile Endpoints:** The proliferation of smartphones has increased employee mobility and productivity. At the same time, careful planning remains essential for BYOD and unmanaged endpoints to avoid becoming the organization's latest vulnerability.

- **GDPR and Security/Data Privacy Legislation:** Whether GDPR impacts your organization or not, there is a piece of legislation in the works that you should be planning for. Anticipating new frameworks for data privacy disclosure and compliance puts the cyber team in a proactive position with the business rather than security as an afterthought.

- **Emerging Trend - Cloud Security:** The cloud offers enterprise cost benefits and other efficiencies. Yet, as with any technological advance, cloud computing becomes an entry point for threat actors. In fact, cloud computing, in an unsecure state, drastically widens the attack surface.

- **Emerging Trend - IoT Security:** IoT is already a part of the enterprise, whether cyber security administrators are ready or not. Thanks to advances in network technology, seizing control of connected devices has become an active threat to the enterprise professional. The need for more cyber awareness and oversight is quickly becoming apparent.

ICS
CYBER SECURITY

# CYBER ATTACKS ON CNI: THE COST OF A DATA BREACH

Ahead of this year's ICS Cyber Security conference taking place 29th April – 1st May in London, Defence IQ compiled information from various sources to highlight the financial cost of a data breach on CNI organisations. This infographic provides a global overview of the evolution of threats and their financial damage on organisations, and shows differences in countries and sectors across the globe.

## TOTAL REACH:

15 COUNTRIES

477 COMPANIES

2,200 INTERVIEWS

FROM DATA PROTECTION, IT AND COMPLIANCE PROFESSIONALS

*A record in this report is defined as information that identifies the natural person (individual) whose information has been lost or stolen.
Source: IBM, Ponemon

## GLOBAL STUDY AT A GLANCE

Average total cost of a data breach for the 2018 time period

**$3.86 MILLION**

Average total one-year cost increase from 2016 to 2017

**6.4%**

Average cost per lost or stolen record in 2017

**$148**

One-year increase in per capita cost

**4.8%**

Likelihood of a recurring material breach over the next two years - this can be predicted by looking at how many records were lost or stolen and the regional location of the incident:

**27.9%**

Average cost savings with an Incident Response team:

**$14 PER RECORD**

# THE AVERAGE TOTAL COST OF A DATA BREACH, THE AVERAGE COST FOR EACH LOST OR STOLEN RECORD (PER CAPITA COST), AND THE AVERAGE SIZE OF DATA BREACHES HAVE ALL INCREASED SINCE 2017.

The average total cost of a data breach increased from **$3.62 to $3.86 million**, an increase of **6.4 percent**

The average cost for each lost record increased from **$141 to $148**, an difference of **4.8 percent**

The average size of the data breaches in this research increased by **2.2 percent**

# INCIDENT RESPONSE AND CONTAINMENT PROCESSES

The faster the data breach can be identified the lower the costs. MTTI and MTTC metrics are used to determine the effectiveness of an organisation's incident response and containment processes. The stealth of recent attacks increases the time it takes to identify and contain these types of data breaches.

01 The mean time to identify/detect (MTTI) that an incident has occurred a breach was **197 days**

02 The mean time to contain/restore service (MTTC) a breach was **69 days**

03 Companies that contained a breach in less than 30 days saved over **$1 million** compared to those that took more than 30 days to resolve

Industry with the highest average response time to contain a breach:

**Healthcare 103 days**

Industry with the lowest average response time to identify a breach:

**Financial Services 163 days**

Industries with the lowest average response times to contain a breach:

**Research, Financial Services, and Energy & Utilities at 53, 54, and 72 days.**

# THIS YEAR MORE ORGANISATIONS WORLDWIDE LOST CUSTOMERS AS A RESULT OF THEIR DATA BREACHES

However, if an organisation's chief privacy officer (CPO) or chief information security officer (CISO) is driving initiatives to improve customer trust in the safeguarding of their personal information, this will reduce the cost of the breach.

## POST DATA BREACH RESPONSE COST

7
4
5
3
13
1
8
9
6
2
10
11
15
14
12

| | | |
|---|---|---|
| 1. | United States | $1.76 million |
| 2. | Middle East | $1.47 million |
| 3. | Germany | $1.31 million |
| 4. | Canada | $1.26 million |
| 5. | France | $1.18 million |
| 6. | Japan | $1.07 million |
| 7. | UK | $0.84 million |
| 8. | Italy | $0.81 million |
| 9. | South Korea | $0.78 million |
| 10. | India spends | $0.75 million |
| 11. | ASEAN (Singapore, Indonesia, the Philippines and Malaysia) | $0.67 million |
| 12. | South Africa | $0.67 million |
| 13. | Turkey | $0.57 million |
| 14. | Australia | $0.47 million |
| 15. | Brazil | $0.37 million |

Post data breach response activities include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions.

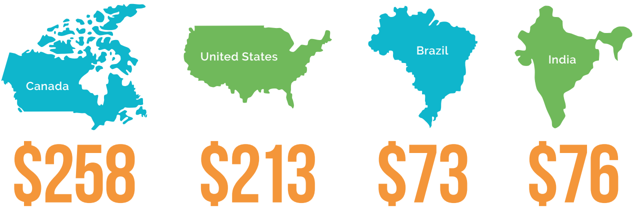
**$81**

Canada had the highest direct cost at **$81** per compromised record. Direct costs refer to the expense outlay to accomplish a given activity such as engaging forensic experts, hiring a law firm, or offering victims identity protection services.

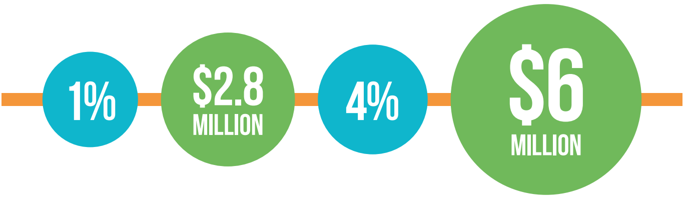
**$152**

The United States had the highest indirect per capita cost at **$152**. Indirect costs include employees' time, effort, and other organisational resources spent notifying victims and investigating the incident, as well as the loss of goodwill and customer loss.

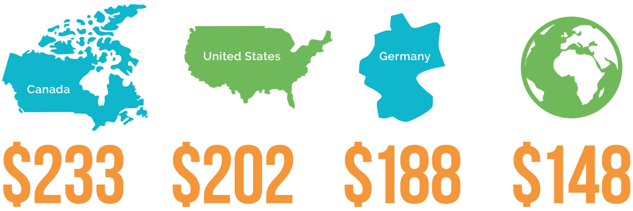
**48%** percent of all breaches between mid 2017 and mid 2018 were caused by malicious or criminal attacks. The average cost to resolve such an attack was **$157**. System glitches cost **$131 per record** and human error or negligence is $128 per record. Companies in the United States **($258 per record)** and Canada **($213 per record)** spent the most to resolve a malicious or criminal attack. Brazil **($73 per record)** and India **($76 per record)** spent significantly less.



There are considerable financial costs when you loss customer trust. On a global scale organisations that lost less than **1%** of their customers due to a data breach resulted in an average total cost of **$2.8 million**. If **4%** or more was lost, the average total cost was **$6 million**.



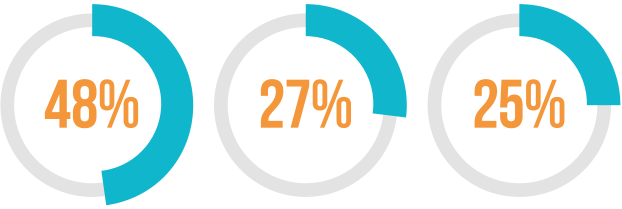
The 2018 per capita cost of data breach by country or region shows the United States **(£233)**, Canada **($202)**, and Germany **($188)** continue to have the highest per capita costs. The global average per capita amounts to **$148**.



The 2018 per capita cost of data breach by country or region shows Turkey, India, and Brazil have much lower per capita costs at **$105**, **$68**, and **$67**, respectively. Heavily regulated industries such as healthcare and financial organisations have a per capita data breach cost substantially higher than the overall mean.

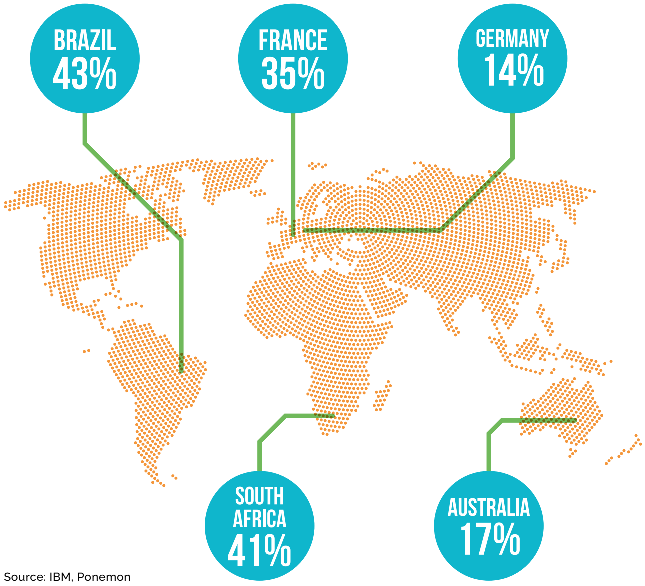
Turkey
India
Brazil
$105
$68
$67

**48%** of incidents involved a malicious or criminal attack, **27%** were due to negligent employees or contractors and **25%** involved system glitches, including both IT and business process failures.



# FUTURE PROBABILITY OF A DATA BREACH

Brazil, South Africa, and France appear to have the highest estimated probabilities of a data breach at **43.0%**, **40.9%**, and **35.1%**. Germany and Australia have the lowest probability of data breach at **14.3%** and **17.0%**.



Source: IBM, Ponemon

featured articles

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.

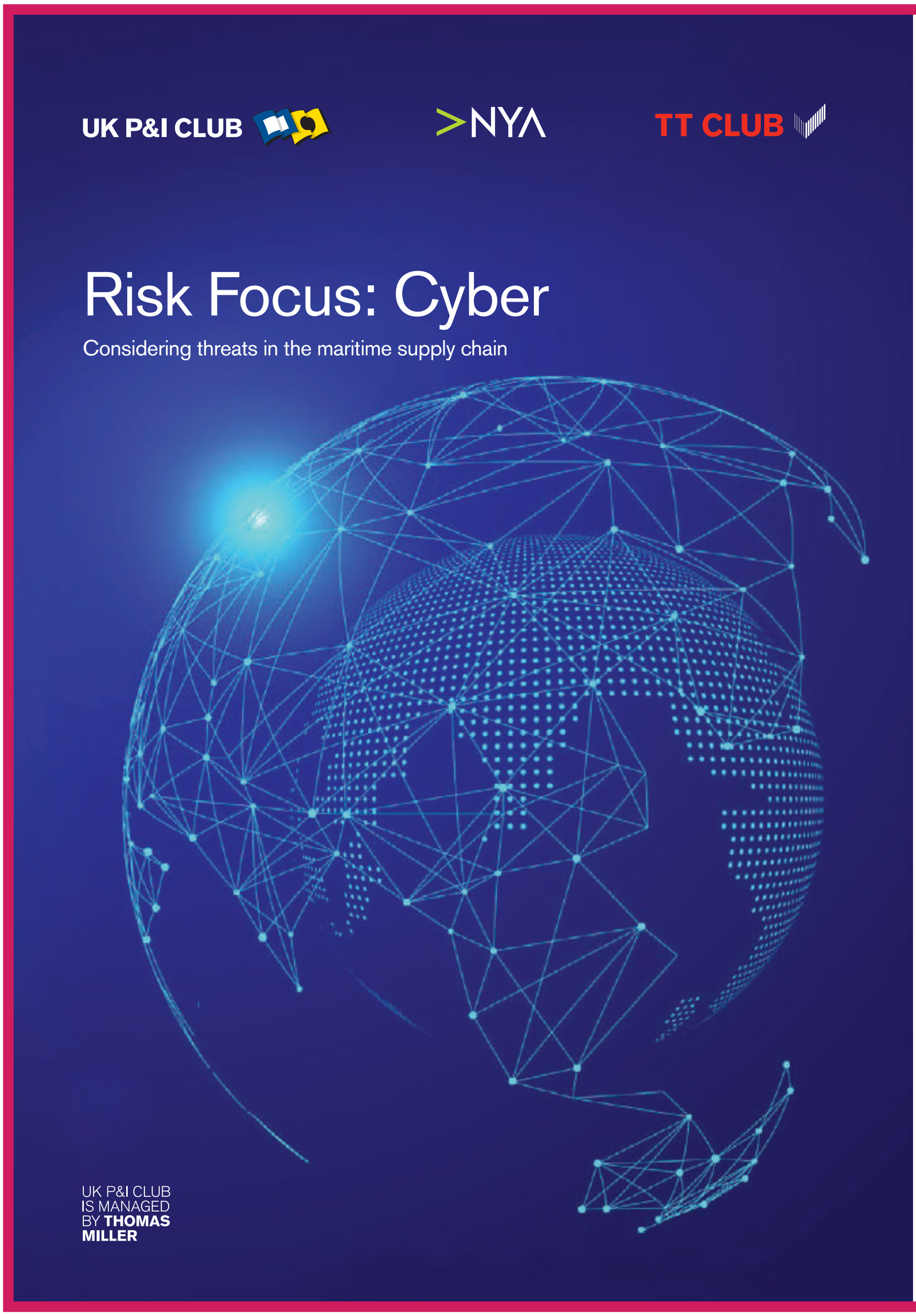
The US Coast Guard issued a draft Navigation and Vessel Inspection Circular (NAVIC) titled *Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities*. The circular currently under review requires incorporation of personnel training, drills and exercises 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. ■



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**

**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.**

Photo: Rawpixel

What can the maritime industry do to be more cyber-secure

# Digital defence

by **Nikos Späth**, *Head of Media & Public Relations, DNV GL Maritime Communications*

**Although the notion of a ship in the middle of the ocean being disabled by a software malfunction or by hackers was initially greeted with considerable scepticism and denial, a spate of incidents, including most notably an attack that disrupted operations at COSCO, has transformed attitudes. Today the maritime industry acknowledges the potential dangers and is taking steps to address the cyber risk at various levels. As owners act to fortify their ships and shore-side operations against cyber risk in the face of evolving threats and imminent regulation, DNV GL has expanded its services to cover control systems, software, procedures and human factors.**

DNV·GL

The Høvik-headquartered DNV GL is a classification society and accredited certification body. Since its foundation in 1864, DNV GL's purpose has been to safeguard life, property, and the environment. Today, the organisation is structured into five business areas: Maritime, Oil & Gas, Energy, Business Assurance, and Digital Solutions, alongside a Global Shared Services function and Group Centre. For more info please click www.dnvgl.com

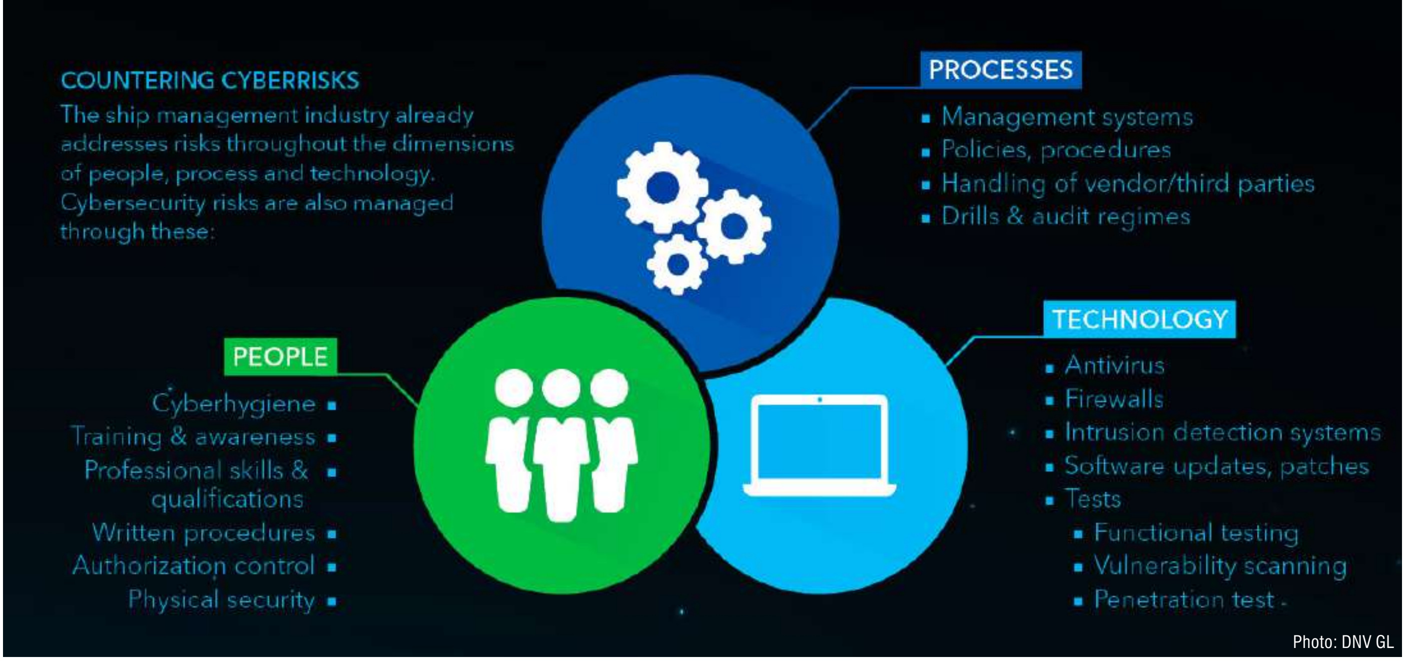
Cyber security is a moving target. Threats continue to grow in reach and complexity, with new vulnerabilities discovered on a seemingly daily basis. In the space of a few years, hacks and security breaches have jumped from being an exceptional event confined to a special breed of technology companies to becoming a fact of life-impacting everyone. No industry is immune.

While in earlier decades office IT systems were the predominant target, these days more incidents are affecting operational technology (OT) – the programmable control systems responsible for operating machinery. The trend reflects the growing complexity of such systems and a general increase in connectivity, which in turn increases the attack surface of a vessel.

This increase is borne out in the statistics: The number of attacks on OT in 2016 was double that of the preceding year and quadruple the 2013 level. So whereas before it was mostly a company's finances and reputation that were at risk, now the threat has escalated to confront the safety of life, property and the environment. The stakes are much higher. For this reason cyber security must now be considered an integral part of overall safety management in shipping and offshore operations.

### Regulatory response

Fortunately, industry policymakers have not been asleep at the wheel. The year 2017 saw two particularly significant milestones in the regulatory environment. A section dedicated to maritime security – including cyber risk – was introduced in the third edition of the Tanker Management Self Assessment (TMSA), which came into effect in January 2018, as well as in the seventh edition of the Vessel inspection questionnaire (VIQ7) from the Ship Inspection Report Programme (SIRE), effective from September 2018. Because TMSA and SIRE



COUNTERING CYBERRISKS

The ship management industry already addresses risks throughout the dimensions of people, process and technology. Cybersecurity risks are also managed through these:

PROCESSES

- Management systems
- Policies, procedures
- Handling of vendor/third parties
- Drills & audit regimes

PEOPLE

- Cyberhygiene
- Training & awareness
- Professional skills & qualifications
- Written procedures
- Authorization control
- Physical security

TECHNOLOGY

- Antivirus
- Firewalls
- Intrusion detection systems
- Software updates, patches
- Tests
  - Functional testing
  - Vulnerability scanning
  - Penetration test

Photo: DNV GL

are imperative to gaining charters, tanker operators now have a commercial incentive to demonstrate they have given systematic consideration to potential vulnerabilities and implemented appropriate mitigations and safeguards to address them.

Shortly after, IMO's Maritime Safety Committee inserted Maritime Cyber Risk Management into the list of International Safety Management Code requirements. Strongly encouraged to start on 1 January 2021, the amendment leaves non-tanker vessel owners with little more than two years to achieve a similar level of preparedness as their tanker-owning colleagues.

### Risky job

Managing cyber risk is ultimately no different to managing any other risk, remarks Svante Einarsson, DNV GL's Senior Cyber Security Advisor. "The equipment and terminology may be unfamiliar and somewhat daunting but the approach is fundamentally the same as, say, preparing for and carrying out hot work modifying a vessel's structure."

Software changes, for example, should not be done on a whim, which can often happen on ships. Because IT engineers don't frequently visit vessels, when they do come aboard to update the Electronic Chart Display and Information System or set up the latest version of a maintenance management application, the temptation is to be helpful. They click to install a new service pack and a backlog of other app updates. Nine times out of ten, this is fine. But occasionally it can disrupt settings elsewhere on the system. Moreover, the consequences won't become apparent until long after the engineer has left and the ship has set sail.

Instead, updates should be carefully planned, tested, approved and recorded. They should be categorized as minor or major to ensure personnel with the appropriate authority can approve them. This, Einarsson says, is virtually identical to the process for gaining approval prior to carrying out welding.

### Lessons learned from NotPetya

If there was one positive outcome of the NotPetya ransomware attack on Maersk in 2017, reasons Einarsson, it was the awakening of owners and operators to the fact that cyber threats are not hypothetical. "Today there is much greater awareness of the real-world implications and acceptance that cyber risk has to be tackled," he says. However, shipowners and operators are at different stages of the learning curve in formulating a response. Einarsson also observes, "Some are bewildered by the scale of the problem and don't know where to begin; others have introduced some countermeasures but are uncertain whether they've covered everything they need to cover."

In its role as a classification society DNV GL has adapted and expanded its cyber security services to assist owners and operators in protecting their assets against evolving threats and ensuring their safeguards satisfy new industry rules and regulations. DNV GL now provides services for educating and raising the awareness of all stakeholders both onshore and at sea; assessing and implementing defensive and reactive countermeasures; and monitoring and reviewing the effectiveness and robustness of barriers with an emphasis on continuous improvement.

These services are purposely designed to be non-system specific so as to work equally for conventional IT and industry-specific operational technology, which is important when systems are interlinked. This also avoids obsolescence. While the consequences of an OT outage are likely to be more serious, they can often be traced back

*Scan the code to download DNV GL's Cyber Secure class notation*

*Scan the code to obtain your copy of DNV GL's Recommended Practice on cyber security resilience management for ships and mobile offshore units in operation*

*Scan the code to watch DNV GL's video about cyber security awareness*

Photo: DNV GL

to a weakness in IT systems, particularly if they originate from an external source.

### Practical advice

In September 2016, DNV GL published a Recommended Practice (RP) to educate shipowners and operators on how to deal with cyber risk. “It was designed to demystify a subject the industry was still getting to grips with. We took care to write it in a maritime language and context,” stresses Einarsson. The focus was on practical steps. “Most advice coming from industry bodies at the time, while produced with noble intentions, was very high-level. Our idea was to close the gap between theoretical concepts and the real world,” he underlines. For example, DNV GL’s RP accounts for common constraints such as limited budget and resource availability. The core approach is to identify weaknesses, assess their severity, then prioritize the most serious ones. The RP has been released as a free resource.

The next step for vessel operators would be to carry out a cyber security assessment. DNV GL can support this by sending interdisciplinary teams to help on- and offshore personnel identify and address specific business risks. “While operators typically understand the written guidance, translating those principles into action is sometimes more challenging,” notes Einarsson. This collaboration results in a highly methodical approach to developing effective risk mitigation procedures that mesh neatly with the operator’s structure and working practices. Apart from closing cyber security gaps by technical means, this appraisal also considers system management and the human factor.

Once countermeasures and a new risk management regime have been implemented, they can be followed up and qualified by penetration testing. “Testing the robustness of barriers is essential to ensure that assets are secure and nothing has been overlooked,” explains Einarsson. In this process, authorized “white-hat” hackers do their best to compromise the IT and OT defences to validate that safeguards work as they should and risks have been eliminated.

### Life cycle management

DNV GL also provides third-party verification of cyber security requirements throughout the newbuild project life cycle. “Our cyber security team recently worked with a major cruise line on devising a process for embedding cyber resilience from the very beginning of the vessel design phase,” reports Einarsson. This was accomplished by introducing defined risk handling and accommodating procedures to all stakeholders in the project – not only the owner and yard but also the vendors. Incorporating technology and systems from third-party suppliers unavoidably adds complexity to a project and, from a cyber security perspective, increases potential exposure to malevolent actors. Meanwhile, shipyards are as much on the learning curve as vessel owners.

“For a large, sophisticated vessel like a cruise ship, which is dependent on technology for both operational and hotel needs, collaboration is absolutely critical,” Einarsson stresses and then adds, “Cyber risks are multifaceted. The response has to mirror that. Everyone has to be involved in the conversation, because, as the saying goes, a chain is only as strong as its weakest link.” The feedback from the project, he notes, was overwhelmingly positive, “Tackling cyber security right from the beginning of a vessel’s life cycle enables stakeholders to take a proactive, rather than reactive, approach to the problem. It provides more opportunities to insert barriers.”

Based on these advisory services, DNV GL has developed its first class notations covering cyber resilience. The Cyber Secure notations have three qualifiers: Basic, Advanced and “+”. Basic is primarily intended for ships in operation; Advanced is designed to be applied throughout the newbuilding process. The ‘+’ qualifier is available for systems not covered by the scopes of Basic and Advanced. Furthermore, DNV GL has introduced a Type Approval scheme to verify and test the cyber security reliance of components. The utilization of these reference standards ensures state-of-the art cyber security based on the 62443 standard of the International Electrotechnical Commission. The standards are applicable for the whole life cycle of a vessel from the perspective of manufacturers, yards and shipowners.

### The human element

Of course, cyber security is not just a matter of firewalls and antivirus software. Up to 90% of incidents are attributed to human behaviour. Phishing and social engineering, unintentional downloads of malware, etc., remain common issues. At the same time, most crews and onshore staff are not taught how to respond to cyber attacks or major technology failure and consequently fail to contain the damage.

DNV GL has therefore expanded its options for training through its Maritime Academy. Courses cover cyber security from both management and technical angles and even include lessons in hacking to give participants an insight into how cyber attackers operate. Additional new tools incorporate friendly phishing campaigns and simulations of other social engineering techniques as well as features for assessing staff alertness so customers can fine-tune the level and frequency of cyber awareness training.

DNV GL can help vessel operators combine traditional IT security best-practices with an in-depth understanding of maritime operations and industrial automated control systems. DNV GL understands the importance of tackling and integrating the human factor when devising and implementing a cyber risk management strategy because ultimately, it is people who drive our industry. ■

Time for transportation & logistics to up its cyber security as hackers put it on target list

Photos: Rawpixel

# Making the hackers’ job hard

by **Claus Herbolzheimer**, *Partner and Head of Digital, Technology & Analytics in Germany & Austria,* and **Max-Alexander Borreck**, *Principal, Transport and Logistics, Oliver Wyman*

OLIVER WYMAN

Oliver Wyman is a global leader in management consulting. With offices in 50+ cities across nearly 30 countries, Oliver Wyman combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation. Oliver Wyman is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC]. For more details on the company’s capabilities, please go to www.oliverwyman.com This article first appeared in *Forbes* on 28 June 2017.

**When the Danish shipping giant A.P. Møller-Mærsk’s computer system was attacked on June 27, 2017, by hackers, it led to disruption in transport across the planet, including delays at the Port of New York and New Jersey, the Port of Los Angeles, Europe’s largest port in Rotterdam, and India’s largest container port near Mumbai, according to reports. That’s because Maersk is the world’s largest shipping company with 600 container vessels handling 15% of the world’s seaborne manufactured trade. It also owns the port operator APM Terminals with 76 port and terminal facilities in 59 countries around the globe.**

For the transportation and logistics (T&L) industry, the June 27 cyber attack is a clarion call to elevate cyber security to a top priority. Besides Maersk, press reports said other T&L industry giants were affected, including German postal and logistics company Deutsche Post and German railway operator Deutsche Bahn, which was also a victim of the WannaCry ransomware hack in May the same year.

While up until now hackers have seemed more preoccupied penetrating computer systems at banks, retailers, and government agencies – places where a hacker can find access to lots of money and data and create substantial disruption – the most recent ransomware attacks demonstrate that the T&L industry is now on hackers’ radar.

**What is the Darknet?**

Part of the increased interest in the industry is because of its own efforts to digitize. Over the past couple of years, the industry has been in the process of automating systems, turning paper into digits, and using advanced analytics to stay on top of needs of their customers. That has put more systems online and vulnerable to various attack weapons now so readily available on the Darknet – the hidden underbelly of the Internet where hackers, terrorists, and criminals cavort anonymously buying malware, stolen data, arms, and drugs.

The early, more obvious targets have upped their game in cyber security, and hackers who are relentless look down the chain for new avenues of entry. Hacking also has become not only a corporate

Loading...
/ / Bon - persisted properties
<html> $errorMessage = ko , observable() ;
10480 Benefits 10 : 37 NSA
35246 Payroll taxes 10 : 12 NSA
76745 Salaries 11 : 01 NSA
78023 Commissions and bonuses 12 : 44 NSA
23674 Personnel Total 13 : 32 NSA
Stocks Exchange : bye 44% food
Company (As) : centre
Worminnud against Motice team
0.83745r7t +453u594
77% --------m AP Marketing
0000.09 -02,75583+ Times

business, but a nation state's business. Here, nation states are looking for places where things are crossing borders regularly and for access to major industries and public infrastructure, such as the airports and ports that T&L companies operate.

The T&L industry also has characteristics that make it a particularly tempting target. First, the industry is a global one with tentacles into so many different industries around the world. Complex logistical chains are created around manufacturers, and often logistics companies are embedded within production facilities controlling inventory and handling on-demand needs of a plant.

Simultaneously, the industry is fragmented with large T&L giants working alongside tiny companies responsible for one short leg of a product's long journey from raw materials, to production, to retailer, to consumer. This almost always means multiple technology systems are being employed, and multiple cyber security procedures of various degrees of rigor being followed. This fragmentation provides more opportunities for hackers.

### Looking for the weakest link

Like with all forms of warfare, attackers will seek out the weakest link in any chain – the most vulnerable element – as a target. Why steal money from the bank with all its infrastructure and protections when you can steal it on the way to the bank? While efforts to protect it along the way are made, almost any criminal could tell you, it is almost always more insecure in transit.

We already see malware that allows for hacking of delivery robots and parcel lockers. Drones can be hacked as well as autonomous cars, and as these are used more and more for deliveries the potential for hijack increases. Drones could be flown into no-fly zones posing the possibility of attacks on planes. When we reviewed the Darknet, we found personnel data from a major T&L company, car entry hacks, and means to create a fake parcel station identity.

Until now, the T&L industry has not prioritized cyber security except in cases where life was on the line, such as with aerospace manufacturers or airlines where the most sophisticated protections are used. But the direct costs from cyber security breaches are growing exponentially, and companies – even small ones – need to invest in new systems and more comprehensive risk management. By our projections, they can be expected to grow from $1.7b in 2015 to more than $6.8b by 2020. No industry will be entirely safe from the threat of cyber attacks.

### Bringing security to fragmentation

The industry's fragmentation and its requirement to operate within the various IT systems of its customers makes figuring out cyber security solutions more challenging and has led to lower investment. The industry also operates on low margins, making extensive capital expenditure on cyber security unattractive. That may be offset by the potential liability costs from hacks.

Increasingly, shippers and regulators will require T&L companies to guarantee the integrity of product and transport data, as well as ensure compliance with stricter cyber security laws. This will include carriers and forwarders, who are assuming central roles in supply chains as hubs for data exchange, making them high-value targets.

Taking precautions by installing security systems, such as firewalls and detection systems for denial of service attacks and other malware, is crucial, but insufficient by themselves. Cyber risk management also needs to take into account personnel and organization failure.

Ultimately, adopting proactive cyber security risk management provides an opportunity for T&L companies to differentiate themselves. Forward-looking companies will begin to see a safer logistical offering as a competitive advantage, especially if the attacks continue.

In the end, no industry will be entirely safe from the threat of cyber attacks. But every industry must do its part to at least make the job of hackers hard. ■

How identity management will change in 2019
to provide the ultimate cyber protection

Photo: Pxhere

# The enemy within

by **Mark Rodbert**, *CEO, idax Software*

**It seems that the peak of data breaches is upon us, with a different story hitting the headlines each day – although I've been saying that every year since 2015. When imagining where the threat is coming from, most people picture a hooded hacker in a dark room or a state-sponsored covert operation. As a consequence, most organisations are focussing their defence on implementing solutions to prevent intruders from getting in, relying heavily on solutions such as firewalls or antivirus protection. But what about the people who are already in and pose a threat to the internal security of the organisation?**

It turns out that the real threat lies a lot closer to home, with 66% of organisations considering malicious insider attacks or accidental breaches more likely than external attacks, according to the 2018 edition of the CA Technologies' *Insider Threat* report. Whether they are the result of bad actors attempting to sell sensitive company data, collusion, or unwitting accomplices using a work laptop on a Starbucks Wi-Fi, most breaches are simply a matter of access and opportunity.

Ultimately the outcome is the same, whether the intent is malicious or not. But, if we can identify who has access to what data and applications, and which of these are out of the ordinary, maybe there is a way to prevent internal threats after all.

**An inside job**

Clearly, an external threat is still a priority for businesses, and it's no surprise with many well-known enterprise businesses, like T-Mobile, Facebook, and Google, all facing damaging external cyber breaches last year. Yet, this shouldn't distract companies from the internal threat, which can be just as damaging; *Insider Threat* reported that 90% of organisations feel vulnerable to the insider threat, and the majority of employees have access to data they shouldn't. However, an insider threat becomes an external threat when compromised access is used by unscrupulous attackers. By tightening up the internal security vigilance, controls, and access processes, external hackers will find it harder to break through and entice staff with a phishing email.

So what can businesses do to start building their cyber defence to insider threat? Unfortunately, the answer is not as easy as simply implementing a new security system or process. Companies need to recognise the need for a cultural

idax
identity analytics

Using identity analytics, idax is the world's leading company in automatically analysing the access rights for an organisation, quantifying the risk, and determining who has excessive access requiring adjustment. Protecting digital information is critical for modern companies. Most cyber fraud is committed by employees. As technology becomes more complex, knowing whether or not someone should have access to systems is beyond the capability and knowledge of managers and traditional systems. What is required is a new approach. Using proprietary algorithms, idax enables organisations to manage access changes in real-time, making it possible to dynamically enforce the principle of 'least privilege'. For more information, please visit www.idaxsoftware.com

INSIDER THREAT

2018 REPORT

Cybersecurity Insiders

Crowd Research Partners

PRESENTED BY:

ca technologies

*Scan the QR code to directly access the 2018 edition of the CA Technologies'* Insider Threat *report*

shift and change in attitude, to the point where everybody in the organisation understands that cyber security is their responsibility. In order to change the culture around protecting assets, organisations need to make everyone – from the CEO to the person at the door – feel responsible, involved, and empowered, putting employees at the front of the fight. This requires building tools not just available to the IT security department but targeted at the whole organisation.

However, we're discussing a transformational change which won't take place overnight but over a significant period so that each individual comes to recognise the part they play. The first phase of this is access management being the job of specific security teams. The issue here is that employees feel as though it's a job for the security or IT team, and has nothing to do with them.

The next phase, which is becoming increasingly widespread among organisations, is steering away from having just the security team tackle the cyber issue and instead putting line managers in charge of access rights. Currently, this often involves the line manager having to deal with a highly complicated, confusing access details spreadsheet, with no context or explanation about what in the list refers to what data and what files are required for a role. Moreover, the risk with reviewing access to assets is asymmetric. If access to something that an employee does need is taken away, there is a very high chance of a small issue. However, if somebody keeps access to something they shouldn't have, there is a very small chance of a huge breach. Human beings need help comparing these risks.

In the long run – the eventual third phase of this shift – companies can look to become part of the security revolution that will see everyone in a company self-certificating their own access rights, with oversight and ultimate approval from line managers. With an engaging, end-user-friendly user interface, employees are encouraged to take responsibility for their own actions and aim to be as secure as possible.

**Step your cyber skills up now!**

2019 is looking like it may be the year for organisations to finally take a step back – or in fact, step *up* – and analyse their own internal security measures. The internal threat is and always has been overlooked as a significant cyber threat. Why wait any longer to crack down on your internal security? By implementing software to manage access rights, employers can start their journey to change company culture towards security immediately. ■

Photo: Wikimedia Commons

# A long way to go

by **Peter Broadhurst**, *Senior VP of Safety and Security, Inmarsat Maritime*

**Whether in pursuit of personal data or money, cyber crime is now a big and highly automated business, ready to strike at the most vulnerable part of an organisation's defence 24/7, anywhere in the world.**

inmarsat
The mobile satellite company

Inmarsat was set up in 1979 by the International Maritime Organization to enable ships to stay in constant touch with shore or to call for help in an emergency, no matter how far out to sea. Today, the company's fleet of 13 satellites serves not only the needs of merchant shipping but also governments, humanitarian aid agencies, airlines, the broadcast media, and the oil & gas, mining, and construction industries. For more info, please click www.inmarsat.com

As a case in point, speaking on a panel at the World Economic Forum earlier this year, Jim Hagemann Snabe, Chairman, A.P. Møller-Mærsk, revealed that responding to the NotPetya ransomware attack of June 2017 had required the reinstallation of 4,000 new servers, 45,000 new PCs, and 2,500 applications, all within ten days. During this period, the company reverted to manual systems. In hitting a company equipped with experienced cyber security specialists, NotPetya showed that the cyber threat is as real for shipping as it is for any other connected business, especially where legacy systems proliferate.

### Cyber ambivalence

If the warning should be sinking in, an Inmarsat Research Programme report from 2018, *The Industrial IoT on land and at sea*, suggests that maritime minds are slow to change. The unique study drew on testimony from 750 survey respondents across a range of industries to establish preparedness and perceptions regarding the adoption of solutions based on the Industrial Internet of Things (IoT).

The survey found 87% of maritime respondents saying they believed that their cyber security arrangements could be improved. It also saw more of them identifying data storage methods (55%), poor network security (50%), and potential mishandling/misuse of data (44%) as likely to lead to breaches in cyber security as an outright cyber attack (39%).

Given the self-diagnosis, it is perhaps surprising to find that only 25% of maritime respondents said they were working on new IoT-based security policies. In fact, Inmarsat's research exposed ambivalence as one of shipping's leading feelings towards IoT-based solutions. With some owners engaging at the level of blockchain, others take their lead from their need to comply with regulation: this is an industry which simultaneously sustains just over 30% of shipping respondents as 'IoT leaders' and just under 30% as 'IoT laggards,' the report says. For every owner signed up to the benefits of condition-based monitoring and predictive maintenance based on real-time connectivity, there appears to be another for whom maintenance is something that takes place at regular and predictable intervals, or whenever is most convenient.

Inconsistent views on cyber security also appear free to coexist with immature ones. Around 70% of respondents identify reducing marine insurance premiums as the main driver for IoT uptake, where insurers have shown themselves as especially sensitive to cyber threats. At the same time, other studies have found attitudes such as “I’m not the target/we have security in place, don’t we?/I will be protected by AntiVirus” alive and well among seafarers.

### How to maintain integrity

For those prepared to engage in the IoT, today ships sustain crews in small numbers, representing both an opportunity and challenge for automation, and indeed for cyber security. On the one hand, low crew numbers align strongly with operational technology (OT) that is remotely updated, self-managing, and supported by automated security and from third parties and OEMs, such as voyage planning, weather routing, navigation, fuel management, etc. On the other hand, the opportunities to ‘patch’ embedded OT safely are not frequent, and patches usually require certification by control system manufacturers.

The broader point, though, is that cyber security is not just about software patching and system configuration. Ship operators do not buy computer processors, disk storage, and software, and then build them into a system: they procure turnkey systems. Again, shipboard engineers may well be IT-literate, but no space has been made on the crew roster for cyber security specialists.

In these circumstances, the integrity of the systems on ships is best maintained by software which can identify, contain, and resolve threats wherever they appear in the network. Such Unified Threat Management (UTM) detects all deviations from the ‘known good’ configuration as anomalies and potential threats to security and can update securely, even during operation. Some specialised functions, such as an in-depth analysis of alerts or security forensics, will need to be delivered remotely.

Inmarsat believes that a collaborative approach – that includes shipboard systems as well as the crew operating them and the processes involved – is vital to develop the maturity response demanded by multiple threats from cyber villains, whatever their origin. For this reason, we have been working with some of the best security-focused experts available, to tailor products and services to meet the shipping industry’s requirements. Our work with Trustwave, a cyber security subsidiary of Singtel, for example, has brought Fleet Secure into the industry as the first independent service designed to detect vulnerabilities, provide alerts, respond to threats, and protect ships from cyber attacks. In fact, Fleet Secure is a UTM, available without additional outlay on hardware which also has no impact on contracted bandwidth. It can identify external attacks through high-speed broadband connectivity, including malware introduced accidentally to the ship’s local area network. It then isolates that part of the operating system infected to prevent wider disruption.

### What makes for good cyber security practice

However, software is only part of the answer: cyber security and vigilance for ‘the human element’ and a well-thought-out recovery strategy to mitigate against multiple, automated assaults are also critical. Process failures and mistakes made by people can present the security loophole that, if unchecked by the UTM, can compromise the entire network. Weaknesses in the first line of defence (to phishing, plugging in an infected USB, downloading from an unreliable source, etc.) are common, but in the case of satellite-connected ships, it is also common to see updates turned off and no antivirus software in operation. Today, cyber security training is not compulsory for the world’s 1.6m seafarers, while expertise in antivirus software is inevitably more likely to be based ashore.

As far as awareness is concerned, it is fair to say that there is likely to be more temptation to risk plugging in a memory stick that might be infected once a vessel is underway. Creating awareness for seafarers and staff is a continuous task because good cyber security practice is the shipping’s first line of defence against a cyber intrusion.

Inmarsat has recently participated in discussions with academics at the World Maritime University in Malmö over what future classroom-based and e-learning cyber security course content might include for Maritime Safety and Security Diploma students. While Inmarsat is not and does not aspire to be a training company, it is, nevertheless, an interested party that’s very much concerned with what’s happening in the cyber domain. As such, we are fully aware that training is not just a tick box exercise and must be backed up with monitoring and reinforcement. We also know that using tools to identify breaches of policies, such as USB usage, help reinforce the message: constant reminders and real-life examples are often the quickest ways to stop a bad practice.

But to address future cyber security risks effectively, we need the involvement of ship designers, builders, regulators, verifiers, equipment manufacturers, service providers, and, of course, owners and operators. We were, therefore, one of the founding partners in a Joint Working Group run by the International Association of Classification Societies (IACS) whose members survey and certificate more than 90% of the world’s commercial vessels, ensuring that ships are fit-for-purpose and comply with safety and quality regulations. The Working Group, which includes representatives from across the maritime sector, has developed a cyber security framework that is likely to form a basis for risk management that will contribute to future seafarer training requirements and the International Maritime Organization’s International Safety Management (ISM) Code, a standard for the safe operation of ships. A further outcome is likely to be a recommendation relating to how a cyber security module can be best integrated into standard seafarer training courses, probably as part of the Standards of Training, Certification and Watchkeeping (STCW) Code.

For its own part, Inmarsat does issue guidelines covering best practice, but it is also evolving capabilities that support greater cyber maturity in the seafaring community, most recently through Fleet Secure Endpoint and Fleet Secure Cyber Awareness. The first of these has been developed together with digital security specialist ESET and is powered by Port-IT to protect desktop computers and other devices connected to shipboard networks and has been available since the beginning of 2019. Fleet Secure Cyber Awareness, meanwhile, has been developed in collaboration with Stapleton International and the Marine Learning Alliance to help seafarers educate themselves on the possible tactics that cyber criminals can use to infiltrate a company’s IT infrastructure.

### Over the line

There is no doubt that digitalisation and new smart technologies are transforming ship operation at an exponential pace, but Inmarsat’s view is that to accelerate this transformation all stakeholders interested in optimising the efficiency of ships and crew welfare must exert themselves if the industry is to be carried over the line.

This means we must not only be training our seafarers more effectively, better managing our processes and protecting our systems but nurturing awareness of best cyber security practice, even on vessels that have little or no cyber security protection at all. Clearly, there is still a long way to go. ■

Photo: Pexels

Interview with Itai Sela, CEO, Naval Dome

# The cyber security seal

by **Przemysław Myszka**

Naval Dome is an Israel-based cyber security specialist providing security detection and protection solutions to the international maritime industry. The multi-award-winning Naval Dome solution is the first maritime multi-layer cyber defence solution for mission critical on-board systems. For more info, please visit https://navaldome.com

**One could almost perceive it as a miracle that the world continues to spin, following all the breaking news on cyber attack, scams, and scandals that cost the global economy billions of dollars each year. Coming increasingly more to the cyber limelight is the transport and logistics industry, until recently somewhat unmindful of the consequences of being too cyber-remiss. We're talking to Itai Sela, the man behind setting up Naval Dome, about the maritime industry's awareness of the threat, what's in the perpetrators' malicious toolbox, and what his company has in store to blunt the potential intrusion.**

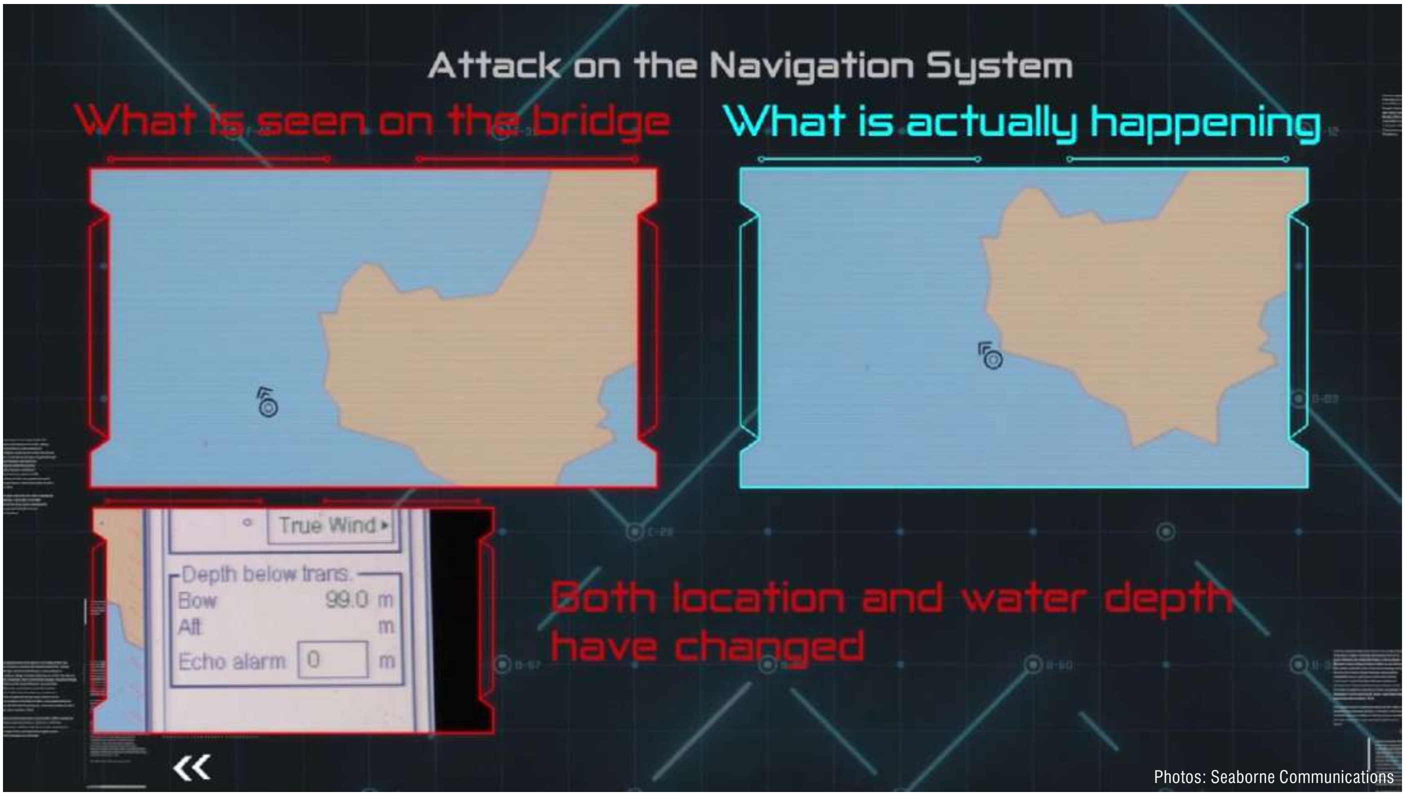
- **What's the company's story – why was it established and what are its main goals?**

I'm a former Israeli Navy officer. During my 25 years' service, I recognised a potential security blind spot in the maritime industry, believing if someone can breach a security facility eight floors underground, then it cannot be very difficult for someone to breach a vessel at sea. When I shared such thoughts with the commercial maritime industry, they initially resisted. "The vessel is like an island," they said. "No one can hack a ship!"

Despite that reaction, my team and I were undeterred and looked at developing the optimum maritime security solution, drafting in some of the brightest minds in naval intelligence and cyber security with whom we established Naval Dome. To show the industry the extent of the problem the Naval Dome team first carried out ethical cyber attacks on live navigation, engine, and other machinery control systems, succeeding in attacking different electronic systems from different manufacturers. The breach was carried out in the same way in which a hacker would operate. However, the difference was that the operators and system manufacturers knew of the "attack." Had an actual hacker carried out the same intrusion, they would have had no idea.

- **What's in the company's portfolio? Specifically, what is the multi-layer cyber defence solution for mission-critical on-board systems?**

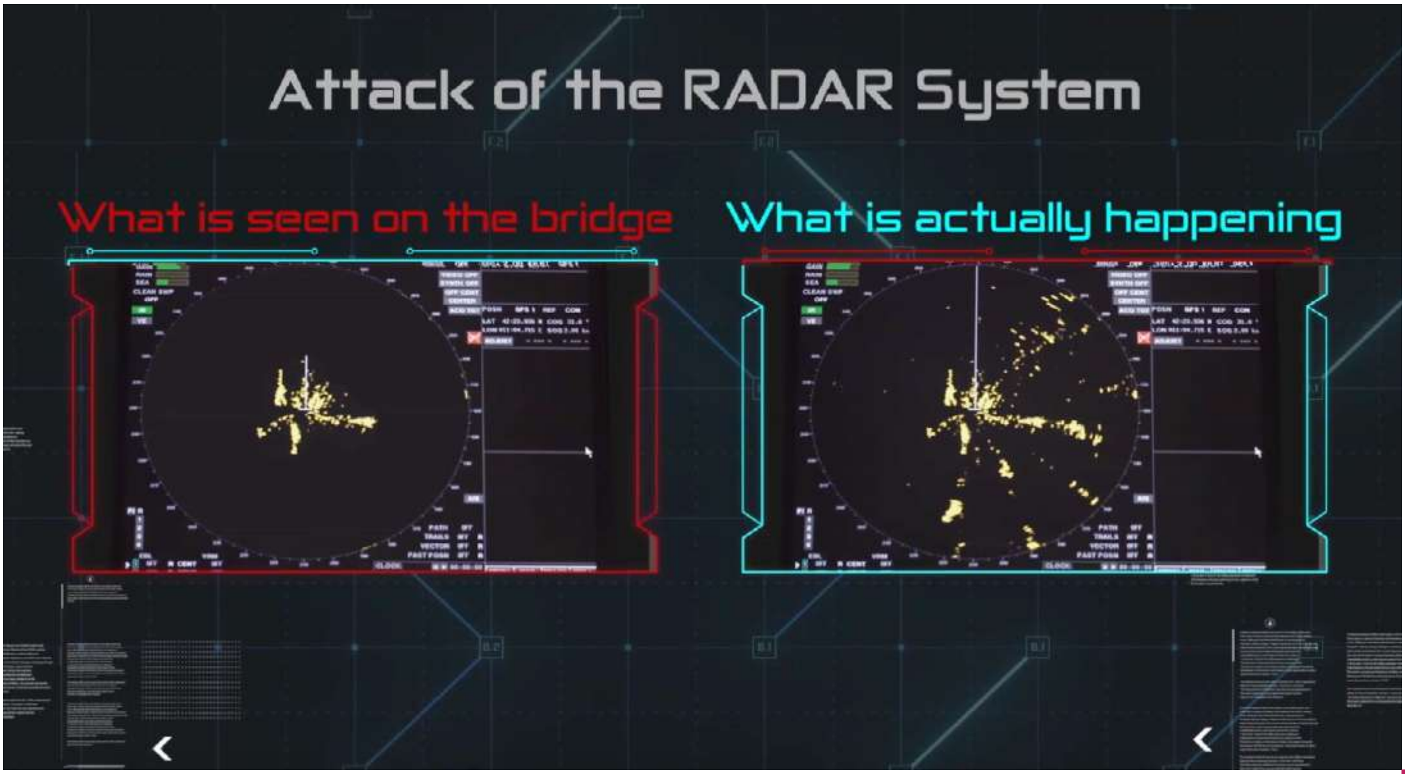
What Naval Dome discovered from these carefully managed attacks was that there wasn't just one blind spot,

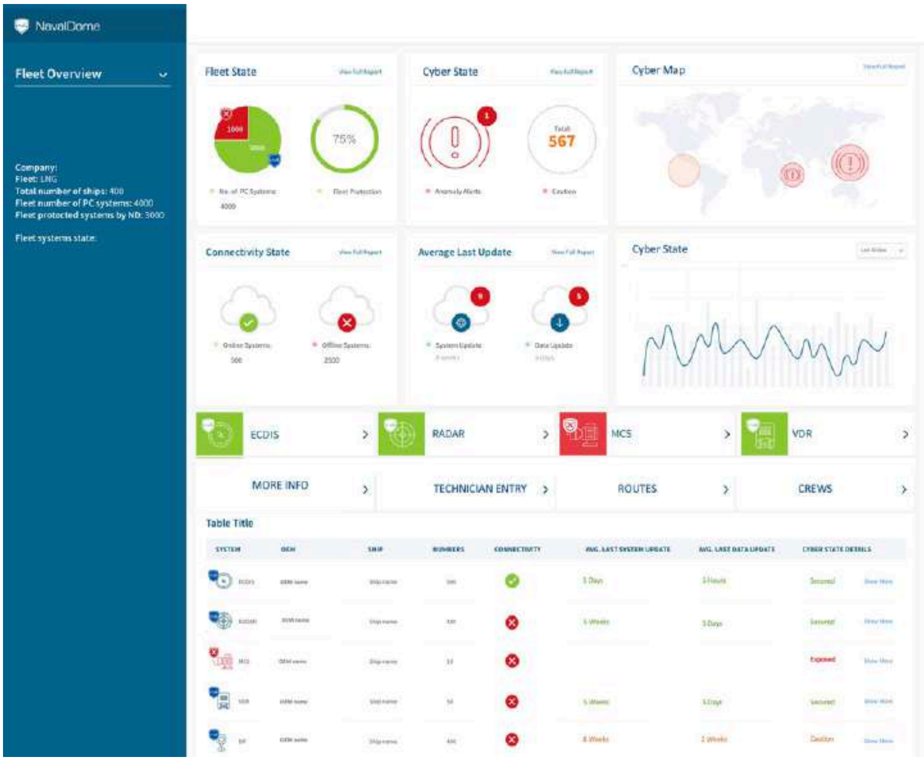

Attack on the Navigation System
What is seen on the bridge
What is actually happening
True Wind
Depth below trans.
Bow 99.0 m
Aft m
Echo alarm 0 m
Both location and water depth have changed

Photos: Seaborne Communications

there were many. A lot of the systems were unprotected. It was at this point that the team and I began developing the Naval Dome Endpoint solution to deliver the highest level of cyber security for all floating assets. Earlier this year, the company's Secure Endpoint product achieved the highest level of security certification/type approval, Security Level 4 (SL4), from the classification society DNV GL.The Naval Dome solution is a two-step, multi-layered cyber protection system. The first stage, the Secure Endpoint, prevents internal cyber attacks by replacing the on-board systems' hard disk with the Endpoint "hard disk." Once installed, the ship's system functions in the same way, but it's now secured to SL4 grade protection. It can work with different operating systems, including Windows and Linux.

The system also ensures ship operators can assess the security of all systems that have been installed with Endpoint. The Secure Naval Dome App and Dashboard indicated what systems are protected, those that have detected and protected against intrusion, and real-time


Attack of the RADAR System
What is seen on the bridge
What is actually happening



Company:
Fleet: LNG
Total number of ships: 400
Fleet number of PC systems: 4000
Fleet protected systems by ND: 3000

Fleet systems state:

Table Title

| SYSTEM | OEM | SHIP | NUMBERS | CONNECTIVITY | AVG. LAST SYSTEM UPDATE | AVG. LAST DATA UPDATE | CYBER STATE DETAILS |
|---|---|---|---|---|---|---|---|
| ECDIS | OEM name | Ship name | [illegible] | ✓ | 3 Days | 3 Hours | Secured Show More |
| RADAR | OEM name | Ship name | [illegible] | ✗ | 6 Weeks | 3 Days | Secured Show More |
| MCS | OEM name | Ship name | [illegible] | ✗ | | | Exposed Show More |
| VDR | OEM name | Ship name | [illegible] | ✗ | 5 Weeks | 3 Days | Secured Show More |
| [illegible] | OEM name | Ship name | [illegible] | ✗ | 8 Weeks | 2 Weeks | Caution Show More |

security monitoring/alerts for the ship and shore personnel.

The second aspect of the Naval Dome solution is the Secure Naval Dome Cloud. This protects all data delivered to and from the vessel and prevents external cyber attacks. What Naval Dome has done is integrate its own Secure Cloud with the customers' existing Cloud-based infrastructure so only the client's "cloud" is needed.

Today, I can proudly say Naval Dome is the leading supplier of multi-layered maritime cyber defence and analytical solutions. To date, we have secured the PC-based systems onboard a significant number of commercial vessels and super yachts. Naval Dome is working with leading original equipment manufacturers (OEMs) to help protect their systems in a way that it becomes an integral part of suppliers' existing and new software. The OEMs are now integrating the Naval Dome software with the systems to provide their customers with the utmost protection. This is much easier for end users as they only have one point of contact – the OEM – to provide all the service and support. In recognition of our works, we've won several industry awards, including the Marine Propulsion Marine Intelligence Award 2018, Lloyd's List Cyber Security Innovation Award 2018, and the Seatrade Cyber Security Award 2018.

### ■ What do cyber criminals have in store to target the shipping and port industries?

Typically, cyber criminals will use malware or ransomware-type viruses capable of infecting complete ship networks, and operators will be unaware until the virus has been activated. This is because many of the systems are based on old operating systems and designed and manufactured without considering the cyber risk.

There are two main threats: untargeted and targeted attacks. The former is when someone attacks several companies at once, and the virus spreads until it finds an unsecured network. The latter, in turn, is when specific companies or industry sectors are infected directly.

An attack can be successful when operators make a mistake and inadvertently upload an infected file, e.g., by opening an email or connecting an infected file. This creates connectivity. The second way is when an OEM or technician is attacked, and the infected files are inadvertently spread during system updates or servicing. The second method is more effective in spreading a virus.

### ■ How the shipping industry reacts to (cyber) security threats?

Unfortunately, the industry has been slow to react, relying mostly on operator training as a precautionary measure. However, reliance on the human factor in the cyber protection cycle is not the answer.

There is also limited control over the vendor's maintenance, updates, and test equipment which could, if they aren't properly protected, inadvertently infect the network. Typically, most networks are not segmented, so if an attack has been detected in one area of the network, it usually means the entire system is infected.

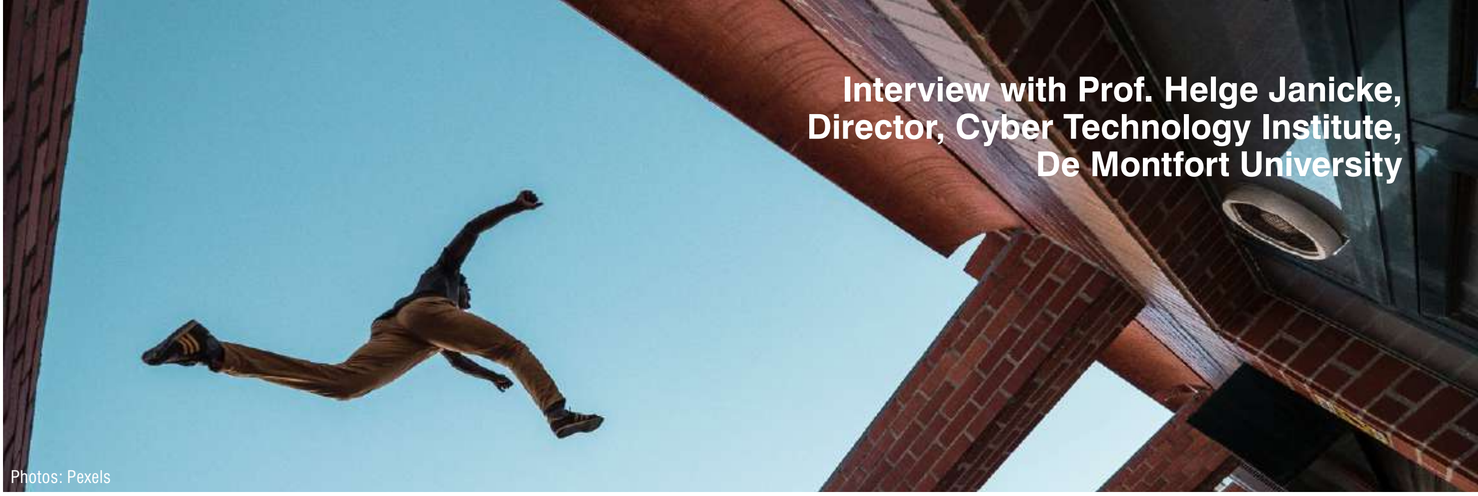
Another aspect that impacts the security of ship systems is that there are no mandatory requirements, only guidelines. There should be binding instructions.

### ■ What's the company's take on the so-called cyber clause introduced by BIMCO? The clause will require, "[…] the parties to have plans and procedures in place to protect their computer systems and data, and to be able to respond quickly and efficiently to a cyber incident."

The BIMCO cyber clause is very much a move in the right direction, but this does need to be adopted widely. Maritime insurance companies also need to develop consistent and comprehensive maritime cyber insurance policies and remove the CL380, the clause that removes any insurance relating to computer-based problems. Every ship system should be protected to SL4 as well as implement the BIMCO guidelines. Ship operators should also segregate their operational (OT) and information technology (IT) networks. The problem is that these are often connected. There is no real network segmentation. This is very important.

### ■ What's the company's outlook about how the shipping business will tackle the cyber threat in the near future?

We encourage more and more OEMs to integrate the Naval Dome solution with their systems and equipment prior to delivery to their customers. This way, both the OEM and the end user are confident that their systems are protected at the highest level from the outset. This also means that the end user no longer has to worry about cyber protection as the OEM provides the requisite services and upgrades that are protected by Naval Dome. In the future, all equipment could have the Naval Dome "seal of security," to show that such and such equipment is "Protected by Naval Dome."



Interview with Prof. Helge Janicke,
Director, Cyber Technology Institute,
De Montfort University

Photos: Pexels

# The need to create a culture of agile incident response in Industrial Control Systems

by **Alice Clochet**, *Content Manager, Defence IQ*

**With the digitisation of networks comes the risk for Industrial Control Systems (ICS) to be cyber attacked, creating the need for all stakeholders involved to take measures and avoid any damages made on their business. Ahead of Defence IQ's ICS Cyber Security conference taking place 29 April-1 May in London, Professor Helge Janicke, Director of the Cyber Technology Institute at De Montfort University, shares his insights on agile incident response in ICS. He discusses here risk management of Supervisory Control and Data Acquisition (SCADA) systems, the effectiveness of the current ICS instant response capability, and what the key elements are to secure the digitised network connected to ICS.**

ICS
CYBER SECURITY

Preparing your industrial control systems for the new phase of cyber security. As the most established Industrial Control Systems (ICS) Cyber Security Event in Europe, the ICS cyber security conference brings together leading practitioners, operators, and decision makers from across Europe to share a wealth of practical experience in implementing cyber security in organisations, and best practice on defending against cyber security risk to ICS. Attend the event to understand how leading organisations are operating in the post-NIS implementation phase (the EU directive on security of network and information systems), assessing new threats to IP and data theft, and maintaining an effective secure network against cyber threats. Use the event to understand how industries are engaging with cyber risk internally and externally, and expanding their cyber security capabilities against the total cyber threatscape. For more info, please visit www.defenceiq.com/events-icscybersecurity

- **SCADA systems are widely used by a vast array of organisations from sectors such as energy, oil and gas, power, transportation, etc. How can they best manage the risks associated with a digitised real-time data analysing system and thus avoid any malicious intrusion?**

This question is a little complex. Obviously, SCADA systems are widely deployed in almost our entire critical national infrastructure (CNI). How you best manage the risk is a very good question because we are all collectively still trying to find the answer to it.

One of the key starting points is making sure that we are actively looking at the risks because traditionally these infrastructures were disconnected from the network, and nowadays they are popping up everywhere. They are connected to business systems through the regular IT side of an enterprise, for purposes such as real-time monitoring, monitoring throughput, power production and logistics – logistics systems today are deeply integrated into the control systems that underpin them.

In terms of risk management, understanding what the links are and having architect solutions that pay attention to cyber risk is crucial, especially when we build new installations. Segregating the data flows in there is also important, to make sure that not a single component is accessible from everywhere, and used by an attacker to pivot through the system. I think controlled flows and the use of data diodes for example, to ensure that the flow of information is unidirectional to some parts of the system through that network, are very good practices to manage and deal with some of the risks.

However, many of the risks come from widely different fronts. If you look at the supply chain surrounding the building of these SCADA systems, you can find there are a lot of suppliers working in concert in a production plant. This creates issues because the integration of all of these at the interface level might not go as smoothly as it should.

Any system is only as secure as its weakest link, so there is a reliance on the security of your supply chain. If we look at the European NIS directive (on the security of network and information systems), it is important for operators of essential services to focus on their supply chain because they have, at least in the UK, the responsibility to ensure that adequate protection of their supply chain is being implemented and that suppliers are applying the same rigorous levels of security and risk management.

■ **Operators of essential services are responsible for making sure their suppliers are secure, but are they currently doing this? Are they aware of their need to do this?**

That depends on the sector you are talking about, as some sectors are significantly better in managing their supply chains than others. In the energy sector, there is a detailed logging of the supply chain, what is being used and what is being implemented; aircraft manufacturers have a very detailed trace of where the parts come from and when there were manufactured.

■ **On a range of one to ten, how would you rate the current ICS instant response capability?**

Again, this depends a lot on the sector. The more critical the sector is, the higher the number would be; the broad stroke, however, is possibly somewhere around two or three on this scale.

There is a lot of work to do, especially when it comes to small manufacturing plants that have sometimes zero cyber security and no awareness of cyber security. Machines can be 20 years old and in this type of setting there is very little response capability on the cyber part, even though they are effective in the incident response mechanisms on the safety part. I believe that the operation technology (OT) side needs a lot of development; we come much further with IT incident response, where the issues are much better understood than in the operations technology side.

■ **Is there a push from CNI organisations to work with industry in order to build agility in incident management solutions? If not, where does the push to become more agile come from?**

This question links very nicely to the current project we are running, about agile incident response and industrial control systems. So far the push really comes from the realisation that incident response is taking place quite often in isolation of A) the business, and B) the ICS context, with the engineers and the operators of these technologies. You often find that the security operations centre and the incident response management teams are IT-focused and do not understand or cannot operate OT.

While there are things that these stakeholders can afford to lose, others are absolutely critical and must be maintained. Bringing teams together to know which ones are which and to share this knowledge is particularly relevant in case of a response to an incident, as it will enable them to make the right decision quickly in a stressful situation; it is less relevant in the preparation and post-incident phases, as it is all about limiting damages. The real trick in ICS is not to make matters worse when responding to an incident.

■ **What do you believe to be key in securing the digitised network connected to ICS? What about in ensuring an effective incident response?**

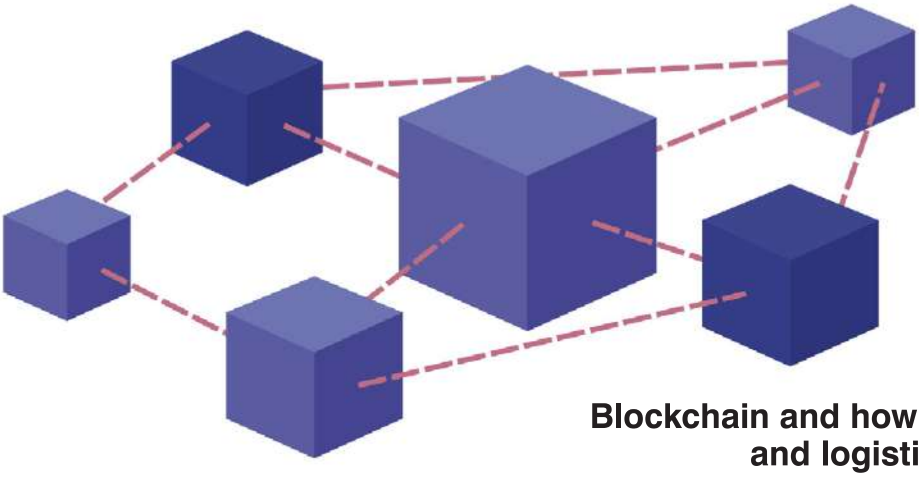
The key in securing the digitised network is the attitude towards ICS because often these are built for a single purpose and a production line is being set up for them. Currently, we find it very difficult to patch ICS; we can patch them, but the process invalidates some of the safety certification that these plants have undergone, so this is a big additional cost that we don't manage effectively at this point. Changing a software configuration in the digitised network might invalidate the safety case established in a plant. Making any changes requires a complete recertification of the plant and there are very few people who can do that. That loss of regularity is financially not viable to run, so we need to look at some different ways to maintain and secure the systems that have the benefits of being connected, but not falling foul of the operating nature of these control systems.

I very strongly believe that an effective incident response is only possible if you understand your systems and know what assets you have deployed, what configurations are running, what kind of patch levels have already been applied throughout the system, to be effective in managing it; it is not necessarily the case in all incidents at the moment.

Moreover, you need to have the right stakeholders on board and the management buy-in, to deal with an incident effectively and quickly move and respond. You also need to get access to the right people such as engineers and business people, and bring them together in a value-focused approach to responding to an incident. I believe this is the key for the future.

■ **Do you believe there is enough management buy-in now, in order to achieve this?**

Currently, there is significant awareness among managers that cyber security is an issue and the question is to make it an internal business case. To a large extent and in the finance sector for example, because it is too expensive to proactively put controls into place, people just accept the risks associated with having less controls. There are some protections, but there is also the ability for them to pay up for any mistakes that are happening. The key element here is to have management buy-in to change the organisational culture effectively, all the way down to the employees who are operating these systems. This can happen through rigorous security awareness programmes and putting the right architectural solutions and infrastructure in place when the plants are built or refurbished; this will help to anticipate incidents and be able to segregate attacked networks or production lines, to avoid the spread of an attack.



Blockchain and how it can make transport and logistics more cyber secure

# The trust factor and human error in supply chain security

by **Marcin Lewicki**, *CEO & Founder, Sternkraft*

**The global supply chain network is a system of self-existing individuals connected to each other in an undefined way. Information goes from one organization to another according to rules that aren't specified globally. In most of the cases, two cooperating organizations have their individual methods of exchanging information – analogue, like paper invoices or certificates, or digital such as the state and the position of the transported cargo. Sometimes organizations agree to use the same processes, procedures, and tools to exchange data. This, however, doesn't mean they all have the same internal rules. These companies store our data, so it's crucial for us to know if our partner has put in place the proper internal rules and processes thanks to which the data infrastructure is safe. The question arises: can we take the human factor out of the 'trust equation'?**

STERNKRAFT TELEMATICS

the business of transport and logistics suffers from growing numbers of threats like cargo and fuel theft or burglary. This has led the Berlin-headquartered Sternkraft to develop Safeway, an advanced cargo security system that combines hardware with the latest technology. For more info, please click www.sternkraft.com/en

We all know that one thing is to gain a certificate, but actually sticking to the rules is another pair of shoes altogether. The latter is undermined by factors such as trust and human error. Is working with Maersk a safe option? It should be. Why? Because the Light Blue means something in the industry. I know I can trust them.

### One hard drive to save them all

Yet, I'd be very surprised back on 27 June 2017. Such a respectful and well-certificated corporation, with a lot of great minds on-board, was hacked by a piece of malware that wasn't even targeted at Maersk in the first place! The fallout was nothing short of epic – no more no less, but the giant went analogue for two whole weeks. Conclusion? One cannot simply take trust on, well, trust.

It's hard to say what was Maersk's main shortcoming back two years ago. Surely they weren't prepared for what happened. What we know now, though, is that the whole company was using systems that weren't upgraded with the latest patches while passwords were of really low complexity. End result? One small NonPetya malware destroyed the entire infrastructure. Like in an action movie, Maersk survived because they were able to retrieve the single last copy of their system that wasn't hijacked – in Ghana. For comparison, all – all! – of their 150 domain controller backups were down. At that time, it was the most important hard drive disc for the entire container shipping industry. Mission – get to Ghana and bring that HDD to England. One existing backup server rescued the whole 45,000 computers and 4,000 servers-big company.

Photo: Sternkraft

So, even if I had trusted Maersk – the incident would affect me. Making simple Windows updates and having to go through two-factor authentication on each and every computer – this would have saved Maersk $300m that summer. But it isn't that the Danish conglomerate is the only whipping boy; other heavyweight players also lost millions because of the NotPetya attack. Merck admitted to their shareholders they lost $870m because of shutting down the ability to manufacture drugs. The French Saint-Gobain, which delivers construction and high-performance materials, saw $400m going down the pipe; FedEx – $400m; Mondelēz, the manufacturer of i.a. Cadbury chocolates – $188m; Reckitt Benckiser, the British producer of Durex condoms – $129m; and so on and so forth.

**One, big, decentralized, yet shared by everyone shipment registry**

What if we could grasp human trust with a mathematical formula? Imagine a situation where you know exactly where your shipment is; what is the temperature inside the container; whether somebody has tampered with the seals; opened the doors; or even stolen the entire unit. Carriers, suppliers, intermediaries, insurers, regulators are involved in the supply chain, meaning there's plenty of room where communication, data transparency, and safety can be compromised.

SAP, Oracle, Salesforce – they all work on cloud-based solutions to improve freight and order management, transportation planning, costs, reporting, and analytics. What if we could use one big database to identify and track each cargo globally? What if we could allow access to this database to everyone and, while using it according to the rules, change the registry of each transport in time? What if we create one, big registry of shipments, totally inaccessible for unauthorised parties?

The so-called Distributed Ledger Technology (DLT) – better known as blockchain – provides such a global format. It's interoperable, immutable, and secure. It's a data standard that's accessible by authorized parties and cannot be changed. Each transport's ledger is shared by many, delivering a decentralized database that's synchronized by each member. Blockchain cryptography and smart contracts make rules visible to everyone and used by everyone, but data are only accessed by those who own a "password." Such a database and interface layer allows connecting any end-user application to it. Decentralization, which stands for immutability and having a synchronization backup strategy, helps to secure the data. The role model to follow is Samsung SDS, a member of the Transported Asset Protection Association, and its ongoing project with the Port of Rotterdam and ABN Amro Bank. "Our blockchain based project is the answer to the cyber security of our times. It will secure and improve freight processes like nothing before," says Jacques De Smit, Regional Logistics Director, Samsung SDS.

**Secure the future**

In Sternkraft's Internet of Things project called Safeway, a test DLT solution, is being implemented. Safeway is a solution that combines hard- and software and allows monitoring goods in both curtainsider and semi-trailers, and doing it in- and externally. All algorithms implemented in our cameras help to prevent thefts. The alarm is activated whenever something strange is happening, e.g., someone is next to the cargo and behaves suspiciously, or the temperature inside the unit changes rapidly. BinarApps creates a management system for logistics to monitor transport and generate an alert if any unwanted situation occurs. Each transport ID number with its attached documentation will be stored in a partially public DLT database. Each of the Safeway's users will be the owner of at least one copy of the database node. Nodes are synchronised and, thanks to cryptography, 100% valid. This way they'll participate in creating a decentralized copy of what could be called the data centre's heart.

Maersk is probably well-secured by now. The management board took up the challenge and started to treat cyber security seriously. Meanwhile, blue chip companies need to take on the responsibility to not only secure the present, but also the future. There's a way of feeling more cyber comfortable, as long as it's called blockchain. ■

Should I or my company be concerned?
No. You should be terrified

Photo: Wikimedia Commons

# Cybercrime

by **Julian Clark**, *Global Head of Shipping, Hill Dickinson LLP*

**In May last year, Liam Fox, the International Trade Secretary, announced that the UK government would be investing £1.9 billion of transformational investment to support the country's strategy of becoming secure and resilient to a cyber-threat by 2021. Describing the scale and speed of the technological revolution as a "Pandora's Box," he said, "It is the responsibility of government to lead the field in our global cyber security standards and to promote the UK's world-leading expertise and strengthen capabilities in the UK and allied countries." It has been estimated that the global cost of cybercrime will reach $2 trillion by the end of this year, with a 2017 report estimating that a five-day loss of the Global Navigation Satellite System would cost the UK in excess of £149 million.**

HILL DICKINSON

hill Dickinson is a Liverpool-headquartered international commercial law firm with more than 850 people, incl. 175 partners and legal directors. From its offices in the UK, mainland Europe, and Asia, the company delivers advice and strategic guidance spanning the full legal spectrum. Hill Dickinson's clients include, among many, multinationals and major corporations, insurance companies, British and foreign banks and financial institutions, public sector organisations, private individuals and professional bodies. For more details please click www.hilldickinson.com

as one of the world's leading maritime legal and emergency disaster response operations, with an in-house team of nine ex-mariners (all either legally qualified or in the process of legal qualification), we are frequently on board vessels investigating a range of incidents, not all necessarily cyber-related. However, our mariners report to us that they are constantly discovering breaches of shipboard cyber security, illegal downloads, malware and absence of security protocols and procedures – all of which could seriously compromise a vessel's seaworthiness.

**Seaworthiness in the digital age**

Despite the high-profile nature of recent incidents involving key market players such as Maersk and COSCO, it seems that the maritime community stakeholders are still, in certain quarters, burying their heads in the sand saying that these stories are either "fake news" or one-off incidents. In reality, what we read about in the press is the tip of the iceberg. Indeed, so significant is the risk that in July 2018 NATO issued requests for reports of instances of GPS or AIS interference in the Mediterranean, noting that in the past few months several electronic interferences had been detected.

In the maritime context, we have yet to see a case based upon a vessel's unseaworthiness due to a cyber issue. This absence must, however, only be a matter of time. Let us then test that hypothesis. The following three are central tenets of the traditional concept of seaworthiness of the vessel. First, a ship is seaworthy if she has that degree of fitness which an ordinary careful owner would require his vessel to have at the commencement of her voyage, regarding all its probable challenges.

Photo: Pixabay

Second, a vessel's seaworthiness extends beyond its physical fitness for the relevant voyage, requiring the vessel to have sufficient, efficient and competent crew, as well as adequate and satisfactory systems on board to address matters that might be encountered during the voyage.

Finally, whether a vessel is seaworthy should be considered in reference to the state of knowledge in the industry at the time.

**When SOLAS compliance is not enough**

In the context of the threat of cybercrime in shipping, it will become increasingly difficult for shipowners to argue successfully that the state of knowledge in the industry permits them to do nothing to address the potential of a cyber attack. A wide range of publications and guidelines from all the major shipping operations, organisations and underwriters has now highlighted this risk to a sufficient degree that preventative action should be taken. The implementation of proper cyber risk management systems and protocols (both on- and offshore) go directly to the requirement of having adequate and satisfactory systems on board as well as sufficient, efficient, and adequately trained crew.

This type of risk of the vessel being found to be unseaworthy has severe consequences, not only in the potential loss of the right to deploy the defences currently found within the Hague Visby Rules but also in the possible loss of a right to limit liability. Article IV of the 1976 Limitation of Liability Convention provides that, "a person liable shall not be entitled to limit his liability if it is proved that the loss resulted from his personal act or omission, committed with the intent to cause such loss, or recklessly and with knowledge that such loss would probably result." One may say that it is unlikely that a cyber attack would be committed with intent to cause a loss, unless of course in the context of a "modern-day scuttling case." But the real issue here is the application of "recklessly." In circumstances where a vessel owner has allowed his vessel to proceed to sea without adequately training the crew, without having implemented a cyber risk protocol and regular drills, with out of date firewalls and inadequate protections, there must be scope to argue recklessness.

In the Hague Visby Rule context and the possibility of losing the right to deploy the standard defences, one needs only consider how that right was lost in the case of the car carrier *Eurasian Dream*. If one takes the factors listed by the court as to why the owner was unable to rely upon the defences in that case and apply them to a cyber context, the result becomes obvious. The factors identified were the inexperience of the master, lack of training in relation to the risk for the type of vessel concerned, an ineffective regime of training and drills, a basic handover and general induction, and absence of vessel-specific procedures. Simply having manuals on board and compliance with the International Convention for the Safety of Life at Sea (SOLAS) was not enough. As lawyers often say – the facts speak for themselves.

**Are you a soft target?**

No longer just concerned but now terrified? What do you need to do? The maritime sector is increasingly looking like a soft target. Examination of traffic on the so-called dark web shows that a number of factions are now starting to target the maritime field.

In response, we need to implement threat modelling for ships, undergo regular penetration testing and introduce monitoring systems and information sharing between all actors in the maritime community in order to exchange experience of cyber vulnerabilities. In short, we need to ensure that all maritime organisations have an up-to-date and thorough cyber response plan and adequate training, not only for their crews but also their shore-based personnel. Shipping corporations need to work in close cooperation with the experts in the field – legal, risk avoidance and technological – to develop and implement effective systems and know how to deal with the attack when it comes. In other words, it's about adopting the mantra from the original song *Ghostbusters*, "Who you gonna call?" ■

# What's next

## TOC Europe 2019

## Modern ports, shipping, and logistics

## China-Europe transport & logistics

# partnership events

**AntwerpXL**
*7-9 May 2019*
*BE/Antwerp*

**Unmanned Maritime Systems Technology**
*8-9 May 2019*
*UK/London*

**Posidonia Sea Tourism Forum 2019**
*28-29 May 2019*
*GR/Athens*

**transport logistic**
*4-7 June 2019*
*DE/München*

**Nor-Shipping Conference**
*04-07 June 2019*
*NO/Oslo*

**European Environmental Ports Conference 2019**
*12-13 June 2019*
*BE/Antwerp*

**Multimodal 2019**
*18-20 June 2019*
*UK/Birmingham*

**Mediterranean Ports and Shipping**
*25-27 June 2019*
*MA/Casablanca*

**SIL Barcelona**
*26-28 June 2019*
*ES/Barcelona*

▪ **PUBLISHER ▪ Baltic Press Ltd** ▪
▪ ul. Pułaskiego 8 ▪ 81-368 Gdynia ▪ Poland ▪ tel.: +48 58 627 23 21/95 ▪
▪ editorial@baltic-press.com ▪ **www.harboursreview.com** ▪

▪ *President of the board:*
Bogdan Ołdakowski

▪ *Board Members:*
Ewa Urbaś, Alan Arent

▪ *Managing Director:*
Przemysław Opłocki ▪ po@baltic-press.com

▪ **EDITORIAL TEAM** ▪
▪ *Editor-in-Chief:* Przemysław Myszka ▪ przemek@baltic-press.com
▪ *Assistant Editor:* Agnieszka Pacholczyk ▪ agnes@baltic-press.com
▪ *Proofreading Editor:* Ewa Kochańska
▪ *Art Director/DTP:* Danuta Sawicka

▪ **MARKETING & SALES** ▪
**(advertising, exhibitions & conferences)**
▪ *Marketing and Sales, Marketing & Communications Specialist:*
Krystian Wasielke-Wit ▪ krystian@baltic-press.com

▪ *Subscriptions:* www.harboursreview.com ▪

*If you wish to share your feedback or have information for us,*
*do not hesitate to contact us at: editorial@baltic-press.com*

We invite you to cooperate with us!
If you wish to comment on any key port issue, share your feedback or have information for us, do not hesitate to contact us at:
**editorial@baltic-press.com**
**+48 58 627 23 21**

**To join our 15,000+ maritime transport sector users society click HERE**

# previous editions

**HR#23** FUELS

**HR#24** OFFSHORE WIND INDUSTRY

**HR#25** PORT EQUIPMENT