A tale of two viruses

With cybercrime surging over the past few months, the global pandemic has been a wake-up call for the maritime industry

WORDS / AMY McLELLAN

Digital tools have come into their own during the COVID-19 crisis, sustaining businesses, education and family life. As in other industries, marine businesses rapidly mobilised to support home-working for those who could, as well as ensuring far-flung crews could remain in touch despite more challenging shift patterns.

"COVID-19 definitely accelerated some trends that were already underway," says Professor Kevin Jones, executive dean at the University of Plymouth's Faculty of Science & Engineering. "Companies achieved in three months what would have taken three years in normal times."

These trends include a surge in demand for cloud services to deliver the agility and scalability needed to cope with a sudden switch from physical to digital services, and the need to support a distributed work-from-home environment. The speed and scale of the mobilisation was impressive, but experts are warning that the pandemic has created a perfect storm for a rise in cybercrime originating from organised crime networks, nation states, hacktivists and even bored lockdown opportunists. Israeli cybersecurity consultancy Naval Dome, for example, reported a 400% increase in attempted hacks on the maritime sector from February to June, with malware, ransomware and phishing emails the main attack points. In August, cruise ship operator Carnival Corp was the target of major ransomware attack.

"COVID-19 definitely accelerated some trends... Companies achieved in three months what would have taken three years in normal times"

Tenfold increase

By triggering an abrupt change in operations, the pandemic has created new vulnerabilities by pushing companies out of their tried-and-tested IT comfort zone. California-based cybersecurity firm McAfee, for example, reports that use of cloud services spiked by 50% between January and April, and use of cloud collaboration tools surged by 600% as organisations that normally rely on legacy on-premises applications and networking turned to the cloud to scale their digital capacity. This pivot was shadowed by a 630% rise in threat events from external actors over the same period, including large-scale attempts to access cloud accounts with stolen credentials. What's more, access to the cloud by personal devices doubled over the period, adding another layer of unexpected risk. Quite simply, as more employees in the sector work online from remote locations, the 'surface area' for attack increases massively.

Operational risks

However, the maritime sector doesn't rely exclusively on the remote connectivity of devices and IT. The typical ship is also a floating factory, with operational technology (OT) systems controlling navigation, engines, cranes and other industrial processes. This is the aspect that worries Ian Bramson, ABS Group's global head of cybersecurity and chair of the IMarEST's Maritime Cyber Risk Management SIG.

> ***"Now the crime isn't just stealing data, it has kinetic effects, whereby you can take control of ships, shut things down and blow stuff up"***

"It's a game-changer in terms of risk," he says. "Now the crime isn't just stealing data, it has kinetic effects, whereby you can take control of ships, shut things down and blow stuff up."

He points out that the importance of shipping means the attacks don't even have to be dramatic to have significant real-world impacts. "In today's world, if you slow ships down, you can snarl up supply chains or manipulate energy and financial markets. Or with GPS spoofing, you can send a ship into hostile waters and create geopolitical tensions."

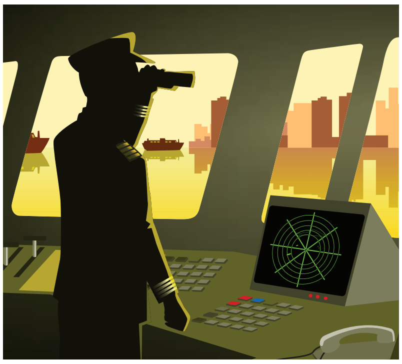
The pandemic's physical distancing rules have created new

DON'T LEAVE CYBER-SEAWORTHINESS TO CHANCE

We must not put the burden of cybersecurity solely on ship's captains

It is a fact that the state of a vessel's cybersecurity will affect its seaworthiness. This means that a captain with a limited understanding of cybersecurity will need to make a call on the cyber vulnerabilities and processes of a vessel under their command.

We should not leave the weight of this decision on a captain's shoulders; they must have tools and resources at their disposal, together with expertise and assistance. In my experience, many captains are tech-savvy – happy to operate a computer, mobile phone, electronic charts, integrated bridge and plenty more – yet would likely struggle to ensure their ship was cyber-secure.



Cybersecurity understanding in the maritime sector is growing, but there are still some knowledge gaps in crews. This is no surprise – vessels were primarily unconnected entities, exposed only when in port. Satcoms were very expensive. However, with the advent of cheap VSAT, most vessels are now 'always on' and require connectivity to function efficiently. The combination of connectivity and old, unmanaged on-board networks equals a significant cyber-risk.

Dig deep

Cyber issues can be subtle, buried deep in complex systems that have been modified over the years, through partial refits, 'enthusiastic' engineers accidentally breaking network segregation, cyber-incompetent support organisations and maritime technology providers who don't understand or prioritise cybersecurity.

These subtle issues have counterparts in physical maritime incidents: for example, the slow start-air leak that eventually leaves a vessel immobile or a GPS antenna cable breaking, leaving the vessel dead reckoning.

Masters will not be able to 'see' all cyber-incidents at sea, but there are probing questions that a master could and should ask about the cyber-seaworthiness of their vessel. Most importantly, they should ask for evidence that the various networks on board are suitably segregated, and they should ask which systems on the various networks can connect to each other. For example, can the integrated bridge communicate with the engine management systems, but not the crew Wi-Fi network? They should also ask for proof that all systems on board are running the latest software and patches.

And passwords. I cannot overstate the importance of changing passwords. Simple, re-used, default or even blank passwords are the key to almost every vessel and corporate network compromise we have achieved over the last 22 years.

Easy wins

There are also plenty of changes that can be made to delay the spread or reduce the impact of an incident. For example, a ransomware attack that takes out one ECDIS is less likely to spread to a second ECDIS if it's from a different vendor, has different passwords or is on a different network.

It's also easy to check for wireless networks that aren't authorised. Even walking the vessel with a

Left: Ian Bramson, ABS Group. Right: Professor Kevin Jones, University of Plymouth

ABS GROUP

vulnerabilities. OEMs, technicians and vendors are increasingly providing a 'remote, COVID-safe service', which requires on-board operators to connect often stand-alone OT systems to shoreside networks, in the process sometimes bypassing normal security protections, in order to carry out diagnostics and servicing. This creates a whole new category of vulnerabilities, with IT and OT systems no longer segregated, providing gateways to OT systems.

Worryingly, Bramson says, maritime OT is "extremely immature" when it comes to security. Given the long life cycle of ships, many of these systems were not designed with security in mind and lack even basic monitoring. "Too often, there's zero visibility into the OT environment," he says.

Professor Jones adds that the maritime industry lags behind others on cyber-awareness: "I used to get a lot of blank faces when I raised this, but there's definitely a growing sense of urgency."

Cyber insurance

This view is backed by Kelly Malynn, senior risk manager and cyber specialist for Beazley, who reports a "steady increase" in enquiries for cyber insurance since March, both for shoreside IT and on-board OT. She points out that new IMO rules which come into effect at the end of 2020, and which incorporate cyber-risk into existing risk management processes, are

mobile phone while at sea will reveal most Wi-Fi access points. Are they legitimate, or has an engineer installed something to allow them to access engine systems from their cabin? Or has another crewmember run out of internet allowance and hooked up a back door to the business network to get more access?

Too much bluster

There can be no argument: security vulnerabilities in ships are a major problem. There is far too much bluster in the maritime cyber sector, and too many self-declared cybersecurity 'experts' driving meaningless checklists. I also have extensive concerns about cybersecurity certification, as we have never tested a vessel that we would consider to be suitably cyber-secure, even those fresh out of the yard with the latest systems on board.

Assessing a vessel's cyber-seaworthiness properly takes a sizeable, rare skill set. It is not something we should leave solely at the captain's door.

Ken Munro is a consultant for Pen Test Partners, a provider of cybersecurity services to a variety of industries and organisations

helping to focus minds. “Companies only have so much bandwidth, and they’re still preoccupied by the fall-out from the pandemic, but this threat isn’t going away,” she says.

Maersk memories

No doubt the experiences of Danish shipping giant Maersk will be front of mind. In 2017, the transport and logistics giant was hit by a huge outage due to the NotPetya malware attack that disrupted companies around the world. Once the virus was activated within Maersk, it propagated within just seven minutes, devastating the group’s systems. All end-user devices, including 49,000 laptops, were corrupted, 1,200 applications became inaccessible and around 3,500 of its 6,200 servers were disabled and couldn’t be reinstalled. Landlines were inoperable and contacts wiped from mobiles. The cost of the damage was estimated to be between US$250m and US$350m.

“If your valves open and you’re pumping oil into the middle of the ocean, then you’re not calling the IT department, you’re calling operations”

The attack on Maersk made the headlines, but cyber experts say it is far from a lone case: most companies don’t choose to go public, fearing damage to their reputation. From GPS spoofs to malware attacks that impair on-board systems, there’s a growing mood of unease among insurers and cybersecurity experts about the vulnerabilities of the maritime sector.

The first line of defence is proper training for all employees, moving from the basic hygiene factors of password security and email protocols up to resilience training and ensuring there’s a designated crew member on board who knows how to detect an intrusion and how to respond. “A well-trained crew is an asset; a poorly trained crew is an increased point of vulnerability,” says Professor Jones. The University of Plymouth has built the ‘Cyber-SHIP Lab’, a real-world simulation whereby owners and operators can test their systems and processes.

The £3m Cyber-SHIP Lab at the University of Plymouth was supported by funding from Research England

Part of this journey involves understanding where the risk lies. “The budget and accountability need to sit in operations, not IT, because they own the risk,” says Bramson. “If your valves open and you’re pumping oil into the middle of the ocean, then you’re not calling the IT department, you’re calling operations.”

Close the gaps

There is some good news. Bramson says that if maritime is behind the curve, then so too are many of the bad guys, presenting a window of opportunity for the industry to pull together and close off some of the vulnerabilities before there’s a devastating incident.

“There’s a unique opportunity to do this together,” he says. “We have to look across the whole chain, from ship builders and owners to charterers and insurers, and find a common language and cohesive approach to deal with this. We’re much stronger together than by adopting different standards and a piecemeal approach.”

One key ingredient might be the formation of neutral clearing houses where companies can anonymously trade information about threats and attacks to inform others and share best practice.

In the meantime, the risk from shadowy players grows. Already Bramson is worrying that, as lockdowns ease and those working from home return to the office, there will be what he calls a “snap-back risk”.

“It’s a latent cyber-risk where your IT network has been expanded, with people plugging their laptops and devices into their home networks, and now they’re coming back to your office,” he cautions. “You will check them for temperature and symptoms, but COVID-19 might not be the only virus your workers are bringing back with them.” ■

FURTHER READING

To read an in-depth interview with Ian Bramson, chair of the IMarEST’s Maritime Cyber Risk Management SIG, go to bit.ly/33mHw5g. The Maritime Cyber Risk Management SIG has been established to identify and appraise new and emerging cyber-risks; to develop preventative guidance to strengthen understanding and offer practical remedies; and to disseminate this information to marine engineers, scientists and technologists using the systems affected. Visit Nexus for more information and to join the group.