SUBSCRIBE: www.harboursreview.com

no. 1/2020 (31) april

Harbours review

ISSN 2449-6022

Cyber--security

Photo: Pete Linforth/Pixabay

Experience the progress.

Mobile Harbour Crane & Reachstacker

- Advanced container handling equipment for increased productivity and safety
- Reachstacker: Up to 40% less fuel consumption than market average
- Mobile Harbour Crane: 360° mobility – outstanding in the MHC market
- Stepless hydrostatic power transmission for smooth and sensitive operation
- Proven Liebherr quality & full access to the Liebherr global service-network

maritime.cranes@liebherr.com
facebook.com/LiebherrMaritime
www.liebherr.com

LIEBHERR

red-hot port matters

Photo: All-free-download

Maritime incumbents partnered with start-ups

Rainmaking, a corporate innovation and venture development firm, has matched **Cargotec**, **HHLA**, **Inmarsat**, **Shell**, and **Wärtsilä** with a total of eight start-ups through its Trade & Transport Impact Programme. Start-ups in this round of the Programme – **Bigyellowfish**, **CyberOwl**, **i4sea**, **Jujotech**, **KoiReader Technologies**, **Scoutbase**, **Signol**, and **Teqplay** – specialise in port- and cyber-security, energy-optimisation, and crew welfare. The parties will now work on 13 separate projects related to safety, security and crew welfare, optimisation of port and vessel operations, and autonomous operations and equipment. The third cycle of the Programme begins in Q1 2020, at which point more organisations will be able to join. At the same time, Rainmaking is also launching a decarbonisation programme in Singapore, which specifically focuses on start-ups with solutions that support the transition to a zero-carbon future for shipping. "There is growing recognition that the maritime industry needs to innovate and fast. As appetite for fresh thinking, insight, and technology swells, bringing together established maritime leaders with technology start-ups is what's needed to deliver genuine business results quickly," **Nicklas Viby Fursund**, Partner, Rainmaking, commented. **Clara Wahnich**, Digital Innovation Partnerships Lead, Inmarsat, also said, "The Trade and Transport Impact Programme made a big difference to us because it pushed people to act. Both Inmarsat and CyberOwl felt compelled to ensure that something happened within the initial six weeks, and this allowed us to validate the opportunity. We have now built a great foundation for our engagement and joint exploration going forward." **Michael Andronicou**, Project Lead – New Marine Ventures, Shell, said, "We have had great success working with Scoutbase, whose technology collects data to reduce human error. Our business has been hugely engaged – everyone is really keen and loves the energy that Scoutbase has brought to the table, as well as the product itself. Going forward in 2020, we are really excited to hopefully start rolling this product out." **Tero Hottinen**, Director for Emerging Digital Business, Cargotec, shared his company's experiences, "The Trade and Transport Impact Programme provides an excellent framework to explore collaborations with start-ups – not only for scouting and finding the good ones but also to encourage impetus and progress within a certain timeframe. We are working with two different companies that have truly complementary offerings to ours. We probably wouldn't have trialled both at the same time in a synergistic manner without Rainmaking, so it really has been beneficial from that perspective." While **Till Schlumberger**, Strategy Consultant in Digital Transformation, highlighted HHLA's, "We're working with KoiReader to make improvements in the detection of container damage. While it's currently a proof of concept, we hope to continue with the project and without Rainmaking's Trade and Transport Impact Programme, we probably would never have met KoiReader." Last but not least, **Steffen Knodt**, Director New Ventures, Wärtsilä, said, "Energy efficiency is one of the most important factors in shipping today, and we are trying to find new ways of improving it. Signol has enabled us to reach the decision-makers on-board and better support them with fuel consumption, energy efficiency and operations. We need to bring in start-ups and knowledge from outside the industry to support us in finding ways to do things better. And Rainmaking is helping us to do just that."

New Liebherr equipment lands in China

The LH 150 ET Gantry Port Litonic, world's largest electrically operated port handling machine with gantry undercarriage is also the company's first-ever produced of this scale. It was handed over and commissioned in **DaFeng Port** in the Chinese province of Jiangsu. All components were developed, produced, and tested by **Liebherr**, from the attachments to the work equipment, the hydraulic cab elevation and uppercarriage, as well as the rail-mounted portal of the enormous machine. The giant, weighing approx. 200 tonnes, is fitted with Liebherr's standard ERC system in addition to the engine power and can also store energy when lowering equipment available. This allows the machine to achieve an output of up to 614 kW at a 30% energy saving rate. An integrated high-voltage transformer reduces the 10kV supply voltage of the local mains network to 400V which is then used to operate the 400kW electric main drive. Due to off-centre positioning of the uppercarriage, the LH 150 ET Gantry Port Litronic can cover the entire working area of a 10k tonne timber-handling ship and over 70% of a 30k tonne counterpart of such vessel with its 16.5m-long angled boom, and 15m-long straight stick. Operator's cab is freely positionable and fitted with a hydraulic quick coupler system, allowing to change the mechanically operated attachments from within. The colossus follows two Liebherr A 934 C material handling machines and will improve the efficiency of large-scale timber handling operations at DaFeng. **Lin Feng**, Vice General Manager, DaFeng Port, said, "The LH 150 ET Gantry Port Litronic is 2.5 times more productive than jib cranes for unloading wood. This shortens the waiting times of the ships and significantly reduces the cost of unloading the timber per tonne […]."

Green energy coming to Oostende

Port of Oostende, **DEME Concessions** and **PMV** partnered up to construct an operational plant for green hydrogen production by 2025. The end product, **HYPORT Oostende**, will serve as an energy source for electricity, transport, heat and fuel purposes, as well as raw material for industrial needs. Phase one will encompass general feasibility analysis and the creation of a development plan, followed by a demonstration project with mobile shore-based power and an electrolyser of approx. 50 MW. A large-scale, shore-based power project, running on hydrogen, is planned to go live by 2022. Completion of a commercial green hydrogen plant, planned in the context of new offshore wind concessions, should happen by the end of 2025. By the end of 2020, 399 wind turbines will be operating off the Belgian coast with a combined installed capacity of 2.26 GW. The new marine spatial plan leaves space for several hundred more wind turbines, which will generate around an extra 1.75 GW. That makes a total green energy generating capacity of around 4 GW, supplying half of the Belgian households with electricity. However, the wind turbines' production peaks rarely coincide with consumer demand peaks, meaning that there is an opportunity to compensate for the discontinuity between production and consumption. If hydrogen is produced with electricity by means of electrolysis, no CO2 is released in the process. However, the hydrogen produced can only be called green if the electricity used in the process has also been generated in a green fashion. The term 'green hydrogen' is thus used when green electricity is available that converts water into hydrogen via electrolysis. The plant will ultimately deliver a CO2 reduction of around 500k to 1m tonnes per year. Port of Oostende is expanding its activities in the Blue Economy with this area-specific development. The planned location is in the Plassendale 1 port area. Financing intricacies will be taken care of by PMV, who see great potential for the energy source. The necessary experience package is rounded up by DEME.

APM Terminals presents Poti expansion project

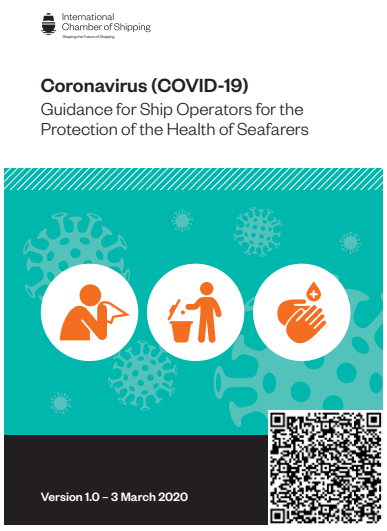
The operator unveiled its plans for the creation of a deep-water port to the Georgian government. An investment of over $250m in private capital for phase 1 and a similarly substantial amount for phase 2 is required for Poti's infrastructure and superstructure development. A 300m container quay, equipped with three STS cranes will be constructed during the second stage of the project, doubling the port's annual container capacity, bringing it up to 1m TEU. The whole project's timeline is estimated at 24-30 months. Close cooperation with the Georgian government will be necessary in order to keep the deadlines, due to numerous permits that need to be granted. **Keld Christensen**, Managing Director, **APM Terminals Poti**, commented on working with the Georgian officials, "We are confident in the Government's support and will continue our effort and cooperation with the authorities to make sure Poti Sea Port Corporation remains the main gateway to the Caucasus and beyond."

COVID-19: Port of Algeciras remains open for business

According to the Spanish Port's Authority, all operations commence as normal, and both container terminals – **APM Terminals Algeciras** and **TTI Algericas** – are fully operational. Connections to the **Ports of Ceuta** and **TangerMed** are live, although passenger traffic between Algeciras and TangerMed has been suspended until further notice. All traffic between **Tarifa Port** and **Tangerville Port** has been suspended as well. The Border Inspection Point (PIF) is fully operational. All incoming ships must submit, as has always been the case, the Maritime Declaration of Health (MDH) 24h before calling at the port, in which the ship's master must declare whether there is any illness or suspected illness on board, together with a list of the last ten ports called at.

ICS issues new Coronovirus guidance

The 22-page document produced by the International **Chamber of Shipping** (ICS), in collaboration with the **World Health Organization** (WHO), the **International Maritime Organization** (IMO), the **European Centre for Disease Prevention and Control** (ECDC), and the **International Maritime Health Association** (IMHA), aims to help the shipping industry combat the spread of COVID-19. Included in the guidance are advice on managing Port Entry Restrictions and practical protective measures against COVID-19 for seafarers, as well as an outbreak management plan. It also provides information on pre-boarding screening, education, and suggested responses when faced with suspected cases of infection. More basic advice on hygiene measures, managing high-risk exposure, case handling, isolation and cleaning, disinfection and waste management is also a part of the document. **Guy Platten**, Secretary-General, ICS, offered the following comment on the current situation related to the outbreak of the virus, "With no vaccine currently available to tackle the Coronavirus, all industries and governments must take appropriate steps to contain the spread. Shipping is responsible for 90% of global trade and recognises its responsibility in helping tackle this global health issue whilst ensuring that the wheels of global trade continue to turn. This document is the result of careful and considered collaboration with international partners. It is intended to be comprehensive but also easy to understand and implement. Providing shipowners and operators who are dealing with the sharp end of the crisis with the reassurance and guidance needed to continue to carry out their operations." The information included in the guidance is viable for all types of vessels which operate in international waters. The document can be downloaded directly from the ICS website.



Capbreton goes green

The popular holiday destination on the Atlantic coast of France saw its first all-electric passenger ferry go into service in July 2019, replacing an older diesel-burning vessel. The 35-passenger aluminium vessel, called *e-Boucarot*, is powered by an integrated electric propulsion system developed by **Torqeedo**. It consists of two 10 kW electric outboards and four 48V 5 kWh lithium batteries with helm controls and display. Top speed of the 10m aluminium catamaran clocks in at eight knots, but the ferry usually cruises at three knots around the harbour, the most efficient pace. Estimated running time between recharging at berth is 20 hours. According to **Loys Leclercq**, naval architect responsible for the design of the boat, environmental consciousness played a major part during the development process. Aluminium was chosen as the hull material, as it can be fully recycled when one day the ferry completes its last trip. The catamaran hull form, on the other hand, improves efficiency by reducing water resistance. Air and water pollution, as well as noise levels, have been reduced to zero thanks to the propulsion system provided by Torqeedo. **Jean-Claude Ollivier**, Deputy Head, **Port of Capbreton**, said, "The new solar boat is a popular attraction on the Capbreton waterfront. Our passengers love the experience of gliding silently and smoothly through the harbour under electric power when commuting or touring the harbour."

Cavotec stays at the top of the e-charging market in Norway

The company received a repeat order from Fjord1, one of the world's largest operators of e-ferries, to equip two new berths on the **Halsa-Kanestraum** route, with its Automatic Plug-in System (APS). The Norwegian e-charging market is estimated to be worth €60m in the next five years. **Cavotec** received orders for over 20 APS systems in the past two years, bringing its market share in Norway to approx. 50 per cent. The country is expected to equip about 200 more berths with automatic e-ferry charging systems before 2025. APS connects ships to shore-side electrical power during on- and off-loading prior to subsequent sailings, maximizing the amount of time vessel batteries are charged. Other benefits include increased safety and emission reduction. **Mikael Norin**, CEO, Cavotec, said,"[...] Our success in Norway also positions us strongly in neighbouring markets in Denmark, Finland and Sweden, where we are actively pursuing opportunities that exist there. In addition, we are also seeing interest for similar solutions in the US and Canada."

P&O Ferries doubles rail capacity at the Europoort hub

The company launched a second rail line to its terminal at the continental hub. The 650m-long track will complement the existing one, increasing the handling capacity up to four trains of either 36 trailers or 42x45 ft containers per day, totalling eight services to and from various locations in Europe. According to a press release, customers will be able to ship cargo between Britain and Europe using **P&O Ferrymasters** rail service. It features integrated planning, scheduling, and transport management systems, with increased transparency as the main benefit. **Janette Bell**, Chief Executive, **P&O Ferries**, said, "To connect with the UK market, we provide three sailings a week to Teesport and seven sailings a week to Hull, with a commitment to providing customers with the most reliable and cost-efficient service possible. This initiative underlines our commitment to growth and going to places where our customers want us to go." Both P&O branches also plan to expand the rail network towards new destinations. Apart from fast-moving consumer goods across Europe, **Europoort**'s second rail line is also expected to handle automotive parts and products en route to the North East of England.

Rotterdam selects INFORM for software optimization

The company will deliver the Capacity and Planning Platform (CAPP), comprised of a plug-in set of optimization modules, for **Port of Rotterdam**'s front-end user interface, the Container Exchange Route (CER). CER itself is a novel concept that comprises and links dedicated infrastructure, logistics agreements, and IT systems, allowing for shorter turnaround times of deep-sea vessels, as well as increased planning flexibility. By bundling container flows and eliminating the need for trains, barges and feeders to call all terminals individually, CER increases the reliability and efficiency of container transshipments. Partners of the project include **Hutchinson**'s **ECT-Delta**, **ECT-Euromax**, **APMT Rotterdam**, **Rotterdam World Gateway** and **APMT MVII** as well as **Dutch Customs**, **Distripark**, empty depots, and the barge feeder terminals on the Maasvlakte. On the technical side, the project is comprised of a front-end user interface (CER Platform) and a Capacity and Planning Platform (CAPP), to be provided by **INFORM**. CAPP receives data from the CER Platform, analyses it, and sends back optimized proposals for execution. The analyses include determination of whether a new order is feasible given current workload and constraints, a journey plan for containers, the generation of schedules, and finally a schedule of jobs for the Automated Road Trucks to transport containers to their destinations. INFORM will employ artificial intelligence (AI) solutions, as part of their Syncrotess optimizers, for the project. **Emile van Rijn**, Projectmanager Capacity & Planning CER, Port of Rotterdam, said, "Optimization algorithms are crucial to the success of CAPP and therefor for the CER Project; due to the high number of parameters to be considered, it is not realistic for a staff member to manually plan the CER movements on the back of a cigar box." The project will be delivered using an Agile Development project approach with iterative releases planned regularly throughout the development process. **Dr. Eva Savelsberg**, SVP, Logistic Division, INFORM, elaborated on the approach, "Being able to deliver increments as early as possible brings benefits for both parties at the beginning of the project. Small steps towards the integration and communication between the CER Platform and CAPP mean huge benefits for the projects overall progress due to the possibility to continuously test the software throughout the course of the implementation." **Robin Audenaerdt** MSc MA, Technical Manager CER Systems, Port of Rotterdam, summed up the partnership, "[…] As the CER project is like going to the moon for the first time, it's good to have a partner that knows how to build an efficient rocket."

Cargo keeps flowing through Felixstowe despite COVID-19

The **Port of Felixstowe** remains fully operational in the face of the recent crisis linked to the global coronavirus pandemic. A number of special measures have been introduced in order to reduce the risks and ensure minimal hindrance of port activities. All ships are required to submit a Declaration of Health Statement before arrival, with any vessels failing to do so being restricted from entering the port. The intensity of cleaning arrangements has been increased, including haulier check-in points. Special plans have been put in place to deep clean the facilities and plant, should it become necessary. A Coronavirus Steering Group (CSG) has been established to oversee and direct the response to the crisis. Latest government advice regarding the best ways of maintaining personal hygiene and behaviour while travelling is being relayed through a variety of channels. The port authorities also created a second operations centre in a separate building and split the control tower operation into two teams for increased resilience. New rest-period arrangements based on team membership rather than job function are in place to reduce the risk of contamination across key roles, such as crane drivers. Work from home has been introduced where possible. The port authorities also took upon themselves to help arrange welfare visits in order to make sure that the employees receive the necessary support. All non-business critical visits have been restricted. There are currently no delays for cargo moving through the port.

Zeebrugge is 5G-ready

Nokia completed phase one of its 5G-ready, industrial-grade wireless network deployment at the **Port of Zeebrugge**. The company's Digital Automation Cloud platform will provide connectivity to over 100 endpoints across the entire port operations. Zeebrugge will now be able to track, analyse and manage connected devices across multiple port-based applications in real-time. It will unlock new path to innovation, related to the deployment of Internet of things (Iot)-based solutions, autonomous vehicles, augmented reality, and drones. Currently, the network is being used for connectivity with tugboats, air pollution detectors, security cameras and quay sensors. Its high-bandwidth and low-latency connectivity will also be leveraged during the upcoming construction of a new sea lock and during building and maintenance of offshore wind farms. Phase one has established increased automation in Zeebrugge's outer port area. Phase two, due for completion in mid-2020, will focus on the inner port. Several external suppliers have also signed up to the network, which will be used by port-based companies for dispatching, connectivity with straddle carriers, track and trace systems, and integrated communications. The project has been delivered in close cooperation with Citymesh. It will continue to assist with end-to-end support and network commercialisation.

COVID-19: Port of Antwerp Taskforce update

Members of the taskforce confirmed that keeping the port operational is a shared priority and expressed their full commitment to the task at hand. A port monitor has been set up in order to survey the daily operation of the port and identify additional safety measures if necessary. The taskforce is multidisciplinary and cross-border. Members include **Port of Antwerp**, **Alfaport-Voka**, **ASV, Cepa**, **ESPO**, **Essenscia**, **Antwerp Fire Department**, **Antwerp Shipping Police**, the **Agency for Maritime Services & Coast (MDK)**, **Vlaamse Waterweg** (waterway operator), **Customs & Excise**, the cabinet of **Flemish Minister of Mobility and Public Works Lydia Peeters** and the **Dutch Ministry of Infrastructure and Water Management**, as well as the **Dutch Common Nautical Management**, due to its control of access via the Scheldt. For now, the port platform remains operational. Handling of the terminals is going ahead normally, there is sufficient manpower available to deal with cargo, and drivers are arriving and departing without too much delay. That said, the taskforce identified two areas in need of attention. First, due to the varying safety regulations implemented by Belgium and the Netherlands, and the Port of Antwerp being served by both Flemish and Dutch pilots, the MDK is working on an approach in consultation with the Netherlands in which the undertaken measures are not contradictory. Second, manpower needs to be closely monitored, as the availability and allocation of employees are essential for the correct functioning of all port services. Fall-back scenarios are being drawn up to assure continuity thereof. At the moment, the Port of Antwerp has not seen any decline in the freight volume. However, it is expected that fewer ships will call at the port in the coming days and weeks because of the coronavirus outbreak. Fifteen fewer large container carriers from Asia will call, corresponding to 115k TEU less freight being carried from and to China. Peaks in market demand are being dealt with, e.g. there has been a rise in demand for foodstuffs and healthy foods such as bananas. Therefore, according to the port's press release, it is essential to keep Europe's borders open for all forms of freight transport.

Kings of Spain check in with the Port of Valencia

Their Majesties took a closer look at the maintenance of the supply chain in one of Spain's biggest ports. During a videoconference, the heads of the **Valencia Port Authority** (PAV) stated that all port services are 100% operational and keeping the cargo flowing. PAV's President, **Aurelio Martínez Estévez**, pointed out, that 70% of what the country does not produce and needs to import goes through the ports and underlined the critical role the industry plays in guaranteeing the supply of essential products. He also noted the significant spike in cargo traffic to island communities which has occurred since the outbreak of the COVID-19 pandemic. Recent weeks saw a notable increase in the movement of agri-food and hygiene products and a drop in the traffic of industrial products (e.g. chemical products, iron and steel, wood). Food and hygiene products traffic registered an average daily growth of over 15%, at times reaching the 40% mark. Estévez also underscored that the unhindered flow of goods is only possible due to the efforts of the whole port community. Stevedores, truckers, pilots, mooring lines, tugs, port security, maintenance staff, shipping companies, freight forwards and customs agents, border inspection services and PV personnel – everyone is working tirelessly in order to keep the supply chains open.

Inmarsat takes active role in decarbonising shipping

The company became one of the founding members of Asia's first 'Decarbonising Shipping' initiative, aimed at bringing startups together with backers with maritime expertise in order to help the industry meet the targets on greenhouse gas (GHG) emissions. Based in Singapore, the regional initiative is part of the Trade & Transport Impact (TTI) programme, led by **Rainmaking**. **Inmarsat** joined the first two cycles of TTI, held in Europe in 2019, which scouted over 1.2k start-ups and led to 24 collaboration projects. Backed by the **Maritime & Port Authority of Singapore**, the new initiative is expected to identify further 1k projects offering models to tackle decarbonisation, with selected startups to be matched with maritime industry leaders willing to collaborate. Other confirmed partners include **Cargill**, **DNV GL**, **Hafnia**, **MC Shipping Inc.**, **Vale** and **Wilhelmsen**. **Ronald Spithout**, President, Inmarsat Maritime, said, "Shipping and its customers are demanding solutions and technology to address the decarbonisation targets set by regulators, and this is where startups and market disruptors come in." According to Inmarsat's recent report on how startups contribute to driving maritime trade, the value of Ship Technology (ShipTech) will rise from $106bn to US$278bn by 2030. Companies offering solutions helping to monitor and cut emissions will take up a significant chunk of the market. Inmarsat also supports startups via its Certified Application Provider (CAP) programme. It allows the selected companies to accelerate the scale-up of their application through extended outreach and removing the need for their own solution-specific hardware. Over 20 providers are now part of CAP, including **ABB**, **NAPA**, **Hyundai Global Serives** and **Nautilus Labs**.

Agricultural producers tip their hats to truckers

The **SanLucar** group and its closest partners – **Fresaflor**, **Llusar** and **Poveda** – joined forces in order to support truck drivers in times of global crisis. They made free food kits available to drivers transporting goods to and from their sites in Spain, Germany, and Austria. **Stephan Rötzer**, Founder and Owner, SanLucar, explained the reasons behind the initiative, "At SanLucar, we know that truckers are facing new challenges these days, enduring long queues at border crossings or the absence of open bars and restaurants along the way. And even so, they continue to strive, aware of how crucial the work they do is. They are our anonymous heroes." According to Rötzer, in times such as these, closer collaboration is the key to keeping the food sector's value chain going.

PSA International flirts with hydrogen

Together with five Singaporean and two Japanese partners, the company signed a memorandum of understanding (MoU) aimed at exploring the potential of hydrogen as an alternative, low-carbon fuel for Singapore. The involved parties focus on research and development of new technologies related to the transportation and storage of hydrogen. Signees include **Jurong Port Pte Ltd**, **City Gas Pte Ltd**, **Sembcorp Industries Ltd**, **Singapore LNG Corporation Pte Ltd**, **Chiyoda Corporation** and **Mitsubishi Corporation**. Chiyoda's SPERA Hydrogen, Liquid Organic Hydrogen Carrier (LOHC) technology will play a key role in identifying and demonstration of possible use cases. It allows for the safe transportation of hydrogen in chemical tankers at normal atmospheric temperature and pressure. According to the press release, it was the "very real challenge of climate change," that prompted Singapore's Government to engage stakeholders and interest them in creating solutions for the country's Energy Story. The **National Research Foundation** (NRF) Singapore will also work with the **Maritime and Port Authority of Singapore** (MPA) to tackle the maritime decarbonisation challenge through research and technology development. Professor **Low Teck Seng**, CEO, NRF, noted that these efforts would be met with support from the side of public sector agencies, in order to speed up the potential switch to hydrogen as a low-carbon solution, thus lowering Singapore's carbon footprint.

COVID-19: TT Club's guidance repository

The insurance provider warns that the scenarios faced by the industry will be many, various and complex. Every branch of the logistics and supply chain will be affected to some degree, from port, terminal, and warehouse operators to carriers across all modes of transport, forwarders, and logistics companies. Levels of uncertainty are bound to rise, as the global economy slows, governments keep prioritising specific supplies, consumer spending falls, and personnel shortages become more prevalent. That said, the need for essential supplies, such as foodstuffs, pharmaceuticals, and medical equipment, will remain robust. Reliability, efficiency, and flexibility of the services provided will prove key in surviving the crisis. Additionally, according to **Peregrine Storrs-Fox**, Risk Management Director, TT Club, communication between stakeholders will be of similar importance. "The physical movement of cargo is understandably experiencing delays due to cancelled ship sailings, shortage of air freight capacity and land border checks, and these disruptions to the norm will cause friction between the various links in the chain. An understanding of 'what is going on' by participants in the chain will serve to ease such friction," Storrs-Fox says. The crisis poses other dangers as well. Where contractual relationships are in place, the supplier is generally obligated to explore all reasonable options to mitigate a potential loss arising in the circumstances, such as presented by this coronavirus outbreak. As Storrs-Fox comments, "Any party seeking in the event of a future dispute to rely on a 'force majeure' defence may well face the burden of evidencing that they took all reasonable steps to mitigate the loss". Risk mitigating strategies suggested by the insurance provider include staying well informed and maintaining open channels of communication with the national or local authorities relevant to the business obligations. Established crisis management plans might still prove relevant, despite the scale and scope of the current disruption. They can assist in identifying vulnerabilities that may impact the ability to fulfil usual obligations or carry out standard business requirements. That said, the nature of the virus, e.g. exposure through contact with surfaces, will necessitate the implementation of additional prevention methods and additional staff training, as well as make usual personnel and site security procedures more complex. In order to provide support and up-to-date advice, TT Club is building a dedicated page of available guidance, accessible through the company's website.

Stena Line sends more employees on a leave of absence

The operator announced the plan to furlough 600 employees with 150 redundancies across the **UK** and the **Republic of Ireland**. According to the press release, the decision is an unavoidable response to the on-going global crisis, a result of the COVID-19 pandemic. Since the beginning of the crisis, **Stena Line** experienced a large decline in travel bookings and freight volumes, as many countries restricted cross-border passenger traffic. It is estimated that passenger figures will not recover until well into 2021. The resulting drop in revenue forces the company to take drastic steps in order to cut costs. **Ian Hampton**, Director, Stena Line, explained, "The COVID-19 crisis has meant that Stena Line is experiencing a significant decline in passenger and freight volumes across all its 20 European routes. We are having to make some very difficult decisions that we hoped we would never have to make." The announcement of furlough and redundancies relates to both UK and Ireland shore-based and sea-based employees, including those working on vessels on the Irish Sea and the North Sea. It follows a reduction of the number of sailings on a number of routes. Several vessels have also been taken out of service. According to Hampton, the decisions made are crucial to securing the continuity of Stena Line's freight operations, as the company is committed to keeping vital supply lines open for the UK and Ireland. Furloughed employees will receive 80% of their salaries. Where the UK and Irish government schemes don't cover the full amount, the remainder will be paid by the firm. Mid-March, the company was forced to announce 950 redundancies affecting workers employed in Scandinavia. A number of these employees have since also been furloughed. Further job losses have subsequently been made in Denmark and the Baltics. Stena Line does not rule out further furlough, redundancy or changes to its current sailing schedules or routes as the situation keeps developing.

GEODIS sets up an air bridge between Asia and Europe

The company has been commissioned by the French Government to organize the emergency supply of millions of masks from China to France. Over the coming weeks, two Antonov 124 aircraft will make 16 planned flights, which translates to an approx. capacity of 2.4k m3 per week. The planes are specially designed for the transport of cargo in large quantities. If necessary, the schedule could be extended into the month of May. According to the French Minister of Solidarity and Health, the air bridge is part of a bigger plan, set to deliver 1bn masks to France over the next 14 days. The first flight from Shenzhen Airport in China, containing 8.5m masks, landed in France earlier this week at the Paris-Vatry airport. A second flight is scheduled to arrive later this week, carrying 13m additional masks.

market sms

Photo: Pixabay

PORT OF VALENCIA:
11.45mt handled in I-II 2020 (-0.03% yoy)

General cargo registered slight growth, with 11.06mt (+0.71% year-to-year) handled, while the highest drop in turnover was observed in the solid bulk segment, with 0.17mt (-30.41% yoy) handled.

Port of Valencia's volumes

	I-II 2020	Yoy
General cargo	11.06mt	+0.71%
Liquid bulk	0.20mt	-1.35%
Solid bulk	0.17mt	-30.41%
Total	**11.45mt**	**-0.03%**
Container traffic (million TEUs)		
Total	**0.85**	**-1.03%**
Passenger traffic (units)		
Ferry	70.423	+7.62%
Cruise	20.723	-7.47%
Total	**91.155**	**+3.77%**

PORTS OF GENOA:
8.70mt handled in I-II 2020 (+0.6% yoy)

While container traffic has been on the rise during the first two months of 2020, with 0.43m TEUs handled (+6.0% year-on-year), drops were registered in the liquid bulk and dry bulk segments, with 2.68mt (-5.0% yoy) and 0.07mt (-35.8% yoy) handled respectively.

Ports' of Genoa volumes

	I-II 2020	Yoy
General cargo	5.95mt	+2.6%
Dry bulk	0.07mt	-35.8%
Liquid bulk	2.68mt	-5.0%
Total	**8.70mt**	**-0.3%**
Container traffic (million TEUs)		
Total	**0.43**	**+6.0%**
Passenger traffic, out of which		
Ferries	102.364	+17.8%
Cruises	89.369	+25.0%
Total	**191.733**	**+21.0%**

DFDS' FERRY & RO-RO DIVISION:
41,280k lane metres filled in 2019 (+3% yoy)

When translated into cargo units, counting 18m per one truck, the Danish shipping line's fleet carried approx. 2,293,333 trucks & trailers Europe-wide.

DFDS' volumes

Business unit	2019	Yoy
Ferry & ro-ro – freight (thousand lane metres)		
Channel	18,995	-3.4%
North Sea	12,815	-2.0%
Baltic Sea	4,613	+0.8%
Mediterranean*	4,365	+97.9%
Passenger	491	-11.7%
Total	**41,280**	**+3.0%**
Ferry – passengers (thousand travellers)		
Channel	3,520	-8.6%
Passenger	1,351	-1.0%
Baltic Sea	245	+9.4%
Total	**5,116**	**-5.9%**
Logistics (thousand ro-ro cargo units)		
Continent	240.9	-8.0%
UK & Ireland	190.5	+11.7%
Nordic	Nordic	-13.2%
Total	**548.3**	**-3.3%**

ROSTOCK SEAPORT:
25.7mt handled in 2019 (+0.4% yoy)

Freight brought on-board ferries and ro-ros, the main source of volume taken care of in Rostock, noted a downtick of 4.1% year-on-year, totalling 16.2mt. The port's 2019 ro-ro traffic amounted to 523,506 cargo units (-4.1% yoy), out of which trucks summed up to 379,812 units (-6.5% yoy), trailers to 125,306 (+0.9% yoy), and railcars to 18,388 (+17.8% yoy). Rostock seaport rail-handled a total of 87k cargo units, an increase of 11.5% on the result from 2018. With 2.5m passengers, ferry traffic stayed at the same level as in the previous year. Other freight segments went up last year - dry bulk by 1.9% yoy to altogether 5.93mt, liquids by 29.6% yoy to 2.98mt, and break-bulk by 1.8% yoy to 570kt. Lastly, the nearby fishing and chemical ports turned over 1.5mt, less by 16.7% yoy.

PORT OF BARCELONA:
65.96mt handled in 2019 (-0.1% yoy)

It was a year of consolidation for the Port of Barcelona, mainly due to general slowdown of the industry, marred by economic disruptions. That said, it is worth noting that hinterland traffic maintained records achieved in 2018, with 35mt handled. Container traffic dropped to 3.32m TEUs (-3.2% year-on-year), still being the second-best year in the history of the port in terms of containers.

Port of Barcelona volumes

	2019	Yoy
Liquid bulk	16.13mt	+5.3%
Dry bulk	4.07mt	-3.6%
General cargo	45.75mt	-1.5%
Total	**65.95mt**	**-0.1%**
Container traffic		
Total (milion TEUs)	**3.32**	**-3.2%**
Passenger traffic, out of which		
Ferry	1.49m	+3.0%
Cruise	3.14m	+3.0%
Total	**4.62m**	**+3.0%**

PORT OF BARCELONA:
10.00mt handled in I-II 2020 (-5.3% yoy)

Drops in traffic can be observed all over the cargo type spectrum, with highest losses registered in the general cargo and dry bulk segments, with 6.96mt (-5.4% year-on-year) and 0.72mt (-8.4% yoy) handled respectively.

Port of Barcelona volumes

	I-II 2020	Yoy
General cargo, out of which	6.96mt	-5.4%
containerised	5.15mt	-8.6%
non-containerised	1.80mt	+5.0%
Liquid bulk	2.31mt	-3.7%
Dry bulk	0.72mt	-8.4%
Total	**10.00mt**	**-5.3%**
Container traffic (million TEUs)		
Total	**0.5**	**+5.0%**
Passenger traffic (thousands)		
Total	**279.510**	**-4.8%**

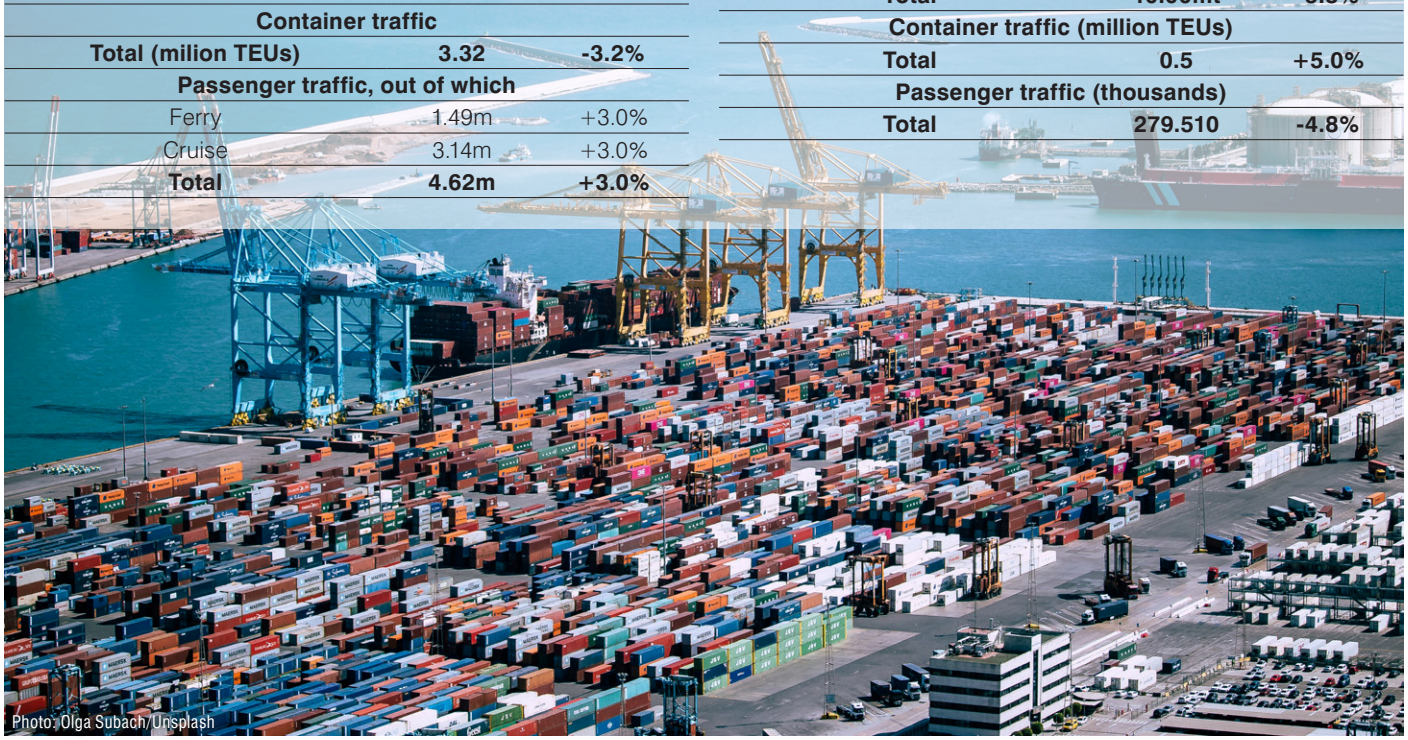


Photo: Olga Subach/Unsplash

PORT OF ZEEBRUGGE:
45.8mt handled in 2019 (+14.2% yoy)

Highest volumes were registered in the RoRo segment, with 16.5mt (+3.7 year-on-year) handled. A drop in ro-ro traffic with destination UK (-2.5% yoy) was offset by a shift towards Ireland (+6.3% yoy). Liquid bulk rose sharply (+60.8% yoy) thanks to the doubling of LNG-volumes (+107.5% yoy).

Port of Zeebrugge's volumes

	2019	Yoy
RoRo	16.5mt	+3.7%
Containerized	16.2mt	+7.0%
Liquid bulk	10.8mt	+60.8%
Dry bulk	1.3mt	+7.6%
General cargo	1.0mt	-13.5%
Total	**45.8mt**	**+14.2%**
Container traffic		
TEUs	1.7m	+4.8%

PORT OF LIEPĀJA:
49,296 ro-ro cargo units handled in 2019 (+7.8% yoy)

Tonnage-wise, wheeled cargo totalled 760.5kt, an uptick of 0.2% on the result from 2018. Overall, however, the Latvian port took care of less cargo last year, a decrease of 2.7% year-on-year to 7.33mt, including 5.57mt (-2.8% yoy) of dry bulk, 1.19mt (-13.2% yoy) of general cargo, and 571.5kt (+32.2% yoy) of liquid bulk. Liepāja's passenger traffic dropped as well, by 14.4% yoy to a total of 39,987 travellers.

PORT OF ST. PETERSBURG:
2,221,724 TEUs handled in 2019 (+4.3% yoy)

Overall, the Port of St. Petersburg took care of nearly 59.88mt last year, marking an increase of 0.9% on the result from 2018. The container total includes 255,285 reefers, the handling of which noted a downtick of 5.6% year-on-year. The turnover of general cargo amounted to 40.97mt (-1.1% yoy), including 27.42mt of containerised freight (+5.7% yoy). With 9.82mt (+7.7% yo) liquid bulk came in second, followed by 9.08mt of dry bulk (+3.5% yoy).

PORT OF SINGAPORE:
98.51mt handled in I-II 2020 (-1.3% yoy)

The drop in overall throughput can be mainly attributed to a decrease in the liquid bulk segment, with 33.24mt (-10.9% year-on-year) handled.

Port of Singapore volumes

	I-II 2020	Yoy
General cargo	4.00mt	+0.5%
Containers	57.99mt	+3.8%
Liquid bulk	33.24mt	-10.9%
Dry bulk	3.27mt	+19.7%
Total	**98.51mt**	**-1.3%**
Container throughput (million TEUs)		
Total	**6.08**	**+5.9%**

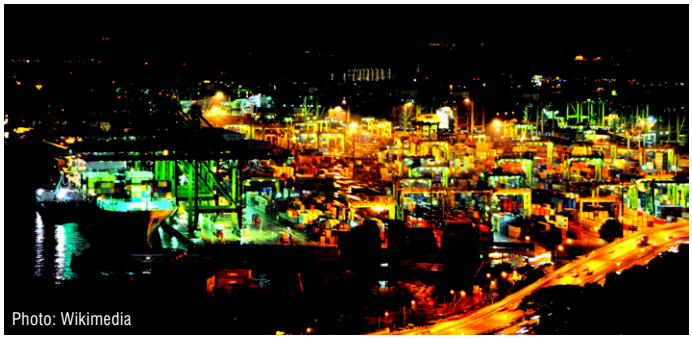


Photo: Wikimedia

PORT OF GÄVLE:
5.6mt handled in 2019 (+3.5% yoy)

After 2015 (5.92mt) and 2017 (5.68mt), it was the port's third- best result noted over the last decade (which started from the level of 4.50mt in 2010). A total of 839 vessels visited the Swedish port in 2019, two more than the year before.

PORT OF RIGA:
32.76mt handled in 2019 (-10.1% yoy)

The Latvian port noted decreases across the board, in the turnover of dry (-12% year-on-year to 20.83mt) and liquid (-7.1% yoy to 3.83mt) bulk as well as of general cargo (-6.1% yoy to 8.09mt). Riga's container traffic marked a downtick of 0.5% yoy to altogether 466,889 TEUs. The ro-ro segment went down, too, by 9.8% yoy to a total of 77,434 trucks & trailers. On the whole, passenger traffic contracted as well, by 0.2% yoy to 868,653 travellers, incl. 69,207 cruise (-7.5% yoy) and 799,446 ferry (+0.4% yoy) passengers.


Photo: Port of Riga

PORT OF KLAIPĖDA:
703k TEUs handled in 2019 (-6.3% yoy)

On the other hand, the Lithuanian seaport took care of 300.5k ro-ro cargo units, more by 4.1% on the result from 2018. In total, 46.25mt went through Klaipėda's quays, a decrease of 0.7% year-on-year. The port's cruise traffic contracted, too, by 2.3% yoy to altogether 68k passengers brought on-board 51 cruisers (seven less than in 2018).

PORT OF LOS ANGELES:
207.3mt handled in 2019 (+6.5% yoy)

An increase in the general cargo segment, with 193.1mt (+8.4% year-on-year) handled, was the main factor behind an overall positive end of the year result.

Port of Los Angeles' volumes

	2019	Yoy
General cargo	193.1mt	+8.4%
Liquid bulk	13.4mt	-15.6%
Dry bulk	0.8mt	-20.0%
Total	**207.3mt**	**+6.5%**
Container traffic (million TEUs)		
Total	**9.3**	**-1.2%**

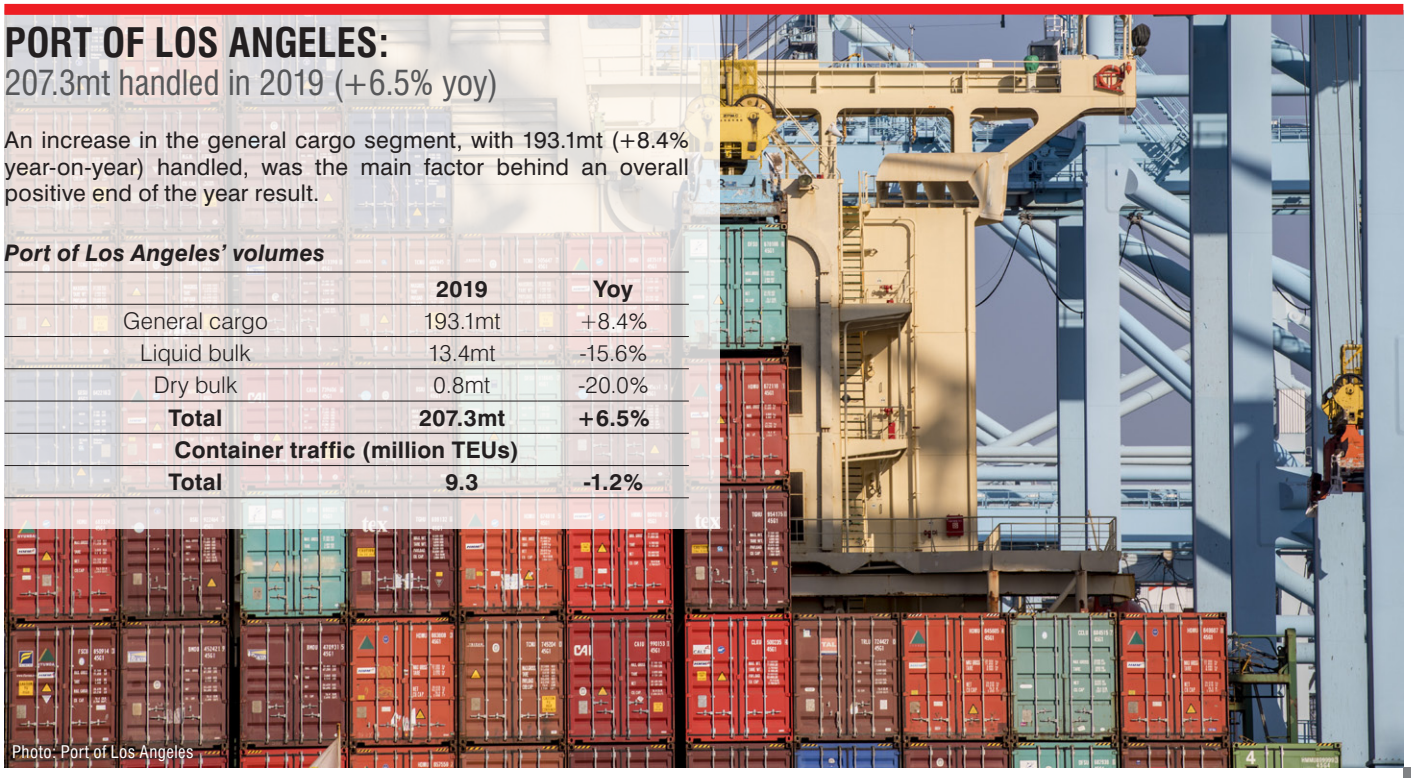


Photo: Port of Los Angeles

Short Stories

Photo: Pexels

European consortium formed to deliver new Shift2Rail project

Seven companies from Spain, Italy, the Netherlands, and France have been selected to deliver EU's **4SECURail** programme, funded through Horizon 2020. Started in December 2019 and officially launched in January 2020, 4SECURail is coordinated by the engineering consulting firm **Ardanuy Ingeniería, S.A.**, in collaboration with **Consiglio Nazionale delle Ricerche (CNR)**, **FIT Consulting**, **Hit Rail**, **SIRTI**, **Tree Technology** and **International Union of Railways** (UIC). Hit Rail B.V., specializing in IT solutions, will work alongside partners UIC and Tree Technology, an R&D company, to deliver the co-design and testing of a model and collaboration platform for a European Railway Computer Security Incident Response Team (CSIRT). The system is designed to coordinate the cybersecurity response actions of the separate railway security teams. CSIRT will extend that collaboration and will be demonstrated and tested in 2020/2021 to support future consideration of the feasibility of deployment by the **Shift2Rail** joint undertaking and its work in X2RAIL3 supporting the EU Rail ISAC and Rail Community. CNR will join forces with Ardanuy, FIT, and SIRTI to provide a demonstrator for the evaluation, in terms of cost, benefits and required learning curve, of the impact of the use of formal methods for the rigorous specification of the components of a railway signalling infrastructure. Shift2Rail is a European rail initiative supporting Research and Innovation (R&I) aimed at integrating new and advanced technologies through its Horizon 2020 funding, with the goal of completing the Single European Railway Area (SERA).

Port of Ashdod starts cyber-security programme

Called **Port-Dome**, the new cyber protection initiative, started in partnership with **Naval Dome**, will, in its final form, secure vital systems across the port's whole network. These include traffic control systems (VTMS/VTS), berths, bridges, locks and gates, terminal cranes and storage facilities, and all access points and gateways. Pilot trials are set to kick off at the beginning of 2020 on a limited number of systems at first. **Itai Sela**, CEO, Naval Dome, briefly summed up the project, "Port-Dome is the leading solution for port and terminal operators as it provides the highest level of cyber defence without having to upgrade systems or change existing infrastructures. No training is required, and the Port of Ashdod's OT systems will continue to operate the same as they did prior to the installation. The only difference being hackers will be unable to gain access." Sela promises that after Port-Dome has been successfully tried and installed, Ashdod will become one of the most secure terminals in operation. **Paola Rossi**, VP, Navam Dome, added, "[…]With expanding OT-based systems and network-based technologies, alongside the increase in systems using GPS-based location services, seaports will become increasingly susceptible to attack. If successful hackers can paralyse the supply chain's central artery, it will shut down port operations, damage systems, result in human casualties, and financial and reputation loss." **Ashdod Port** is located approx. 40km away from Tel Aviv and is the foremost entry point to the State of Israel. With an annual container throughput of more than 1.5MTEU, it handles the largest volume of containers of all Israeli ports.

Alpha Ori hits another cyber-security landmark

The company has been recently awarded the ISO 27001:2013, a globally recognized standard that certifies the successful establishment, maintenance and continual improvement of a company's Information Security Management System (ISMS). It confirms that **Alpha Ori** has put in place a system of technical, administrative and physical controls which secure the company's own information, and customer and employee information, within the context of overall business risks. Captain **Rajesh Unni**, Co-CEO, Alpha Ori, said, "[…] We achieved ISO certification at our first attempt, showcasing the completeness and rigour of our information security systems." The decision to work toward ISO 27001:2013 accreditation was part of an ongoing commitment to continually improving products and services. To become ISO 27001:2013 compliant, the company's teams based in the USA, India, and Singapore underwent an extensive companywide audit that included information data security management system development, a management system documentation review, pre-audit, initial assessment, and clearance of non-conformances.

ClassNK launches cyber security training

ClassNK recently announced the launch of a cyber security training service (e-learning), developed in cooperation with **KDDI CORPORATION** (KDDI) and **KDDI Digital Security Inc.** (KDS). The initiative focuses on issues specifically important to the maritime industry. It is available in both Japanese and English and provides a certificate upon successful passing of a comprehension test. The certificate can be used for an education record of Cyber Security Management System. Certified by ClassNK in compliance with the Guidelines on Cyber Security Onboard Ships Version 3, the programme is supported by BIMCO. It is accessible globally and at any time via smart devices and personal computers. This initiative is a direct response to cyber risks arising from the increased use of solutions relying on 'Big Data' and Internet of Things (IoT) technologies. Thus, it becomes ever more important for maritime professionals to expand their knowledge and skillset in order to prepare for these new, emerging threats.

Coronavirus crisis is a paradise for online scammers

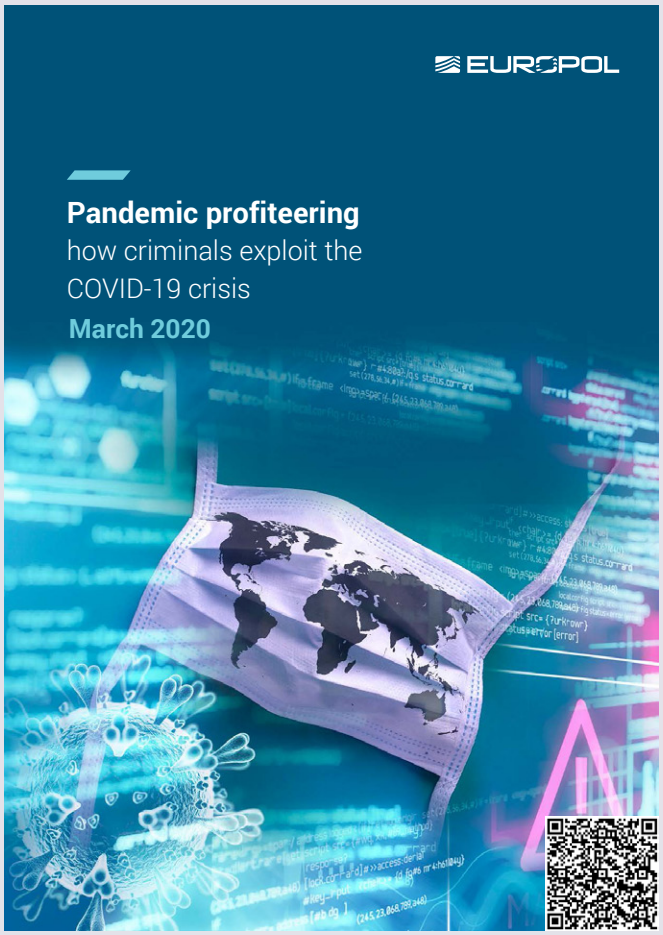
GTMaritime warns that maritime security faces a new and highly unpredictable threat as scammers line up to exploit fears surrounding the COVID-19 pandemic, as the industry moves to encourage remote working to minimise the spread of the pathogen. **Jamie Jones**, Operations Director, GTMaritime, said, "Shipping companies are looking into reconfiguring their shore-based operations in response to the spread of Coronavirus, but employees can expect to receive unsolicited messages geared to exploit their personal anxieties about the epidemic. As organisations ramp up physical hygiene, it is important they don't take their eye off cyber-hygiene." Researchers at **Sophos** recently identified a trojan campaign specifically targeting Italian email addresses attempting to play on worries about the virus. The phishing email comes with an attached Word document that claims to contain advice on how to prevent infection – but is, in fact, a Visual Basic for Applications (VBA) script that drops a payload to steal confidential information. Scammers are also setting up websites to sell bogus products, and use fake emails, texts and social media posts to seek out personal information or financial reward. Under cover of promoting awareness, offering prevention tips or providing fake information about cases local to the recipient, fraudsters can request donations for 'victims' or deliver malicious email attachments to spread malware or steal log-in credentials. At the same time, Jones offers words of encouragement, "On the one hand, IT professionals working at shipping companies are at an advantage as they are already familiar with the challenges of remote working – as nothing can be more remote than a ship in the middle of the ocean. On the other, they must monitor and contend with emerging risks across multiple territories rather than managing a response within a single country." Cyber response plans should be reviewed and, if necessary, updated, to ensure that they can withstand the new threats emerging due to the crisis at hand. GTMaritime suggests for companies to proof whether their IT infrastructure is sufficiently secure. The company also provides its customers with free phishing penetration tests. The **US Cybersecurity and Infrastructure Security Agency** (CISA) issued a set of guidelines for organisations to better prepare for cyber-related threats. Divided into advice for IT professionals and crew and shore-based employees, these include, among other items, ensuring that systems are fully patched and equipped with intrusion prevention software, being wary of e-mails from unknown sources or ignoring online offers for vaccinations, treatments, or cures.

Cyber-sec best practices for container vessels

The Digital Container Shipping Association (DCSA) recently published the 'DCSA Implementation Guide for Cyber Security on Vessels', aimed at facilitating vessels readiness for International Maritime Organization's (IMO) resolution on Maritime Cyber Risk Management in Safety Management Systems. Aim of the document is to provide shipping companies with a common language and a manageable, task-based approach for meeting IMO's January 2021 implementation timeframe. The guide aligns with existing BIMCO and US National Institute of Standards and Technology (NIST) cyber risk management frameworks, enabling shipowners to effectively incorporate cyber risk management into their existing Safety Management Systems (SMS). Thomas Bagge, CEO, DCSA, warns, "As shipping catches up with other industries such as banking and telco in terms of digitisation, the need for cyber risk management becomes an imperative. Due to the global economic dependence on shipping and the complex interconnectedness of shipping logistics, cyberattacks such as malware, denial of service, and system hacks can not only disrupt one carrier's revenue stream - they can have a significant impact on the global economy […]." DCSA's guide breaks down the BIMCO framework into themes and maps these themes to the controls that underpin the NIST functional elements: Identify, Protect, Detect, Respond, Recover. It provides non-technical explanations and specific actions to be taken to address each NIST element in accordance with a company's level of cyber maturity within each BIMCO theme. Jakob Larsen, Head of Maritime Safety & Security, BIMCO, added, "[…] Initially thought of as a tool for container carriers, the guidance can also inspire the thinking in other shipping sectors as well as the ongoing update of the major shipping associations' benchmark document 'Guidelines on Cyber Risk Management Onboard Ships'." The DCSA cyber security guide, 'DCSA Implementation Guide for Cyber Security on Vessels', can be freely downloaded from the DCSA website.

Pandemic profiteering

Europol's recent report provides an overview of how criminals adapt their tactics in times of the COVID-19 pandemic, featuring a comment on threats to cyber security. The report has been compiled based on data received from EU Member States on a 24/7 basis. Cyber-related risks result from a number of factors identified as having an impact on crime. These include high demand for certain goods, such as protective gear and pharmaceutical products, with cyber criminals offering these through infected e-mails. Heightened anxiety plays into it as well, making people more likely to be fooled by these attempts. Working from home means increased reliance on digital solutions, providing hackers with more access points. The report mentions social engineering attacks, namely phishing e-mails distributed through spam campaigns and more targeted attacks, such as business e-mail compromise (BEC). Also noted is the impact on Darkweb operations, with certain illicit goods becoming more expensive, as source materials become unavailable. Vendors on Darkweb run scams, offering special 'corona goods' at discounts. Europol's 'Pandemic profiteering – how criminals exploit the COVID-19 crisis' can be downloaded directly from the organisation's website.



MAN's cyber-attack resistant engine safe

Announced by **MAN PrimeServ**, **MAN Energy Solutions**' after-sales division, the MAN EngineVault revitalises existing engines, machinery, auxiliary systems, instrumentation, and control systems that have already operated in the field for multiple years, protecting main-engine networks from online and physical cyberattacks. The initiative becomes even more relevant, considering the guidelines **IMO**, **SIRE**, and **SOLAS** are set to introduce come January 1, 2021, requiring operators to address the issue of marine cyber security. MAN's new solution provides firewall protection, comprehensive whitelisting, and application-layer protection that seals engine networks off from virtually any known threat – including on-board attacks via compromised USB flash drives and similar, physical media. **Michael Petersen**, VP, Head of PrimeServ Copenhagen, said, "[…] We realise that the increase in digitisation and network-based systems also increases vulnerability for cyberattacks that can potentially paralyse entire businesses. Therefore, implementing defensive barriers – also for your vessels' main engines – should be an essential element in proactive cybersecurity management." Critical security components of the EngineVault include: full network hardening via port protection, encryption of all data received and transmitted, and advanced network segment segregation; critical hardware protection via main operating panels for the engine control and management systems; application-layer protection and extensive whitelisting that only allows MAN-certified software on your engine network. It also enables the system to immediately return engine networks to their last-known safe state in case of a successful cyber-attack. Starting May 2020, the technology will come as standard in all newly built ME-engines.

Holland America and Princess report security breach

Both brands of the **Carnival Corporation** disclosed a cybersecurity breach involving the release of personal information, which occurred in 2019. Suspicious network activity has been noticed in late May 2019. A cybersecurity forensic team has been brought in for investigation, in order to identify what data was affected. According to their findings, an unauthorized third party gained access to a number of employee e-mail accounts from 11 April to 23 July 2019. E-mail suspected to be compromised includes employee, crew, and guest data of varying nature, such as name and address, Social Security, passport or driver's license or credit card numbers, as well as financial and health-related information. There have been no reports of misuse of personal data by the two cruises so far. Talking to CNBC, **Jim Van Dyke**, co-Founder and CEO, **Breach Clarity**, a cyber-fraud risk rating startup, described the breach as particularly dangerous. According to Van Dyke, it could make the affected persons vulnerable to fraudulent charges on their existing financial accounts or fraudulent creation of new credit accounts under their name. Carnival advised anyone suspecting they might be affected by the breach, to take up a number of routine security measures, including staying alert for phishing e-mails, keeping a careful eye on account statements and credit history and being sure to report suspected identity theft to law enforcement.

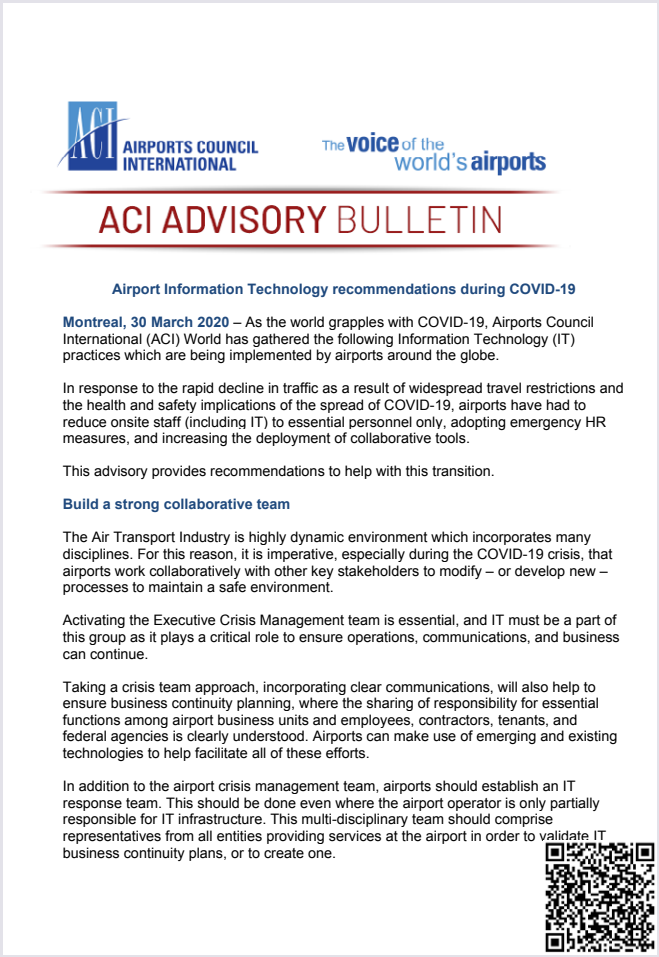
MSC hit by potential cyber-attack

The suspected malware attack, blamed for the shipping company's website going down and closure of one of its data centres, is said to have occurred on Thursday, April 9. With its website down, the company communicated the following via Twitter on April 10, "We are sorry to inform you that http://MSC.com and myMSC are currently not available as we've experienced a network outage in one of our data centres. We are working on fixing the issue." **MSC**'s online booking tools ceased to be operational, but alternative booking platforms such as **INTRA** and **GT Nexus** were not affected, allowing for business to continue. According to a press release issued by the company, the incident was confined to its HQ in Geneva.

During that time, MSC agencies remained fully functional. The investigation into the specific reasons for the network outage is still underway. The company also assured that it is safe to use its services and share data, as well as open e-mails from MSC. The press release states that the incident had only limited impact on MSC's business and has been fully resolved.

ACI addresses cyber-sec in view of the COVID-19 pandemic

Airports Council International (ACI) published a set of guidelines on IT practices implemented by airports globally, in order to raise awareness in times of increased disruption. With a growing number of staff working remotely and relying on digital solutions, the threat of cyber-attacks becomes greater. Best practices highlighted in the document include reviewing current policies in order to ensure there are established guidelines for remote work and access to airport systems, additional cyber-security training for employees, focusing on risks, threats and vulnerabilities of remote working, establishing secure networks (e.g. by using dedicated VPN and making sure they're updated) and limiting access to protected information remotely only to essential personnel. The document also provides guidance on establishing strong collaborative teams with other stakeholders in order to develop new safety measures, as well as ensuring effective and secure IT infrastructure for remote access. It also features recommendations for handling events requiring a full system shutdown, backup, and restoration. ACI's guidance can be downloaded directly from the Council's website.


AIRPORTS COUNCIL INTERNATIONAL

The voice of the world's airports

ACI ADVISORY BULLETIN

Airport Information Technology recommendations during COVID-19

Montreal, 30 March 2020 – As the world grapples with COVID-19, Airports Council International (ACI) World has gathered the following Information Technology (IT) practices which are being implemented by airports around the globe.

In response to the rapid decline in traffic as a result of widespread travel restrictions and the health and safety implications of the spread of COVID-19, airports have had to reduce onsite staff (including IT) to essential personnel only, adopting emergency HR measures, and increasing the deployment of collaborative tools.

This advisory provides recommendations to help with this transition.

Build a strong collaborative team

The Air Transport Industry is highly dynamic environment which incorporates many disciplines. For this reason, it is imperative, especially during the COVID-19 crisis, that airports work collaboratively with other key stakeholders to modify – or develop new – processes to maintain a safe environment.

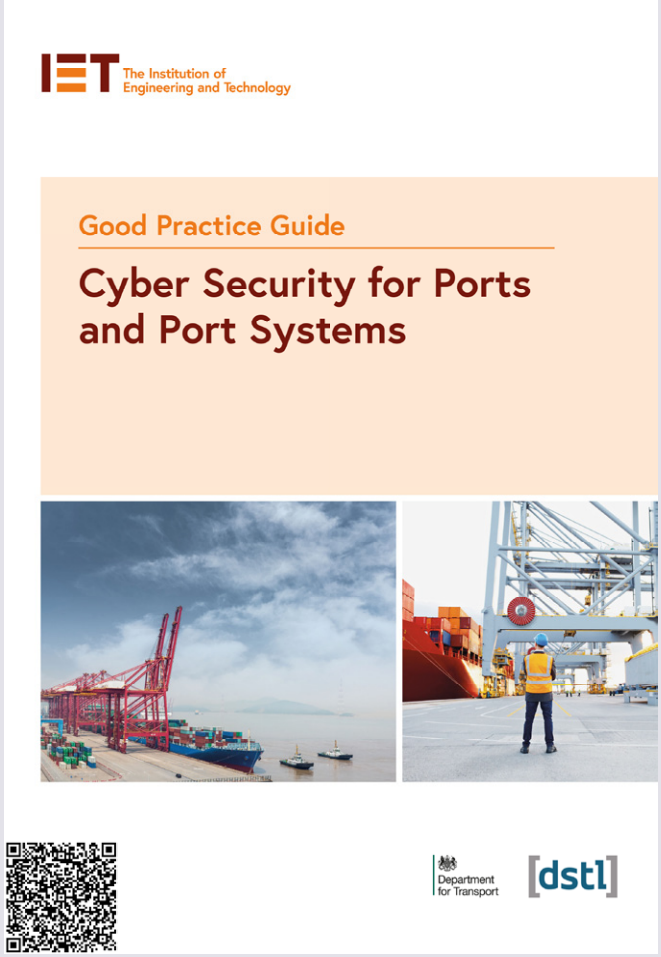
Activating the Executive Crisis Management team is essential, and IT must be a part of this group as it plays a critical role to ensure operations, communications, and business can continue.

Taking a crisis team approach, incorporating clear communications, will also help to ensure business continuity planning, where the sharing of responsibility for essential functions among airport business units and employees, contractors, tenants, and federal agencies is clearly understood. Airports can make use of emerging and existing technologies to help facilitate all of these efforts.

In addition to the airport crisis management team, airports should establish an IT response team. This should be done even where the airport operator is only partially responsible for IT infrastructure. This multi-disciplinary team should comprise representatives from all entities providing services at the airport in order to validate IT business continuity plans, or to create one.

UK Government publishes cyber-sec guidance for ports

The **UK Department of Transport** (DtF) released its new cyber security code of practice on cyber security for UK ports as an answer to the growing threat of cyber-based attacks, which can be no longer neglected by the industry. According to the published information, cyber-attacks on port systems are not a hypothetical threat. Given examples include the 2017 NotPetya virus attack on **Maersk**, which led to losses estimated at well over $200m. Also mentioned are incidents in which port assents have been infected with malware, and there has been unintentional jamming of interference with wi-fi networks. The document poses four questions, related to possible disruption of operations, physical or reputational loss or damage or vulnerability of assets and underscores that if even one of these were to be answered with a 'yes', then the guidance should be considered 'essential reading'. Release of the report coincided with the beginning of UK ports by the country's Maritime Minister, **Nusrat Ghani MP**. Ghani said in a statement, "[…] I'm clear this Government is committed to ensure the UK continues to benefit from our world-leading maritime sector. That's why we've released refreshed cyber security guidance for ports today, to make sure that our ports aren't just some of the best in the world but also some of the safest too." DfT produced the report in collaboration with the **Institution of Engineering and Technology**. It is a revised version of code on cyber security for ports published back in 2016. DfT noted that the guidance should be used in conjunction with the Cyber Security for Ships Guidance, published in 2017. The document can be downloaded from DfT's website.


IET The Institution of Engineering and Technology

Good Practice Guide

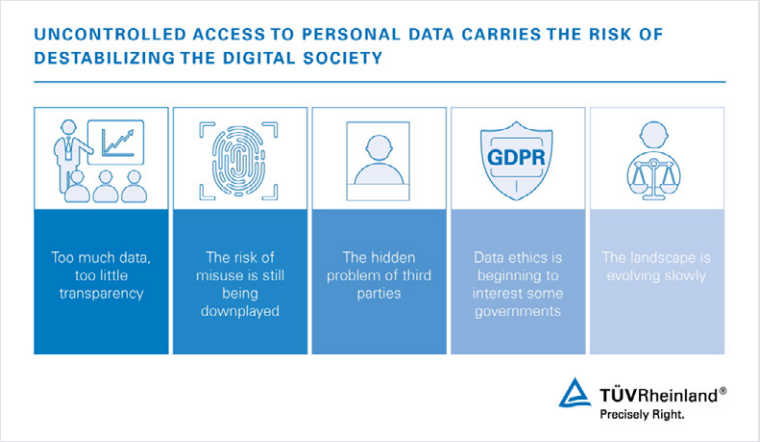
Cyber Security for Ports and Port Systems

Seven cyber-security trends for 2020

Compiled by TÜV Rheinland, a German provider of testing, inspection and certification services, the list includes attacks on smart supply chains, threats to medical equipment and weaknesses in real-time operating systems.

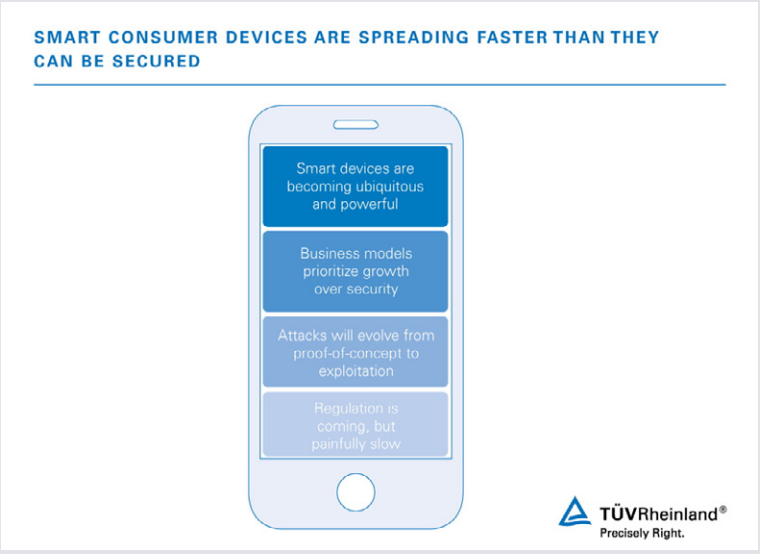
I. Uncontrolled access to personal data carries the risk of destabilizing the digital society

In 2017, Frenchwoman Judith Duportail asked a dating app company to send her any personal information they had about her. In response, she received an 800-page document containing her Facebook likes and dislikes, the age of the men she had expressed interest in, and every single online conversation she had had with all 870 matching contacts since 2013. The fact that Judith Duportail received so much personal data after several years of using a single app underscores the fact that data protection is now very challenging. In addition, this example shows how little transparency there is about securing and processing data that can be used to gain an accurate picture of an individual's interests and behavior.



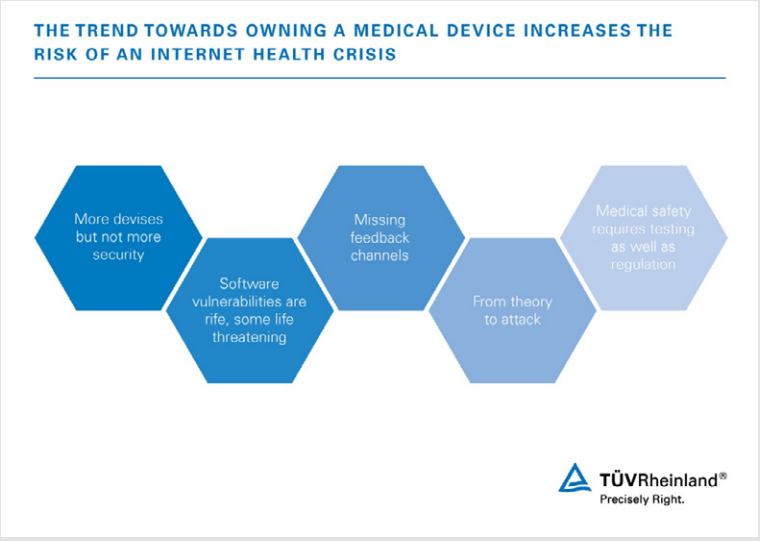
II. Smart consumer devices are spreading faster than they can be secured

Smart speakers, fitness trackers, smart watches, thermostats, energy meters, smart home security cameras, smart locks and lights are the best-known examples of the seemingly unstoppable democratization of the "Internet of many Things". Smart devices are no longer just toys or technological innovations. The number and performance of individual "smart" devices is increasing every year, as these types of device are quickly becoming an integral part of everyday life. It is easy to see a future in which the economy and society will become dependent on them, making them a very attractive target for cyber criminals. Until now, the challenge for Cybersecurity has been to protect one billion servers and PCs. With the proliferation of smart devices, the attack surface could quickly increase hundreds or thousands of times.



III. The trend towards owning a medical device increases the risk of an Internet health crisis

Over the past ten years, personal medical devices such as insulin pumps, heart and glucose monitors, defibrillators and pacemakers have been connected to the Internet as part of the "Internet of Medical Things" (IoMT). At the same time, researchers have identified a growing number of software vulnerabilities and demonstrated the feasibility of attacks on these products. This can lead to targeted attacks on both individuals and entire product classes. In some cases, the health information generated by the devices can also be intercepted. So far, the healthcare industry has struggled to respond to the problem - especially when the official life of the equipment has expired. As with so many IoT devices of this generation, networking was more important than the need for Cybersecurity. The complex task of maintaining and repairing equipment is badly organized, inadequate or completely absent.



IV. Vehicles and transport infrastructure are new targets for cyberattacks

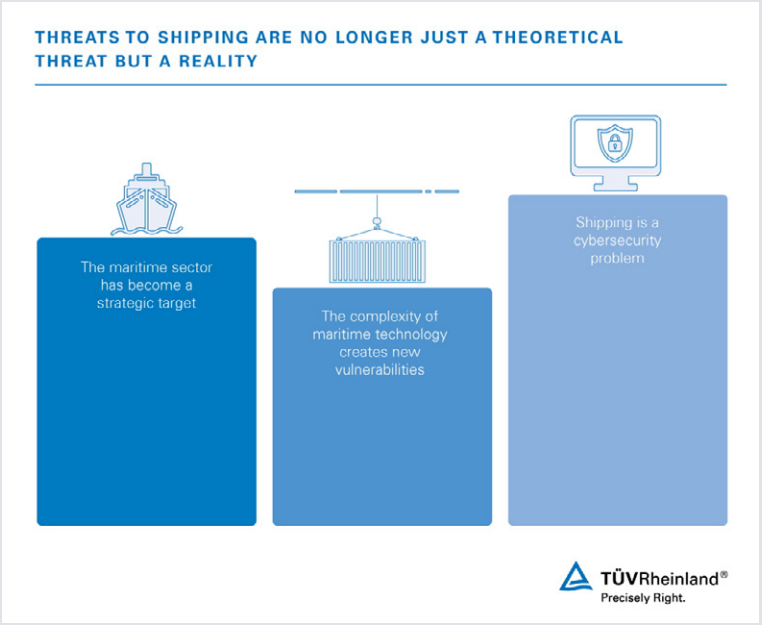
Through the development of software and hardware platforms, vehicles and transport infrastructure are increasingly connected. These applications offer drivers more flexibility and functionality, potentially more road safety, and seem inevitable given the development of self-propelled vehicles. The disadvantage is the increasing number of vulnerabilities that attackers could exploit – some with direct security implications. Broad cyberattacks targeting transport could affect not only the safety of individual road users, but could also lead to widespread disruption of traffic and urban safety.

V. Hackers target smart supply chains and make them "dumb"

With the goal of greater efficiency and lower costs, smart supply chains leverage Internet of Things (IoT) automation, robotics and big data management – those within a company and with their suppliers. Smart supply chains increasingly represent virtual warehousing, where the warehouse is no longer just a physical building, but any place where a product or its components can be located at any time. Nevertheless, there is a growing realization that this business model considerably increases the financial risks, even with only relatively minor disruptions. Smart supply chains are dynamic and efficient, but are also prone to disruptions in processes. Cyberattacks can manipulate information about deposits. Thus, components would not be where they are supposed to be.

VI. Threats to shipping are no longer just a theoretical threat but a reality

In 2017, goods with an estimated weight of around 10.7 billion tons were transported by sea. Despite current geopolitical and trade tensions, trade is generally expected to continue to grow. There is ample evidence that states are experimenting with direct attacks on ship navigation systems. At the same time, attacks on the computer networks of ships used to extort ransom have been reported. Port logistics offers a second, overlapping area of vulnerability. Many aspects to shipping that can be vulnerability to attack such as ship navigation, port logistics and ship computer network. Attacks can originate from states and activist groups. This makes monitoring and understanding a key factor in modern maritime Cybersecurity.



VII. Vulnerabilities in real-time operating systems could herald the end of the patch age

It is estimated that by 2025 there will be over 75 billion networked devices on the Internet of Things, each using its own software package. This, in turn, contains many outsourced and potentially endangered components. In 2019, Armis Labs discovered eleven serious vulnerabilities (called "Urgent/11") in the real-time operating system (RTOS) Wind River VxWorks. Six of these flaws exposed an estimated 200 million IoT devices to the risk of remote code execution (RCE) attacks. This level of weakness is a major challenge as it is often deeply hidden in a large number of products. Organizations may not even notice that these vulnerabilities exist. In view of this, the procedure of always installing the latest security updates will no longer be effective.

Photo: Wikipedia

featured article

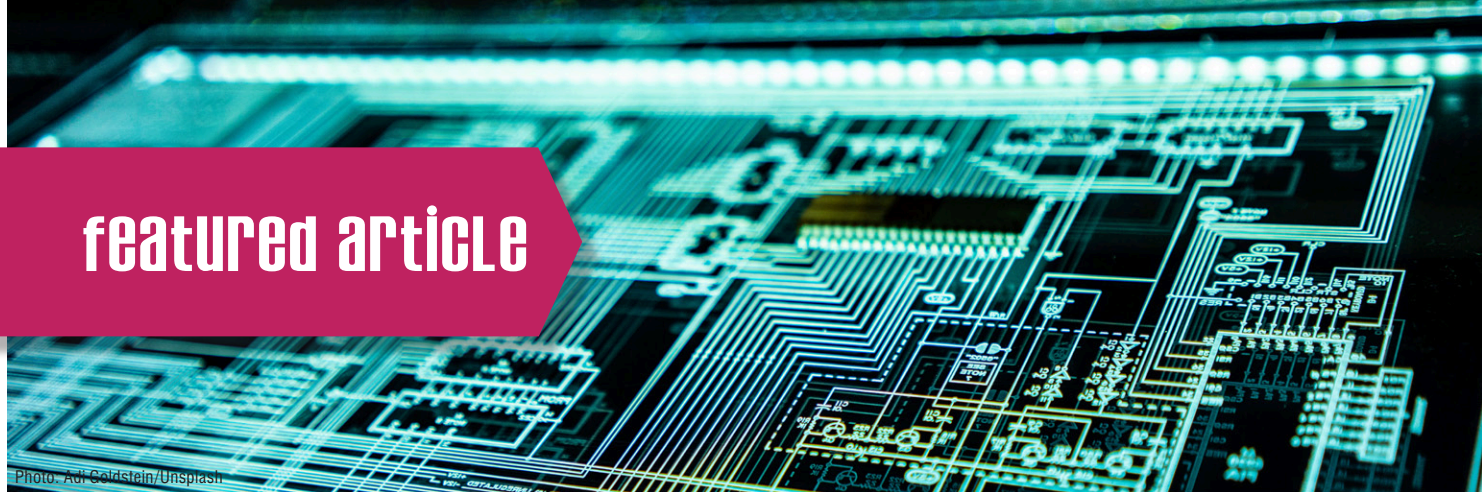


Photo: Adi Goldstein/Unsplash

After the pandemic: Cyber security becomes more important than ever

by **Lars Jensen**, *CEO, SeaIntelligence Consulting*

The world is in the midst of an economic downturn brought on by the pandemic spread of the coronavirus. Clearly, this means that in the short term most companies, including those in the maritime sector, are focused on economic survival.

One of the crucial aspects faced by the companies right now is the ability to continue to operate critical business functions while the staff is working from home. Another critical aspect is how to keep ports and vessels functioning when there is a clear problem related to port closures when workers fall ill, as well as how to keep vessels in operation when crew changes are near impossible in many locations.

But, eventually, the world will emerge after the initial impact of the pandemic, and we should, therefore, also consider how the pandemic might impact the maritime industry longer term. One of the major influences will be a sharp acceleration of the digitalisation of the industry – but with this acceleration also comes a new systemic risk which must be taken into account at the outset.

The acceleration of digital tools

The digital transformation has already been underway for a long time in the maritime industry. The first wave took place in the early 2000s, where a range of digital tools was developed and deployed. These were tools such as, for example, electronic bills of lading, online booking facilities, online brokerages, electronic exchange of shipping instructions, capacity allocation auction tools, and a plethora of other tools. With very few exceptions, the majority of these digital tools failed to gain traction in the maritime industry. The stakeholders – shipping lines and customers alike - simply did not have the motivation to transform their business models accordingly.

In the past three to four years there has been a new surge in the development of maritime digital tools – both related to software as well as hardware related to sensor technology and Internet of Things in general. Before the pandemic, we were at a point where many promising technologies had been implemented on a pilot-testing basis, and a few were also beginning to see a more rapid wide-spread adoption. In other words, the industry was literally at the cusp of a genuine digital transformation.

The pandemic suddenly forced most people to work from home, and this became an overnight test of the usefulness and resilience of the digital tools. In terms of a digital transformation for the industry, this will serve to sharply accelerate the development for two reasons.

One reason is that everyone in the supply chain will get to experience firsthand which tools and functionalities work well in getting the job done. The tools that pass this test will be implemented quickly and widely after the pandemic since they have clearly proven their value.

The other reason is that the current situation mercilessly exposes the gaps in the shipping processes where we still rely on manual processes. We have seen cases where cargo could not be taken out of the port because the necessary customs documents were not available. The reason they were not available was that the exporters did not provide the requested documentation to the importer – documentation which had to be in the form of signed physical papers. The importer was

unable to provide these as they were under curfew due to the pandemic. These gaps are now becoming extremely visible and provide a clear and unmistakable business case for why and how to also digitalise these processes rapidly once we are through the pandemic.

The net-effect of the pandemic will, therefore, be a sharp acceleration of a trend which was already slowly gearing up.

The same effect will happen to the automation of equipment in ports as well as the development of more autonomous functions on vessels. Existing tools are being "battle-tested," and the case for more automation to make the business more resilient will be made clear. This is also a trend that was already in motion but perhaps just slightly earlier on the curve than the software dealing with the informational flow.

The need to build cyber security into our processes

But as we accelerate the digital transformation, it is imperative to also consider the cyber security aspects. The use of more digital tools will naturally increase the industry's vulnerability to cyber- attacks. This should not be used as an argument to hold back on digitalisation but instead be seen as an argument to think cyber security into the new tools and business processes.

The problem right now is that the maritime industry has been somewhat slow in embracing cyber security. Positive developments have been seen in recent years, but when we are the cusp of a rapid digital transformation, the cyber agenda needs to be elevated as well.

But is the risk real? The problem is that many cyber-attacks are not publicly reported as companies for a variety of reasons elect not to make such information available. This means there is an element of under-reporting which also leads some to the conclusion the risk is not that great.

But looking at just the past few years amply demonstrate that the risk is real and genuine. The largest example was the cyber-attack that hit Maersk in June 2017 and brought all digital functions down for the carrier for days, and a full restoration of all systems and functions took up to a year. COSCO was then hit by a cyber-attack in 2018 which brought a range of tools in the US down, but the attack did not spread beyond the US apparently due to their systems not being very interconnected. At the time of writing this article, MSC's online tools have been down for four days as their servers at the headquarters had to be shut down. The carrier has not publicly confirmed that this was due to a cyber-attack, but the unfolding events strongly suggest this to be the case. This means that within less than three years, we have seen cyber-attacks bring down key digital functionalities for all of the three largest container carriers.

As we are embarking on a digital transformation, this means that maritime companies will increase their reliance on digital tools sharply in the coming years. This, by extension, also means that the impact of a successful cyber-attack just a few years from now will be much more severe than what we are seeing today.

The reality is that it is not possible to 100% prevent a cyber-attack. More clearly can, and should, be done in the industry to reduce not only the likelihood of a cyber-attack being successful but also to reduce the magnitude of the impact when an attack is successful. But even when this is done, there is still an element of risk. This is no different than operating a ship – we have a wide range of safety procedures, yet we cannot 100% prevent accidents at sea. We still see ships catching on fire, colliding with each other or getting grounded. On the topic of cyber, we need to minimize the risk, and more can clearly be done in the industry.

But just as importantly, all maritime companies need to have a very clear contingency plan for how to handle a situation where they have been successfully impacted. This can happen to anyone – as evidenced by the three largest container carriers. The contingency plan needs to include not only a robust plan for getting critical systems back up and running quickly but also a practical plan for leveraging the one asset which is not impacted by a cyber-attack: people. Having skilled people who are able to handle the critical functions in an interim period while the systems are down should be seen as an integral part of the cyber readiness posture.

Move ahead – with speed and care

In conclusion, all maritime stakeholders need to prepare for a rapid digital transformation. Perhaps not as much in 2020 where the objective is pure financial survival while the pandemic rages, but when the market rebound happens, most likely in 2021, the change will be swift.

At the same time, it becomes necessary to carefully develop and plan a cyber readiness strategy to minimize the systemic risks which inevitably follow the digitalisation. And it is much more efficient to do this at the planning stages of the digital transformation than trying to apply it "on top of" an already agreed digital plan. ■

Jars Jensen is a leading container shipping expert, having analyzed the industry for the past 20 years, as well as the founder of several companies in the sector, covering analytics, cyber security and training.

Photo: Alex Andrews/Pexels

Navigating in an Online World

by **Anu Khurmi**, *Managing Director, Global Services, Templar Executives*

The world remains in the grip of a global pandemic and alongside essential frontline sectors, our dependency on the maritime industry and seafaring community has never been greater. The International Maritime Organisation (IMO) Secretary-General Kitack Lim has noted: "In these difficult times, the ability for shipping services and seafarers to deliver vital goods, including medical supplies and foodstuffs, will be central to responding to, and eventually overcoming, this pandemic."

Anu Khurmi is an experienced business leader, working across all of Templar Business divisions in the development and delivery of strategic global business. This involves engaging with Governments, regulators and private sector organisations across key industries, including maritime, to promote and provide Cyber Security and Information Assurance Advisory services and solutions. Anu is also leading on the Maritime Cyber Response Team (MCERT), an international industry initiative aimed at helping achieve the IMO 2021 requirements, and the Templar Cyber Academy for Maritime (T-CAM), focused on developing Cyber resilience and awareness within the Maritime sector.
For more information please contact: enquiries@templarexecs.com, or phone: +44 (0)844 443 6243 or visit: www.templarexecs.com

As the response to COVID-19 dominates political and national agendas, the global lockdown is having major impacts on the critical issues of crew changeovers, repatriation of personnel and port entry for vessels. There are growing calls from industry leaders to urgently address these challenges and support the key workers who are making the flow of goods, services and trade possible. However, these are not the only issues facing maritime stakeholders at a time when safety, security and stability are paramount.

The maritime sector has long been combatting threats posed by state and non-state actors, pirates, organised criminal gangs and in recent times, growing Cyber Security risks. Almost overnight the requirements for social distancing, travel restrictions, curfews, port closures and lockdowns, have thrown into sharp focus the ruthlessness and digital prowess of these threat actors, who are unhampered by any rules. The COVID-19 pandemic has highlighted their ability to exploit vulnerabilities and we are seeing a proliferation of Cyber attacks and scams being reported on an unprecedented scale.

This month, the International Chamber of Commerce (ICC) warned of scammers exploiting the spread of the COVID-19 pandemic to carry out fraudulent activities and Cyber threats. The US Navy is not alone in advising that, "… the COVID-19 pandemic presents an opportunity for malicious actors to conduct spear-phishing campaigns, financial scams, and disinformation campaigns via social media to collect sensitive information, steal money via fake donation websites, spread false information and deliver malware to victims." A joint alert from the United States Department of Homeland Security (DHS), Cyber Security and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) notes the various methods that Advanced Persistent Threat (APT) groups and Cyber criminals are using to target individuals, small and medium enterprises, and large organisations with COVID-19 related malicious Cyber activity. These Cyber exploits are also more likely to

Photos: Templar Executives

succeed as businesses rapidly deploy and ramp up remote working for employees.

Yet the current situation is also serving as a wakeup call and opportunity for individuals and businesses who are having to adjust en masse to different ways of working. The maritime sector like many other industries, has been automating and digitalising at pace to create greater operational efficiencies and productivity, but it has been notoriously slow in addressing the accompanying Cyber Security issues. Flag states, regulatory bodies and maritime associations have been advocating the need for better 'Cyber hygiene' to enable the safety and security of all those working in the sector and to ensure its future resilience. The International Maritime Organisation's Resolution on 'Maritime Cyber Risk Management in Safety Management Systems', due to be implemented in January 2021, mandates that shipping firms properly address Cyber risks within existing safety management systems. These regulations require stakeholders to "raise awareness on the Cyber risk", "embed a culture of Cyber risk awareness", "respond quickly to a Cyber incident" and "notify other parties quickly".

The Digital Container Shipping Association this month unveiled its 'DCSA Implementation Guide for Cyber Security on Vessels', a document intended to support cargo ships as they prepare for the IMO Resolution. In addition, national data protection laws and requirements, such as the General Data Protection Regulation (GDPR), are forcing compliance and accountability at Board-level for reporting data breaches of sensitive and personal information. In all of these instances, common recommendations include the need for greater Cyber Security awareness amongst employees and for organisations to have effective business continuity plans.

The same guidance also applies for those who have been catapulted into a world of working and socialising online. Education and training are key to creating a vigilant workforce and embedding a culture of "Cyber risk awareness" and best practices. A proactive approach to organisational resilience includes implementing measures such as regular patching, equipping all devices with up-to-date antivirus software, threat monitoring and email services with protective features. International industry initiatives such as the Maritime Cyber Emergency Response Team (MCERT)[1], offer a platform for sector collaboration and Cyber emergency response services, invaluable when IT skills and resources are finite and budgets stretched.

Today business leaders face a complex and uncharted landscape; as they navigate how their organisations survive the present, they also have an opportunity to consider how they can thrive in the future. For the maritime sector and its significant seafaring community, this is a time for acknowledging that effective Cyber Security is integral to business resilience and enablement. Proactive and defensive measures usually left to the ICT Department should be part of an informed business process, delivering quantifiable benefits and reflecting upon the level of risk the Board is willing to take and justify. Investment in education and Cyber best practices should create a sustainable culture to keep employees safe and productive, and businesses protected and operational. This is critical in a sector responsible for carrying over 90% of the world's trade by sea and essential for future prosperity . ■

[1] *https://www.maritimecert.org/*

The Port of Opportunities

The Port of HaminaKotka is a versatile Finnish seaport serving trade and industry. The location of HaminaKotka at the logistics hub makes the port truly unique – it opens up connections to all parts of the world.

Welcome to the port of HaminaKotka!

haminakotka.com

PORT OF HAMINAKOTKA

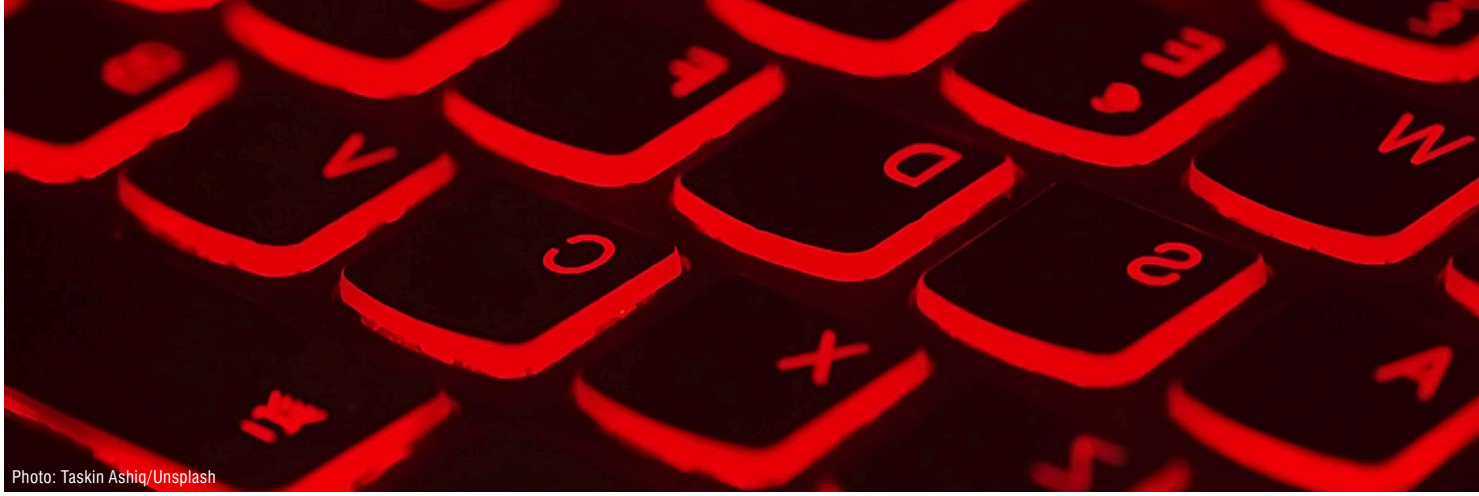


Photo: Taskin Ashiq/Unsplash

The risk-based approach to cybersecurity

by **Jim Boehm, Nick Curcio, Peter Merrath, Lucy Shenton,** and **Tobias Stähle**

The most sophisticated institutions are moving from a "maturity based" to a "risk based" approach for managing cyberrisk. Here is how they are doing it.

Top managers at most companies recognize cyberrisk as an essential topic on their agendas. Worldwide, boards and executive leaders want to know how well cyberrisk is being managed in their organizations. In more advanced regions and sectors, leaders demand, given years of significant cybersecurity investment, that programs also prove their value in risk-reducing terms. Regulators are challenging the levels of enterprise resilience that companies claim to have attained. And nearly everyone – business executives, regulators, customers, and the general public – agrees that cyberrisk is serious and calls for constant attention (Exhibit 1).

What, exactly, organizations should do is a more difficult question. This article is advancing a "risk based" approach to cybersecurity, which means that to decrease enterprise risk, leaders must identify and focus on the elements of cyberrisk to target. More specifically, the many components of cyberrisk must be understood and prioritized for enterprise cybersecurity efforts. While this approach to cybersecurity is complex, best practices for achieving it are emerging.

To understand the approach, a few definitions are in order. First, our perspective is that cyberrisk is "only" another kind of operational risk. That is, cyberrisk refers to the potential for business losses of all kinds – financial, reputational, operational, productivity related, and regulatory related – in the digital domain. Cyberrisk can also cause losses in the physical domain, such as damage to operational equipment. But it is important to stress that cyberrisk is a form of business risk.

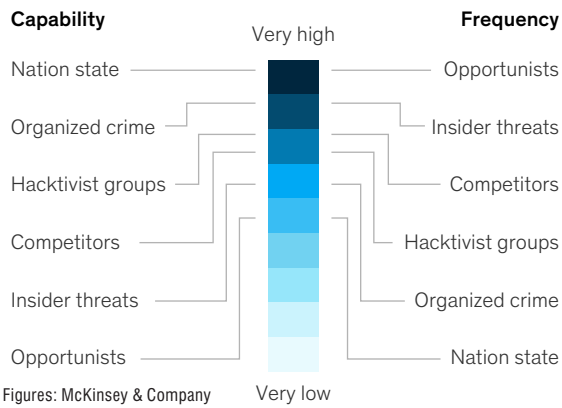
Furthermore, cyberrisks are not the same as cyberthreats, which are the particular dangers that create the potential for cyberrisk. Threats include privilege escalation, vulnerability exploitation, or phishing. 1 Cyberthreats exist in the context of enterprise cyberrisk as potential avenues for loss of confidentiality, integrity, and availability of digital assets. By extension, the risk impact of cyberthreats includes fraud, financial crime, data loss, or loss of system availability.

Decisions about how best to reduce cyberrisk can be contentious. Taking into account the overall context in which the enterprise operates, leaders must decide

Exhibit 1

Cyberthreats are growing in severity and frequency.

Cyberthreat capacity and frequency today, threat actor



Figures: McKinsey & Company

Jim Boehm is an associate partner in McKinsey's Washington, DC, office; Nick Curcio is a cyber solutions analyst in the New York office; Peter Merrath is an associate partner in the Frankfurt office, where Tobias Stähle is a senior expert; and Lucy Shenton is a cyber solutions specialist in the Berlin office. The authors wish to thank Rich Isenberg for his contributions to this article.

which efforts to prioritize: Which projects could most reduce enterprise risk? What methodology should be used that will make clear to enterprise stakeholders (especially in IT) that those priorities will have the greatest risk reducing impact for the enterprise? That clarity is crucial in organizing and executing those cyber projects in a focused way.

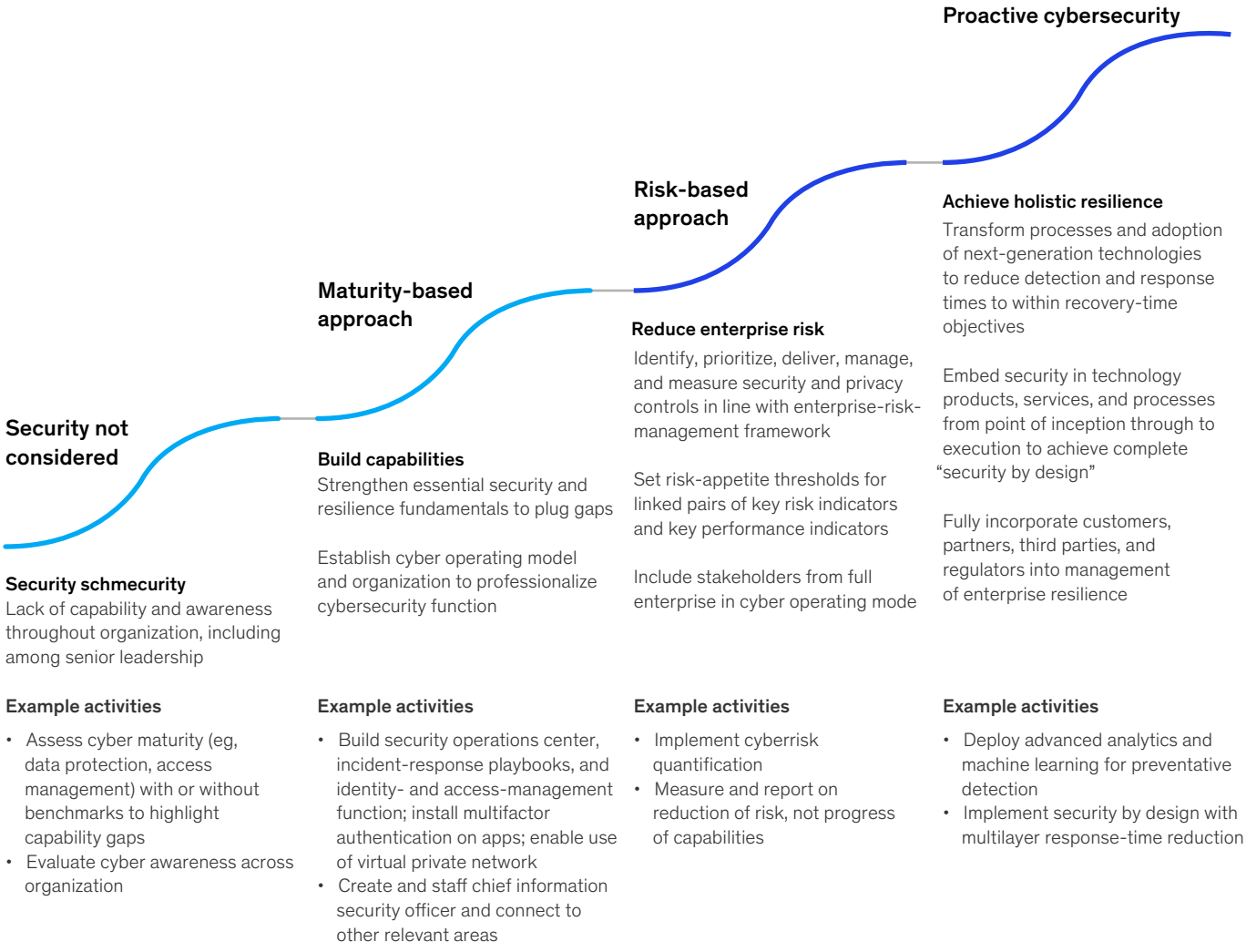
At the moment, attackers benefit from organizational indecision on cyberrisk - including the prevailing lack of clarity about the danger and failure to execute effective cyber controls. Debilitating attacks on high-profile institutions are proliferating globally, and enterprise-wide cyber efforts are needed now with great urgency. It is widely understood that there is no time to waste: business leaders everywhere, at institutions of all sizes and in all industries, are earnestly searching for the optimal means to improve cyber resilience. We believe we have found a way to help.

The maturity-based cybersecurity approach: A dog that's had its day

Even today, "maturity based" approaches to managing cyberrisk are still the norm. These approaches focus on achieving a particular level of maturity by building certain capabilities. To achieve the desired level, for example, an organization might build a security operations center (SOC) to improve the maturity of assessing, monitoring, and responding to potential threats to enterprise information systems and applications. Or it might implement multifactor authentication (MFA) across the estate to improve maturity of access control. A maturity-based approach can still be helpful in some situations: for example, to get a program up and running from scratch at an enterprise that is so far behind it has to "build everything." For institutions that have progressed even a step beyond that, however, a maturity-based approach is inadequate. It can never be

Exhibit 2

For many companies, the risk-based approach is the next stage in their cybersecurity journey.



more than a proxy for actually measuring, managing, and reducing enterprise risk.

A further issue is that maturity-based programs, as they grow organically, tend to stimulate unmanageable growth of control and oversight. In monitoring, for example, a maturity-based program will tend to run rampant, aspiring to "monitor everything." Before long, the number of applications queued to be monitored across the enterprise will outstrip the capacity of analysts to monitor them, and the installation of monitors will bog down application-development teams. The reality is that some applications represent more serious vulnerabilities – and therefore greater potential for risk – than others. To focus directly on risk reduction, organizations need to figure out how to move from a stance of monitoring everything to one in which particular applications with high risk potential are monitored in particular ways.

Another issue related to the monitor-everything stance is inefficient spending. Controls grow year after year as program planning for cybersecurity continues to demand more spending for more controls. But is enterprise risk being reduced? Often the right answers lie elsewhere: for example, the best return on investment in enterprise-risk reduction is often in employee awareness and training. Yet a maturity-based model does not call for the organization to gather enough information to know that it should divert the funding needed for this from additional application monitoring. Spending on both will be expected, though the one effort (awareness and training) may have a disproportionate impact on enterprise-risk reduction relative to the other.

If the objective is to reduce enterprise risk, then the efforts with the best return on investment in risk reduction should draw the most resources. This approach holds true across the full control landscape, not only for monitoring but also for privileged-access management, data-loss prevention, and so forth. All of these capabilities reduce risk somewhat and somehow, but most companies are unable to determine exactly how and by how much.

The final (and most practical) drawback of maturity-based programs is that they can create paralyzing implementation gridlock. The few teams or team members capable of performing the hands-on implementation work for the many controls needed become overloaded with demand. Their highly valuable attention is split across too many efforts. The frequent result is that no project is ever fully implemented and program dashboards show perpetual "yellow" status for the full suite of cyber initiatives.

The truth is that in today's hyperconnected world, maturity-based cybersecurity programs are no longer adequate for combatting cyberrisks. A more strategic, risk-based approach is imperative for effective and efficient risk management (Exhibit 2).

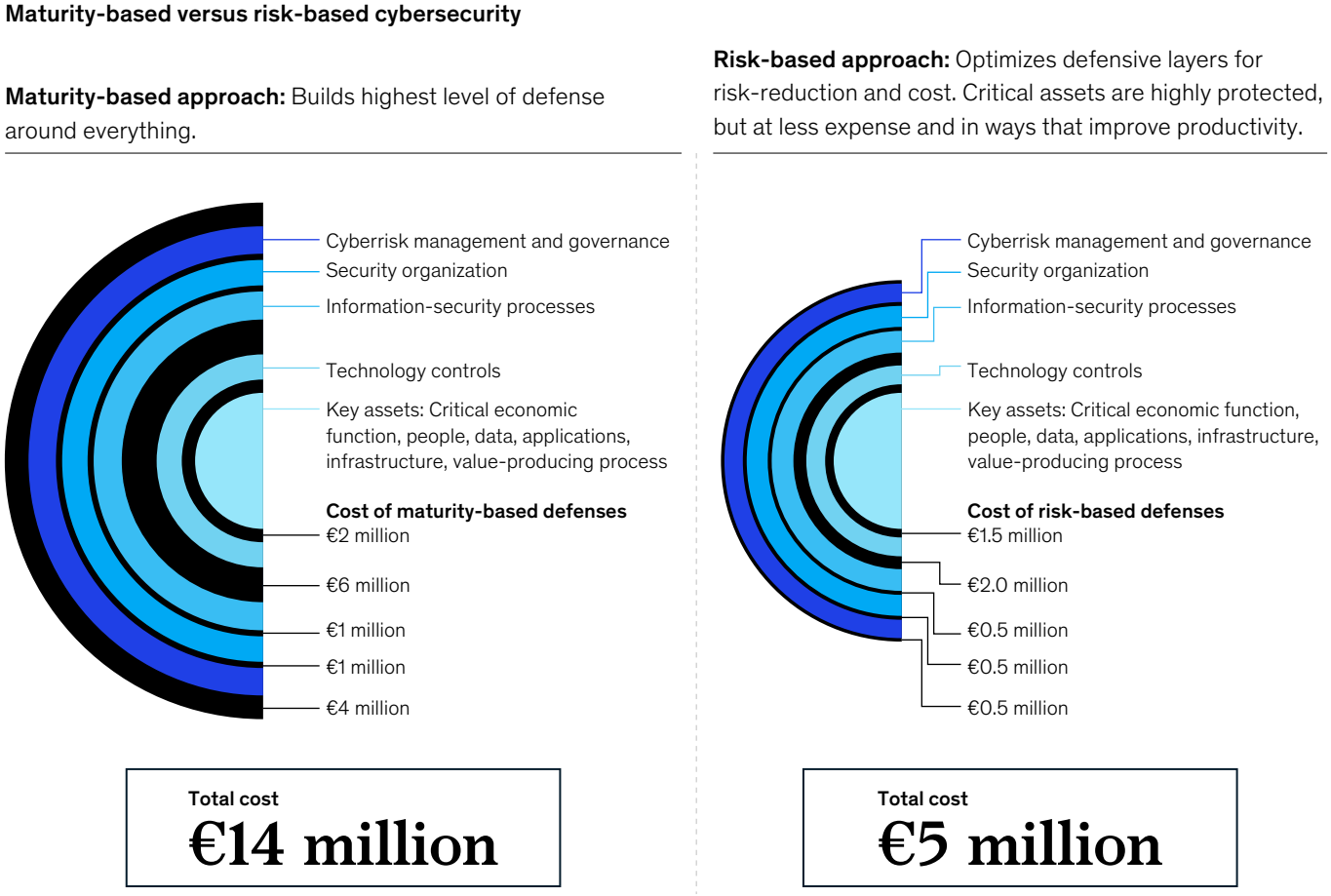
Reducing risk to target appetite at less cost

The risk-based approach does two critical things at once. First, it designates

Exhibit 3

A risk-based approach builds customized controls for a company's critical vulnerabilities to defeat attacks at lower overall cost.

Maturity-based versus risk-based cybersecurity



Note: Costs are illustrative but extrapolated from real-world examples and estimates.

risk reduction as the primary goal. This enables the organization to prioritize investment – including in implementation-related problem solving – based squarely on a cyber program's effectiveness in reducing risk. Second, the program distills top management's risk-reduction targets into precise, pragmatic implementation programs with clear alignment from the board to the front line. Following the risk-based approach, a company will no longer "build the control everywhere"; rather, the focus will be on building the appropriate controls for the worst vulnerabilities, to defeat the most significant threats – those that target the business's most critical areas. The approach allows for both strategic and pragmatic activities to reduce cyberrisks (Exhibit 3).

Companies have used the risk-based approach to effectively reduce risk and reach their target risk appetite at significantly less cost. For example, by simply reordering the security initiatives in its backlog according to the risk-based approach, one company increased its projected risk reduction 7.5 times above the original program at no added cost. Another company discovered that it had massively overinvested in controlling new software-development capabilities as part of an agile transformation. The excess spending was deemed necessary to fulfill a promise to the board to reach a certain level of maturity that was, in the end, arbitrary. Using the risk-based approach, the company scaled back controls and spending in areas where desired digital capabilities were being heavily controlled for no risk-reducing reason. A particular region of success with the risk-based approach has been Latin America, where a number of companies have used it to leapfrog a generation of maturity-based thinking (and spending). Instead of recapitulating past inefficiencies, these companies are able to build exactly what they need to reduce risk in the most important areas, right from the start of their cybersecurity programs. Cyber attackers are growing in number and strength, constantly developing destructive new stratagems. The organizations they are targeting must respond urgently, but also seek to reduce risk smartly, in a world of limited resources.

A transformation in sequential actions

Companies adopting the risk-based approach and transforming their "run" and "change" activities accordingly inevitably face the crucible of how to move from maturity-based to risk-based cybersecurity. From the experience of several leading institutions, a set of best-practice actions has emerged as the fastest path to achieving this transformation. These eight actions taken roughly in sequence will align the organization toward the new approach and enable the appropriate efforts to reduce enterprise risk.

1. Fully embed cybersecurity in the enterprise-risk-management framework.
2. Define the sources of enterprise value across teams, processes, and technologies.
3. Understand the organization's enterprise-wide vulnerabilities – among people, processes, and technology – internally and for third parties.
4. Understand the relevant "threat actors," their capabilities, and their intent.
5. Link the controls in "run" activities and "change" programs to the vulnerabilities that they address and determine what new efforts are needed.
6. Map the enterprise risks from the enterprise-risk-management framework, accounting for the threat actors and their capabilities, the enterprise vulnerabilities they seek to exploit, and the security controls of the organization's cybersecurity run activities and change program.
7. Plot risks against the enterprise-risk appetite; report on how cyber efforts have reduced enterprise risk.
8. Monitor risks and cyber efforts against risk appetite, key cyberrisk indicators (KRIs), and key performance indicators (KPIs).

1. Fully embed cybersecurity in the enterprise-risk-management framework

A risk-based cyber program must be fully embedded in the enterprise-risk-management framework. The framework should not be used as a general guideline, but rather as the organizing principle. In other words, the risks the enterprise faces in the digital domain should be analyzed and categorized into a cyberrisk framework. This approach demystifies cyberrisk management and roots it in the language, structure, and expectations of enterprise-risk management. Once cyberrisk is understood more clearly as business risk that happens in the digital domain, the organization will be rightly oriented to begin implementing the risk-based approach.

2. Define the sources of enterprise value

An organization's most valuable business work flows often generate its most significant risks. It is therefore of prime importance to identify these work flows and the risks to which they are susceptible. For instance, in financial services, a loan process is part of a value-creating work flow; it is also vulnerable to data leakage, an enterprise risk. A payment process likewise creates value but is susceptible to fraud, another enterprise risk. To understand enterprise risks, organizations need to think about the potential impact on their sources of value.

Identifying the sources of value is a fairly straightforward exercise, since business owners will have already identified the risks to their business. Cybersecurity professionals should ask the businesses about the processes they regard as valuable and the risks that they most worry about. Making this connection between the cybersecurity team and the businesses is a highly valuable step in itself. It motivates the businesses to care more deeply about security, appreciating the bottom-line impact of a recommended control. The approach is far more compelling than the maturity-based approach, in which the cybersecurity function peremptorily informs the business that it is implementing a control "to achieve a maturity of 3.0."

The constituents of each process can be defined – relevant teams, critical information assets ("crown jewels"), the third parties that interact with the process, and the technology components on which it runs – and the vulnerabilities to those constituent parts can be specified.

3. Understand vulnerabilities across the enterprise

Every organization scans its infrastructure, applications, and even culture for vulnerabilities, which can be found in areas such as configuration, code syntax, or frontline awareness and training. The vulnerabilities that matter most are those connected to a value source that particular threat actors with relevant capabilities can (or intend to) exploit. The connection to a source of value can be direct or indirect. A system otherwise rated as having low potential for a direct attack, for example, might be prone to lateral movement – a method used by attackers to move through systems seeking the data and assets they are ultimately targeting.

Once the organization has plotted the people, actions, technology, and third-party components of its value-creating processes, then a thorough identification of associated vulnerabilities can proceed. A process runs on a certain type of server, for example, that uses a certain operating system (OS). The particular server–OS combination will have a set of identified common vulnerabilities and exposures. The same will be true for storage, network, and end-point components. People, process, and third-party vulnerabilities can be determined by similar methodologies.

Of note, vulnerabilities and (effective) controls exist in a kind of reverse symbiosis: where one is present the other is not. Where sufficient control is present, the vulnerability is neutralized; without the control, the vulnerability persists. Thus, the enterprise's vulnerabilities are most practically organized according to the enterprise-approved control framework. 2 Here synergies begin to emerge. Using a common framework and language, the security, risk, IT, and frontline teams can work together to identify what needs to be done to close vulnerabilities, guide implementation, and report on improvements in exactly the same manner and language. Experience confirms that when the entire organization shares a common way of thinking about vulnerabilities, security can be significantly enhanced.

4. Understand relevant threat actors and their capabilities

The groups or individuals an organization must worry about – the threat actors – are determined by how well that organization's assets fit with the attackers' goals – economic, political, or otherwise. Threat actors and their capabilities – the tactics, techniques, and procedures they use to exploit enterprise security – define the organization's threat landscape.

Only by understanding its specific threat landscape can an organization reduce risk. Controls are implemented according to the most significant threats. Threat analysis begins with the question, Which threat actors are trying to harm the organization and what are they capable of? In response, organizations can visualize the vulnerabilities commonly exploited by relevant threats, and appropriate controls can then be selected and applied to mitigate these specific vulnerability areas.

In identifying the controls needed to close specific gaps, organizations need to size up potential attackers, their capabilities, and their intentions – the threat actors' strength and will (intention) to create a risk event. This involves collecting information on and understanding how the attackers connect, technically and nontechnically, to the people, process, and technology vulnerabilities within the enterprise.

5. Address vulnerabilities

To defeat threat actors, vulnerabilities discovered in the third action we describe will either be closed by existing controls – normal run activities or existing change initiatives – or will require new control efforts. For existing controls, the cyber governance team (for "run") and the program management team (for "change") map their current activities to the same control framework used to categorize vulnerabilities. This will show the controls already in place and those in development. Any new controls needed are added to the program backlog as either stand-alone or composite initiatives.

While an organization may not be able to complete all initiatives in the backlog in a single year, it will now be able to choose what to implement from the full spectrum of necessary controls relevant to the enterprise because they are applicable for frustrating relevant threat capabilities. The risk-based approach importantly bases the scope of both existing and new initiatives in the same control framework. This enables an additional level of alignment among teams: delivery teams charged with pushing and reporting on initiative progress can finally work efficiently with the second and third lines of defense (where relevant), which independently challenge control effectiveness and compliance. When the program-delivery team (acting as the first line of defense) sits down with the second and third lines, they will all be speaking the same language and using the same frameworks. This means that the combined groups can discuss what is and is not working, and what should be done.

6. Map the enterprise-risk ecosystem

A map of enterprise risks – from the enterprise-risk-management framework to enterprise vulnerabilities and controls to threat actors and their capabilities – makes visible a "golden thread," from control implementation to enterprise-risk reduction. Here the risk-based approach can begin to take shape, improving both efficiency in the application of controls and the effectiveness of those controls in reducing risks.

Having completed actions one through five, the organization is now in a position to build the risk-based cybersecurity model. The analysis proceeds by matching controls to the vulnerabilities they close, the threats they defeat, and the value-creating processes they protect. The run and change programs can now be optimized according to the current threat landscape, present vulnerabilities, and existing program of controls. Optimization here means obtaining the greatest amount of risk reduction for a given level of spending. A desired level of risk can be "priced" according to the initiatives needed to achieve it, or the entry point for analysis can be a fixed budget, which is then structured to achieve the greatest reduction in risk.

Cybersecurity optimization determines the right level and allocation of spending. Enterprise-risk reduction is directly linked to existing initiatives and the initiation of new ones. The analysis develops the fact base needed for tactical discussions on overly controlled areas whence the organization might pull back as well as areas where better control for value is needed.

By incorporating all components in a model and using the sources of value and control frameworks as a common language, the business, IT, risk, and cybersecurity groups can align. Discussions are framed by applying the enterprise control framework to the highest sources of value. This creates the golden-thread effect. Enterprise leadership (such as the board and the risk function) can identify an enterprise risk (such as data leakage), and the cybersecurity team can report on what is being done about it (such as a data-loss prevention control on technology or a social-engineering control on a specific team). Each part is connected to the other, and every stakeholder along the way can connect to the conversation. The methodology and model is at the center, acting both as a translator and as an optimizer. The entire enterprise team knows what to do, from the board to the front line, and can move in a unified way to do it.

7. Plot risks against risk appetite; report on risk reduction

Once the organization has established a clear understanding of and approach to managing cyberrisk, it can ensure that these concepts are easily visualized and communicated to all stakeholders. This is done through a risk grid, where the application of controls is sized to the potential level of risk (Exhibit 4).

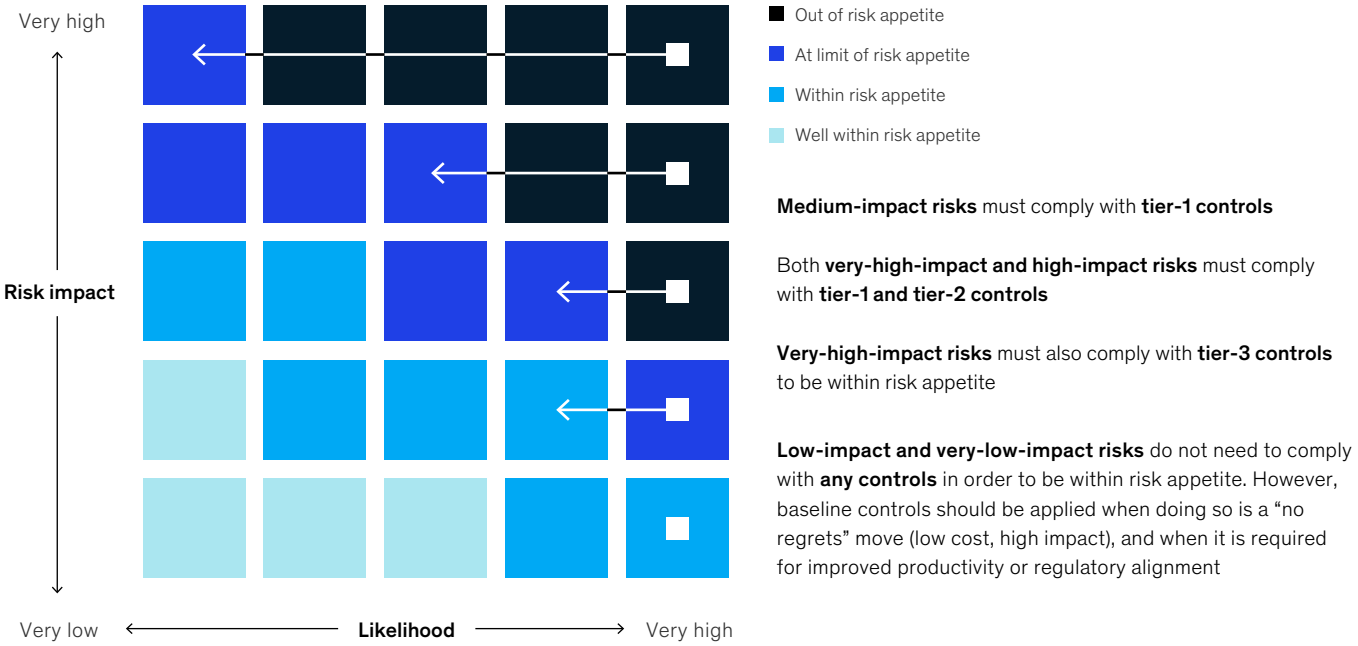
The assumption in this use of the classic risk grid is that the enterprise-risk appetite has been defined for each enterprise risk. The potential impact for each enterprise-risk scenario can then be plotted on the risk grid. Once the relationships among the threats, vulnerabilities, and applied controls are modeled and understood, the risks can be evaluated according to their likelihood. As more controls are applied, the risk levels are reduced to the risk appetite. This is the way the cyber program can demonstrate impact in terms of enterprise-risk reduction.

As new threats emerge, new vulnerabilities will become apparent. Existing controls may become ineffective, and enterprise risks can move in the opposite direction – even to the point where risk-appetite limits are exceeded. For

Exhibit 4

The risk-based approach applies controls according to the risk appetite and the likelihood and potential impact of a risk event.

Risk events by size of impact and likelihood of occurrence



information-security-management systems, the risk grid allows stakeholders to visualize the dynamic relationships among risks, threats, vulnerabilities, and controls and react strategically, reducing enterprise risks to the appropriate risk-appetite level.

8. Monitor risks and cyber efforts using risk appetite and key cyberrisk and performance indicators

At this point, the organization's enterprise risk posture and threat landscape are understood, and the risk-based cybersecurity program is in place. The final step is to monitor and manage for success.

Many companies attempt to measure cyber maturity according to program completion, rather than by actual reduction of risk. If a security function reports that the data-loss-prevention (DLP) program is 30 percent delivered, for example, the enterprise assumption is that risk of data leakage is 30 percent reduced. If a multifactor authentication initiative is 90 percent implemented, the assumption is that the risk of unauthorized access is almost eliminated. These assumptions are false, however, because actual risk-reducing results are not being measured in these examples.

Metrics need to measure both inputs and outputs; inputs in this case are risk-reduction efforts undertaken by the enterprise, while the output is the actual reduction in enterprise risk. The input metric here is a key performance indicator (KPI): measuring the performance of a program or a "run" function. The output metric is really a key risk indicator (KRI), measuring the risk level associated with a potential risk scenario. The thresholds for the KRIs must be tied directly to risk-appetite levels (the KPI thresholds can also be linked in this way). For example, if risk appetite for data leakage is zero, then the systemic controls (and corresponding "red" thresholds) must be higher than they would be if a certain percentage of leakage is allowed over a certain period. Of course, tolerances for cyber incidents may be not always be set at zero. In most cases, it is impossible to stop all cyber attacks, so sometimes controls can be developed that tolerate some incidents.

One way to think about KRIs and KPIs is with regard to the relationship between altitude and trajectory. A KRI gives the current risk level of the enterprise (the "risk altitude") while the KPI indicates the direction toward or away from the enterprise-risk-appetite level ("risk trajectory"). An enterprise may not yet have arrived at the leadership's KRI target but a strong KPI trajectory would suggest that it will soon. Conversely, an enterprise may have hit the desired KRI threshold, but the KPIs of the run activity may be backsliding and give cause for concern.

Executives are often forced to make sense of a long list of sometimes conflicting metrics. By linking KRIs and KPIs, the cybersecurity team gives executives the ability to engage in meaningful problem-solving discussions on which risks are within tolerances, which are not, and why (see the sidebar, "Linking a KRI to a KPI").

The risk-based approach to cybersecurity is thus ultimately interactive – a dynamic tool to support strategic decision making. Focused on business value, utilizing a common language among the interested parties, and directly linking enterprise risks to controls, the approach helps translate executive decisions about risk reduction into control implementation. The power of the risk-based approach to optimize for risk reduction at any level of investment is enhanced by its flexibility, as it can adjust to an evolving risk-appetite strategy as needed.

Many leading companies have a cyber-maturity assessment somewhere in their archives; some still execute their programs to achieve certain levels of maturity. The most sophisticated companies are, however, moving away from the maturity-based cybersecurity model in favor of the risk-based approach. This is because the new approach allows them to apply the right level of control to the relevant areas of potential risk. For senior leaders, boards, and regulators, this means more economical and effective enterprise-risk management. ■

170+ operators

620+ ports

1,130+ services

1,150+ terminals

EUROPEAN
TRANSPORT
MAPS

EUROPE:

all over the ro-ro & ferry,
container, and rail maps

www.**european**transportmaps.com

What's next

Modern ports, shipping, logistics

Small ports vs big issues

EU transport projects

partnership events

ITS European Congress
18-20 May 2020
PT/Lisbon

Baltic LNG & Gas Forum
27-28 May 2020
LT/Klaipeda

Grain & Maritime Days 2020
27-30 May 2020
UA/Odessa

European Environmental Ports Conference 2020
24-25 June 2020
NL/Rotterdam

RailFreight Summit 2020
1-3 September 2020
PL/Poznań

GlobMar 2020
15-17 September 2020
PL/Sopot

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

▪ **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:*** Alan Arent

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

▪ **EDITORIAL TEAM** ▪
▪ ***Editor-in-Chief:*** Przemysław Myszka ▪ przemek@baltic-press.com
▪ ***Content Editor:*** Andrzej Urbaś ▪ andrew@baltic-press.com
▪ ***Proofreading Editor:*** Ewa Kochańska
▪ ***Art Director/DTP:*** Danuta Sawicka

▪ **MARKETING & SALES** ▪
(advertising, exhibitions & conferences)
▪ ***Managing Director:*** Przemysław Opłocki ▪ po@baltic-press.com
▪ ***Marketing & Communications Intern:*** Ewelina Synak ▪ ewelina@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

previous editions

HR#28 PORTS, SHIPPING AND LOGISTICS: MODERN-TURNED-FUTURE

HR#29 CHINA-EUROPETRANSPORT & LOGISTICS

HR#30 BREXIT