Safety at Sea and BIMCO cyber security white paper

Supported by ABS Group

2019

IHS Markit®

BIMCO comment

Open dialogue

BIMCO began raising cyber-risk awareness long before shipping realised it was vulnerable to attacks. The sector has come a long way since then, but must stay vigilant

BIMCO: 5120756

Aron Sørensen, head of maritime technology & regulation at BIMCO

BIMCO takes cyber security very seriously and is working together with IACS on technical criteria, which will ensure that more cyber resilient ships are delivered in the future. We believe that software on operational technology systems (OT) and information technology systems (IT) needs to be maintained in a cyber resilient way, which is why BIMCO is collaborating with the International Organization for Standardisation (ISO) on such a standard.

We are also continually working on raising awareness among shipowners about cyber risk and issuing guidance for what to do when something goes wrong. This year, BIMCO, CLIA, ICS, INTERCARGO, InterManager, INTERTANKO, IUMI, OCIMF and WSC published version 3.0 of *The Guidelines on Cyber Security onboard Ships*, which offers guidance to shipowners and operators on how to assess their operations and develop the necessary procedures and actions to improve resilience and maintain integrity of systems onboard their ships. The level of practical guidance in the newest version has also been increased in accordance with recent developments.

The IMO resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS) is an important milestone, as the approved SMS should now take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code. Cyber risk should be addressed in the same way as any other risks that may affect the safe operation of a ship and protection of the environment. The industry Guidelines have been aligned with this decision and describe how to incorporate cyber risk management into a company's SMS.

Considering that a ship is an integral part of the global supply chain, we have also issued guidance on how to handle the relationship between the shipowner, ship agent, ship manager and vendors. These relationships should not only be based on trust but also a common understanding of a mutually acceptable level of cyber risk management.

BIMCO's publically avaialable Cyber Security Clause fulfils three important functions. The first is to raise awareness of the cyber risk and manage it. Shipowners should implement appropriate measures and systems and endeavour to maintain the cyber risk management system.

The second aim is to provide a mechanism for ensuring that parties have procedures and systems in place to minimise the risk of a cyber incident happening in the first place. For example, a party who becomes aware of a cyber security incident should notify all stakeholders. It should be noted that this obligation is not limited to incidents within the party's own systems.

The last is to ensure that parties mitigate and resolve the effects of an incident when it occurs, while also cooperating with each other and providing necessary assistance. For example, the clause contains a limitation of liability to be agreed by the two parties.

Additionally, seven examples of verified cyber incidents onboard ships have been added to the guidelines to highlight and illustrate potential problems. Incidents happen all the time, but small or large incidents are rarely reported. More openness in the industry is needed to enable stakeholders to target mitigating measures.

***SAS* editorial comment**

Know the drill

Shipping has come a long way in its attitudes and approach to cyber security, but organisations must ensure all staff are prepared for the likelihood of an attack

IHS Markit/Richard Gleed:5078000

Tanya Blake, editor, *Safety at Sea*

In the four years we have run our maritime cyber security survey with BIMCO, there has been a notable shift in industry attitudes to a greater understanding of the threats it faces. Largely boosted by the 2017 Maersk cyber incident, conversations have evolved from 'awareness' to 'preparedness'. This year's survey showed that companies are working to protect their IT systems, operational technology and against vulnerabilities introduced by third parties. However, as our surveys consistently show, companies still view their 'people' as their biggest cyber weakness.

Blaming shoreside staff or crew when a cyber incursion occurs overlooks deeper issues that can lie in a businesses' security protocols, safety culture, and technologies used to keep vessels secure. Organisation's workers should be taught to take responsibility for their actions, how to spot common cyber threats and ways to prevent accidentally introducing a cyber risk. But expecting them to prevent all attacks from occurring, or blame them when one slips through the defences, is unreasonable. Particularly as the attacks grow more sophisticated and target our industry.

Let's approach cyber threats the way we do with piracy. Would we blame crew if they adhered to safe working procedures but the ship was still boarded by pirates? Would we blame shoreside staff for not spotting a piracy threat quick enough? A determined, 'bad actor', whether a pirate or hacker, will always find a way to carry out an attack. Instead, companies must assess where the biggest cyber risks lie at sea and on shore, prepare crew as much as possible, identify weak spots unique to each vessel, and importantly, have a widely known plan for what exact steps to follow if an attack occurs.

While Maersk was the first maritime organisation to endure a major, public cyber-attack, its laudible response holds valuable lessons. The largest is understanding that an attack impacting your organisation is more a case of 'when' not 'if'. As such, Maersk has put emergency plans in place and ensured its employees know what to do and who to contact in the event of a future attack, including one clear point of call for reporting incidents.

All companies should follow suit, asking, among other things; what are the first steps for all levels of staff at sea and shore when an attack has been detected, who should be alerted and who will be leading and coordinating recovery efforts? A company should notify key stakeholders and alert the wider industry. Crew must know what processes they should follow at sea if onshore IT systems are out of action and what should be done if onboard systems are impacted. It is worth planning for communicating with media during and after a cyber event, as well as a social media policy for employees while an incident is being resolved. Just as we run piracy drills on board, so crew and onshore staff should be drilled in what to do during a cyber incident.

The cyber threat to maritime is continuously evolving. Without plans for an attack in place for all staff it will be far more difficult to limit the spread of an attack inside and outside an organisation, putting profit, assets and even lives at risk. A recent safety alert issued by the US Coast Guard says it best; "maintaining effective cybersecurity is not just an IT issue but is rather a fundamental operational imperative in the 21st century maritime environment".

Contents

Cover Image: Getty Images/fatido: 5120885

ABS Group

Message from sponsor

Cyber security is the new frontier in maritime safety and the industry is beginning to understand the scale of the challenge it faces to achieve an end-to-end solution.

The IMO has given shipowners and managers until January 1, 2021 to incorporate cyber security into safety management systems required under the ISM Code. But no shipowner, port facility operator – or any other stakeholder – should wait that long.

The huge cost and apparent ease with which cyber crime can be committed helps to explain why cyber security topped insurer Allianz's 2019 Risk Barometer as the most feared trigger of business interruption scenarios. Few industries understand this better than shipping where we have witnessed a string of stark demonstrations of the power of digital actors to adversely impact vessels and facilities.

This is not a problem that can be solved with software patches, new hardware, or training that ticks boxes and assumes the job is done. The Cyber team at ABS has made the problem simple; this is an issue that doesn't need to be complicated, provided you understand where the issues lie.

The award-winning ABS FCI Cyber Risk™ Methodology, developed following a two-year research process, is that answer.

ABS Solutions
https://www.eagle.org

Introduction

As part of its remit to shine a spotlight on safety issues for the maritime sector, *Safety At Sea (SAS)* has had cyber security on its radar for a number of years, and has been conducting surveys with the assistance of its parent company IHS Markit and partner BIMCO. This whitepaper, supported by ABS Advanced Solutions, combines an analysis of four years (2016-2019) of survey findings and feedback from relevant experts at focused roundtable events and matches them to cyber behavior and investment trends observable in the wider maritime industry. Readers will gain a comprehensive overview of the key cyber security issues facing maritime, touching upon past major incidents and industry-best practice, as well as practical advice on prevention and recovery.

Report summary

Human element: Looking deeper

Technology is designed, implemented and ultimately used by workers, and interactions between the two are increasingly complex. The 'human element' has consistently topped the *SAS* annual survey list of 'weaknesses', but the instinct to blame the seafarers or shore-based employees may mask deeper more systemic issues and is shortsighted. Mistakes are inevitable and incidents must be investigated to discover the true cause as blame culture not only introduce 'barriers' to preventing future events, but also risks lowering morale and creating an atmosphere of fear. We must foster a safety culture that embraces openness and a willingness to admit mistakes.

2017: An industry turning point

The NotPetya attack on Maersk in the summer of 2017 confirmed the need for shipping to have effective cyber security and crisis management plans in place. NotPetya was a state-sponsored cyberweapon (disguised as ransomware) that knocked out the entire back-office IT infrastructure of the world's largest shipping company for almost a fortnight. It was the final nail in the coffin for the cyber-risk sceptics and deniers and likely spurred many vessel operators into accelerating the implementation of countermeasures and the provision of training for staff.

Indeed the 2018 IHS Markit/BIMCO Maritime Cyber Security Survey revealed that more than half of respondents (58%) confirmed that cyber-security guidelines had been incorporated into their company or their fleet – a substantial increase over the 37% recorded in the preceding year's research. It also goes to explain a significant drop in the number of maritime companies reporting in the 2108 survey that they had fallen victim to a cyber-attack within the last 12 months – 22% compared to 34% in the 2017 survey.

The year 2017 was pivotal in another respect. The IMO declared that cyber-risk management should be incorporated into vessel safety management systems (SMS) in accordance with the requirements of the International Safety Management Code. The resolution encourages IMO member states to ensure cyber risks are addressed in SMS from 1 January 2021.

Risk assessment: Look inside yourself

The shipping industry must be ready to deal with a broad range of threats. Characterising potential attackers based on who you are, where you are and what you're doing; an important element of drawing up worst-case scenarios as part of a wider risk assessment process. Carrying out a rigorous risk assessment – particularly for the first time – is a taxing and sometimes overwhelming exercise. Some elements of risk are static, while others are dynamic and must be periodically reassessed. Deciding which are which is not always straightforward and there are no solid rules to follow. The owner of brand-new luxury cruise ship will take a very different view to an operator of half a dozen ten-year-old workboats. There is no one-size-fits-all answer.

Risk prevention policies must be realistic, practicable and flexible to accomodate staff behaviour. A balance needs to be drawn between security and productivity and rules alone won't be effective unless they are compatible with the prevailing culture of an organisation. Sometimes small adaptations can yield a large impact: one shipping company participating in the 2019 roundtable found displaying a message indicating how to report a cyber risk or possible incident on the log-in screen of every PC eliminated the problem of staff not knowing who to contact.

Training and cultural change

Above all, cyber-risk is no longer a matter that can be offloaded to or should be handled exclusively by the company IT department. It is an organisation-wide challenge. Crew at sea and staff on shore all have to be taught what risks to look out for and what mitigation actions they 'own'. Training has to factor in its target audience and level of knowledge: an organisation's finance team will face different threats and have different needs to a new joiner rating. Making cyber-risk management as integral to an organisation as safety will take time. It requires buy-in from senior management as well as guidance for those on the frontline.

Insurance: The pendulum has swung

Until recently insurance companies tried to exclude or at least separate cyber risks from more traditional risks. That a ship could be lost due to cyber-attack was inconceivable. However, as cyber-risk has become more pervasive across the industry and society more broadly, attitudes have changed. In fact, the pendulum has swung so far in the opposite direction that we are reaching a point where inadequate protections against cyber-risk could render a vessel unseaworthy.

Operational technology: A real-world challenge

An unexpected result from this year's survey was the attitude of respondents towards operational technology (OT) – i.e. digitally controlled systems for handling real-world equipment. While the potential consequences of OT systems being hacked are being scrutinised closely by classification societies, research institutions and various regulatory authorities, the 2019 survey indicates that they are mostly considered a marginal risk. However, speakers at the 2018 and 2019 roundtables highlighted that shipping is among an emerging group of industries in which a cyber breach could go beyond IT functions (taking bookings or payroll) to affect physical systems on a vessel ranging from power plant and propulsion equipment to navigation and cargo handling systems.

One explanation for this possible disconnect in attitudes is that vessel owners are preoccupied with tackling more immediate threats and are yet to focus on more complex scenarios that have a lower likelihood of occurring.

However, as recent guidance issued by the U.S. Coast Guard has shown, there are a growing number of cyber attacks that are specifically targeting maritime systems, making it only a matter of time before a catastrophic vessel-based cyber incident hits international headlines.

It is vital that cyber-risk management at maritime organisations goes beyond the basics of erecting defences against deliberate intrusions and malicious actions by external actors. It must also set up a framework to anticipate failure modes and build resilience against issues with complex control and automation systems, whether due to a coding error not picked up in factory testing, poor configuration or any other reason.

Collaboration: Stronger together

Transparency and collaboration are essential in order to share best-practice in areas such as risk management, recovery plans and ongoing actions to improve resilience. Sectors such as banking and aviation have taken a visible lead in this arena and have demonstrated the mutual benefits of knowledge sharing and joint action. Although maritime has struggled to keep pace with digital change, it is showing some signs of improvement.

Shipowner groups and insurers are increasingly providing their members with practical guidance and advice on emerging regulation. With regional disparities in legal approaches to regulation, national authorities (such as MAIB) are a useful resource for collating and disseminating information about incidents. Some associations have taken to including case studies to help stakeholders relate to the growing problem of cyber attacks including specific incidents such as a complete failure of a vessel's primary and back-up navigation systems. The research arms of classification societies and universities are also collaborating with equipment manufacturers to set up cyber forensics labs for testing in real world conditions.

However, the size and scope of the cyber security threat within the maritime sector are still largely unknown, due in part to shipowners' reluctance to share their experiences for fear of reputational damage.

Outlook: preparing for the future

As global IT systems have become increasingly interconnected, so has the shipping industry. This process is set to accelerate in the future as vessel systems become increasingly automated in their operation and shipping sets its eyes on remote controlled and possibly even autonomous or semi-autonomous vessels.

Have you ever shared your password with a colleague?

Yes 16%

No 84%

With how many colleagues did you share your passwords?

1–3	4–6	7–12	+12
88%	4%	4%	4%

Source: Survey 2019 (Sample size: 166)

What was the impact of any cyber breaches?

48% Loss of corporate data

67% IT system functionality

21% Financial loss

4% Shipborne system functionality

Source: Survey 2016

Reality check

In June 2017, Maersk was the unintended victim of NotPetya – a state-sponsored cyber-weapon disguised as ransomware. The incident remains one of the largest supply-chain attacks ever to take place. In a continually evolving threat landscape, it demonstrated that an indirect attack can be as devastating as a direct strike.

NotPetya took its name from its resemblance to the ransomware Petya, a piece of criminal code that surfaced in early 2016 and extorted victims to pay for a key to unlock their files. But NotPetya's ransom messages were no more than a smokescreen: the malware's goal was purely destructive. It irreversibly encrypted computers' master boot records, which tell the machine where to find its own operating system. Any ransom payment that victims tried to make was futile, as keys to restore the computer's contents did not exist.

NotPetya was powered by two hacker exploits working in tandem: a penetration tool known as EternalBlue, created by the US National Security Agency that was leaked, and an older invention known as Mimikatz, created as a proof of concept to demonstrate that Windows left users' passwords lingering in computers' memory.

The malicious code entered Maersk via its accountancy systems in the Ukraine and quickly spread across the organisation, disabling 49,000 endpoints (PCs, servers and other networking apparatus) at 600 sites across 130 countries. The code was honed to spread automatically, rapidly, and indiscriminately. While accountancy systems may seem remote from vessel operation, the repercussions were immense: a Maersk ship arrives at port somewhere around the world every 15 minutes.

Although the computers on Maersk's ships weren't infected, the terminal software used to receive the electronic cargo manifests from those ships was entirely wiped, which left ports with no guide to load and unload containers. The infected machines – which amounted to nearly the company's entire infrastructure – had to be rebuilt manually. Amazingly, the operator managed to get most systems up and running again within the space of ten days. Maersk's losses of between USD250-300 million - widely considered to be deliberately underestimated by the company's accountants - pale in comparison to the wider, immeasurable cost of the disruption to the global logistics and supply chain.

NotPetya made the industry sit up and pay attention more than any other incident in the maritime arena. It proved that there is no guaranteed defense against an attack, Maersk cyber-security expert Lewis Woodcock told those attending the 2019 *SAS*/BIMCO roundtable. "The approach changes from an if-it-happens problem to a when-it-happens problem. For this reason, we need to find a better balance between defence and disaster recovery."

Key lessons from the Maersk incident

Maersk's valient response to the NotPetya attack and subsequent industry engagement on the topic have created a template for best practice. Maritime stakeholders crafting a cyber resilience and recovery plan would do well to consider the following factors:

As shipping companies integrate information technology (IT) with operational technology (OT), the boundary between the real and virtual worlds becomes increasingly blurred. This convergence, while operationally beneficial, significantly expands the potential attack surface and makes it much harder to contain the impact of an attack in the case of a successful intrusion.

The responsibility for assessing risk, introducing preventative measures, and planning response and recovery actions spans the whole organisation from management and HR down to shipboard crew. Cyber-security can no longer be treated as a 'technology problem for IT to fix'. It is necessary to understand all processes in the company as well as the chains of dependencies between them.

Because this approach demands more resource and engagement from departments, thought should be given to the order in which identified risks are addressed. In the immediate wake of NotPetya, Maersk channelled its energies into restoring booking and other commercial systems, but later changed course when it became apparent that vessels were effectively frozen in ports, unable to load or unload cargoes.

When an attack happens, effective communication is vital both internally to initiate and coordinate the response, but also externally to reassure customers and the wider public (depending on the nature of the incident). Maersk was applauded within shipping circles and earned praise from outside the sector for the open and honest stance it took during the recovery from NotPetya. Its COO gave a dozen interviews to media in the first week alone and the company continues to raise awareness of cyber best practice. The goal is to communicate quickly and accurately.

Arguably Maersk's approach raised eyebrows because most companies that fall victim to cyber attacks instinctively try and conceal the incident for fear of damaging their reputation. However, details inevitably leak and, once on social media, they essentially become public knowledge. Furthermore, cover-ups can arouse suspicions about other issues a company may be trying to hide.

Ironically, at a time when effective crisis communication was most needed, Maersk had none of the usual tools available. The attack rendered email and corporate intranet useless for much of the first week and contact details for remote offices and agents were also stored electronically. The company's employees resorted to WhatsApp and other non-corporate platforms to exchange messages. Meanwhile, action plans and checklists were updated on office whiteboards and flipcharts.

The incident underlined the importance of contemplating worst-case scenarios in disaster planning. In short, to think the unthinkable. Who will coordinate operations whilst IT personnel are battling to restore services? How can a company liaise with customers and suppliers when the finance system is offline? How can seafarer care continue? What is the plan for media interaction? All these questions must be considered. In addition to planning what must be done and response options, it is important to allocate authority at different levels. Effective disaster response requires well-defined roles and responsibilities so that a plan can be executed without bottlenecks.

Training is essential in tackling what is consistently considered to be the weakest link in cyber-risk management: the human element (i.e. people). In 2017, the year in which Maersk's global operations ground to a halt as a result of NotPetya, more than one-third of those polled in the annual survey were not providing awareness training or distributing guidance to their shore-based staff or crews at sea.

It would be reasonable to assume that a headline-grabbing incident of that magnitude would spur vessels owners to teach their personnel how to manage cyber-risks into action and incentivise those with some sort of training already in place to explore ways of enhancing it. Yet the responses from the 2019 IHS/BIMCO annual cyber security survey (see infographic) suggest that enthusiasm for education is in decline – or at least tailing off. The decrease in those offering training to their staff is quite small, so this trend may simply be a blip. Accordingly, this will be an area of focus for the 2020 *SAS*/BIMCO survey.

Half of those providing cyber training in 2019 said that this was delivered using a course developed and run by an in-house team, while one-fifth sent their staff to an external training provider. One in ten went the extra mile by carrying out cyber crisis management exercises to prepare their staff to respond in potential scenarios.

When considering the curriculum and materials used in cyber-risk training it is easy to fall into the trap of treating the shipping industry as a single homogenous entity. However, the reality could not be less true. Not only are there multiple stakeholders – each with their own roles, motivations and responsibilities – but each of these stakeholders consists of different elements, all of which have distinct characteristics.

For example, a fleet operator depends on its seafarers but also on a large team working on shore. These groups can be further divided in terms of characteristics. On board ship, ratings' perception and exposure to cyber-risk will differ markedly from that of senior officers. On shore, operational staff will view risk through a different lens to internal IT departments, and so forth. Commercial teams, HR teams, legal and finance departments will similarly each have their own perspective, right up to the senior executives running the company and charged with making strategic decisions on how cyber risk is treated across the organisation's various regional and global offices.

Neglecting to consider and cater to these differences will significantly diminish the usefulness of the training programme. Clearly, for example, the requirements of a rating who has newly joined the fleet will not align with those of an IT manager who has spent the best part of his career at the company, or match the needs of those taking bookings or managing financial transactions.

Additionally, a one-size-fits-all training solution may signal a perfunctory approach to the problem, prompting employees to question whether cyber-risk is really as important as everyone says. Naturally, this is detrimental to fostering the buy-in needed to engender a long-term change in attitudes.

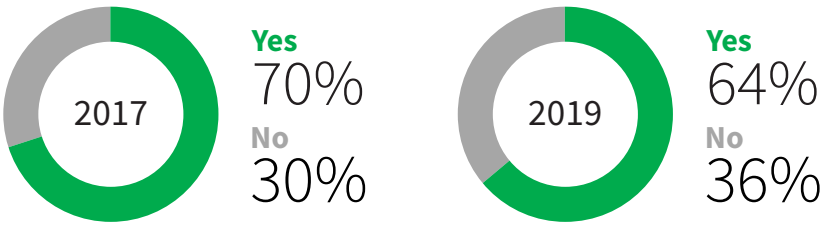
The argument put forward at this year's ABS Advanced Solutions-supported *SAS* and BIMCO roundtable was that some owners see sending crew off to a training course and other superficial measures such as putting up posters as a way of avoiding the more time and effort-intensive work of carrying out a rigorous risk assessment, implementing technical safeguards and introducing new workflows and procedures or changing those that exist.

Others called into question the quality of training currently being provided to crew, maintaining that current options can be "not very helpful and dry", with costs too high per head. However, this last criticism was not borne out in this year's survey data. Half of those polled said that they gather feedback on training quality. Encouragingly, one-sixth of them said that they were impressed by the quality. Three-quarters were mostly satisfied. Only 8% reported that they were disappointed. The positive results may reflect a preference for in-house delivery – where the subjects covered can be tailored to a company's operations and working practices – rather than relying on external providers that will prepare more generic content to appeal to a wider audience.

It is of vital importance that training programmes make realistic assumptions about the needs and prior knowledge of their intended audience. A rating who has just joined the fleet will surely benefit from a formal training session regarding the policies on acceptable onboard use of personal electronic devices (see next page), whereas such a course would be wasted on a seasoned employee.

It is also important that training is incorporated as one part of a broader, more holistic cyber-risk strategy. Simply sending staff on a course and thinking 'job done' is not an adequate response to protecting multi-million dollar floating assets.

Do you provide cyber-risk awareness training to staff?

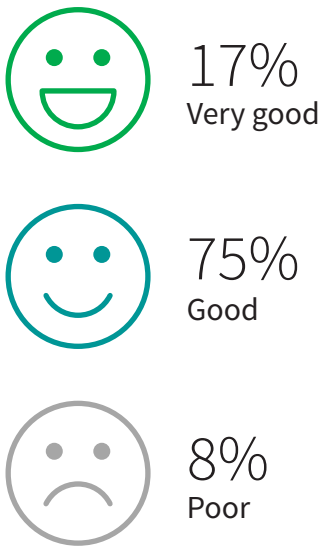


Source: Survey 2017, 2019

What form does that training take?

Source: Survey 2019 (Sample size 72, multiple responses accepted)

How would you grade the quality of training provided?



Source: Survey 2019

Own devices: Introducing external risk

Devices and peripherals personally owned by crew – and visitors on board – are a common malware infection point. In addition to smartphones (which allow crew to maintain contact with friends and family in addition to providing entertainment), tablets and laptops, staff often bring USB gadgets – commonly in the form of memory sticks and portable hard drives.

Such storage devices will likely be packed full of media for off-duty entertainment that are typically obtained in legally dubious ways (such as peer- to peer downloading). Consequently they may, unbeknown to the owner, be packaged with malware, which can leak on to the ship's network.

USB sticks and hard drives are also often faster when transfering files between different systems/networks than officially sanctioned methods. And ironically these shortcuts can be made attractive to crew by measures aimed at bolstering cyber-security - such as network segregation or air-gapping – if they have not been properly thought-out or are implemented overzealously.

Rather than fighting against these natural reactions to the isolation experienced at sea and banning devices outright, it may be fruitful to accomodate these behaviours in a way that won't compromise cyber security. For example, it would engender trust and reduce risk to provide crew with decent facilities to get online in a controlled environment, maintain links with home and for off-duty entertainment.

Clear channels of communications

Companies should introduce clear guidelines so that staff know what to do if they are suspicious about a particular email or unusual system behaviour. They need to be trained to report it and be given clear guidance on how to do so. Organisations must also make it clear that staff won't be punished if they accidentally open malware.

Taking punitive measures against employees is widely regarded as counterproductive and the wrong route to take. Punishing staff can create a climate of fear and will deter employees from admitting mistakes. This may delay the discovery of an incident and complicate efforts to contain the impact.

Having a single point of contact for crew (or any staff) to call during a cyber emergency is vital. It is analogous to make arrangements for other serious incidents such as a fire on board, or a vessel casualty.

Just over two-thirds of those polled in 2019 said their company had a designated cyber security point of contact. One in five had no-one to pass this information on to, which would conceivably allow the incident to escalate, causing greater damage and making recovery efforts harder. Meanwhile one in six were uncertain whether or not their company had a reporting channel, suggesting that greater emphasis is needed in internal communications or during training sessions.

In addition to dedicated cyber hotlines, survey respondents said they would drop a note to their IT department and tell their line manager and immediate colleagues. It is not enough to have a single point of contact for cyber incidents, the details must also be visible and incorporated into regular training such that staff have the information in the fore-front of their minds.

Does your organisation have a dedicated hotline for reporting cyber incidents?

Source: Survey 2019 (Sample size: 101)

The economic costs of large-scale cyberattacks are already on par, or in some cases exceed losses caused by natural disasters. As the maritime logistics supply chain takes action to protect itself, demand for insurance products is growing. Insurance companies are obviously keen to reduce their exposure to large pay-outs, making them among the industry's strongest advocates for awareness raising campaigns. They disseminate a wealth of loss prevention guidance on technical countermeasures and, more recently, are drawing attention to the importance of developing rapid response plans and recovery programmes that can be called into action following an incident.

In 2018, survey respondants were asked whether cyber breaches they experienced were covered or not by insurance. Where breaches were covered by insurance, two-thirds said the claim was made through a cyber specific policy, while one-third was cleared through traditional P&I. It's probable that those with specialised insurance products would be more likely to seek a claim in the wake of an attack, whereas those protected by normal products may have concluded this was not an option or were deterred by the prospect of having to argue the case with their insurer.

As insurers have grown more involved in cyber defense and recovery, there is an increasing clarity on the obligations of customers and those providing cover. An owner's duty to provide a seaworthy vessel can be broken down into two requirements: firstly, the vessel, crew and equipment must be sound and able to withstand the ordinarily perils of a voyage. Secondly, the ship must be suitable to carry the contractual cargo. The obligation includes the physical state of the vessel, proper systems, manning, documents and also electronic navigational and communication equipment. Failing to protect these systems, and by extension a vessel, against a cyber-attack could be construed as a failure to exercise due diligence to make the ship seaworthy. A further complication is that cyber-risk transcends the traditional wet/dry incident divide.

Insurers will look at what steps an owner has taken to increase resilience before paying out on a claim. This could involve checking whether a company has provided adequate training to its staff; has carried out a formal risk assessment; has introduced sufficient technical safeguards; has conducted penetration testing; and has defined a well-considered response plan.

Do insurance companies pay out?

Yes
16%

No
84%

Source: Survey 2019 (Sample size: 101)

Operational technology

Shutterstock/Mr. Amarin Jitnathum: 512318

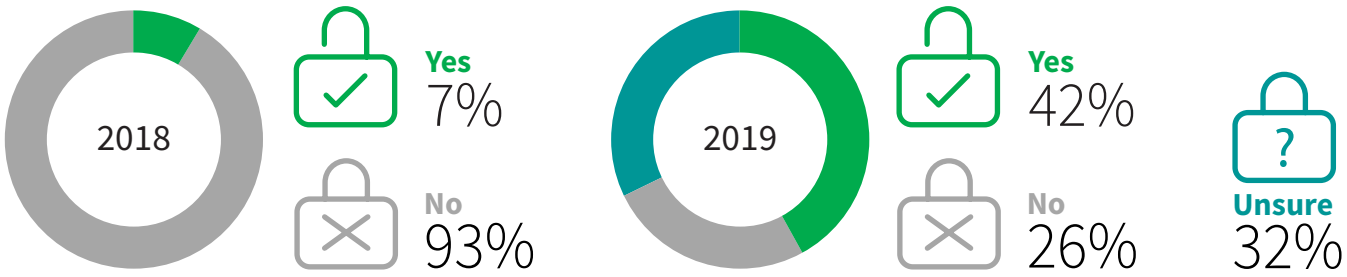
Cyber-threats continue to grow in reach and complexity, with new vulnerabilities discovered on a seemingly daily basis. In the space of a few years, attacks and security breaches have jumped from being an exceptional event to becoming a fact-of-life impacting almost every aspect of ship operation.

One of the reasons for this escalation is that while historically office IT systems were the predominant target, these days, more incidents are endangering operational technology (OT) - the industrial control systems responsible for controlling machinery. This trend reflects a general rise in connectivity, the growing complexity of the systems involved, and the increasing sophistication and expertise of those seeking to disrupt them.

OT systems employ digital technology to manage physical processes and machine operations through the direct sensing, monitoring and or control of physical devices (motors, valves, pumps, etc). In a vessel these systems include plant and machinery for power, propulsion, cargo handling and habitability services as well as navigation hardware.

A roundtable held to discuss the findings of the 2018 survey asked the assembled industry experts to describe how they would go about build a cyber-resilient vessel from scratch. The quickly reached consensus involved standardising onboard systems and embedding cyber security deep in the design of OT solutions from the onset. However, this represents an idealised scenario.

Does your company protect your vessels from OT cyber threats?



Source: Survey 2019

In reality, most vessels sailing today are ageing and using legacy OT that, whether shipping admits it or not, opens the ships, their operating companies and even third-party stakeholders up to cyber threats.

While IT system breaches can temporarily disrupt back-office functions or lead to data loss, resulting in financial or reputational damage, this is true of any industry. An OT cyber breach, on the other hand, could trigger a physical event where someone gets killed, a ship is damaged, or oceans are polluted. These kinds of large-scale events come with high financial and reputational costs, not just to a company but potentially to the entire industry.

It's worth stressing that OT systems cannot be protected from cyber breaches by disconnecting it from the internet or keeping it separate from the rest of the vessel's network. While segregating networks can improve resilience, it will not necessarily stop a crew member from plugging in a USB or tampering with systems. It only takes a single infected USB device to be connected or someone deciding to override a manufacturer's recommendation and connect two disparate systems for a virus or malware to spread (see box story on issues surrounding reliance on air-gaps below).

Only two in five of those polled in *SAS'* 2019 survey could say with certainty that operational technologies (OT) are incorporated in their organisation's cyber-risk assessment and prevention programmes. One quarter said they were yet to be considered, while one third weren't sure either way. Nevertheless, this represents a dramatic improvement over the 2018 study when only 7% of those polled reported OT as a concern.

Measures commonly taken to protect OT from cyber threats among this year's respondents include carrying out internal and third-party risk assessments, training for personnel who use such systems, and introducing rules controlling the use of personal devices on board.

The myth of air gaps

The theory behind the air gap is that in a well-designed system, there is a physical gap preventing any communications between the control network and the business network. Since digital information cannot cross such a gap, bad things like hackers and worms can never get into critical control systems.

However, air gaps are easily overcome. The humble USB is renowned for bridging them. Indeed the now infamous Stuxnet worm that was first revealed to the public in 2010 was believed to have been introduced into a "secure" facility by a USB stick. The all-powerful smartphone is another convenient mechanism to cross air gaps when switched into Wi-Fi hotspot mode.

An innocuous hardware change, such as the connection of a wireless printer to two different networks to produce logs, could expose entire OT networks to an information technology interface. There are automated exploit tools designed to take advantage of such situations.

It was recently reported that Fancy Bear (a group of hackers linked to Russian spy agencies) are using internet of things devices to break into corporate networks. They compromised popular internet of things devices, including a VoIP handset and a printer in order to gain access to corporate networks. Although desktop computers are often top of mind when it comes to security, it's often the peripherals that leave a door open for a hacker to exploit, thanks to the widespread use of default passwords.

Third parties & OEMS

Cyber risk management is further complicated by interactions that shipping companies have with other stakeholders in the maritime supply chain. The role of vendors of equipment and other systems deserves particular attention in this regard.

Many suppliers see potential for delivering added value to their products through digitalisation. This typically takes the form of collecting and siphoning off data about the equipment's operating status, which can be analysed to optimise efficiency and to detect tell-tale signs of potential faults before they become critical. These are noble objectives that will benefit the vessel operator through reduced running costs and prevented downtime.

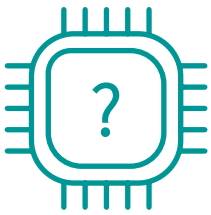
However, these advanced functionalities also bring additional complexity and result in risks becoming opaque. Maritime original equipment manufacturers (OEMs) create specialised solutions with production runs of a only few thousand units - sometimes significantly less. This means they will take a markedly different approach to cyber security than manufacturers addressing larger markets. They simply won't have the same resources to pour into risk management as, say, a major car maker.

These disadvantages of scale however do not excuse OEMs that fail to take even simple measures to protect their offerings and their customers. There have been several instances of white-hat hackers (who specialise in penetrating electronic systems to reveal potential vulnerabilities and weaknesses so they can be made secure) managing to 'break into' equipment using default passwords. Furthermore, these passwords are included in product documentation that is sometimes available online in the public domain for anyone to download.

An overwhelming 83% of respondents to the 2019 survey said they would cancel a contract with a third-party supplier if poor cyber security came to light or their products services were found to be the cause of a cyber incident. There is a clear business case for OEMs to make sure their products are properly hardened against cyber-risk and to engage with vessel owners to make sure they are correctly installed and commissioned.

The challenges associated with managing systems from multiple vendors came under scrutiny during the 2019 roundtable. Purchasing managers generally focus on cost and lack the technical aptitude to appraise the risks or simply fail to appreciate the seriousness of the problem, it was said. It was suggested that shipping might learn from other industries. In aerospace, for instance, there is much greater standardisation. Passenger airlines can choose between Boeing or Aerospace.

Would you stop doing business with suppliers of systems if the cyber resilience of their products was called into question?



Yes
83%

No
17%

Source: Survey 2019 (Sample size: 160)

Risk assessment

Carrying out a formal risk assessment of IT and OT infrastructure spanning an organisation is paramount to the development of effective cyber security policies and procedures. This task is often delegated to internal IT departments. Because digital technology has become so deeply embedded in fleet operation, there is a danger, however, that they will not have the full picture.

They have far less exposure to operational technology (OT) found on ships than colleagues who routinely work with a vessel's various control systems. As such, they may lack the deep understanding that accumulates from months or years of hands-on experience and, as a result, are more dependent on second-hand knowledge.

Of course, the reverse is also true. Superintendents are unlikely to have specialist knowledge of network architecture, configuration management, database design, and so forth. Not only are the systems themselves complex, but so are the chains of responsibility and ownership. It is not unusual for the maintenance of software or embedded systems that manage more sophisticated equipment to be entrusted to vendors – either through a contractual relationship, or a less formal arrangement based on good faith.

This is why a structured and systematic approach to risk assessment that involves all stakeholders is essential. Some vessel managers take advantage of best-practice guides issued by industry bodies, such as BIMCO or the International Chamber of Shipping (ICS). But these should only act as a starting point because each organisation and each vessel will have their own set of individual requirements and unique characteristics.

The sheer number of systems on board modern ships combined with limited time and finite resources means a degree of prioritisation is inevitable. Ranking is both a qualitative and subjective process, and so the rationale behind these decisions should be explained: why was one system deemed worthy of intense scrutiny, while another merited lighter treatment?

The integrity of a vessel's GPS, for instance, is implicitly linked to safe navigation, while an outage of the onboard CCTV system is unlikely to compromise ship safety, at least not directly. Nevertheless, it may perform an ancillary role, for example, keeping an extra eye on crew members carrying out dangerous tasks.

ISM concentrates, of course, on the safety implications of cyber risk. But the commercial and ethical reasons for locking down a vessel's IT and OT infrastructure should also be considered. Preventing feeds from the CCTV system leaking on to the Internet, for example, is important for maintaining good relations with cargo owners as well as protecting the privacy of individual crew members.

Prioritisation is an important part of formulating a proportionate response. Risk is a product of the repercussions of a particular event occurring and the likelihood that it will happen. This means a low impact incident that happens frequently is comparable to and deserves as much attention as a major episode that may only happen once in the lifetime of a vessel. Having defined criteria to measure total risk avoids the vagueness that result from affixing high, medium and low labels in an arbitrary fashion.

The industry is good at assessing risk at high-level in order to produce a figure for insurance purposes. It is also good at the other end of the spectrum, with OEMs offering detailed risk profiles for individual components or equipment. The difficulties arise when it comes to evaluating risks that emerge from systems working together, rather than looking at each system in turn, independently from the others. A common trait of the companies that have succeeded in this endeavour is that they have set up some kind of internal cyber-security task force to bring together knowledge and expertise from different departments.

Were protection strategies in place before the attack?

Yes
74%

No
26%

What is in place to protect against cyber attack?

Firewalls	74%
Intrusion detection/prevention system	45%
Best practice protocols	39%
Physical segregation of networks	30%
Review of log files	21%
Virtual segregation of network nodes	18%
Independent cyber security consultants	15%
Other	11%

Source: Survey 2016

Overall, how do you rate cyber risk to your organisation?

High	Medium	Low
41%	41%	28%

Does your organisation have a business continuity plan in the event of a cyber incident?

(Sample size: 176)

Yes
52%

No
19%

Unsure
29%

When was the business continuity plan last tested? (months)

<3	3–6	6–12	>12	Not tested
23%	24%	17%	14%	32%

Source: Survey 2019

Buy-in from top management is also crucial to make sure the work is adequately resourced. Carrying out a rigorous assessment – particularly for the first time – is a taxing and sometimes overwhelming exercise. The whole purpose is to reveal previously unforeseen weaknesses or unconsidered vulnerabilities.

After the risk assessment has been completed, attention can turn to developing countermeasures to mitigate identified risks. For some items, the solutions are relatively straightforward, maybe altering a systems configuration or introducing new procedures on usage, but others may require more attention, necessitating software upgrades and hardware replacements or rethinking processes and workflows from scratch. These actions too must be fully documented.

The Safety Management System (SMS) developed under ISM necessitates far more than a technical response. It encompasses the provision of training. It also steers shipping companies to defining and assigning responsibilities, such as reporting channels and chain of command when responding to an incident.

Change management and ongoing resilience

As any smartphone or laptop owner will attest, today software is updated to add new features and functionalities on an almost rolling basis. Updates are also important for patching vulnerabilities and generally keeping IT and OT infrastructure secure from the latest cyber threats. However, in contrast to the offshore and other adjacent industries, shipping has traditionally been behind the curve when it comes to employing rigorous frameworks for change management.

Instead software updates are often done on a whim. Because IT engineers seldom have much chance to visit vessels, when they do come aboard to update the ECDIS or set-up the latest version of a maintenance management application, the temptation is to make the most of the opportunity and do some other jobs.

They click to install a new service pack and a backlog of other app updates. Nine times out of ten, this is fine. But occasionally it can unknowingly disrupt settings elsewhere on the system. Moreover, the consequences may not become apparent until long after the engineer has left and the ship has set sail.

For this reason, updates should be carefully planned, tested, approved, and recorded. They should be categorised as minor or major to ensure personnel with appropriate authority can approve. This is virtually identical to the process for gaining approval prior to carrying out structural ‘updates’ to a ship such as hot work.

Email & Ransomware

GettyImages/Scyther5: 5120889

Shipowners and operators are stepping up when it comes to investing in cyber defence. Some 70% of those responding to the 2018 survey said that they allocated up to USD50,000 on cyber security annually. The remainder of respondents spent more.

Despite climbing investment, the modes of attacks encountered most frequently by shipping companies remain broadly unchanged, with phishing, spear-phishing and malware continuing to top the list. It is worth mentioning that these attacks all infect shipping companies in the same way: they land as messages in email inboxes. One notable change observed in 2018 was a sudden rise in those reporting 'theft of credentials', which jumped to 28% from 2% the preceding year, and overtaking ransomware (23%) in that year's data.

The financial impact of a successful attack varies widely. It's not unusual for shipping companies to spend more than USD100,000 recovering from more serious incidents (2018 data: 14% respondents). However, in the vast majority of cases (2018 data: 70%) the outlay was less than USD5,000. This distribution seems to correlate well with the prevalence of ransomware and phishing attacks geared towards financial gain.

Smaller fleet owners and operators are as vulnerable to falling victim to such attacks as the industry's big names. In fact, as far as the criminals behind them are concerned, they often make an easier target as they are unlikely to put the same resource into cyber defence as large organisations. The problem is compounded as small shipping companies often don't think they're 'worth' hacking. It is thought the amounts demanded are set at relatively low levels to sway that targets' response to simply pay up rather than risk the larger expense or disruption that will arise with employing specialists to recover encrypted machines or getting the authorities involved.

In the economy at large, it is estimated upwards of two-thirds of ransomware attacks are directed at small or medium sized companies. Nearly all of the victims had implemented some type of cyber protection but it proved to be ineffective. Research into computer threats by the European Union Agency for Network and Information Security (ENISA) found email to be the dominant vehicle for delivering such attacks, responsible for 92.4% of infections.

What's more interesting, however, is that ENISA found evidence of phishing attacks becoming much more targeted. Criminals are tailoring emails for specific individuals by doing background research into their targets and by deliberately aiming emails at those with privileged access to valuable data, such as financial records.

For example, they send invoices that appear to be legitimate to finance department staff in an attempt to persuade them to wire money to the fraudsters' bank accounts. Another tactic is to make emails look like they come from the

CEO or other high-ranking employees to convince less senior finance staff to wire money to a particular account or grant the impostors access to workers' personal files that are then stolen by the crooks. Such diversion of funds has led to instances of ships being detained because the agents had not received funds for port clearance.

In fact, an incident in the Gulf of Guinea saw cyber-criminals send spoof emails in an attempt to discover details of containerised cargoes, with a view to possibly attacking the vessel and targeting the boxes with highest-value contents.

The more convincing or appealing the email, the greater the chance employees will fall for the scam. It is quite possible workers are completely unaware of how easily they can be manipulated or exploited, and how great a role they will unwittingly play in the fraudsters' schemes. Attacks via email and PDF are particularly dangerous as they are such staples of daily business and because people can be inclined to drop their guard when receiving and opening them.

Criminals often carry out reconnaissance by scouring the web for seemingly trivial information about employees or the company publicly posted by staff. Such details can assist criminals in making approaches to the company more credible. They also mine social-media networks, such as LinkedIn, for officially sanctioned updates. Photos of staff to celebrate winning a new contract might inadvertently show a company PC in the background, from which the fraudster can ascertain the company's operating system, email platform, email address format etc.

As the industry has ramped up security, cyber criminals have responded in kind by modifying their tactics and becoming more sophisticated. They are no longer taking a scattergun approach and hoping for the best; instead they are carefully targeting specific organisations or even specific individuals within those organisations. Because traditional malware defences were not designed to stop bespoke attacks of this type, a constructive first step is to better address the 'human element' by educating staff about the sort of techniques scammers employ to mislead and psychological tricks use to elicit a certain response.

Checking out of payment fraud

Following a checklist may prevent carelessness and help reduce the chances of disaster provided everyone takes the checklist seriously. If employees treat checklists as perfunctory, believing they're annoying or unnecessary, it is more likely that they will skip over key steps. One way to ensure engagement is to let individuals tweak it according to their needs and work styles, rather than sticking rigidly to standardisation. Checks for an employee who frequently received invoices will differ in emphasis from those aimed at colleagues who seldom process payments electronically.

It is important to carefully check the details of an invoice as well as the email address attaching the invoice. Fraudsters will often change only a single letter of an email address to avoid raising suspicion and increase the probability of the payment request being fulfilled.

When paying a party for the first time, individuals should be encouraged to verify their details before making a payment. Training should ask employees to use a new email chain or call the party to verify that they are the displayed sender. It is also vital to check the details of previous payments against those that are being used for a current payment. If there is a discrepancy, staff must be taught to query the change. Ideally, all changes to payment terms must be authorised by a manager.

Companies should establish and maintain a list or database of 'trusted payees' on internal systems and these must be regularly re-verified by calling the party by phone before making any payments.

Lock down that email platform

Technical measures alone cannot prevent fraud-by-email, but they can still make a difference by reducing the number of manipulative messages that employees are exposed to. Third-party mail filtering services are a popular option. These utilise the latest techniques for identifying and intercepting fraudulent messages and scan for malicious code within attachments before they can reach inboxes. Some services cater specifically for the maritime market.

IT teams at individual companies should also double down and adopt a stronger defensive posture when setting up their email systems. One approach that should be employed as standard is TLS cryptography, which provides a way of verifying any mail is secure before it's received and opened by the human recipient. Email systems can be configured such that they will reject non-TLS messages.

The authenticity of incoming messages can be verified as they arrive. Techniques include setting up domain key identified mail (DKIM) as anti-spoofing, which will ensure all mail received has been sent by the domain it purports to be and has not been interfered with en route. The system works by adding an encrypted element to a mail header that is used to check the Domain Name System (DNS) record of the sending domain. The integrity of a sender can be checked using domain-based message authentication reporting and conformance (DMARC).

Be part of the conversation

Industry engagement and information sharing is a vital part of strengthening the maritime sector's defences against cyber-crime. The pace at which these threats is evolving outpaces the actions that any single individual or organisation can take, which is why *Safety at Sea* is seeking partners to collaborate with in order to raise awareness of and disseminate information about practical solutions and cyber safety best practice.

If you would like to be one of the voices at the table, please reach out to:

Tanya Blake: Editor, Safety at Sea (tanya.blake@ihsmarkit.com)
Namrata Nadkarni: Head of content, Safety at Sea (namrata.nadkarni@ihsmarkit.com)

To keep track of the latest news, please visit **www.safetyatsea.net** or sign up to our free weekly newsletter.

Checklist

Shutterstock/Yevhenii Strebkov: 5120890

1 Assess risk

Cyber Security Assessors (CSAs) should adopt a risk management approach to the cyber security threat. They help companies make appropriate and proportionate investment and prioritise risks.

A CSA will involve the identification of essential or sensitive assets and business processes, the possible threats facing these assets and processes, the security controls that are available and the costs of implementing them.

2 Develop a plan

A Cyber Security Plan (CSP) should be holistic and build upon a vessels' ship security plan and factor in the following:

- Physical – restrict access to sensitive systems and maintain access logs
- Personnel – pre-screen and perform periodic background checks of all administrative, engineering and technical personnel with system access.
- Process – implement processes to monitor and log system users.
- Technical – check removable media for malware and password protect consoles

3 Monitor and review

CSPs Cyber Security Plans (CSPs) should be monitored periodically to ensure that they are being correctly implemented and complied with by ship and shore staff.

CSPs should also be reviewed on an annual basis to ensure that they are up to date with the latest issues facing both the maritime and wider industries.

4 Appoint a Cyber Security Officer (CySO)

A CySO should liaise with the company security officer on aspects relating to physical, personnel and process security, and manage all security aspects of cyber-enabled systems.

They must regularly maintain and update the company CSP.

5 Establish a security operations centre (SOC)

The SOC is a centralised unit to deal with issues affecting all cyber related systems across a fleet, and should sit alongside a company's usual operations centre.

The SOC should study potential, emerging and actual threats faced by a vessel, take proactive steps where possible to minimise risk andhandle any security breaches and incidents.

6 Develop a response plan

The CySO and SOC must have an effective crisis management plan in place to handle a cyber incident. If a vessel or company's IT system is compromised by a cyber attack, it could lead to harm and damage to crew, vessels and cargo, business disruption, loss of sensitive information.

The crisis management plan should be periodically tested and reviewed both internally and with external advisors.

Source: IHS Markit

Contacts

Namrata Nadkarni (she/her)
Head of content | Safety at Sea,
Dredging and Port Construction, Ports & Harbors

25 Ropemaker Street | London | EC2Y 9LY
T +44 20 3159 3348
E namrata.nadkarni@ihsmarkit.com

Sales

Sharon Owen (she/her)
Media Account Specialist | IHS Markit Maritime & Trade

163 Brighton Road | Coulsdon | CR5 2YH
T +44 (0)20 3253 2590
E sharon.owen@ihsmarkit.com

IHS Markit Customer Care

CustomerCare@ihsmarkit.com
Americas: +1 800 IHS CARE (+1 800 447 2273)
Europe, Middle East, and Africa: +44 (0) 1344 328 300
Asia and the Pacific Rim: +604 291 3600

IHS Markit®