June 2026

Cyber Security Survey

by Aude Chocard,
Regulatory Affairs Intern at BIMCO

Contents

Introduction

The maritime industry has experienced a major transformation since the emergence of digital tools. Digitalisation on board vessels has become widespread in shipping companies, for safety and environment matters but also to improve competitiveness and efficiency.

However, digital platforms onboard also present vulnerabilities that cybercriminals can exploit to gain access to systems. Malicious actors can hack communication or navigation systems to disrupt the maritime supply chain or steal sensitive data from a company.

The number of maritime cyber incidents has increased by 103% between 2024 and 2025, according to the *Maritime Cyber Threat White Paper* released in March 2026 by CYTUR. Considering the speed of information transmission, the widespread use of artificial intelligence (AI) and the complexity of foreign politics, interconnected and unexpected cyber-attacks are more likely to happen. Therefore, there is a need to report on the cyber security situation in the maritime sector.

The International Association of Classification Societies (IACS) has established new mandatory Unified Requirements UR E26 on “Cyber Resilience of Ships” and UR E27 on “Cyber Resilience of Onboard Systems and Equipment”. These standards apply to newbuild vessels from 1 July 2024. Information Technology (IT) systems onboard must comply to these regulations and must follow cyber security recommendations to ensure business continuity in case of cyber incidents.

Under the IMO scope, resolution MSC-FAL.1/Circ.3/Rev.3 has been adopted in April 2025, providing the last updated version of *Guidelines on maritime cyber risk management*. More recently, during the 50th Facilitation (FAL) Committee session in March 2026, the International Maritime Organisation (IMO) has initiated work on a goals-based, non-mandatory Maritime Cyber Code, expected to be completed by 2028.

Shipowners and operators can also refer to the *Guidelines on Cyber Security Onboard Ships version 5*, commonly referred to as the Industry Guidelines, conducted by BIMCO, ICS, INTERCARGO, DCSA, SYBAss, InterManager, INTERTANKO, IUMI, OCIMF and WSC, but also the *Cyber Security Workbook for On Board Ship Use* produced by BIMCO, ICS and Witherbys.

To ensure effective cyber security policy within the maritime sector, there is a need for greater links between regulatory bodies and industry. Surveys help to have more knowledge and improve cyber security policies.

Purpose, scope and methodology of the survey

PURPOSE

The **BIMCO Cyber Security Survey 2026** aims at assessing the cyber security practices in shipping companies. Considering new technologies onboard and the involvement of multiple stakeholders, risks are growing in the industry. However, it is still hard to convince companies to share their vulnerabilities, although it helps resolve cyber security. This survey will give an update of the cyber security landscape, based on the last *Safety at Sea and BIMCO cyber security white paper* from 2020 released by IHS Markit, as well as the NIST framework. This survey from 2026 will compare past and new results to conclude on the main changes in maritime cyber security. This analysis will therefore give an understand of the level of cyber protection and awareness within shipping industries, considering also new issues such as the implications of AI and foreign politics.

SCOPE

This survey lasted about two months and received 20 responses. It includes a wide variety of shipping companies, from small to larger ones (less than 10 to more than 10,000 employees). The companies that responded to the survey manage over 2,500 vessels in total.

The survey gathers companies from different segments of the shipping industry. The companies that answered the survey mainly operate 3 kinds of vessels: dry bulk (55%), container (40%), tanker (30%). Cruise lines, offshore supply and heavy lift companies are also represented in the survey.

70% of the companies are involved in at least 2 shipping activities between shipowning, chartering, crew management or technical management, the latter being the most represented activity here.

METHODOLOGY

The survey was targeting shipowner and shipmanager companies responsible for cyber security onboard vessels. The people targeted were especially those who are specialised in cyber security within shipping companies. They have been contacted in various ways: on social media, at cyber conferences, or from BIMCO membership's contacts.

More answers were expected considering the growing importance of cyber security in the maritime sector. However, it may be due to a lack of cybersecurity awareness within the company, or because the survey did not reach the appropriate person who could have responded to it.

Key findings

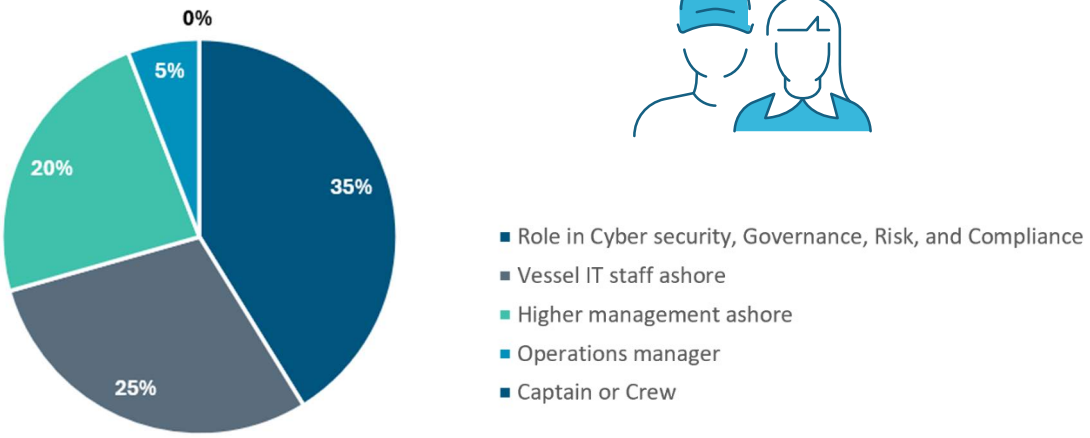
These are the **key findings** from the BIMCO Cyber Security Survey released in 2026.

- **80% reported a cyber threat in the last 12 months**
- **Phishing and malware remain the most common cyber threats**
- **Human factors and IT software are the main vulnerabilities**
- **The company IT manager is the most involved in managing cyber risks**
- **75% have a process to ensure hardware and software are sufficiently updated**
- **95% invest in cyber security training**
- **50% don’t know who the threat actors behind a cyber incident are**
- **45% assess the trustworthiness of suppliers**

1. Cyber security context of shipping companies

Respondents of the survey

60% of the respondents are **people specialised in IT**, whether in cyber security governance (35%) or on a technical aspect (25%). This result was expected since respondents need to know how cyber security is understood and managed within their company to be able to answer. It has helped assessing the company's cyber security practises in a more accurate way.



A well-established digital environment

Digitalisation has become widespread in the maritime industry. It is a way to guarantee real-time information on ship positions, ship-to-shore communication, operational optimisation, cost savings, safety improvements, and a more sustainable business.

Ships contain various new technologies to ensure this reliable connection, which has been confirmed by the survey. **80% of the respondents claimed that more than half of their fleet was connected to the Internet**, and 70% of the respondents have more than 75% of their fleet connected to the Internet. This result highlights the necessity to take into consideration potential disruptions to the fleet in the event of Internet outages.

Additionally, **75% of the respondents said their company has an inventory of digital systems on board**, showing that digital tools are replacing paper documents and play a dominant role onboard vessel.

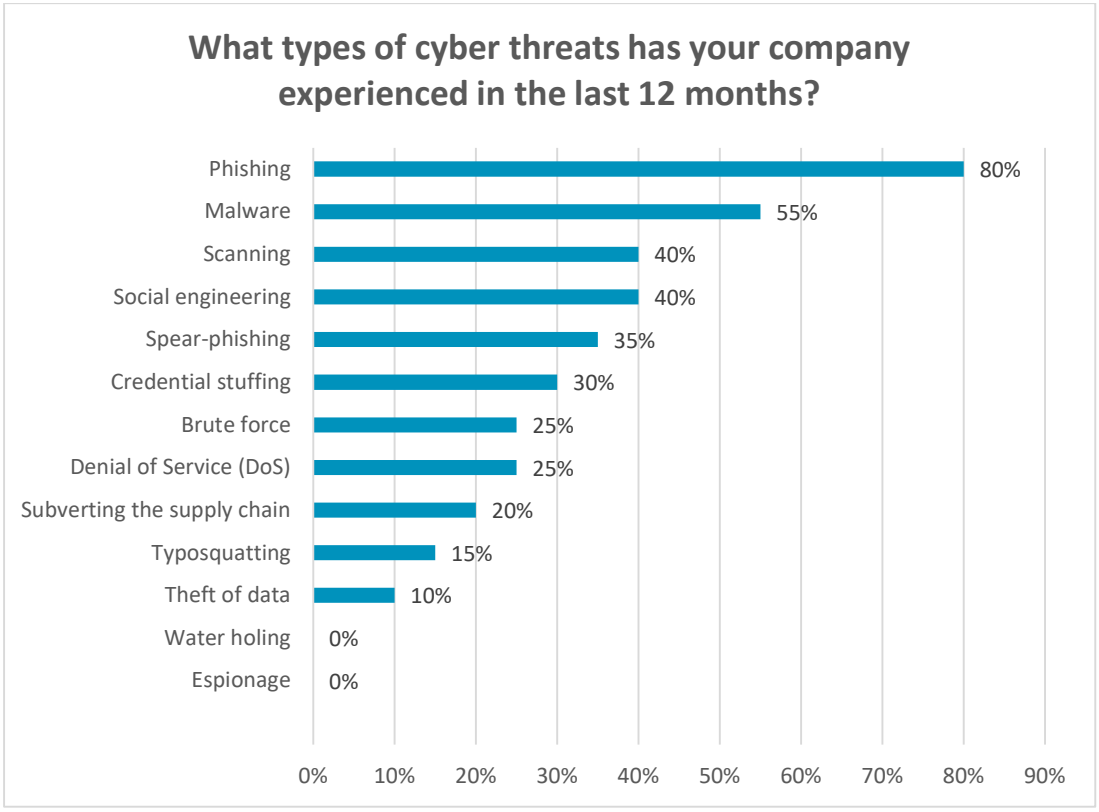
80% of the respondents has more than half of their fleet connected to the Internet

An increase of cyber incidents in the maritime sector

In the 2020 Safety at Sea and BIMCO Maritime CyberSecurity survey, the three most common cyber-attacks experienced in maritime in 2020 were phishing, spear phishing and malware. 68% of the respondents reported they have been the target of a phishing attempt, 41% for spear phishing and 33% for malware.

In this survey from 2026, **phishing and malware are still the main types of cyber threats** that companies in the maritime have experienced in the last 12 months. This tendency also coincides with the cybersecurity landscape in other sectors. Phishing consists of sending a fraudulent message from a supposed trusted entity so that the attacker can steal sensitive data or release malware afterwards. Phishing and malware are the most important cyber threats because they remain the easiest, cheapest and most successful attacks, since they target human behaviour rather than technical vulnerabilities.

Considering that 80% of the respondents of the 2026 survey have experienced phishing attacks, and 55% have been victims of a malware attack, we notice a large increase of these cyber-attacks compared to 2020. On a more general aspect, whereas 31% of the respondents of the 2020 survey said they experienced a cyber-attack in the last 12 months, **80% of the respondents of the 2026 survey reported a cyber threat they experienced in the last 12 months**. It means that a more important part of respondents said they experience a cyber-attack today. This growth can be explained because cyber-attacks happen more frequently in the industry, due to the use of modern interconnected ships and digital platforms onboard vessel. Also, it seems that companies are now more capable of detecting cyber-attacks.



Cyber security vulnerabilities

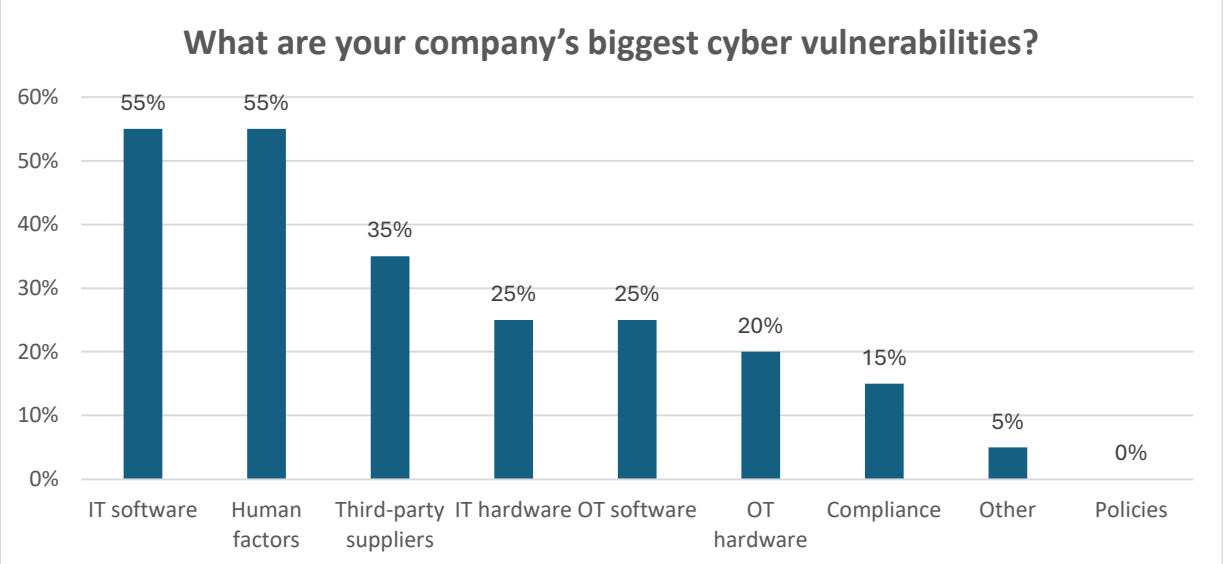
Vulnerabilities in maritime cyber security refer to weaknesses that are exploited by cyber threat actors to disrupt shipping operations. Because the maritime sector is now digitalised, digital tools are used to access the company's data. Vulnerabilities can be present in in the systems, but can also come from external actors, such as employees or third-party suppliers.

This 2026 survey has shown that **the biggest vulnerabilities for shipping companies were human factors and IT software**. In the last survey from 2020, the human element was also the biggest vulnerability, since 52% of the respondents said their organisation's biggest vulnerability was: "our people". Employees or others are not always aware of the best practices in cyber security when it is not their area of expertise. They are nonetheless confronted to the digital systems used by the company. Without realising it, they may allow hackers to gain access to the company's systems.

In 2020, "IT systems" were the second main vulnerability, so it is also like the 2026 results. However, IT systems represented 17% of the respondents in 2020, whereas considering only IT software in 2026, it represents **55%** of the respondents' answers. **IT systems have become widely used by shipping companies** but are also more complex and connected to other digital tools. They represent entry points for hackers, which make the systems more difficult to secure.

In general, **IT systems are also considered as bigger cyber vulnerabilities than OT systems**. It is coherent since IT systems are more connected to the Internet meaning more easily detected by cyber-attackers.

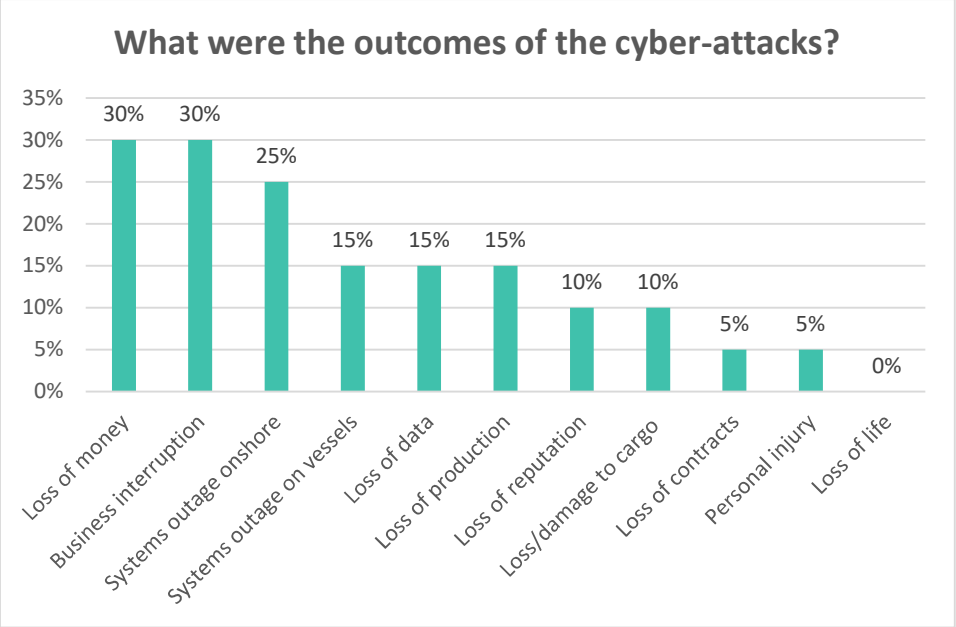
Finally, **third-party suppliers are considered a cyber vulnerability**, because it is difficult to control external people to the company and they often use digital systems in the easiest way, which is not necessarily very secure. **Compliance has also become important**, because when regulations are not respected, vessels may be stopped in ports, leading to business interruption. This vulnerability can have big impacts because it may affect multiple ships at the same time.



Characteristics of the cyber-attacks

In the 2020 survey, the most common outcomes of cyber-attacks identified were loss of money (28%), systems outage onshore (23%), and reputational damage (15%). However, for 47% of the respondents, their outcomes have not been categorised in a single outcome, reflecting the complexity of gathering reasons that can vary a lot. It also shows the difficulty to identify whether they were some consequences of cyber-attacks or their nature.

In the 2026 survey, we have added more categories. Regarding the outcomes of the last cyber-attacks experienced by shipping companies, **loss of money and business interruption are the main answers** (30% for each answer)**. However, no category stands out for a majority of respondents.** Because some respondents didn't answer the question, it confirms that cyber-attacks and their impacts on the company's business can be hard to recognise.



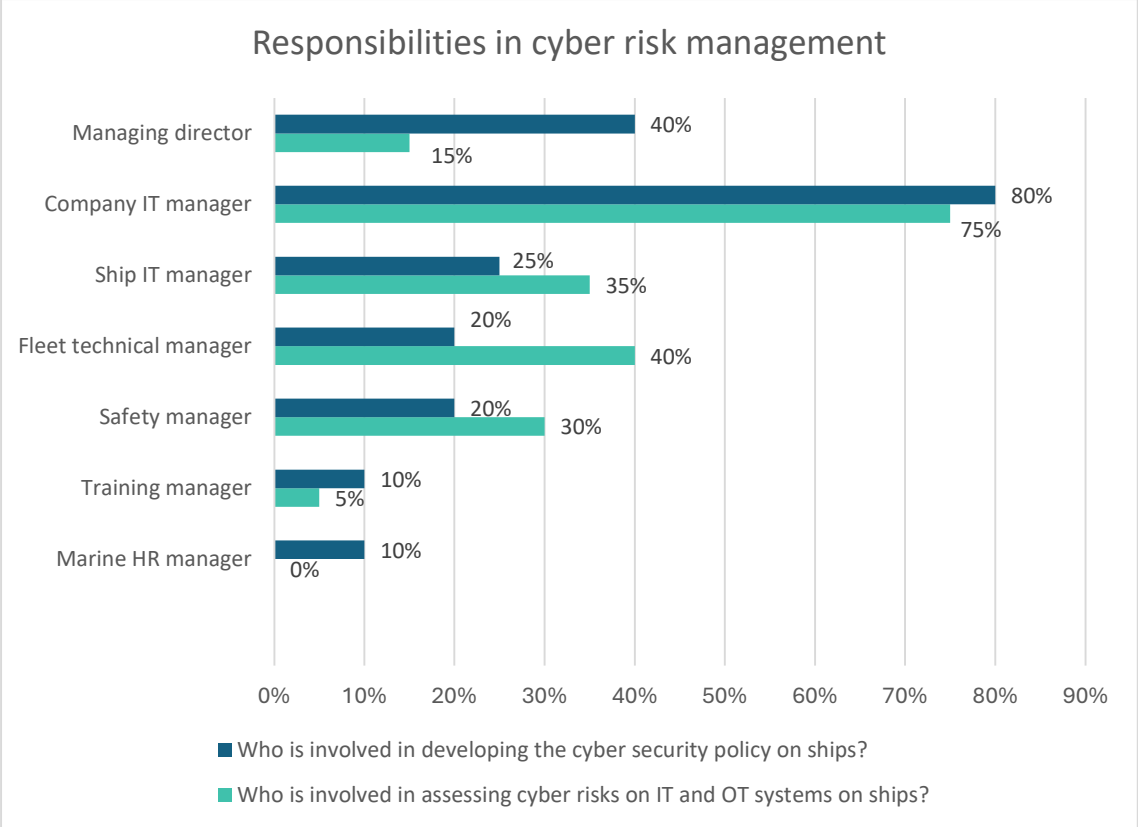
2. Cyber security policies VS Cyber maturity

Distributing responsibilities for effective cyber risk management

The survey asked about the people who are involved in developing the cyber security policy, as well as assessing cyber risks on IT and OT systems on board ships. It is interesting to observe if there is a significant gap between the two questions, since they refer to different steps in the cyber risk management policy.

Results have shown that **the company IT manager is deeply involved** in both developing the cyber security policy (80%) but also assessing cyber risks on systems onboard (75%). This shows that **cyber security is receiving a lot of attention**, since the company IT manager has significant responsibilities and can exert considerable influence on the company's cybersecurity policy.

Then, the **managing director** is the second most-responsible for developing the cyber security policy (40%). It is coherent, since his role focuses on governance and identification of cyber risks. The managing director is well qualified to develop a corporate cyber security strategy. On the other hand, the **fleet technical manager** is largely involved in assessing cyber risks onboard (40%). This result is also very logical, since he is well positioned to verify onboard whether the cyber security policy is truly effective. **Responsibilities seem to be clearly defined and adapted to the staff's skills.**



Finally, **75% of the respondents indicate that at least 2 people are involved in one of these cyber security roles**. It may show that respondents do not exactly know who is responsible for the role, or that the responsibility has not been clearly assigned. It may also mean that responsibility is shared among several people.

Shipping companies must be aware that it can lead to overlapping processes if the processes are not coordinated. It can also be difficult for employees to know who to contact within the company in the event of a cyber incident. However, since the survey didn't ask all the different cyber security tasks delivered, it could also hide the organisation of the cyber security team.

A high level of cyber security awareness

In the last survey from 2020, 77% of the respondents considered cyber-attacks as a medium or high risk to their organisation. In the new survey from 2026, **80% of the respondents said that cyber risk management was considered a significant priority for the company[1].** This result confirms that cyber culture is receiving greater consideration throughout the years and is better integrated into the company's strategy. This is related to the previous finding that the company's IT manager - a person with significant decision-making authority within the company - was primarily responsible for cybersecurity risks.

80% said that cyber risk management was considered a significant priority for the company

Regarding investments in cyber security risk management, whether on protection measures, training or other, **45% of the respondents said that they allocate more than 5% of IT budget to security**. Since 5% or less of the IT budget is generally allocated to security because business efficiency is prioritised, this result is a positive signal that cyber security is receiving great consideration within shipping companies.

However, **35% of the respondents also said they don't know the proportion of IT budget dedicated to security**, which also indicates that some companies may not consider cyber security as a priority. They could also hide how much they invest if they don't have the financial resources yet. **The shipping industry still needs time to adapt to the new digital environment** that requires to integrate cyber security practises.

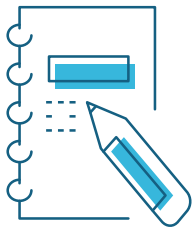
Another interesting result is that the biggest shipping companies are not necessarily those who allocate a significant portion of their IT budget to security. They may spend more money, but cyber security is not part of their main spendings in IT budget.

45% said that they allocate more than 5% of IT budget in security

[1] This result is based on the question "On a scale from 1 to 5, how high is cyber risk management on the company's agenda?". Responses to the survey that received a score between 4 and 5 indicate that cyber risk management ranks "fairly high / or high" on the company's agenda.

Developing strong IT policies

Survey results have demonstrated that **shipping companies have developed robust policies to ensure a high level of cyber security**. The following outcomes prove that investing in cyber security has paid off, and that resources are well allocated.



60% of the respondents rated **the data privacy and GDPR policy as strong or fairly strong.**[2] Most of respondents consider it important to have secure data management and to comply with cyber security regulations. Focusing on compliance addresses with one of the vulnerabilities previously identified.

65% of the respondents said the company has a **process to maintain an updated cyber risk assessment on board**. It means that shipping companies regularly checks if cyber risks can be well identified and managed. Respondents said that this process apply to either critical systems or all the systems. Therefore, **if this process applies at least to critical systems, there is effective monitoring of cyber risks**, which helps to prevent major cyber incidents.

75% of the respondents said that the company has a **process to ensure hardware and software are sufficiently updated.** This shows that the systems are being properly managed, tested and patched, according to the company's needs.

80% of the respondents said the company has a **process to ensure nautical charts are sufficiently updated.** Once again, companies are looking to secure critical navigation systems, which reflects a high level of awareness of cyber threats.

90% of the respondents said the company has a **strong password policy.** This result indicates that effective cyber security measures are in place to prevent hackers from gaining access to the company's systems and data.

[2] This result is based on the question "On a scale from 1 to 5, rate the process of your company to protect data use and privacy (GDPR compliance...). 1 being weak and 5 being strong". Responses to the survey that received a score between 4 and 5 indicate that the data privacy policy is rated as "fairly good / or good".

Cyber security is taken seriously but lacks clear implementation

The survey results have shown a **willingness from shipping companies to integrate cyber security in their business strategy**. They consider cyber-attacks as a real threat. They are also vigilant in following cybersecurity rules to minimize compliance issues (see 1.). **However, they lack confidence when it comes to implementing their cyber security policies**. Results have highlighted that cyber security practices have weaknesses when it comes to put them into practice.

CYBER SECURITY TRAINING	
95% of the respondents said their company was **investing in cyber security training.**	**BUT only 45%** of the respondents **rated the quality and effectiveness of this training as good or fairly good.**[3]
Shipping companies are aware of their exposure to cyber risks and want to ensure the employees know how to face cyber security risks, especially because they consider that employees represent a major vulnerability. They want to limit the impact of cyber incidents on their business.	Companies offer a cyber security training but does not believe it is good enough. This means it could be improved by better adapting it to the complexity of cyber incidents as well as to the needs of the employees.

BUSINESS CONTINUITY PLAN	
90% of the respondents said the company has a **business continuity plan**.	**BUT only 40%** of the respondents said the business continuity plan was **tested less than 12 months ago.**
A business continuity plan is a good signal that the company is aware of cyber risks and wants to anticipate cyber incidents by being able to respond quickly to ensure operational continuity.	The business continuity plan exists but it seems that companies lack capability to ensure its outcome. Without testing the continuity plan on a regular basis, the company can't be certain that its operations will resume in the event of a cyber incident.

Finally, **only 55%** of the respondents **rated the ability of the company to respond to a cyber incident as good or fairly good.** It reflects here that even if a training and a business continuity plan may exist as cyber security measures, **their effect to guarantee a high level of maturity in cyber security seems limited.**

[3] This result is based on the question "On a scale from 1 to 5, rate the quality and effectiveness of the cyber security training of your company. 1 being weak and 5 being strong". Responses to the survey that received a score between 4 and 5 indicate that cyber security training is rated as "fairly good / or good".

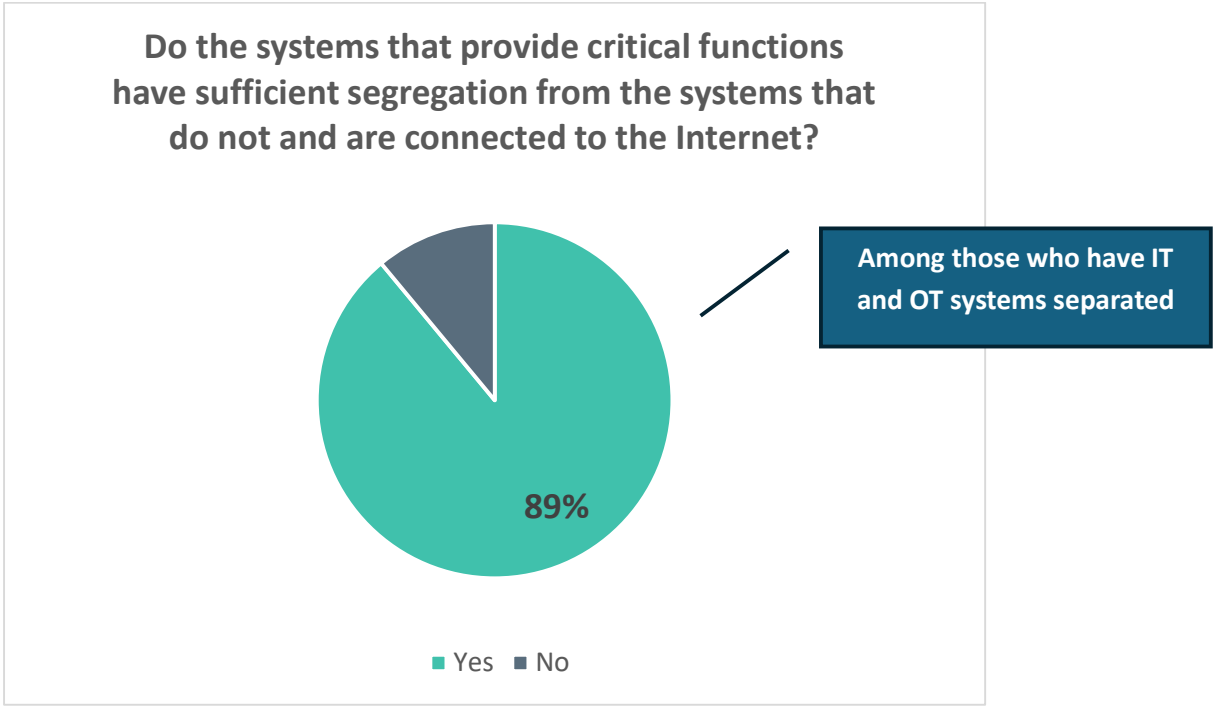
Network segregation between IT and OT systems

Separating the IT systems (interconnected devices that manage data and support business functions) **from the OT systems** (hardware and software that directly monitors/controls physical devices and processes) is fundamental prevent cyber-attacks from spreading to all systems. OT systems are usually harder to patch but they cover critical systems related to safety on board that need to be secure. Effective network segregation can separate systems connected to the Internet from critical systems, which help reduce vulnerabilities in OT systems.

45% of the respondents said that IT and OT systems were separate, showing that **network segregation is not systematically adopted** by shipping companies as a primary cyber security measure. Nevertheless, it is one of the most important precautions to take to prevent any disruption in business operations.

Results from the survey have confirmed that network segregation has a direct effect on the ability to protect critical systems. Among the respondents that said IT and OT systems were separated, **89%** said that the systems that provide critical functions have sufficient segregation from the systems that do not and are connected to the internet.

On the contrary, it's only 57% among those that have a hybrid approach, meaning that some IT and OT systems are converging. It shows that **those who separate their IT and OT systems are more aware of the cyber risk posed by critical systems.**



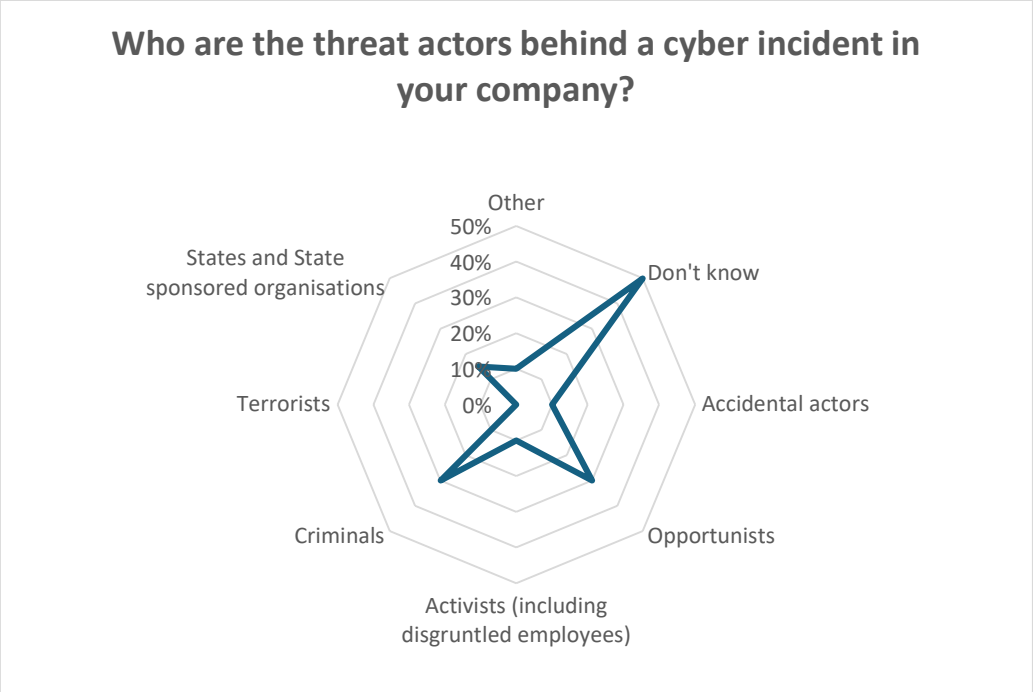
3. New challenges in cyber security: geopolitics and AI

Foreign politics create uncertainty in the cyber security landscape

The survey asked about the main threat actors that are behind cyber incidents. The results have shown that **opportunists are one of the main threat actors** (30%). Opportunists are commonly conducting cyber-attacks, since they exploit vulnerabilities that they find to access to the company's systems and data. Their motivation is the challenge of the attack, but also reputational and financial gain.

Criminals represent also one of the main answers (30%). Like opportunists, their motivation can be financial gain, but they have usually planned the attack against a specific company. They are more prepared and have more resources than opportunists. Additionally, their motivation is espionage. They are becoming more important because more networks of cybercriminals are emerging and sustaining themselves by demanding money through ransomware. **States and States sponsored organisations** are a minority in respondents' answers, but they are still present. It shows a growing concern about their involvement in cyber security, since the cyber-attacks can involve political strategies.

However, a striking result in the end is that **50%** of the respondents said that they **don't know who the threat actors behind a cyber incident are**. If companies find it hard to identify them, this can be because they lack resources or don't allocate them wisely. Budget in cyber security is high, but they may struggle to define methods. Indeed, **only 65% of the respondents rated the ability of the company to detect a cyber incident as good or fairly good.** Additionally, companies may know the people responsible but don't want to name the perpetrators.



Some respondents also said that last cyber incidents **happened because of an attack targeted directly against the company**. It may be due to strategic interests in the company or to political motives involving malicious actors, since shipping companies can be connected to its State's interests from an outside perspective. Among them, **83% consider that international foreign and security politics have increased cyber security threats**[4]. The last cyber security events that companies have experienced influence a lot their consideration of current issues.

Therefore, whether in terms of the malicious actors involved or the causes of cyberattacks, there is a close link between foreign politics and cyber security in the maritime sector.

Managing the risk of third-party suppliers

Third-party suppliers are important according to the survey results, since they are considered as the second main vulnerability (see 1.). This can be explained by the fact that some companies have experienced cyber incidents because of third-party suppliers. Indeed, **30%** of the respondents said **a third-party was involved in a previous cyber-attack.** Third parties can indirectly affect a company's operations if they were originally targeted, or if they didn't secure the systems they have provided. It is difficult to have control over suppliers and to ensure they comply with the company's requirements. They usually have their own rules and may show a lack of concern for cybersecurity as they want to maximise efficiency.

To avoid vulnerabilities from third parties, the company should implement rigorous cyber security policies. It is here the case, since **65%** of the respondents said the company has a **process to verify if a third-party supplier complies with their required cyber security practices**. Most of companies have shown willingness in assessing the reliability and compatibility with their

However, it goes to an average of **45%** of the respondents when **assessing the trustworthiness of suppliers** operating in regions with heightened cyber-threat risks related to software, hardware, and cloud storage solutions. More respondents said they assess suppliers of cloud storage solutions and software systems, which is coherent considering the complex and uncertain shared responsibility with the cloud provider but also the possibility of remote access from software systems. Hardware can be considered as more resistant and harder to attack. Shipping companies need to consider better the geopolitical implications of their suppliers since they can have dependencies with other suppliers. Additionally, they should also make some progress in implementing effectively their policies and processes.

[4] This result is based on the question "On a scale from 1 to 5, rate to what extent has the developments in international foreign and security politics increased cyber security threats to ships in your company in the last 2 years. 1 being low and 5 being high". Responses to the survey that received a score between 4 and 5 indicate that respondents think foreign politics have rather increased cyber security threats.

Cyber incidents have become more sophisticated due to AI

The development of AI has made cyber-attacks faster, more scalable and more difficult to detect. AI is integrated to cyber-attacks, since it is easy to use for cyber threat actors and because it can identify vulnerabilities of the companies and employees' systems. AI can also be used by the company itself, but there is a risk with processing sensitive data without making the AI tools secure. The new complexity of cyber incidents onboard due to AI needs to be considered by shipping companies.

The survey has shown that **45%** of the respondents said **AI has increased cyber security threats** to ships in the company in the last 2 years. Like foreign politics, this is coherent since it is a relatively new factor that was not considered before.

However, there is a challenge in translating the company's concerns into concrete terms and policies. It comes to **only 35%** of the respondents that have a **process to assess the security of AI tools** on ships before deploying them. By not ensuring that AI tools are updated, they can present vulnerabilities and are entry points for cyber-attackers. Additionally, **only 30%** of respondents said the company **invest in AI training**, which shows a lack of resources to take more seriously this topic.

Conclusion

The results from the BIMCO Cyber Security Survey 2026 have shown that cyber security is a major topic for the maritime industry. Cyber-attacks have become widespread in the maritime sector since digitalisation. IT and OT systems have become more interconnected, employees can share sensitive data from the company by connecting to the ship's network, and AI tools are increasingly used for operations' efficiency. An increasing number of cyber incidents has been reported in the past year, causing mainly financial loss.

According to the respondents, cyber security is now taken very seriously and at a high level within companies. They are aware of the risks and try to cover every aspect of the risk management policy, from governance to detection and response of cyber incidents. They develop cyber security strong measures and policies to raise awareness on the cyber vulnerabilities of the company.

However, shipping companies need to gain confidence in better implementing their policies and invest in better-quality training so they can feel less vulnerable towards cyber-attacks. They still need time to integrate cyber security requirements onboard and ensure the compatibility of the systems.

Foreign politics are also an issue at stake, since malicious actors involving political motivations are more involved in conducting cyber-attacks (also see the Research Paper on Managing Geopolitical Cyber Security Risks published by BIMCO). Suppliers can also imply complex dependencies related to foreign policy decisions, that is why assessing their level of reliability is essential to ensure business continuity.

Future threats in the maritime domain are likely to become more complex and related to geopolitics, but also to be more in the digital space, especially with the arrival of autonomous systems onboard.