DNV

WHEN TRUST MATTERS

MARITIME CYBER PRIORITY 2023

Staying secure in an era of connectivity

ABOUT THIS RESEARCH

This report is published by DNV, the world's leading classification society and a recognized advisor for the maritime industry. It is part of DNV's Cyber Priority research exploring changing attitudes and approaches to cyber security in key industrial sectors.

This is DNV's first dedicated Maritime Cyber Priority report. It is published alongside our Energy Cyber Priority 2023 report[1].

The research draws on a survey of 801 maritime professionals along with a number of in-depth interviews with leaders and experts. It was developed by DNV in partnership with FT Longitude (a Financial Times company).

Fieldwork was conducted between March and April 2023. Survey respondents represent a range of functions within the industry, including those with in-depth knowledge of cyber security along with general managers and C-suite executives.

ACKNOWLEDGEMENTS

We would like to thank the following interviewees for their time and insight:

Wayne Arguin, Assistant Commandant for Prevention Policy, US Coast Guard

Peter Aylott, Director of Policy, UK Chamber of Shipping

Jalal Bouhdada, Global Segment Director, Cyber Security, DNV

Svante Einarsson, Head of Maritime Cyber Security Advisory, DNV

Sean Gray, Electrical and Electronics Superintendent, Stena Drilling

Kelly Malynn, Product Leader Cyber Physical Damage Underwriting, Beazley

Paul Meyer, CIO + Managing Director of the AI lab of MEYER Group, Meyer Werft

Commander Monte, Bundeswehr (German Navy)

Stefan Nysjö, Vice President Power Supply - Marine Power, Wärtsilä

Dr. Phanthian Zuesongdham, Head of Division Port Process Solution, Hamburg Port Authority (HPA)

The Group CIO of a global energy infrastructure and technology company

[1] Energy Cyber Priority 2023, DNV

801
maritime professionals surveyed

72
countries represented

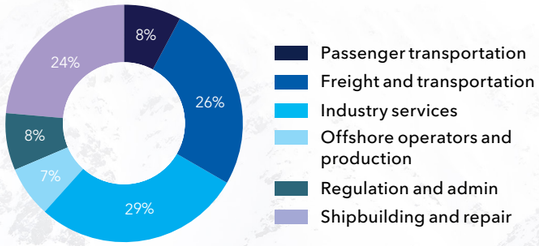
70%
support, develop or operate operational technology

11
in-depth interviews with industry leaders

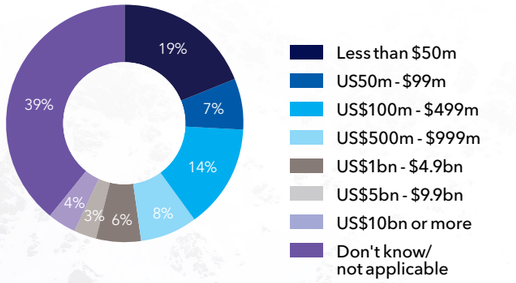
SURVEY DEMOGRAPHICS

We thank our survey respondents from across the maritime industry.

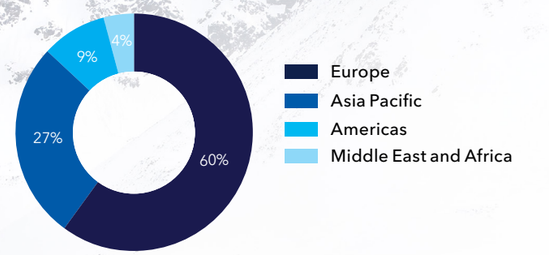
Sector



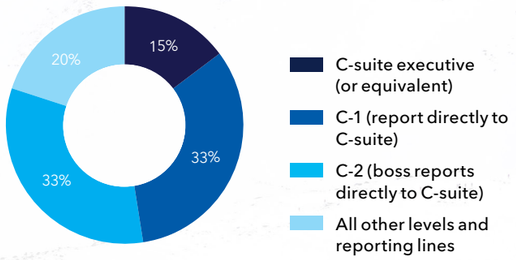
Annual revenue of organization



Region



Seniority



CONTENTS

1 Cyber security is a growing maritime risk 7
OT vs IT: The two sides of the threat 10
Industry recognises safety risk, but business risks still the priority 12
Connectivity is unlocking bold ambitions and new vulnerabilities 14
Profile of adversaries is broadening 16

2 Industry responding, but not fully prepared for the threat 19
Cyber resilience remains a complex task 22
Many factors driving investment and focus on cyber security 24

3 Five key challenges facing the sector 27
Investment is lagging behind what is needed 28
Questions about the effectiveness of regulation 28
Ageing assets and supply chain vulnerabilities 32
Knowledge silos are holding back maturity 35
Talent shortages and workforce vulnerabilities 36

4 Recommendations 41

1 CYBER SECURITY IS A GROWING MARITIME RISK

1 CYBER SECURITY IS A GROWING MARITIME RISK

Maritime professionals expect disruptive incidents in the coming years, including impacts as serious as the closure of major ports and waterways.

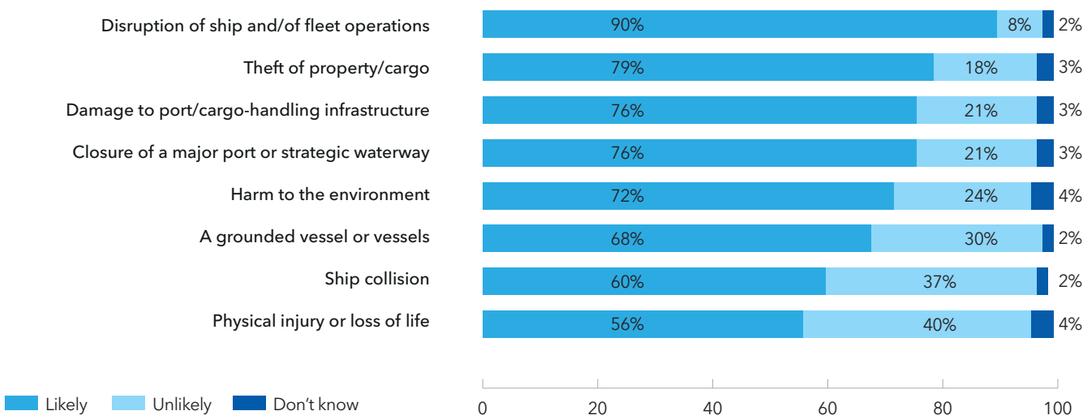
The 'NotPetya' attack on Maersk represented a step-change in awareness about the severity of the cyber threat facing today's maritime sector.

It started one morning when Maersk's employees began receiving strange messages on their laptops – warning them that their files had been encrypted and could only be unlocked with a bitcoin payment worth $300. Two hours later, the company's entire global network had been disconnected. Maersk was unable to process shipping orders until its systems were restored, freezing revenue from its container line business and contributing to a total loss of some $300 million[2,3].

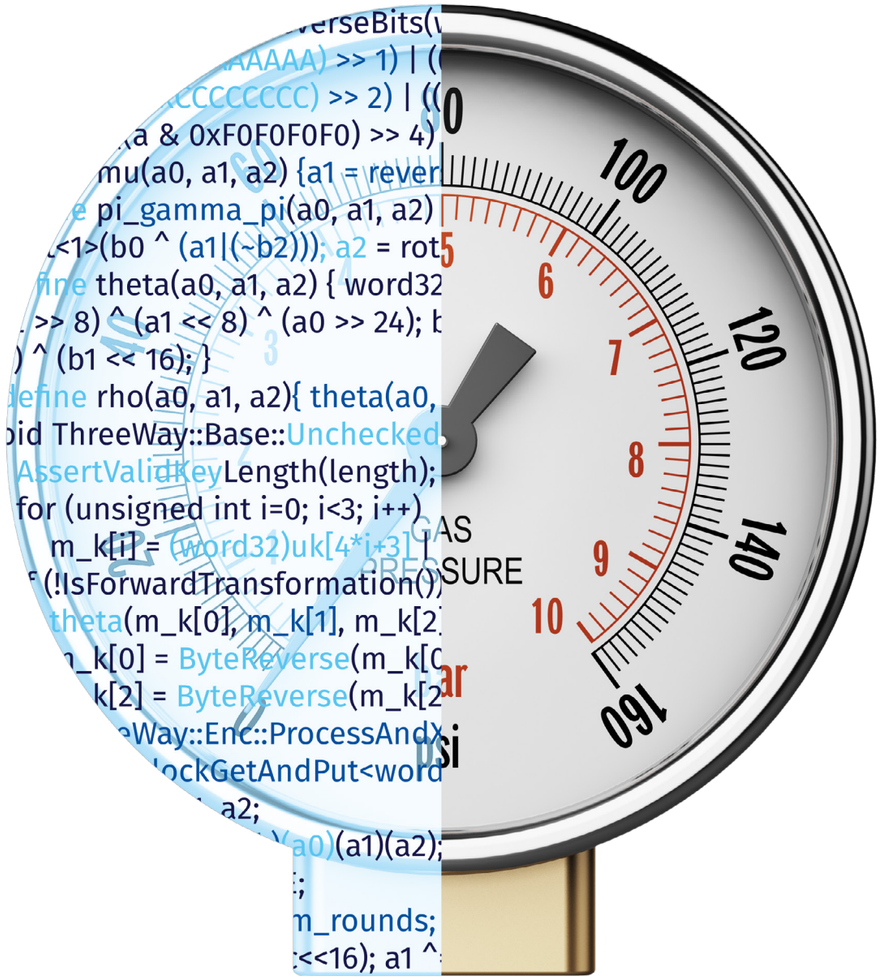
Since this incident in 2017, shipping majors like Cosco, MSC and CMA CGM have all experienced high-profile attacks, with a flurry of incidents in the early 2020s taking e-commerce platforms and vital data centres offline[4,5]. DNV experienced a ransomware cyber-attack on the servers of its ShipManager software in January 2023[6], and other organizations serving the maritime industry such as the International Maritime Organization (IMO)[7] have also been targeted. The Port of Los Angeles recently announced that it records twice as many attacks as it did just a few years ago and must now contend with 40 million ransomware, malware and spear-phishing incidents each month[8].

Although events like these cause significant financial and reputational damage, arguably they don't come close to being a worst-case scenario for a cyber incident in the sector today. DNV's new survey of 801 maritime professionals, carried out between March and April 2023, suggests that cyber-attacks could further disrupt global shipping and are even likely to threaten physical health and safety.

Maritime professionals expect serious outcomes from cyber in the near future



Q: How likely is it that cyber-attacks in the maritime industry, within the next one or two years, could result in the following outcomes? Percentages reflect likely/unlikely (i.e. moderately + highly likely, and moderately + highly unlikely).



According to our research, more than six in 10 industry professionals expect cyber-attacks to cause ship collisions (60%) and groundings (68%) within the next few years. More than three-quarters (76%) believe a cyber incident is likely to force the closure of a strategic waterway. As we saw during the blockage of the Suez Canal in 2021, such a closure can cause a global supply shock – in this case holding up some $10bn worth of cargo every day [9].

[2] The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired
[3] The Cost of a Malware Infection? For Maersk, $300 Million, Digital Guardian
[4] MSC confirms malware attack caused website outage, Seatrade Maritime
[5] CMA CGM targeted by hackers in new cyber attack, Offshore Energy
[6] Cyber-attack on ShipManager servers, DNV
[7] IMO hit by cyber attack, Seatrade Maritime
[8] Cyber-attacks on Port of Los Angeles have doubled since pandemic, BBC
[9] In Suez Canal, Stuck Ship Is a Warning About Excessive Globalization, New York Times

OT VS IT: THE TWO SIDES OF THE THREAT

Growing concern about the severity of cyber-attacks reflects an expansion in the kinds of technology systems that are vulnerable to infiltration.

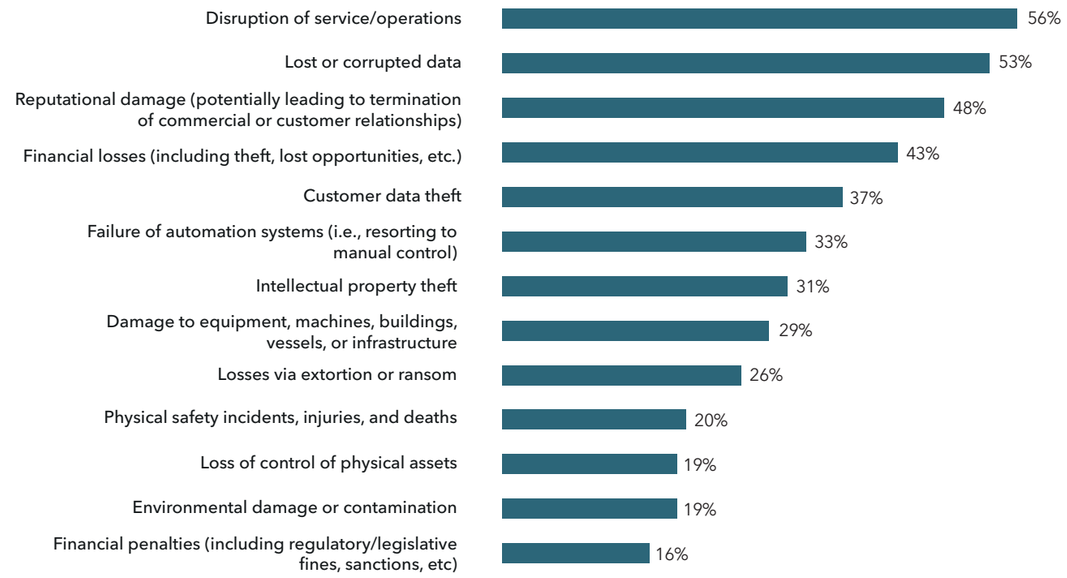
Whereas maritime companies have, for several decades, been safeguarding their data and the IT environments in which that data is stored and transferred, the cyber security of their operational technology (OT) – which governs physical assets including sensors, switches, safety and navigation systems, and vessels – has been less of a priority.

One reason for this is that, until relatively recently, operational systems, particularly aboard vessels, were not connected to wider IT environments, meaning that OT was protected by an air gap that insulated it from connected networks. This air gap is now closing as industry assets and infrastructure become more networked and connected. In turn, the attack surface is widening as potentially vulnerable protocols, interfaces and communications channels come on stream.

In April 2023, an attack on the industrial control systems of Fincantieri Marine Group – a shipbuilder with ties to the US government – left critical manufacturing equipment unusable[10]. The Port of Antwerp experienced attacks on its oil terminals in 2022, affecting the unloading of barges at the height of an energy crisis in Europe[11].

Although attacks on IT environments can and do disrupt normal shipping operations, as was the case during the NotPetya incident, it is through direct attacks on OT that the greatest threat to physical safety and infrastructure becomes possible.

IT security related impacts dominate industry concerns



Q: Thinking about the potential impact that a cyber-attack could have on your organization, which of the following consequences do you think are the most concerning – in terms of their severity combined with their chance of happening?

As well as enabling threat actors to demand ransom, steal intelligence and cause widespread disruption – which hackers can also achieve by breaching IT networks – attacks on OT systems can disable assets or safety controls. Indeed, 56% of maritime professionals expect cyber-attacks to cause physical injury or death in the industry within the next few years.

Paul Meyer, the Chief Information Officer of shipbuilder Meyer Werft in Germany, says OT-related cyber risks are increasingly front of mind for shipping companies.

"The priority is always to make sure that the ship sails safely, but it might not even be manoeuvrable if both the IT and OT systems were compromised," he says.

In terms of the impact of attacks, factors relating to both IT and OT threats – like disruption to operations, financial loss, and reputational damage – are of greatest concern to maritime professionals. However, concerns about impacts relating to the IT environment, such as loss of data, come far ahead of outcomes that are exclusive to OT attacks, including physical safety incidents and loss of control of physical assets. This suggests it is still IT cyber-attacks, not OT attacks, that are top of mind in the industry.

"Ship systems are being increasingly connected with the outside world," says Jalal Bouhdada, Global Segment Director, Cyber Security, DNV. "This brings many benefits, but it also means cyber-attacks on vessels systems are likely to have a greater impact in the future."

[10] US Navy Contractor Fincantieri Marine Group Hit by Cyber-Attack, Infosecurity
[11] Major European ports hit by cyberattack, Port Technology International

INDUSTRY RECOGNIZES SAFETY RISK, BUT BUSINESS RISKS ARE STILL THE PRIORITY

A clear majority of maritime professionals believe that cyber security risks are considered as important as health and safety risks in their industry.

Our assessment is, however, that there is still a gap in maturity in how the industry manages the two risks in practice, with cyber security having significant room for improvement before it could be said to be treated as seriously as physical health and safety. Maritime businesses are committed in principle to improving the security of their OT systems, and thereby minimizing the risk of cyber-related safety incidents, but their actions and priorities – with respect to regulations, workforce and investment – suggest they are still more focused on the IT rather than the OT side of cyber security, and on its business risk rather than its safety risk implications.

At the UK Chamber of Shipping, Peter Aylott suggests that safety risk is likely to remain a higher priority than cyber risk until charters apply more scrutiny to the cyber resilience of vessels and other maritime infrastructure. This aligns with our finding that charter requirements, although seen as drivers of cyber investment by 56% of maritime professionals, are still less likely to unlock budgets than financial and reputational damage (84%) or regulatory stipulations (84%).

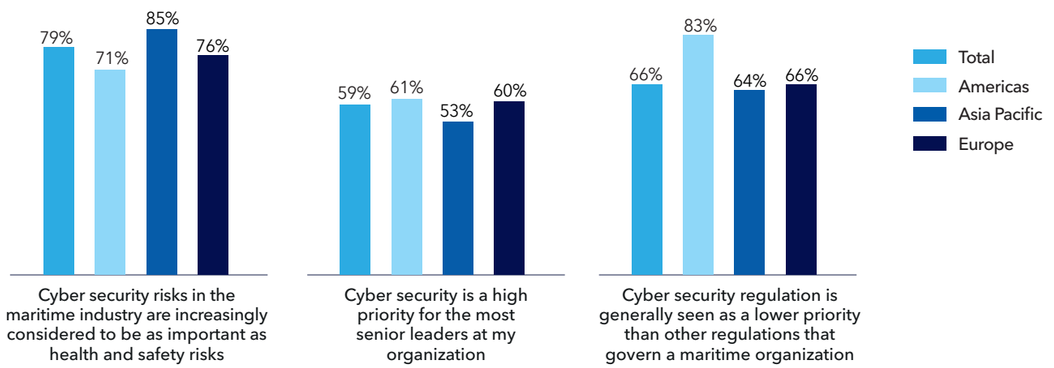
"A charter's vetting inspection of a ship will look at safety and, these days, at its carbon footprint," Aylott says. "It won't look necessarily at the risk of an ICT incident, but I think we are getting towards the place where that will need to be carried out."

Moreover, despite the effort they are putting into securing OT systems – in recognition that a cyber-attack may lead to a safety incident in the future – maritime professionals will inevitably give greater priority in the short term to an immediate physical safety risk.

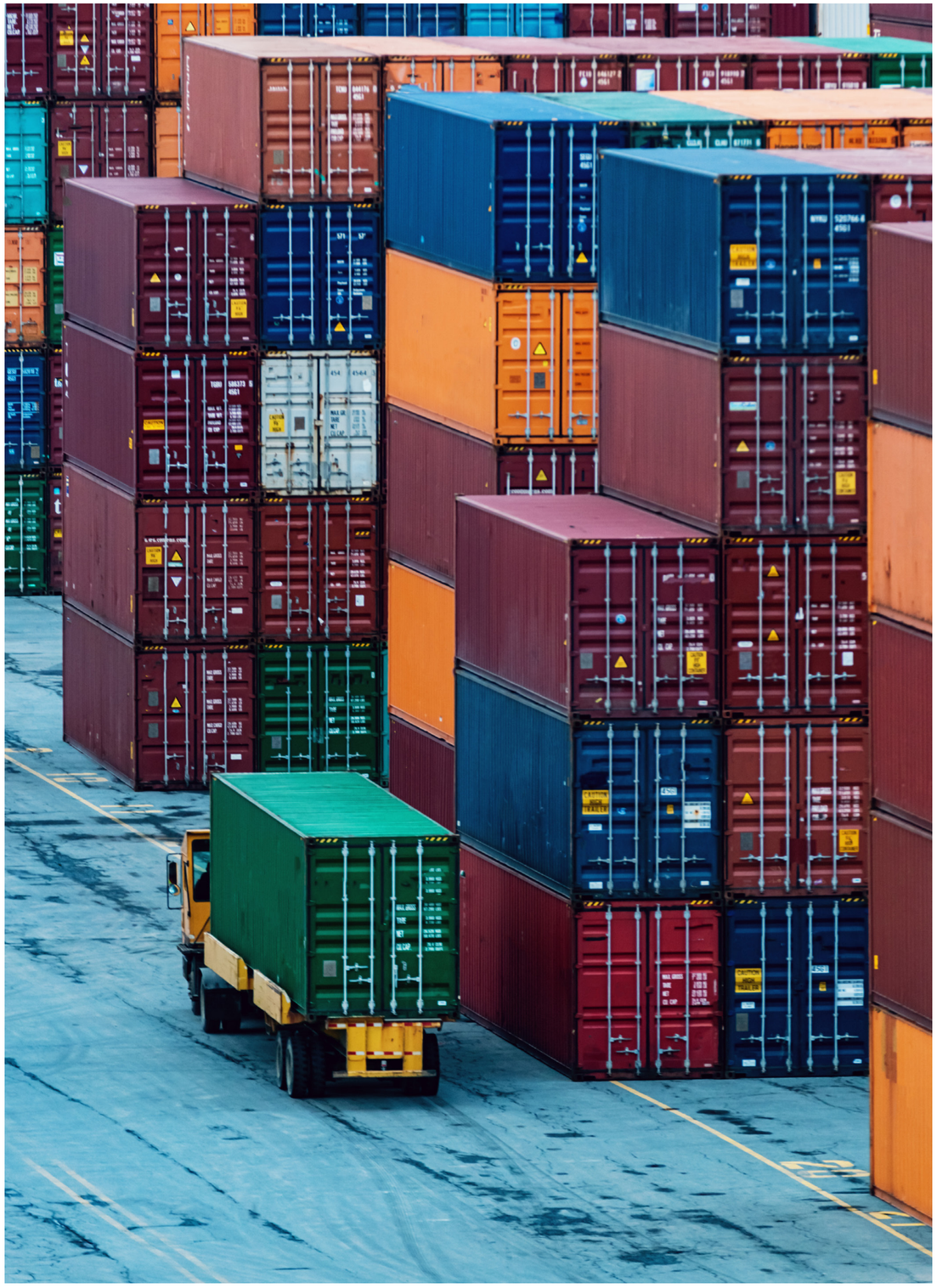
Sean Gray at Stena Drilling explains that there can even be a conflict between implementing cyber-security upgrades to OT and maintaining safety principles onsite.

"Someone in IT would consider it sacrilege to skip a security update to their laptop, but that is not practical on a control system running safety-critical software," he says. "We've all had updates that stop a computer from working, and we can't risk a similar effect on a blowout preventer or other control system."

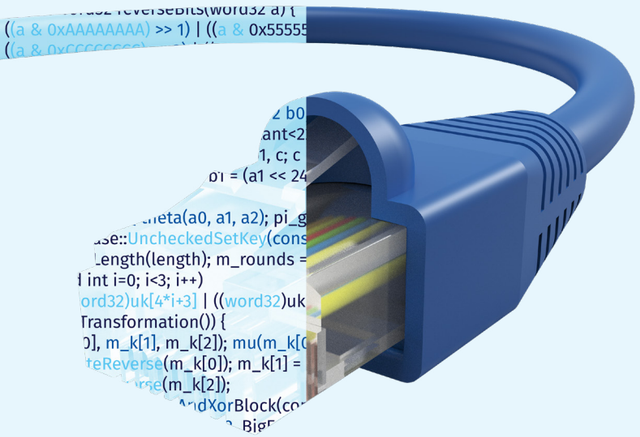
Cyber security a rising business concern, but cyber regulation is a lower priority



To what extent do you agree or disagree with the following? Percentages reflect net agreement (i.e. moderately + strongly agree)



Connectivity is unlocking bold ambitions and new vulnerabilities



Advances in digital and connected technologies are enabling a greener, safer and more efficient global shipping network. In an increasingly competitive industry, these tools represent a major opportunity for maritime companies.

In our research, 85% of maritime professionals believe that connected technologies are helping the industry reduce emissions through fleet and route optimization. Many have already embarked on this journey. More than half (51%) describe digital technology as a key enabler of their existing decarbonization plans, rising to 61% of freight transportation firms, which have faced growing scrutiny in recent years over their use of high-carbon bunker fuel[12].

As well as improving sustainability performance, digital technologies provide safety advantages by automating and streamlining complex processes, which help to enhance safety at ports and at sea. In the words of the United Nations Conference on Trade and Development, digitalization is helping the industry navigate the "efficiency, optimization, reliability, visibility, resilience, predictability, and sustainability" challenges of the post-Covid economy[13].

The upshot of these developments is that maritime businesses today face a choice between connecting their assets and infrastructure at pace or potentially under-performing relative to their peers on several key metrics.

"Every ship owner is looking to optimize and run their ships more efficiently, without having to go in and replace major gear," says Wayne Arguin, Assistant Commandant for Prevention Policy for the US Coast Guard. "To maximize the return on investment, to improve efficiency and effectiveness, you use real-time information that is broadcast directly from ships. If you closed those communications doors to prevent vulnerabilities, you'd be putting yourself at a competitive disadvantage."

The corollary of these developments is that the issue of OT cyber security becomes more pressing every day. Simply put, the more connections that a system has, the likelier it is that a breach will occur. And, when it does occur, the breach spreads further, wider and quicker than ever before.

Moreover, there are some parts of the industry where operators do not have a choice but to connect their existing assets.

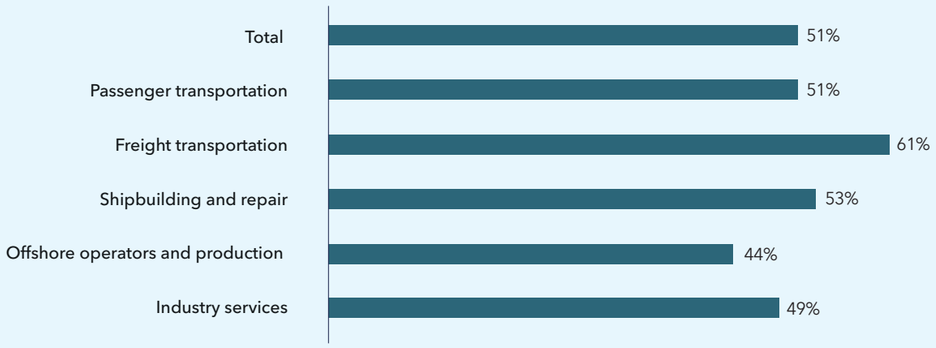
"Governments, regulatory bodies, and clients are all forcing us into the world of digitalization to connect control systems for real-time monitoring.

It's always been islanded in the past, but now there is a requirement for it to send real-time data to shore."

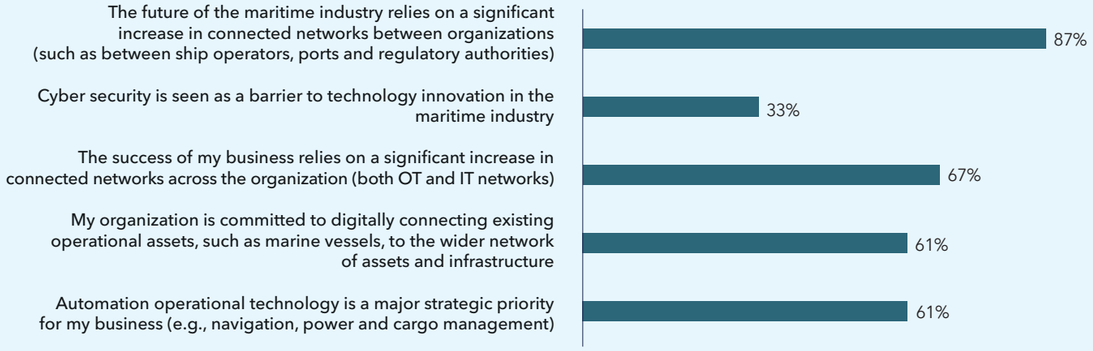
Sean Gray, Electrical and Electronic Superintendent at Stena Drilling

Freight transportation is relying more heavily than other sectors on connectivity to enable decarbonization

Extent to which respondents agree that digital technology is a key enabler of their organization's decarbonization activity.



Strong sentiment that greater connectivity is key to the industry's future



Q: To what extent do you agree or disagree with the following? Percentages reflect net agreement (i.e. moderately + strongly agree).

[12] Pressure grows on shipping industry to accept carbon levy, The Guardian
[13] Review of Maritime Transport 2022, UN Conference of Trade and Development

PROFILE OF ADVERSARIES IS BROADENING

In parallel with the movement towards greater connectivity in maritime, the profile of adversaries is broadening. Today, a growing rollcall of malicious and inadvertent threat actors is targeting maritime companies' OT networks.

As their specific methods vary – comprising everything from phishing tactics that trick employees into downloading malware, to collaborating with insiders with access to restricted networks[14] – individual threat actors are best understood in relation to their ultimate objectives. Whether they are nation states attacking critical infrastructure, criminal gangs looking for ransom pay-outs, or politically motivated hacktivists using tools from the dark web, we can expect a growing number to target OT systems as way to achieve their goals.

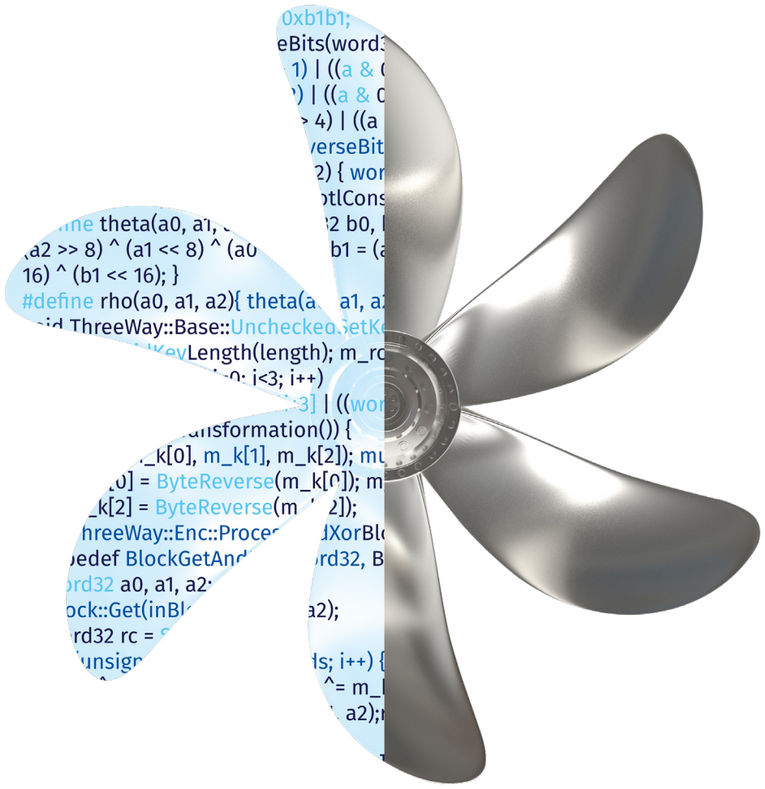
Commander Monte of the German Navy, believes that rising geopolitical tensions increase the possibility that a coordinated attack on OT will take place.

"The attacks focus more on the disruption of trade and infrastructure, rather than purely criminal activity focused on the extortion of money," he says. "Commercial shipping may be the single most important link in globalized trade and logistics. That implies a huge risk for coordinated cyber-attacks on commercial shipping."

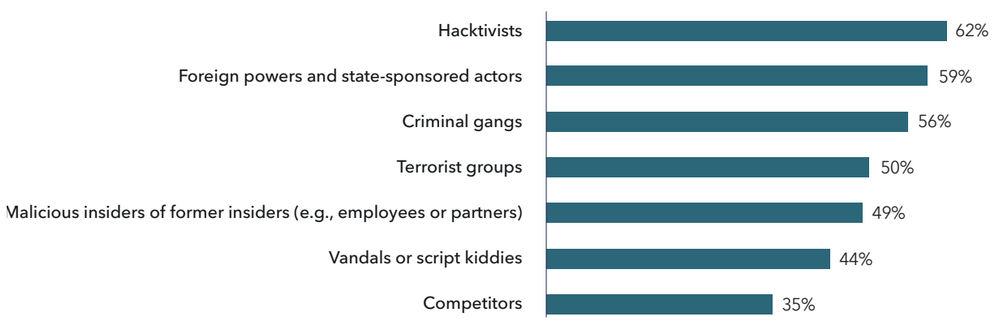
The context is that Russia's invasion of Ukraine has increased cyber security concerns in sectors operating critical infrastructure. In DNV's Energy Cyber Priority 2022 report[15], focusing on the energy industry, we saw an increase in the perceived threat posed by all forms of cyber-criminal in the two weeks following the invasion in February 2022. Attacks on OT materialized soon after with the Russian cyber-attack on satellite internet operator ViaSat[16], which deactivated thousands of wind turbines in Germany. More than a year later, the maritime industry is also on high alert, particularly in Europe.

It is worth noting that, although the Ukraine conflict may explain additional attacks by state actors and hacktivists, other threat actors are likely to have become more wary of attacking OT out of concern that their actions may be mistaken for those of a hostile power.

"None of the financially motivated threat actors wants to be the reason why there's an escalation in the physical war," says Kelly Malynn, Product Leader Cyber Physical Damage Underwriting at the insurer Beazley. "Some are being more careful about who they select and how they deploy ransomware because there might be a very kinetic response if they were to accidentally cause an OT or critical issue."



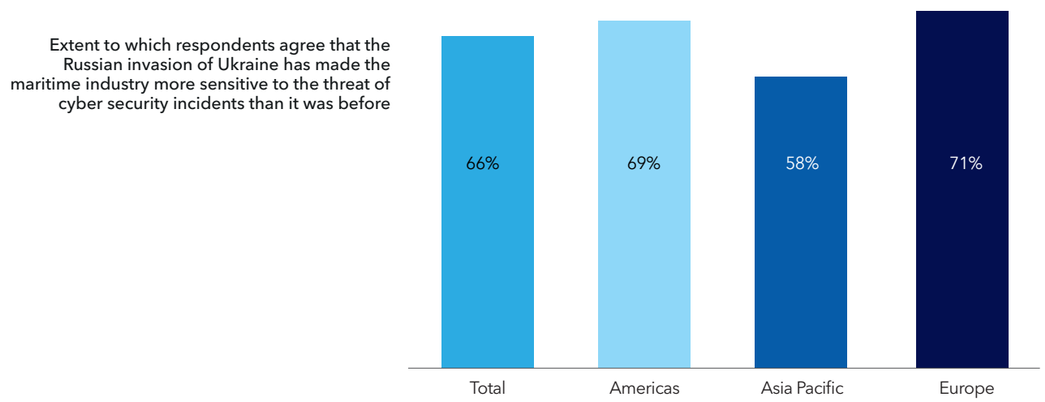
Hacktivists and foreign powers, which may share the same objectives, are the top threat today



Q: How concerned are you about the potential for the following threat to harm your organization? Percentages reflect moderate or major concern

[14] Defining Insider Threats, US Cybersecurity & Infrastructure Security Agency
[15] Energy Cyber Priority 2022, DNV
[16] Russia's Viasat Hack Exposed Satellite Industry's Security Flaws, Bloomberg

Russia's invasion of Ukraine has increased awareness of the cyber security threat in the maritime industry



2 INDUSTRY RESPONDING, BUT NOT FULLY PREPARED FOR THE THREAT

2 INDUSTRY RESPONDING, BUT NOT FULLY PREPARED FOR THE THREAT

The maritime industry is still thinking IT, in an era of connected systems and assets.

As the frequency of cyber-attacks on OT and IT grows, and as regulatory requirements around cyber become more exacting in response to heightened awareness of the threat, maritime leaders are taking steps to strengthen their security posture.

Some 32% of maritime professionals report that they have experienced negative outcomes as a result of IT-targeted cyber-attacks, compared to 23% for OT attacks. Regionally, maritime professionals in Asia Pacific are more likely to report their organizations have been affected by such attacks (38% for IT, 34% for OT).

This relatively high incidence of attacks may explain why 75% of maritime professionals say OT cyber security is a higher priority for their organizations today than it was two years ago.

Among respondents to our survey, we find a broad level of confidence about their organizations' preparedness. More than eight in 10 (82%) believe that they are moderately or well prepared for an attack on their IT systems. Among those who have previously experienced negative outcomes as a result of IT-targeted cyber-attacks, the confidence level rises to 88%, suggesting that their remediation efforts in the wake of the incident may have made their organizations more secure.

It is notable, however, that maritime professionals are less confident about the resilience of their organization's OT cyber security.

Just one in three is confident that their organization's OT cyber security is as strong as its IT security. Around the same proportion (32%) is very confident in their organization's ability to prevent direct cyber-attacks on their OT systems, compared with four in 10 who say the same about their organization's IT environments.

At the same time, less than one in five respondents (19%) says they would describe themselves as very well prepared to respond to and recover from a cyber-attack on a vessel while it is at sea – a sentiment that will give little comfort to stakeholders, not least among the crew on board, who could find themselves stranded in inhospitable waters hundreds of miles from a port facility where help is available.

"I think the maritime industry is not well prepared for the risk of a cyber-attack on a vessel at sea," confirms Commander Monte of the German Navy. "It is a side-effect of the ever more digital and integrated systems on any modern vessel."

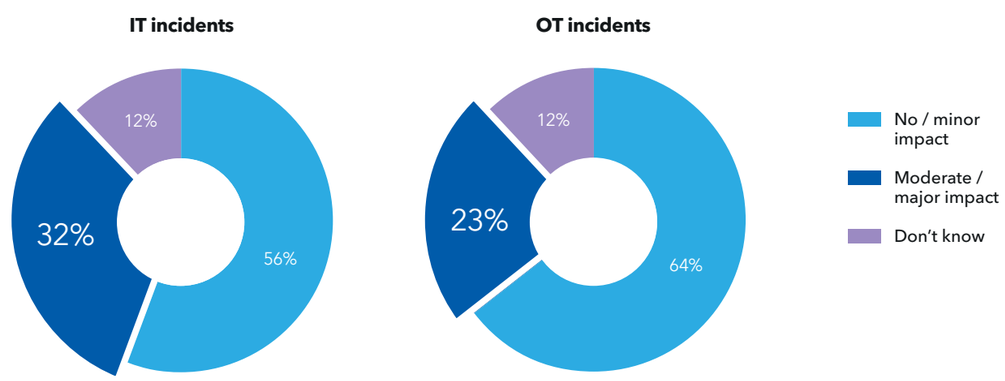
32%
agree that their organization is very well prepared for preventing direct cyber-attacks on its OT systems

40%
agree that their organization is very well prepared for preventing direct cyber-attacks on its IT systems

19%
agree that their organization is very well prepared for responding and recovering from a cyber-attack on vessels at sea

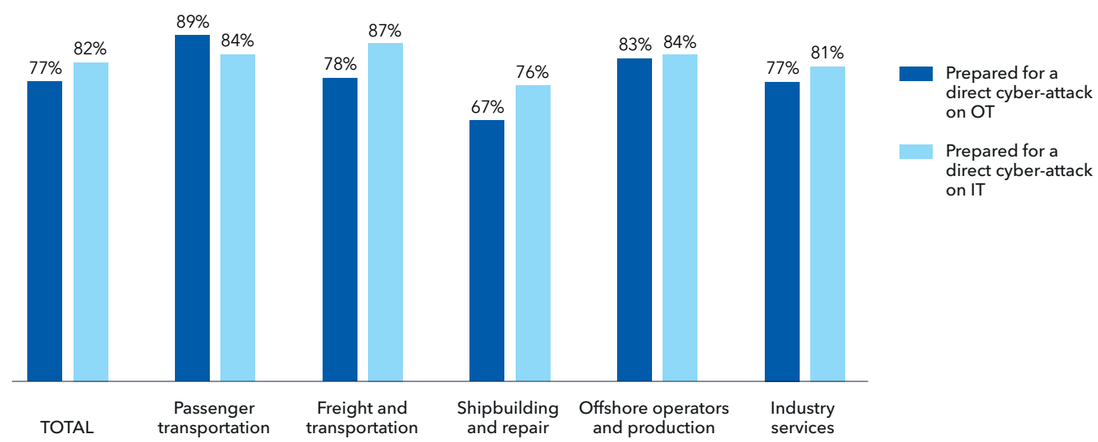
30%
agree that their organization is very well prepared for responding and recovering from a cyber-attack on onshore facilities

Sizable share of maritime professionals say cyber incidents have had a negative impact on their organization



Q: To what extent have cyber incidents had a negative impact on your business during the last five years?

Maritime professionals say they are moderately or very well prepared for a direct cyber-attack on their OT and IT systems



Q: How prepared is your organization for the following aspects of cyber security? Percentages reflect net prepared (i.e. moderately + very well prepared)

CYBER RESILIENCE REMAINS A COMPLEX TASK

Maritime professionals believe they know what to do to embed a stronger security posture. Almost three quarters (71%) claim, for example, that their organizations understand what is required to protect their OT environments from attack.

The danger is that, despite all the controls that businesses can put in place to protect their organizations, it remains extremely difficult to contain a breach within a connected enterprise. Svante Einarsson, Head of Maritime Cyber Security Advisory at DNV, cautions against overconfidence in systems.

"Some assume there is an easy way to isolate compromised operational technologies during an attack, to prevent the worst consequences and to prevent the attack from spreading to other assets," he says. "But because of connectivity, the spread might have already happened. And multiple systems will need to switch to manual, but manual operation of many systems at the same time can be difficult and dangerous."

The uncontainable nature of a major cyber incident is something that Wayne Arguin, Assistant Commandant for Prevention Policy at the US Coast Guard, contrasts with an extreme weather event.

"If a hurricane is coming, the weather service can tell us what its track looks like, what the intensity's going to be and which areas will be impacted, so we can focus our resources. Cyber-attacks don't provide the same indicators and warnings and are not geographically bounded."

Wayne Arguin, Assistant Commandant for Prevention Policy at the US Coast Guard

Arguin adds that an organization's confidence in its cyber security is difficult to quantify because there are so many unexpected consequences of an attack.

"When it comes to recovering from an attack, the potential for cascading effects is pretty high," he explains. "Let's say that a ship on its own gets attacked. This has a small, manageable footprint, but the cascade goes to the rest of the fleet, which could be all the way around the world."

71%

agree that their organization understands what is required to protect its OT systems from cyber attacks

56%

agree that cyber is largely seen as an IT rather than an operational issue in their organization

33%

agree that their organization's OT cyber security is just as strong as its IT cyber security

MANY FACTORS DRIVING INVESTMENT AND FOCUS ON CYBER SECURITY

Asked what drives the most cyber security investment in their organizations, maritime professionals point to two factors above all: financial and reputational damage, and regulation and compliance stipulations - with 84% of maritime professionals saying these factors are driving cyber security investment. But the overall picture is that there are many drivers of investment and focus on cyber security.

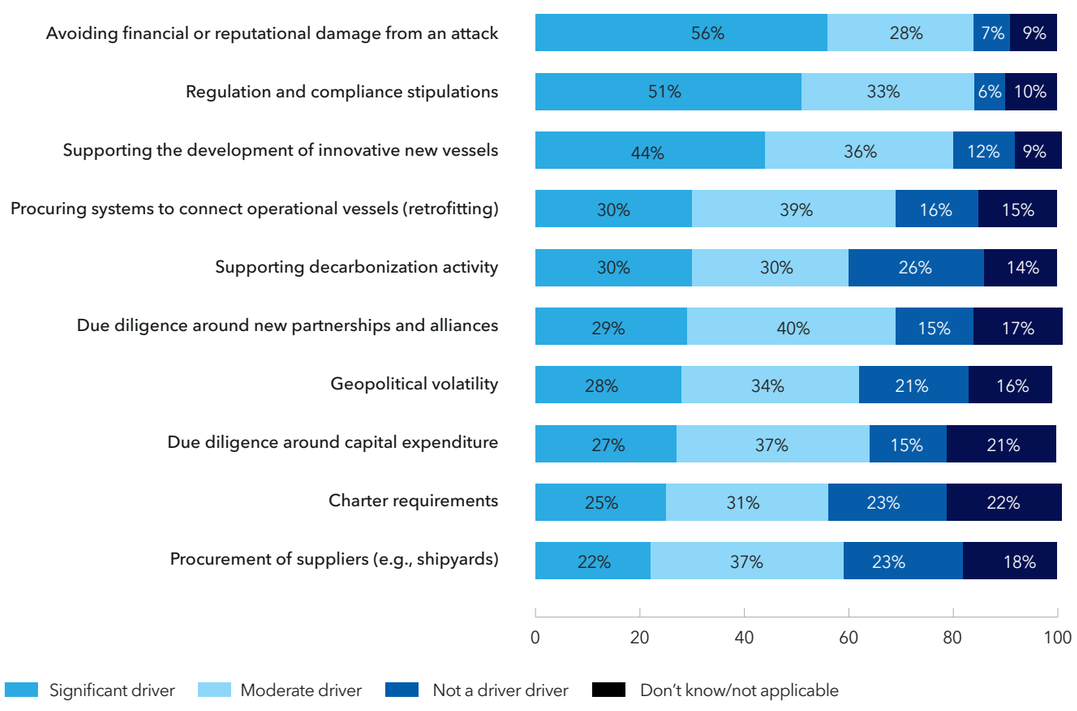
It is in some ways unsurprising that avoiding financial and reputational damage is a key driver of investment, considering that this has been the main consequence of recent cyber-attacks. On the other hand, its prevalence among respondents suggests that, despite the many high-profile attacks that the industry has seen in recent years, maritime organizations may still be waiting for it to happen to them, or for it to happen more severely, before they unlock more investment.

Securing investment can also be a communication challenge. In our interviews, we heard that securing investment for cyber initiatives in the sector is generally becoming easier than it was a few years ago, but only if the case can be made to the board in terms of risk assessment rather than technical upgrades.

"Boards care about the risks for the business, not about technical details or IT vs OT."

Svante Einarsson, Head of Maritime Cyber Security Advisory, DNV

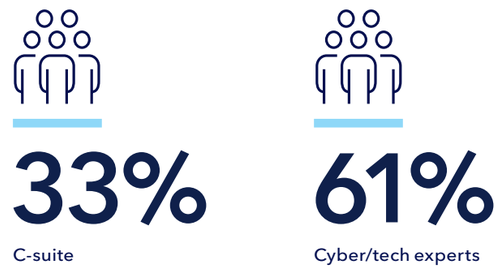
Regulation and reputation leading drivers of cyber security investment



Q: Which of the following factors are currently driving cyber security investment and activity within your organization?

Most senior managers differ from cyber/tech experts, in seeing OT and IT as a single responsibility

Extent to which respondents agree that IT cyber security and OT cyber security are the responsibility of different teams in their organization



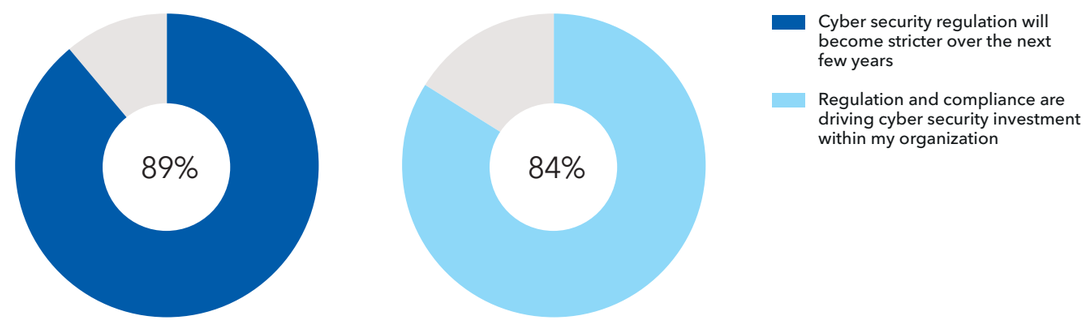
From the C-suite perspective, cyber security often falls under the remit of the CIO or CISO, regardless of whether its focus is IT or OT. With that in mind, it is understandable that C-suite respondents are much less likely than the cyber experts in our research – who have stronger-than-average knowledge of cyber risk, and work in a related profession – to agree that IT and OT fall under different areas of responsibility. To senior management, it is all just cyber security.

The other top investment driver is regulation, which is significant in an era of tightening rules and directives in the industry. The question is whether maritime organizations make the most of this opportunity to translate regulation-driven investment into cyber resilience.

Among other drivers of investment, we see recognition that connectivity and digital innovation will require greater investment in cyber security. We also see the effect of third-party pressure on the industry, in the form of due diligence, charter requirements, and procurement – with more than half of maritime professionals saying these factors are driving their organization's cyber security investment.

Kelly Malynn at Beazley says senior leaders need to be prepared to show how they are mitigating systemic risk. "There is no way that a maritime organization today could claim that it wasn't aware of cyber risk," she says. "Management teams must be able to explain which provisions they have taken to ensure their vessels are seaworthy despite the threat."

Stronger regulation will be a key driver of cyber security investment



Q: To what extent do you agree or disagree with the following? Percentages reflect net agreement (i.e. moderately + strongly agree)

3 FIVE KEY CHALLENGES FACING THE SECTOR

3 FIVE KEY CHALLENGES FACING THE SECTOR

The maritime industry faces major cyber security challenges in investment, regulation, supply chains, organizational culture, and access to talent.

INVESTMENT IS LAGGING BEHIND WHAT IS NEEDED

Despite the threat of cyber-attack in today's maritime sector, and the many factors potentially driving investment, industry professionals say their biggest cyber-related challenge is insufficient funding.

Just four in 10 maritime professionals believe that their organizations have invested enough money in their OT cyber defences to date. As OT cyber security is a relatively new concern, this could be because it takes time to build up a new discipline from scratch. Nonetheless, the figure only rises to 47% when the same respondents are asked whether they have invested enough in their longer established IT cyber programmes.

Perception around investment is noticeably higher among professionals in freight transport than it is among passenger transportation and industry services professionals, perhaps due to the high-profile attacks on major container lines over the last decade, combined with the importance of connectivity in decarbonising this sub-sector. However, industry professionals across the board do not think their organizations are investing enough.

QUESTIONS ABOUT THE EFFECTIVENESS OF REGULATION

Regulation pertaining to cyber security is becoming more stringent in the maritime sector, but compliance alone is unlikely to be sufficient in an industry where the cyber threat is evolving fast. Regulation invariably represents a response to threats and issues that have already been identified.

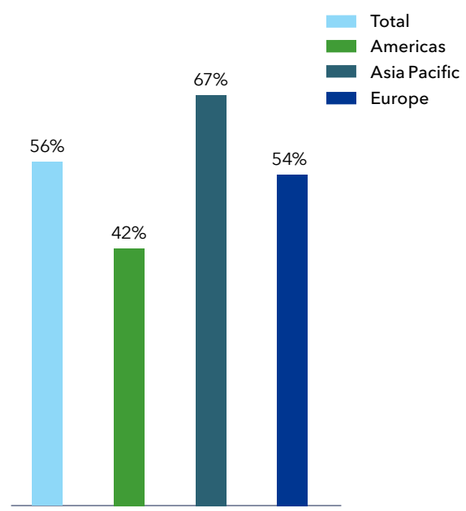
Considering what is at stake, cyber maturity comes down to being proactive rather than 'ticking boxes' – a point that should be highlighted when the case for investment is made. It is worth noting that, in our research, just 56% of maritime professionals believe that regulation alone is enough to keep them sufficiently secure from cyber threats.

Svante Einarsson, Head of Maritime Cyber Security Advisory at DNV, believes that regulation should be seen as a baseline on which to build a best-in-class security posture.

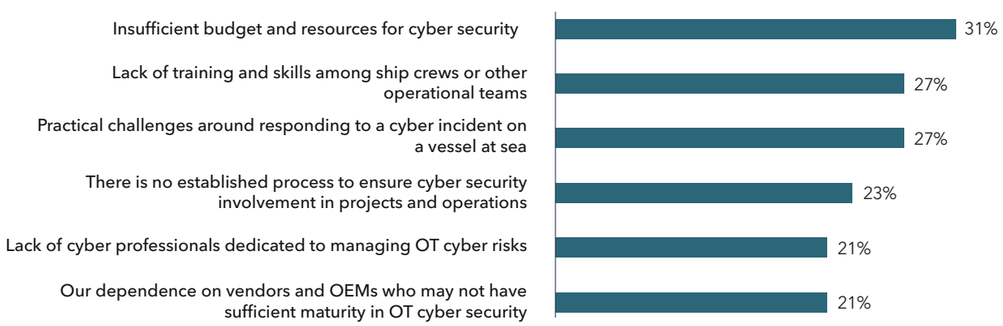
"The preferred way forward is to apply cyber secure technical design rules in combination with tailored cyber risk management – striving for adaptation and continuous improvement," he says. "Compliance needs to be complemented by work to identify and manage new risks and weaknesses with a proactive but practical mindset."

Only half maritime professionals believe compliance will keep the industry secure from cyber threats

Extent to which respondents agree that compliance with cyber security regulation will keep maritime organizations sufficiently secure from cyber threats

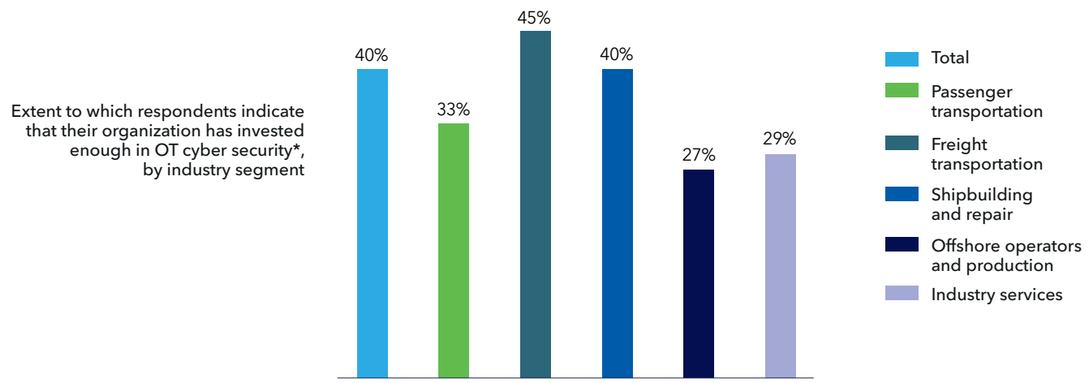


Lack of funding is the biggest cyber-related challenge



Q: What are the top challenges that the cyber security function in your organization faces in managing security risks (select top three)?

Professionals in freight transportation more likely to say their organization has invested enough in OT



**Data is based on net disagreement with "my organization has NOT invested enough in OT cyber security"*

Businesses are struggling to comply with the existing rules

If businesses are to regard cyber regulation as the baseline for cyber security, it is concerning that many in today's sector appear to be struggling to comply with the existing rules.

Only a third of respondents to our survey (36%) agree that complying with cyber regulation is straightforward. In this, we see a difference between the C-suite – 41% of whom believe compliance to be straightforward – and those employed in cyber-security roles, who are likely to be closer to specific requirements (just 29% of whom think the same as the C-suite on this issue).

This disconnect may reflect the speed at which cyber regulation has evolved over the last decade, with regulators being at pains to tackle cyber risk in the industry.

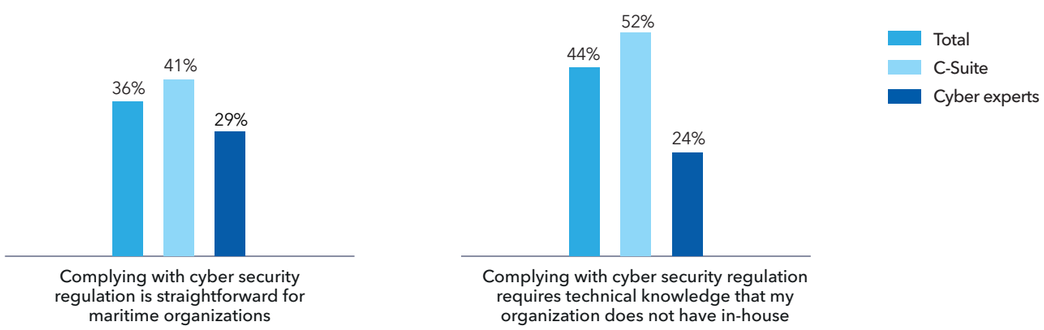
In the late 2010s, for example, the growing number of cyber-attacks in the industry prompted the IMO – which itself was hit by a cyber-attack in 2020[17] – to issue recommendations aimed at improving cyber security across the industry[18], recognizing "the urgent need to raise awareness on cyber risk threats and vulnerabilities".

Today, the International Association of Classification Societies (IACS) is adopting new requirements around the integration of IT and OT, and the systemic integrity of third-party suppliers[19]. Guidelines around this area often include recommendations for secure network architecture, access control, data protection, risk assessment, and incident response.

Operators of essential services within critical infrastructure industries in the EU, including some areas of the maritime sector – including ports, floating storage regasification units and the largest shipping companies – must also prepare for the revised Directive on Security of Network and Information Systems (NIS2), which will be transposed into EU member states' laws during 2024[20]. NIS2 increases the penalties for non-compliance, with provisions for fines of up to €10m or 2% of an organization's global revenues, although limits vary depending on how EU countries transferred NIS1 into national law.

"The Hamburg Port Authority is classified as critical infrastructure by the German Federal Office for Information Security," says Phanthian Zuesongdham, Head of Division Port Process Solution at the port, referring to the requirements of the NIS1 directive. "We need to professionalize our process even further and also all measures that could protect our infrastructure in the best possible way."

Disconnect between senior management and cyber experts, on whether organizations are ready to comply with regulation



Q: To what extent do you agree or disagree with the following? Percentages reflect net agreement (i.e. moderately + strongly agree)

Although the developments in regulation are to be welcomed for helping maritime businesses ensure they have core security measures in place, our research suggests that they are putting strain on cyber resources. Approaching half (44%) of respondents tell us, for example, that compliance today requires technical knowledge that their organizations do not have. Of concern, the C-suite is much more likely (52%) than cyber experts (24%) to believe they do not have the right technical knowledge in place. Here, again, greater investment – along with clearer communication to the board about the challenges of regulation – is required. This also suggests that investment is needed ahead of regulation taking effect, to ensure organizations have the capabilities in place to make effective use of regulation-driven investment.

Where regulation could go further

Although maritime businesses already face challenges around compliance, there is agreement across the industry (89%) that cyber regulation will become stricter in the coming years. However, little more than half (57%) of the professionals responding to our survey agree that regulation is effective at encouraging the right cyber security behaviours.

"Maritime is still behind some of the other industries where cyber is a major challenge, such as in financial services," says the Group CIO of a global energy infrastructure and technology company in Asia Pacific. "The regulators are trying their best to put better rules in place, but whether this is implemented as quickly as possible is another matter."

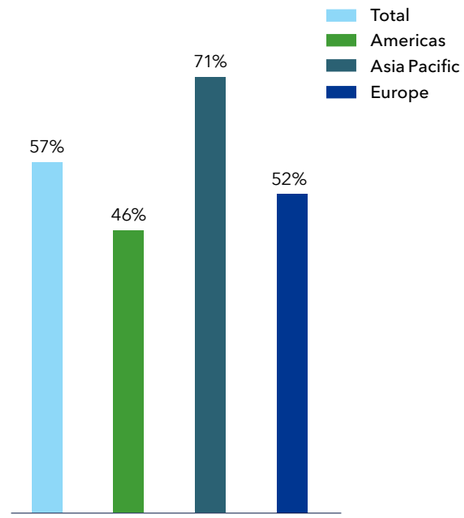
One way that regulation can help maritime businesses strengthen their security postures is by reframing cyber security risks as safety risks, in recognition that cyber-attacks on OT systems can cause harm to life, property and the environment. This is already required by IMO resolution MSC 428(98), but implementation is not consistent across the global industry.

Peter Aylott at the UK Chamber of Shipping favours a regulatory approach that is more akin to the safety oversight protocols that are already in place in the industry. "We normally have to make a safety case to operate, but we don't do that for systems – it's only for people, equipment and process," he explains. "So, we might need another lever here, with an appraisal of the IT system and a recognition of the risks."

Another point of contention with the existing rules, according to DNV's Svante Einarsson, is that they focus on enforcing greater security awareness and skills-development, but do not also require operators to appoint dedicated ship or fleet cyber security officers. "Without a requirement for roles like these, essential cyber protocols fall to ships masters and superintendents rather than dedicated trained crew members and onshore specialists," he argues.

Professionals in Asia Pacific are more confident regulation is driving the right behaviours

Extent to which respondents agree that regulation is effective at encouraging the right cyber security behaviours in maritime organizations



[17] IMO hit by cyber attack, Seatrade Maritime
[18] Preparing for IMO's ISM Cyber Security, DNV
[19] IACS adopts new requirements on cyber safety, IACS
[20] NIS2 Directive: Compliance risk or cyber security opportunity?, DNV

AGEING ASSETS AND SUPPLY CHAIN VULNERABILITIES

Connecting the old with the new

Two in three maritime professionals (67%) believe that their success as a business relies on a significant increase in connected networks. The challenge they face is to pursue their ambitions without finding them overshadowed by a serious cyber-attack.

As the rate of connectivity increases, maritime businesses with a good security posture may not retain that posture for very long, warns the UK Chamber of Shipping's Peter Aylott. "The maritime industry is on a trajectory towards autonomy, as well as remote operating and maintenance," he says. "We need a more in-depth risk assessment at each stage of that shift, to ensure we consider the impact on cyber security."

For many maritime businesses, the main consideration here lies not in securing the next generation of connected OT, but in safely connecting existing assets and infrastructure that were never designed with cyber security in mind. According to our survey, 61% of maritime organizations are in the process of linking their existing assets, including maritime vessels, to their onshore IT networks and across business units worldwide.

"Older vessels are being upgraded with newer systems," says DNV's Svante Einarsson. "But the combination of new connected systems, integrated with older unpatched systems, may provide the loophole for a successful attack."

Kelly Malynn at Beazley agrees that installing new systems on top of legacy technology is a widespread problem in the industry. "You've got IT interfaces used on vessels that are no longer even supported," she says. "We're talking about Windows 10, even Windows 7, systems that we know have vulnerabilities and are unsupported. If you have a laptop that's been in place for years, upgrading the software could affect the OT."

Building resilience down the supply chain

Risks around connectivity are not restricted to loop-holes and other issues that might emerge during upgrades. Maritime businesses source software and technology from multiple layers of the supply chain, which they incorporate into critical infrastructure. The danger is that the software and technology has already been compromised.

Cyber experts are particularly worried about supply chain vulnerabilities

Extent to which they agree that their organization urgently needs to get better at identifying and addressing the gaps in its suppliers' cyber security

56%
C-suite

65%
Cyber/tech experts

Today, 57% of maritime professionals say they urgently need to get better at addressing gaps in their suppliers' cyber security.

Updates to navigation systems provides a good illustration of the problem. "You have third parties providing chart updates to vessels," says Kelly Malynn at Beazley. "These are rarely sandboxed on shore. If you are thinking about an event that could cause disruption, that's one of the most likely entries, using some sort of injection malware at a third-party source."

Achieving a more cyber-secure supply chain is, however, far from easy. For this to happen, operators need to thoroughly audit their vendors' cybersecurity require-ments during procurement, installation and operation of equipment, systems, and software. At the same time, suppliers must ensure they have the right measures in place to defend products and systems, and should conform to industry standards and practices[21].

More positively, IACS' new Unified Requirements (UR E26 and UR E27) for cyber security, which will be mandatory from January 2024, will help ensure that vessels are designed and built according to the latest cyber security standards.

IACS intends for these two URs on cyber safety to provide minimum goal-based requirements for the cyber resilience of new ships and for the cyber security of onboard systems and equipment[22].

[21] DNV Standards and Recommended Practices supporting cyber security, DNV
[22] IACS adopts new requirements on cyber safety, IACS

KNOWLEDGE SILOS ARE HOLDING BACK MATURITY

Reluctance to share experience

According to our survey, barely three in 10 (31%) maritime professionals believe that organizations within their sector are effective at sharing information and lessons learned about cyber security risks, threats and incidents.

Such reluctance to share information may be counter-productive at a time when businesses will benefit significantly from hearing first-hand about the challenges faced by their peers and the methods they are adopting as a result. This is particularly important as the industry pursues its accelerated connectivity agenda, for which the full implications – for connecting and upgrading existing assets and training operational crew – are not yet fully known.

Poor communication also undermines the belief – shared by 79% of respondents in our survey – that the industry is starting to consider cyber security risks to be as important as health and safety risks. If cyber were increasingly treated as seriously as safety, then arguably there would be more forums and networks in place to facilitate open discussion, such as under the Chatham House Rule.

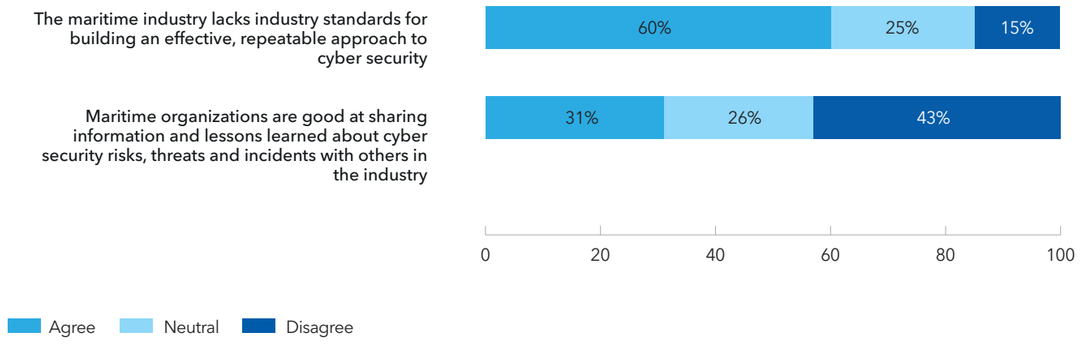
Developing better industry standards

Over time, transparency and information-sharing will be key to creating industry standards that give organizations best practice guidelines to follow, which help them develop a security posture that meets or exceeds regulatory requirements. At present, six in 10 respondents believe that the maritime industry lacks standards for building an effective, repeatable approach to cyber security.

Wärtsilä's Stefan Nysjö is positive about some of the standards that have already been developed around cyber security. "Cyber security standards have created clarity on the vocabulary and made it more tangible for everyone in the industry," he says. "They also enable everyone in the supply chain to understand what is being demanded."

Better information-sharing would also help the regulator, as the US Coast Guard's Wayne Arguin explains. "If you have a cyber incident, telling someone could put you at a competitive disadvantage, but we as a regulatory body want to know," he says. "If someone has information on potential vulnerabilities that could be exploited, that information should be shared in a timely, detailed enough manner to prevent the exploitation of vulnerabilities in other sectors."

Maritime industry needs to get better at sharing information and lessons learned, in order to develop industry standards



Q: To what extent do you agree or disagree with the following? Percentages reflect net agreement/disagreement (i.e. moderately + strongly agree)

TALENT SHORTAGES AND WORKFORCE VULNERABILITIES

Urgent need for specialist skills

Maritime organizations face a significant cyber security skills shortage, which is complicated by the specific expertise that is required to secure remote, fast-moving and increasingly connected operational environments. Research suggests that the cyber-security workforce gap grew by 26.2% in 2022, with the shortage considered to be "particularly severe" within the transportation sector[23].

"It has been a constant struggle to find experts."

Stefan Nysjö, Vice President Power Supply - Marine Power, Wärtsilä

"Within teams developing automation or control systems, for example, we are gradually building cyber security knowhow so that it becomes embedded as part of what we do, but it takes time to get there," says Wärtsilä's Stefan Nysjö.

Just half of maritime organizations in our research think their cyber security function is up to speed with the latest technical developments. The rapidly evolving nature of the threat may explain the difficulty in finding professionals with the right skills, but it also highlights why the need for talent is so urgent.

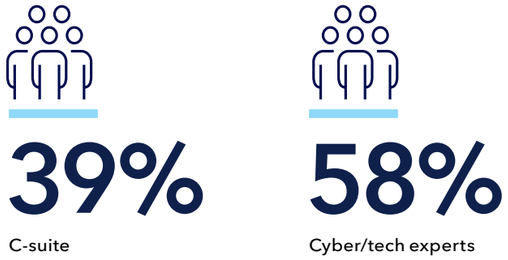
Poor training turns employees into 'friendly threat actors'

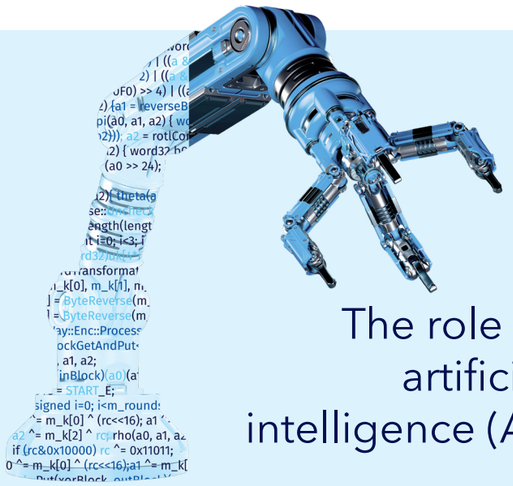
Workforce challenges are not limited to finding the right experts. Another people-related issue relates to employees inadvertently enabling cyber-attacks through carelessness, which points to an underlying problem with the training being made available to staff.

Better and more consistent training will play an important role in establishing a more risk-aware workforce and cyber-secure culture. Today, less than half of respondents (47%) believe that the cyber training in their organizations is effective, with major differences in perception on this topic between C-level and cyber experts.

Cyber/tech experts much more likely than senior management to believe training is effective

Extent to which respondents agree that cyber security training in their organization is effective





The role of artificial intelligence (AI)

New technologies such as AI may help organizations improve their security posture by reducing the workload of an already stretched workforce and giving teams greater visibility of vulnerabilities, threats, and attacks. Companies are, for example, using ChatGPT to help coders identify and fix loopholes before they use software or release it into the supply chain[24].

Nonetheless, more in-house expertise is needed for maritime organizations to understand how emerging technologies should be adopted to reinforce their fight against cyber-crime, as Phanthian Zuesongdham at Hamburg Port Authority explains. "We do not know how algorithms in attacks have been coded, and AI is going to be the next level in the speed of how hackers can change their tools and attack vectors," she warns. "They can get AI to code for them at faster speeds."

As technologies such as AI become available, there is also concern about who will take advantage of it fastest – cyber professionals, or threat actors – and the extent to which the technology can be trusted to carry out the work of a human.

"As this new technology becomes available to our opponents, it also comes available to us," says Commander Monte of the German Navy. "The question should be who integrates new technologies faster. Cyber-crime will, however, benefit much more from this new technology because the victims will most likely not be able to 'upgrade' their defences at the same speed."

[23] Cybersecurity Workforce Study, (ISC)²
[24] ChatGPT Leveraged to Enhance Software Supply Chain Security, Infosecurity

Rolling out training across a diverse and dispersed workforce, many of whom spend months at a time onboard vessels, is far from simple. There is a wide range of training programmes available – from generic videos, through interactive training, to tailored e-learning courses targeted at specific roles and risk management systems – but the most sophisticated can cost money that is in short supply.

One consequence of poor training is weakness even on the most essential requirements. Less than one in five respondents (19%) agrees strongly that they know what to do in the event of a potential cyber-attack, for example – exactly the time that certainty is vital for an effective response. This lack of cyber awareness suggests that the industry's understanding is a long way behind more entrenched industry standards, such as health and safety.

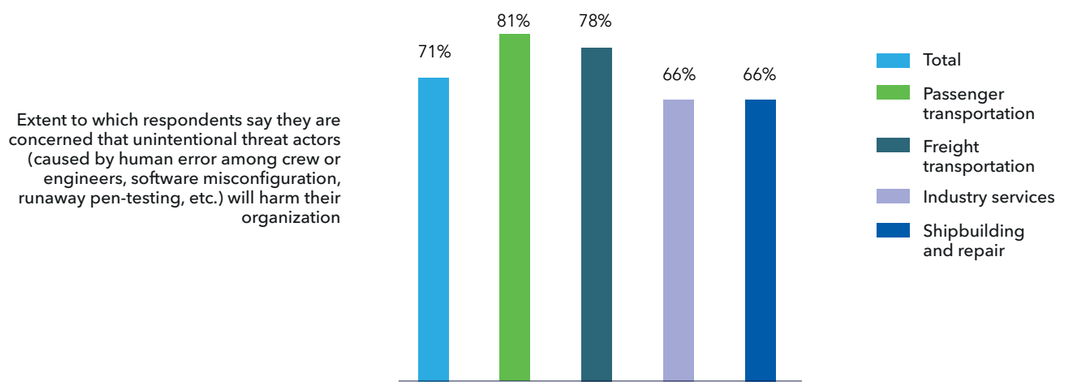
The German Navy's Commander Monte believes that success relies on drilling the message into employees on a regular basis. "Every person should receive basic cyber-security education alongside routine training on board," he says.

"The purpose of that low-level-training is to ensure that every person can detect a potential cyber incident if it happens on the systems they use and can ensure they are not a risk themselves in enabling a cyber incident. Mitigation of system failure should also be integrated into standard damage response drills, such as a fire or machinery-failure drills."

Commander Monte, The German Navy

As it is, more than seven in 10 (71%) maritime professionals worry about the likelihood of staff becoming unintentional threat actors through human error. No other group is regarded as a more serious worry. Today, almost a quarter of respondents (24%) say they know for a fact that cyber security processes and protocols are skipped for expedience in their organization.

Professionals in passenger transportation are most concerned about unintentional threat actors



Q: How concerned are you, if at all, about the potential for the following cyber threat actors or other individuals to harm your organization? Percentages represent moderately + majorly concerned.

This rises to 32% among the respondents who have suffered negative impacts from a cyber-attack on their OT – possibly as a direct result of employee negligence.

Maritime organizations may need to become more creative in how they address this challenge, such as by providing training in multiple formats to suit different learning styles and through a range of media to reach everyone in the organization.

"We have online platforms as well as collaborative and spatial events dedicated to cyber training," says Phanthian Zuesongdham at the Port of Hamburg. "We also have campaigns around the facility that reinforce simple messages like not being too curious if you find a thumb drive in front of the office. Just give it to the IT person."

Ultimately, the industry would benefit significantly if the maritime workforce were to better understand how cyber security incidents can cause safety incidents in industrial environments. Taking the same approach to cyber training as the industry does to safety training – which is a non-negotiable and habitual practice – may be helpful.

4 RECOMMENDATIONS

4 RECOMMENDATIONS

In the short term, we advise maritime organizations to prioritize the following actions.

Consider cyber security as an enabler
Maritime organizations have set themselves clear strategic priorities around digital transformation to enable commercial advantage and decarbonization. Cyber security leaders should be part of these wider strategic conversations from day one, and cyber security should be a key element in the procurement and development processes for new technologies, as well as the next generation of information systems and data. Consider investment in cyber security not just as a cost of business, but as an investment in confidence, competitiveness, and innovation.

Treat cyber like safety and clarify responsibilities
Maritime leaders have long asserted that work is never so important that it cannot be carried out safely. For decades, employees have been encouraged to stop work and blow the whistle if they believe that safety protocols are being neglected. In our view, a similar mantra should be adopted for cyber security. Better communication around the risk – ensuring that cyber, operational and leadership teams are all 'talking the same language' when it comes to the threat in OT environments – is a pre-requisite. To further professionalize their approach, maritime businesses could seek to clarify cyber roles and responsibilities across the enterprise, while enabling system owners to manage the risk from a multidisciplinary team.

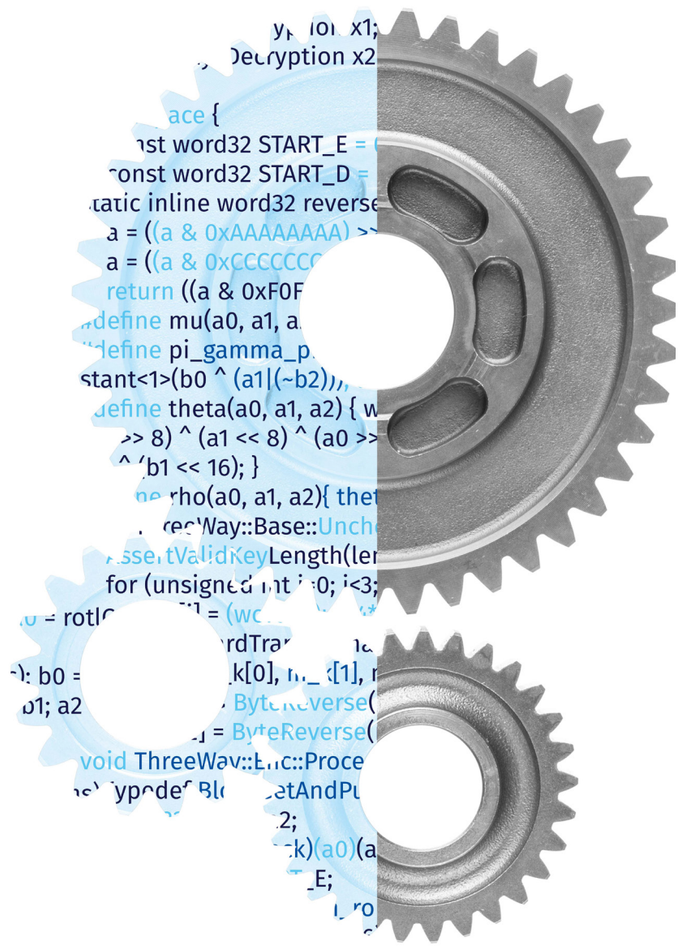
Champion insight-sharing across the industry
We find scope for the sector to collaborate to improve cyber security, such as by sharing information about incidents and near misses with peers and the regulator. It is in everyone's interest to do so in an increasingly connected industry, where an attack on one organization or asset gives rise to contagion risk. Although initiatives to collect and share insight have failed in the past, we hope that growing awareness of the risk among maritime businesses will motivate them to share information about incidents. Only by sharing information and experience will the industry create standards and best practice around cyber security.

Reframe regulation as the baseline to further improve cyber security
Cyber professionals should use impending, tighter regulation to build stronger security postures. The instinct of many in the past has been to focus narrowly on what needs to be achieved now to satisfy the essential requirements of regulation. However, regulation is evolving at pace – illustrated by the new requirements and recommendations set out by the IMO and IACS – so organizations with this mindset risk falling behind. As regulation comes into being at a much slower pace than the hacking methods used by cyber criminals, these businesses also face threats for which they are not prepared. Instead, maritime professionals should strive to reframe regulation as a baseline on which to build a stronger security posture.

Rethink how to manage supply chain vulnerabilities
Including cyber security in the procurement and development processes for new technologies is more efficient than carrying out risk assessments at a later stage. Suppliers may also be able to help address maritime companies' limitations in technical cyber knowledge, turning supply chain risk into supply chain advantage. "We are trying to understand what we can do to support the ship owner in setting the structures when building the ship," says Meyer Werft's Paul Meyer. "What kind of architecture do we need to take care of? Do we need to change the networking infrastructure on the ship?"

Resource a strategy for more effective training
This research suggests that most maritime organizations lack critical cyber security awareness and knowledge across the workforce. Despite the practical challenges of training and education, especially around industry-specific challenges such as ships' crews operating in remote and inaccessible settings, organizations must remedy this issue. Advanced maritime companies combine generic e-learning with interactive training, while the most advanced use tailored e-learning, incident response exercises, and modules designed for specific positions. They should also consider defining specific cyber-related roles for ships' crews and onshore staff. Otherwise, employees will continue to be the weakest link in cyber security.

Maintain an 'analogue fallback option' amid the shift to connected systems
In an increasingly connected industry, ship operators fear the prospect of a ship becoming unresponsive while at sea, as a direct result of an OT-targeted cyber-attack. "The only way to counter this is to prepare to function without the benefits of the attacked IT-systems," believes Commander Monte. "Ships have to be able to run their systems, reach port safely, be moored, loaded, and unloaded without the use of digital systems. Of course, not at the same efficiency and speed, but in a continuous and safe manner." In addition, we would note that fulfilling the latest IACS requirements will help maritime organizations manage the risk.



ABOUT DNV

DNV is an independent assurance and risk management provider, operating in more than 100 countries. Through its broad experience and deep expertise, DNV advances safety and sustainable performance, sets industry standards, and inspires and invents solutions.

DNV combines specialist maritime industry knowledge with engineering expertise and information system best practice to keep critical infrastructure projects and operations confidently cyber secure. We provide many of the sector's most successful and forward-thinking companies with clear and practical advice to uncover their risks, build a powerful force of defence against threats, recover from attacks, and unite stakeholders against security programmes that everyone can believe in.

dnv.com/cybersecurity

Disclaimer
All information is correct to the best of our knowledge. Contributions by external authors do not necessarily reflect the views of the editors and DNV.

© DNV, April 2023
All rights reserved.