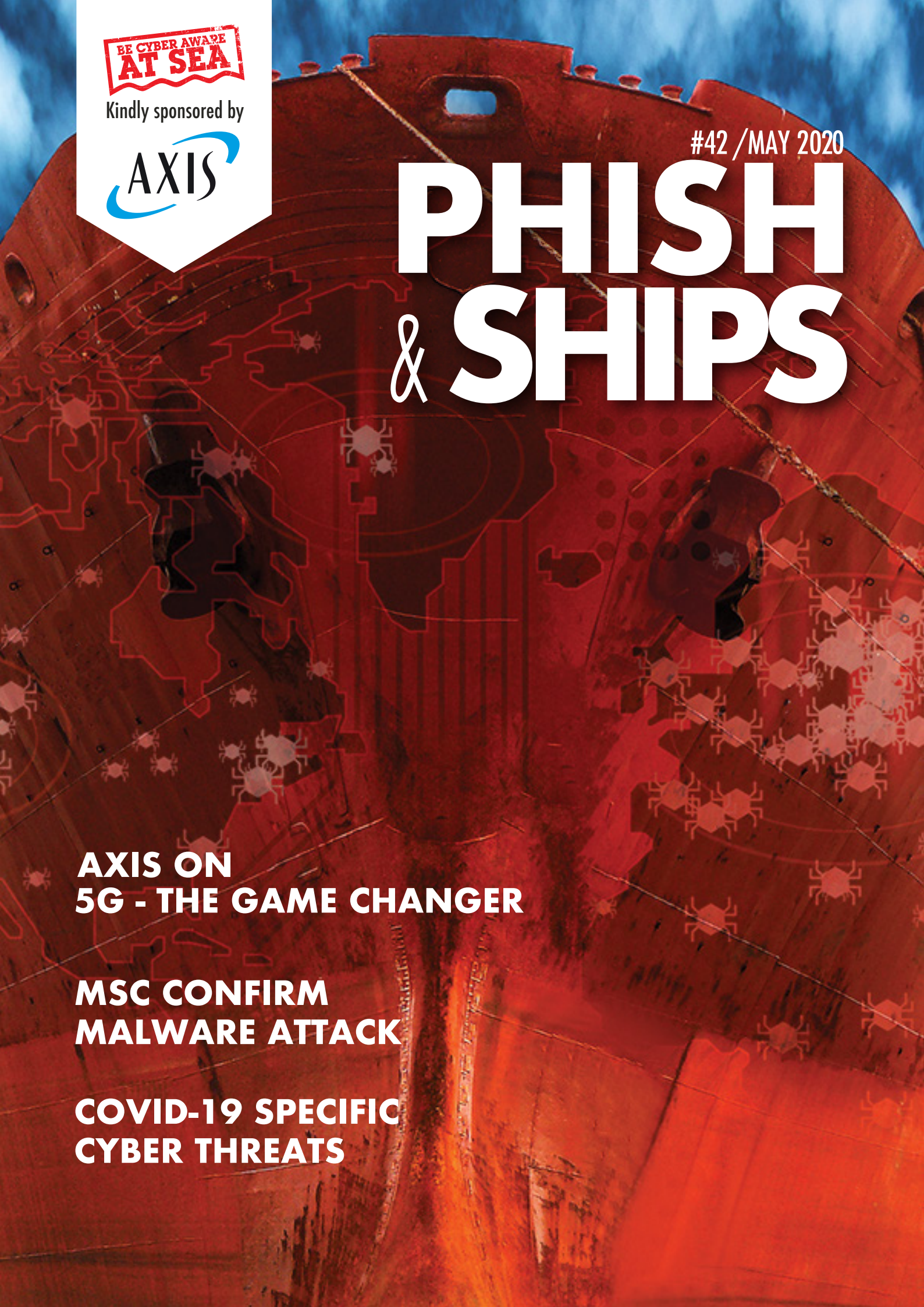

BE CYBER AWARE AT SEA
Kindly sponsored by
AXIS
#42 /MAY 2020
PHISH & SHIPS
AXIS ON 5G - THE GAME CHANGER
MSC CONFIRM MALWARE ATTACK
COVID-19 SPECIFIC CYBER THREATS

FROM THE EDITOR

Welcome to this month's edition of Phish & Ships, brought to you by The Be Cyber Aware at Sea campaign.

COVID-19 continues to dominate the headlines, changing lives worldwide and having a widespread impact upon the maritime and offshore industry, both in terms of the virus and the economic landscape thereafter. We hope that you are all staying safe and well amid the pandemic, wherever you are.

This month we have a mix of news: on the one hand there was another confirmed cyber attack, this time on the MSC, a reminder that online threats are ever present. However, elsewhere we celebrate the steps being taken to protect the industry with the contract between CYSEC and the ESA, a welcome development.

We also look into a few of the ways maritime companies are overcoming obstacles thrown up by COVID-19. With more people requiring more access online to work, cyber challenges continue to flourish but with ingenuity and goodwill, these are being tackled.

Please continue to follow us at:
Website: www.becyberawareatsea.com
Twitter: @CyberAwareAtSea
Facebook: Be Cyber Aware At Sea
Linkedin: Be Cyber Aware At Sea

Your Editor-in-chief,
Jordan Wylie MA, BA (Hons) Founder,
Be Cyber Aware At Sea

OUR AWARDS

WINNER 2018
SMART4SEA TRAINING AWARD

HIGHLY COMMENDED 2017
SAFETY AT SEA AWARDS

WINNER 2017
BEST CYBER AWARENESS CAMPAIGN
INTERNATIONAL CYBERSECURITY AWARD

PHISH & SHIPS

5G - THE GAME CHANGER

BE CYBER AWARE AT SEA
Kindly sponsored by
AXIS

Ostensibly, everywhere you turn these days there are one of three subjects in the news - the coronavirus, U.S. politics and 5G. However, it's 5G that seems to intrigue with the most depth when it comes to cyber-related risks, and an emerging risk we should all try to understand more as it becomes one of the biggest technological advances affecting our lives in 2020 and beyond. This article isn't just about shipping, in fact its about a sweeping technological revolution that will ultimately change all facets of our lives forever…

What is 5G?

5G is the latest (fifth) generation wireless technology for digital cellular networks that will eventually replace - or at least augment, your 4G LTE connection to access the internet and to stay in communication with others, but with exponentially faster download and upload speeds. The time it takes devices to communicate with wireless networks—known as latency—will also drastically decrease. In combination, the remarkably accelerated speed will unlock tremendous opportunities.

A brief history on Cellular telephony

It was introduced some 40 years ago with 1G. Since then, roughly every 10 years we have adopted a new generation – 2G (1990), 3G (2000) and now the widespread 4G (2010). Each generation created a new layer of communication capabilities we now find pedestrian in 2020. The first generation created the framework for wireless phone calls, and was the technology necessary for mobile phones. With the advent of 2G, the networks went digital and could transmit text and image messages. Simply put, 2G brought us texting. The third generation (3G) could transmit much greater amounts of data, meaning users could access the internet, download videos, and moved cellphones beyond calling and texting as the baseline for the smartphone. 4G gifted us the app-based smartphone, with five times faster download speeds than 3G, and allowed the smartphone to take off as arguably essential item in daily life. So what next, with 5G speeds targeted to be 35 times faster than 4G?

How does 5G work?

Virtually every major telecommunication service provider in the developed world has or is developing 5G capable devices - from mobile phones to smart TV's and beyond, and working to deploy antennas in order to connect us to 5G internet speeds. 5G works by connecting our devices to the internet through three unique frequencies of electromagnetic waves: low-band, mid-band and high-band. But it is the high-band spectrum that delivers the highest performance for 5G and truly makes the new generation special.

High-band spectrum can offer peak speeds up to 10Gbps (very fast) and has extremely low latency (almost no delay between device and network communication). However, there is one major weakness. The main drawback of high-band is that it has low coverage area (poor reach, in other words) and building penetration is poor. On land, this will mean replacing giant cell towers with small-cell antennas in close proximity. Still, for shipping according to Telecom 26, 5G has a key role to play as a self-contained ship-based network to serve massive deployments of Internet of Things (IoT) devices and applications in maritime environments. It will allow full ship-wide coverage, across thousands of containers and their cargo, while also supporting new forms of documentation and ledgers.

Why 5G networks pose greater security concerns

5G benefits such as greater speeds, increased efficiencies and automation, and support for up to one million device connections per private 5G network (put this into a shipping context and imagine the possibilities),

should lead to more innovations and a significant change in how we do business. One would be forgiven for being blinded by the benefits of 5G. But 5G also creates many new opportunities for hackers and cybercrime.

As we adopt so many more devices and connections into our lives, we need to be investing as much in cyber security and it's also critical to have security measures in place for both business and personal data.

5G security concerns are mounting after researchers at Purdue University and the University of Iowa found 11 vulnerabilities in the next generation cellular networks. The threats found by the researchers allow real time location tracking and surveillance as well as the ability to spoof emergency alerts to trigger panic. This could include mass scale 'May Day' calls and other critical information flows in shipping. The following are five critical ways in which 5G networks are more susceptible to cyberattacks than their predecessors, off the back of both the above-mentioned university findings and according to a 2019 Brookings report, **Why 5G requires new approaches to cybersecurity** (https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/):

They are:

- The communication network has moved mostly away from hardware that is fixed in one physical place - with switches and routers, to software on a computer which is distributed openly. This is more cost effective, but it opens the network up to attack from multiple places which might not all be protected as the "old" hardware would have been.

- Even if software vulnerabilities within the network are secured in other ways, the 5G network is now managed by software - often early generation artificial intelligence, that itself can be vulnerable. That means an attacker that gains control of the software managing the network can also control the network.

- Physically, low-cost, short range, small-cell antennas deployed throughout urban areas become new hard targets. When software allows the functions of the network to shift dynamically, cyber protection must also be dynamic rather than relying on a uniform lowest common denominator solution.

- One vulnerability that was supposed to be fixed in 5G was the threat from "stingrays", which present themselves as a cell tower to spy on users. But concerningly, researchers found that these attacks were still possible in 5G. Stingrays masquerade as legitimate cell towers. Once they trick a device into connecting to it, a stingray uses the device's identifiers to track the device, and even listen in on phone calls.

- Finally, of course, is the vulnerability created by attaching tens of billions of hackable smart devices (actually, little computers) to the network colloquially referred to as IoT (Internet of Things). Plans are underway for a diverse and seemingly inexhaustible list of IoT-enabled activities, ranging from public safety things, to battlefield things, to medical things, to transportation things—all of which are both wonderful and uniquely vulnerable. Check out shodan.io to see what this means!

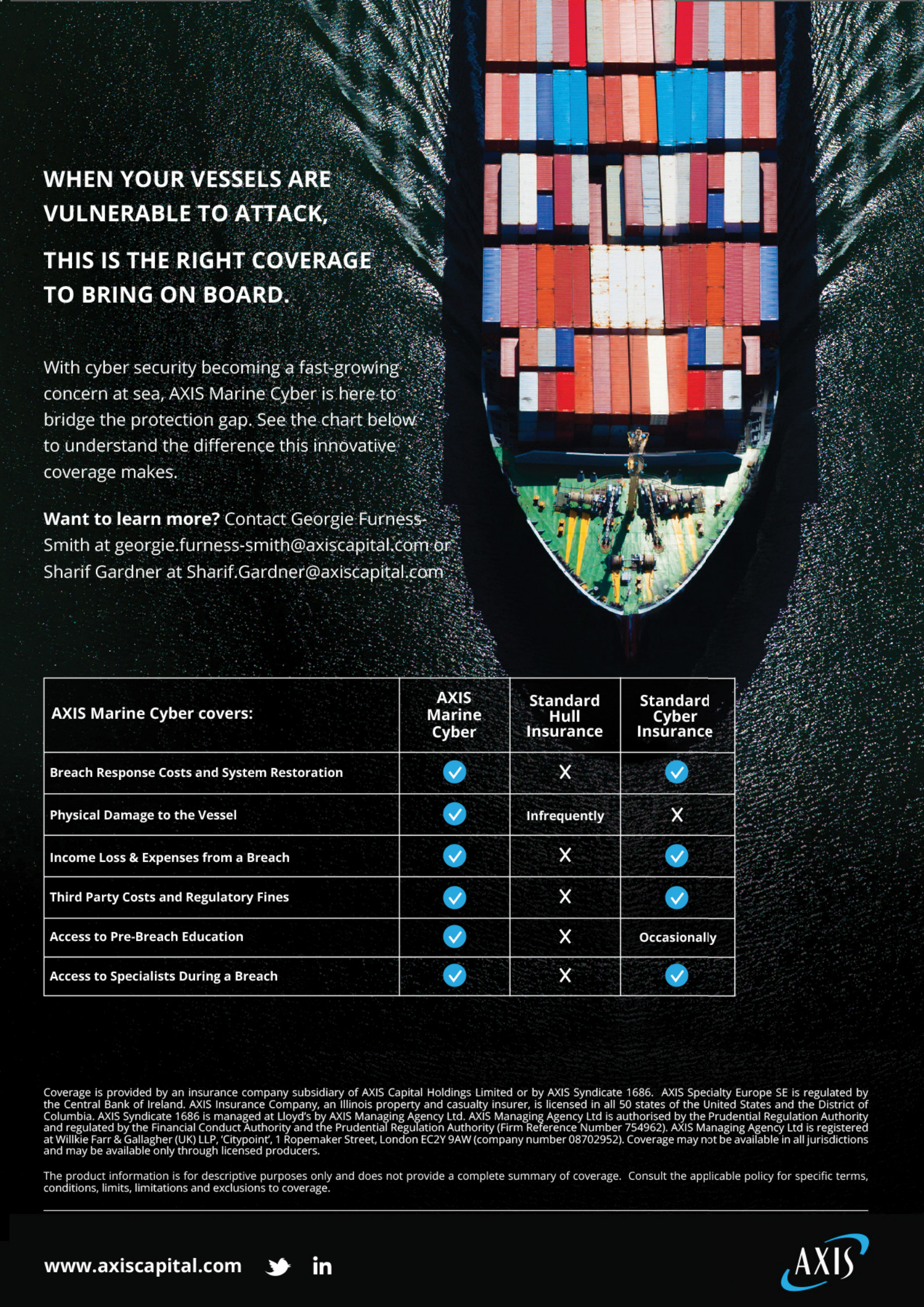
Our societies and industries will soon run increasingly on top of 5G networks, from critical infrastructures to transport systems and even in our homes with IoT. This is exactly why network trustworthiness is – and will always be – a top priority in any high-level discussion. It's cliché to say that everything is connected, but in the Internet of Things, everything actually IS connected.

This alarm has been sounded before. Huawei, the leading manufacturer of 5G equipment for carriers, is still embroiled in a trade war with the U.S. Government over concerns its 5G equipment and consumer devices will allow foreign governments to spy on citizens.

Josh Lemos, VP of Research and Intelligence for BlackBerry Cylance, says a near full-stop is possible: "As cities, towns and government agencies continue to overhaul their networks, sophisticated attackers will begin to tap into software vulnerabilities as expansion of bandwidth that 5G requires creates a larger attack surface. Governments and enterprises will need to retool their network, device and application security, and we will see many lean towards a zero-trust approach for identity and authorisation on a 5G network."

References:

- The Daily Maverick - https://www.dailymaverick.co.za/article/2020-04-13-5g-and-claims-of-its-danger-to-human-health-myth-fact-or-something-in-between/
- The Next Web - https://thenextweb.com/readme/2020/01/08/5-cybersecurity-trends-that-will-dominate-2020-according-to-experts/
- Gertner - https://www.gartner.com/en/newsroom/press-releases/2018-12-18-gartner-survey-reveals-two-thirds-of-organizations-in
- Brookings - https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/
- OpenAirInterface - https://www.openairinterface.org/?page_id=466
- CNBC (https://www.cnbc.com/2020/03/27/coronavirus-can-the-internet-handle-unprecedented-surge-in-traffic.html)



WHEN YOUR VESSELS ARE VULNERABLE TO ATTACK,

THIS IS THE RIGHT COVERAGE TO BRING ON BOARD.

With cyber security becoming a fast-growing concern at sea, AXIS Marine Cyber is here to bridge the protection gap. See the chart below to understand the difference this innovative coverage makes.

Want to learn more? Contact Georgie Furness-Smith at georgie.furness-smith@axiscapital.com or Sharif Gardner at Sharif.Gardner@axiscapital.com

AXIS Marine Cyber covers:	AXIS Marine Cyber	Standard Hull Insurance	Standard Cyber Insurance
Breach Response Costs and System Restoration	✓	X	✓
Physical Damage to the Vessel	✓	Infrequently	X
Income Loss & Expenses from a Breach	✓	X	✓
Third Party Costs and Regulatory Fines	✓	X	✓
Access to Pre-Breach Education	✓	X	Occasionally
Access to Specialists During a Breach	✓	X	✓

STEP FORWARD IN PROTECTING SHIP TRACKING COMMS FROM CYBER-ATTACK

This month there has been a large step forward to mitigating the cyber risks related to ship tracking using satellite communications as CYSEC, a cybersecurity company from Switzerland, was awarded a contract by the European Space Agency to develop a solution in this specific area.

According to their press release, there are vulnerabilities in many existing maritime communication systems that could lead to dramatic consequences when under a cyber-attack. In particular, the Global Navigation Satellite System (GNSS) provided by multiple satellite constellations has been the subject of spoofing and jamming attacks that led to a partial or total loss of the ability to locate ships at sea. Such a failure can be disastrous if the ship is, for example, navigating narrow straits or near the shore.

Another critical piece of equipment onboard is the Automatic Identification System (AIS), which tracks every ship in the world and whose data is used by numerous organisations and downstream services such as insurance companies. Ships have used multiple techniques to tamper with AIS data and entered zones from which they are legally excluded, for fishing or performing other illegal activities.

Both GNSS and AIS signals use satellites and are regarded as critical to improve the safety of maritime navigation and the reliability of data for downstream services. Using its family of secured servers and its experience in satellite communications, CYSEC SA will lead a feasibility study to investigate the protection of both GNSS and Satellite-AIS (SAT-AIS) communications.

CYSEC has established a consortium to develop and test the potential solutions composed of U-blox, a global provider of leading positioning and wireless communication technologies for the automotive, industrial, and consumer markets; and Gomspace, a designer, integrator and manufacturer of high-end nanosatellites for customers in the academic, government and commercial markets. The team will work under the guidance of both ESA and European maritime stakeholders.

CYSEC's objective of securing maritime communications is a natural extension of its current activities in IoT and Space, where its flagship product ARCA is already used to protect communications to satellites and connected devices on ground.

"Cybersecurity is a very important topic at ESA, not only for space infrastructures and missions, but also regarding all the services using satellite-based data and technologies. Ship tracking is one of them and cybersecurity is a complex issue that needs to be addressed. We are delighted that the consortium led by Cysec showed all the technical and business expertise to successfully complete this feasibility study and are looking forward to the outcomes," said Laurence Duquerroy, ESA Space Solutions.

https://www.cysec.systems/2020/04/22/cysec-wins-europe-an-space-agency-contract-to-protect-ship-tracking-communications-from-cyber-threats/

COVID-19 CHALLENGES FOR THE MARITIME CYBER COMMUNITY

As countries throughout the world shut their borders and factories shut their doors, shipping - based entirely upon international travel and delivery of goods - has felt the impact strongly.

Many hundreds of voyages have been cancelled already but there is motivation to keep trade links open, particularly given the globalised economy and valuable supply chains involved, so the industry has had to adjust just like everywhere else.

Where possible, employees will be working from home with the changes in cyber environment that entails. Meanwhile those at sea or returning from a job may now find themselves in an unusual position; perhaps stranded in a foreign country due to travel restrictions, being asked to quarantine on arrival, or - as crew changes are halted to stop the spread of the virus – unable to leave the ship at all. Meanwhile IT professionals may be unable to visit these ships as well.

These curveball conditions are being met by the industry and maritime cyber security teams head-on with a few examples below:

CONNECTING CREW AND SHIPS DURING LOCKDOWN

With crew on lockdown, the importance of communication for seafarers with their families has become central to their welfare. Inmarsat introduced in March several measures to meet the need. They have a 50% discount for crew voice calling services on more than 40,000 ships until the end of June, with calls to the SeafarerHelp service being free of charge over the same timeframe. They are also working to provide a free video call service with a 'trained health professional' regarding Covid-19 among other measures.

Marlink's 'StrongerTogether' initiative is also highly commendable. They set up short term bandwidth upgrades on all Sealink packages to cope with the greater demand for data from crew and offer free minutes for all crew on vessels with Sealink VSAT alongside other offerings.

They have also focused on enabling shore-based teams to monitor onboard IT and access critical operational systems while their technicians and IT staff are unable to visit ships or access onboard IT networks.

REMOTE CYBER SECURITY ASSESSMENTS

Contracted to the job before the crisis became globalised, DNV GL were asked to conduct a 'cyber security assessment and penetration test for an offshore asset'. However, with travel to the location now out of the question, they had to find alternative means of meeting the brief. This involved DNV GL staff from multiple country offices working together as well as personnel from the client ashore and at sea.

THESE MEASURES GO SOME WAY TO ENABLING PEOPLE TO SAFELY NAVIGATE THESE UNUSUAL TIMES, SO LIFE AND WORK CAN CONTINUE.

Thinking laterally and working collaboratively meant that DNV GL could meet their client's needs and ensure their security could be upheld despite the crisis.

WEEKLY CYBER THREAT REPORTS

Maritime security specialists Dryad Global teamed up with cyber consultants Red Sky Alliance to produce a weekly report of the malicious emails and whom they are targeting. They noted that cyber criminals have started impersonating ships, inserting their ship name into the subject line for example. This list has thrown up examples where COVID-19 has been specifically used to lure targets in, with emails circulating purporting to contain an Excel spreadsheet list of ships infected with coronavirus – of course the link or file attached contains malware.

Amid lockdown restrictions, with fear and worry rife and workers and organisations adapting to isolated working-life, the digital environment and satellite comms are becoming more important than ever. Measures like those above go some way to enabling people to safely navigate these during unusual times like these, so life and work can continue.

https://maritime-executive.com/corporate/dnv-gl-delivers-innovative-remote-cyber-security-assessment
https://www.thedigitalship.com/news/maritime-satellite-communications/item/6524-marlink-launches-strongertogether-to-support-operators-and-seafarers-during-covid-19
https://www.thedigitalship.com/news/maritime-satellite-communications/item/6510-inmarsat-supports-seafarers-with-50-voice-call-discounts-and-free-covid-19-video-calling
https://splash247.com/cyber-criminals-target-shipping-with-coronavirus-themed-emails/

SUSPECTED CYBER ATTACK ON MSC

On 17 April the Mediterranean Shipping Co confirmed suspicions that the company had suffered a cyber attack, the third on a shipping line in three years (following Maersk in June 2017 and COSCO in July 2018). The event was suggested to have begun overnight on the Thursday 9 April, and involved a network outage at one of its data centres causing their website and online booking platform to go offline.

In a statement released on Friday 10 April they announced that: "While we do not rule out the possibility of malware, we have decided to close down our servers in our headquarters as a first safety measure. We continue to monitor and evaluate the situation, and we're working towards full recovery in the shortest time possible."

MSC said the outage only impacted its IT systems at headquarters in Geneva, with the agency's other IT networks operating separately in order to prevent any issues transferring.

Fortunately, outages did not impact upon their ability to operate with booking platforms remaining fully functional and other departments, terminals and depots "operating without disruptions". Therefore they were able to continue operating for the duration of the issues which were resolved as of 15 April when all MSC systems and website were back online.

Their latest statement confirmed that it was malware without specifying details. There are rumours that it involved file encryption malware, raising the possibility that the company was targeted by ransomware.

MSC said "We have shared as per industry standards the malware with our technology partners so that mitigations could be made available not only to us"; however they refused to comment further as it would be "counter productive from a security perspective".

> **"We have shared as per industry standards the malware with our technology partners so that mitigations could be made available."**

Once more this incident stands as a reminder of the industry's inherent vulnerability to cyber threats and the repercussions when online systems are brought to a halt.

Source:
https://www.cybersecurity-insiders.com/mediterranean-shipping-company-msc-hit-by-a-cyber-attack/
https://www.joc.com/maritime-news/container-lines/mediterranean-shipping-co/msc-network-outage-sparks-cyber-attack-concerns_20200410.html
https://www.rivieramm.com/news-content-hub/news-content-hub/cyber-attack-closes-msc-headquarters-servers-58933
https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage

HOMEWORKING
SOME ADVICE FROM DRYAD GLOBAL AND RED SKY ALLIANCE

As organisations adjust to new governmental and national rulings and advice on social distancing and self-isolating, home working is becoming the new normal for many who previously were used to operating in a secure, office environment. With cyber criminals on the rise, organisations and individuals now required to work from home must adapt, and fast, according to Dryad Global, who offer sage advice this month in Hellenic Shipping News alongside partner Red Sky Alliance.

They state that while for many businesses remote working has long been factored into their plans and configurations, 'for a large number of businesses and individuals this 'new reality' has caught many unprepared and as such this period of uncertainty has led to significantly increased risks for which many are unprepared'.

Prepare for the long-term

First up, Dryad Global offer their belief that varying disruptions to work patterns are likely to last up to 18 months, and 'whilst it remains impossible to predict the length of time disruption to normal working practises will continue for, it is prudent to ensure that digital office spaces are sustainable and configured for the long term.'

Consider the risks of new technology

According to Dryad, as organisations try to continue business as usual there is a rise in teleconference software such as GoToMeeting, Zoom, Teams etc that nevertheless present risks. For example, Zoom 'was found vulnerable to an exploit which allows attackers to forcibly join meetings, and even activate the webcam (CVE-2019-13450).'

Dryad also illustrate that by using these virtual spaces for the sort of meetings normally conducted face to face, we are putting vulnerable people and significant information at risk online, particularly when used by employees in their home networks which likely lack the various protections and checks an organisation can put in place in the office. For example, should an employee be hacked at home even while connected to the work system, their stolen data will rarely be seen on enterprise network intrusion detection systems, so companies must be vigilant in monitoring the web for exposed credentials.

Maintain vigilance at home

When working from home, away from the office environment, it is perhaps understandable that one may feel more relaxed about email hygiene, less able to follow up suspicious emails with colleagues for example. The upshot, according to Dryad Global, is a noticeable boom in successfully targeted phishing emails.

One solution they suggest is the Threat Recon data available through the Red Sky Alliance RedXRay platform which 'allows companies to monitor project names, domains, mail server IP's, and more to check for phishing emails that may not show up on enterprise mail filters.'

Insider threats, outside the office

Another threat likely to be exacerbated is the insider threat. While companies usually 'have policies and procedures that would prevent an employee from leaking sensitive, controlled, or proprietary information', this protection rarely extends to working from home. Companies will have to deal with the higher risk of their information appearing on sites like Pastebin, where employees can expose valuable information virtually anonymously.

At this time of crisis, organisations are required to make quick decisions to enable the continued running of their business and with those decisions come risks that may not be weighed and evaluated as thoroughly as they should. Unfortunately, the maritime industry will continue to be targeted by cyber criminals and so it is up to the industry to 'target upstream of an attack' and be on the front foot

For Dryad Global's full article:
https://www.hellenicshippingnews.com/home-and-remote-working-threats-to-maritime-and-what-to-do-about-it/

1 Hour MCA Recognised & GCHQ Approved Training

Maritime Cyber Security Awareness Course (MCSA)

The ‘human factor’ is your biggest vulnerability to cyber crime.

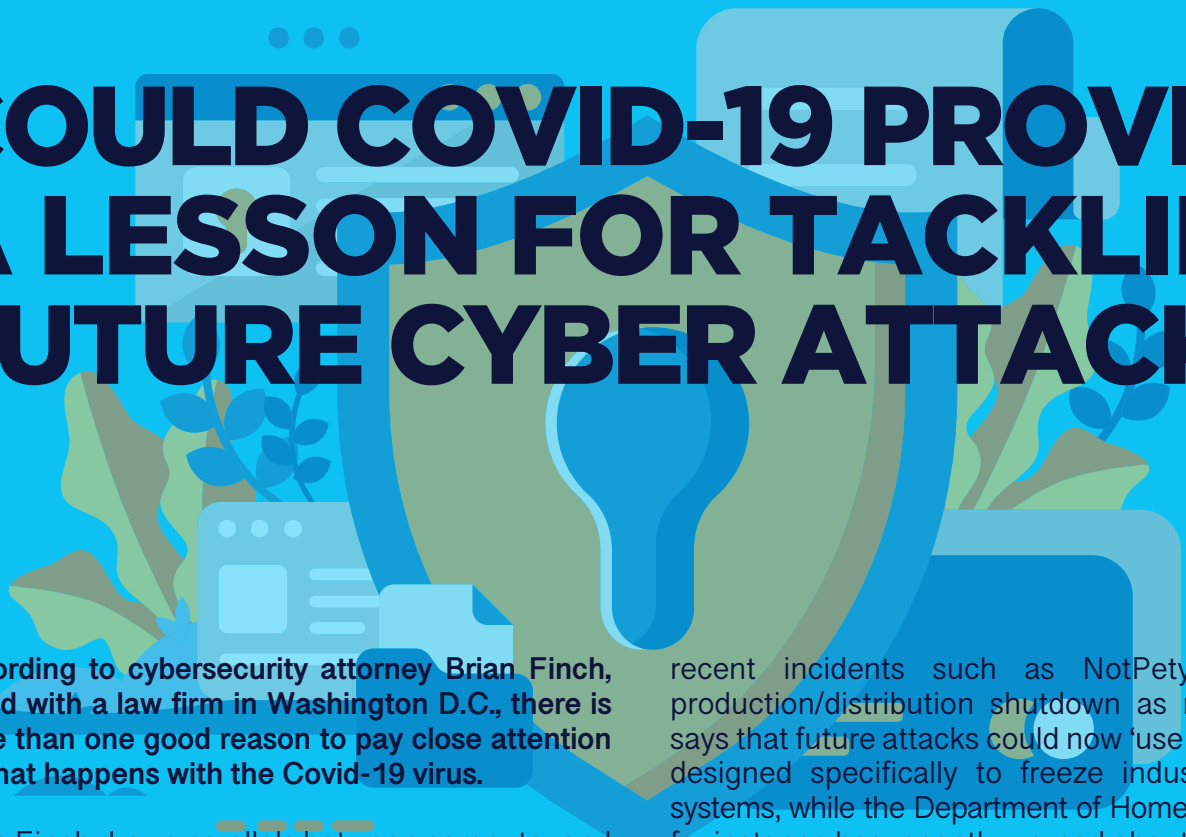
Educate your workforce today to protect themselves and your organisation tomorrow.

- Easy access 1-hour online course
- Designed to complement current approaches to cyber security
- Suitable for all personnel – onboard and ashore
- MCA Recognised and GCHQ Approved

JWC INTERNATIONAL

For more information or to book, please visit us: www.maritimecybertraining.online

COULD COVID-19 PROVIDE A LESSON FOR TACKLING FUTURE CYBER ATTACKS?



According to cybersecurity attorney Brian Finch, based with a law firm in Washington D.C., there is more than one good reason to pay close attention to what happens with the Covid-19 virus.

Brian Finch draws parallels between computer and biological viruses, starting with the provenance of the shared term itself, when a Ph.D. student Fred Cohen 'developed a novel software program that would surreptitiously install itself on host computers and quietly surrender all rights, privileges, and data to Cohen.' The software reminded Professor Len Adelman of his research into HIV infections and so the 'computer virus' term was coined.

For Brian Finch, this example 'illustrates that computer experts recognized from the start the value of using medical models as a way to understand what is now known as cybersecurity' and he sees numerous ways in which the cybersecurity sector has used epidemiology research to model for cyberattacks ever since.

His article published by theHill.com focuses upon the Covid-19 virus and how its spread is 'causing the same severe disruptions and tangible financial harm to manufacturing and transportation sectors predicted to accompany a large scale cyberattack'. By watching the outbreak and the tactics used to mitigate the disruptions, he believes the cyber security sector could learn valuable lessons that may help them plan their own cyber strategies.

His argument is compelling, after all, the first steps taken by an organisation with a computer virus or malware, is to isolate and contain the problem, with recent incidents such as NotPetya requiring production/distribution shutdown as required. He says that future attacks could now 'use ransomware designed specifically to freeze industrial control systems, while the Department of Homeland Security for instance has recently warned about the growing threat of viruses designed specifically to destroy the data on infected computers'.

He draws further parallels between the issues faced by companies in the wake of a computer or biological virus, with lack of adequate insurance being a shared issue. He reports that following SARS, some insurance carriers 'stopped issuing insurance policies that cover epidemics' and that there may be considerable consequences to businesses as a result that may require governments to intervene in order to reduce 'a global slowdown'. Cyberattacks are similarly events that could produce significant losses - Lloyds of London estimating upwards of $200 billion – with low levels of insurance, an estimated 10% of cyberattack losses would be covered by insurance according to Lloyds.

Brian Finch concludes: "When it comes to studying who, what, where, and when of viruses, there is a striking amount of overlap between the real and cyber worlds. And especially in the relatively uncharted world of massive cyberattacks, we would do well to learn as much as we can from the medical textbook so that the financial recovery chapter of the cyber playbook is as close to finished as possible."

Certainly, in these unusual days, it is an interesting thought exercise and is worth considering as we explore how we react to ongoing events.

Source:
https://thehill.com/opinion/cybersecurity/485391-cyber-planners-should-be-carefully-watching-the-coronavirus

BE CYBER AWARE AT SEA

RANSOMWARE

CYBER CRIMINALS CAN BLOCK ACCESS TO YOUR FILES UNTIL A LARGE SUM OF MONEY IS PAID

At the very minimum use reputable antivirus software and a firewall - ensure that all systems and software are up-to-date with relevant patches to better protect your files