JONES WALKER

2022

Ports and Terminals Cybersecurity Survey

joneswalker.com

Inside the Survey

90%

Of all the cargo moving throughout the United States, **90%** of it is transported on water.[1]

8 years

Within **eight years** of the delivery of this report, the volume of cargo traffic moving through US marine ports is likely to double.[2]

> Our national security and economic prosperity are directly dependent upon a safe and efficient marine transportation system, making it an attractive target for disruption by cyber criminals, nation-states, or state-sponsored adversaries. Without question, protecting the marine transportation system from cyber threats is a shared responsibility requiring both government and industry participation.
>
> **CAPT Andy Meyers**, US Coast Guard, Chief of the Office of Port and Facility Compliance

Foreword

US maritime ports and terminals are essential components of the nation's transportation-critical infrastructure. As volume and traffic to these facilities have seen exponential growth, maritime ports and terminals have also undergone significant changes in digitalization and automation of terminal operating and industrial control systems (ICS). Facilities are increasingly using automated operational technology (OT) systems to augment information technology (IT) and to communicate data, operate equipment, track cargo and containers, and manage commercial operations.

For decades now, maritime-industry stakeholders have recognized that more complex technology and widespread automation have heightened the need for security against cyber threats and attacks on ports and terminals. Business-system failures or other compromises of port and terminal systems can disrupt or shut down operations, interrupt supply chains, and cause significant financial, physical, and even geopolitical impacts.

Take a look at some recent events: Ports in San Diego, Houston, Long Beach, Rotterdam, and Barcelona have all suffered cyber attacks within just the past five years. Los Angeles, the western hemisphere's largest port, recently reported that it is battling 40 million cyber attacks per month — an astounding onslaught — that take the form of ransomware, malware, spear phishing, and credential harvesting. The situation worsened during the pandemic.

According to the International Association of Ports and Harbors (IAPH), the maritime industry globally suffered a fourfold increase in cyber attacks between February 2020 and May 2020. Across a longer timeframe, and looking at one threat vector in particular, from 2017 to 2020, attacks against OT systems increased by a whopping 900%.

In contrast, just over 20 years ago, cybersecurity was barely a blip on the radar. Enacted in the wake of the September 11, 2001, attacks, the Maritime Transportation and Security Act of 2002 (MTSA) focused on shoring up port and waterway "hard" security to deter, prevent, and respond to physical terrorist threats. (Indeed, the word "cyber" — or even the word "computer" — does not appear anywhere in the MTSA.)

More recently, and as technology has advanced, physical dangers have given way to cyber threats that, in turn, have generated greater attention from governmental agencies including the US Coast Guard (USCG) and the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), as well as maritime industry associations such as the Baltic and International Maritime Council (BIMCO) and the International Maritime Organization (IMO).

Awareness, Then Action: An Ongoing Process

We believe that regular surveys like ours have contributed to an increased awareness of and action toward improved cybersecurity. For example, in 2018, the inaugural year of our survey, we found a false sense of industry preparedness among maritime-operator respondents, with 69% confident in the sector's overall cybersecurity readiness, but a full 64% believing that their own companies were unprepared to handle the far-reaching business, financial, regulatory, and public relations consequences of a data breach. Over the course of the past four years, however, as our firm has been reporting on our cybersecurity survey findings, maritime players have expressed increasing preparedness. In this year's survey, 95% of respondents said that the ports and terminals industry is prepared to withstand cybersecurity threats and 90% believe that their own companies can do the same.

Beyond cyber-specific hazards, recent negative impacts on the global supply chain have underscored the need for enhanced attention to cybersecurity and facility cyber resilience. At the same time, the economic effects of the global COVID-19 pandemic, labor shortages, war in Eastern Europe, and escalating inflation all justify an intensified focus on the secure operation of blue- and brown-water transport facilities.

Against this backdrop, one point merits emphasis:

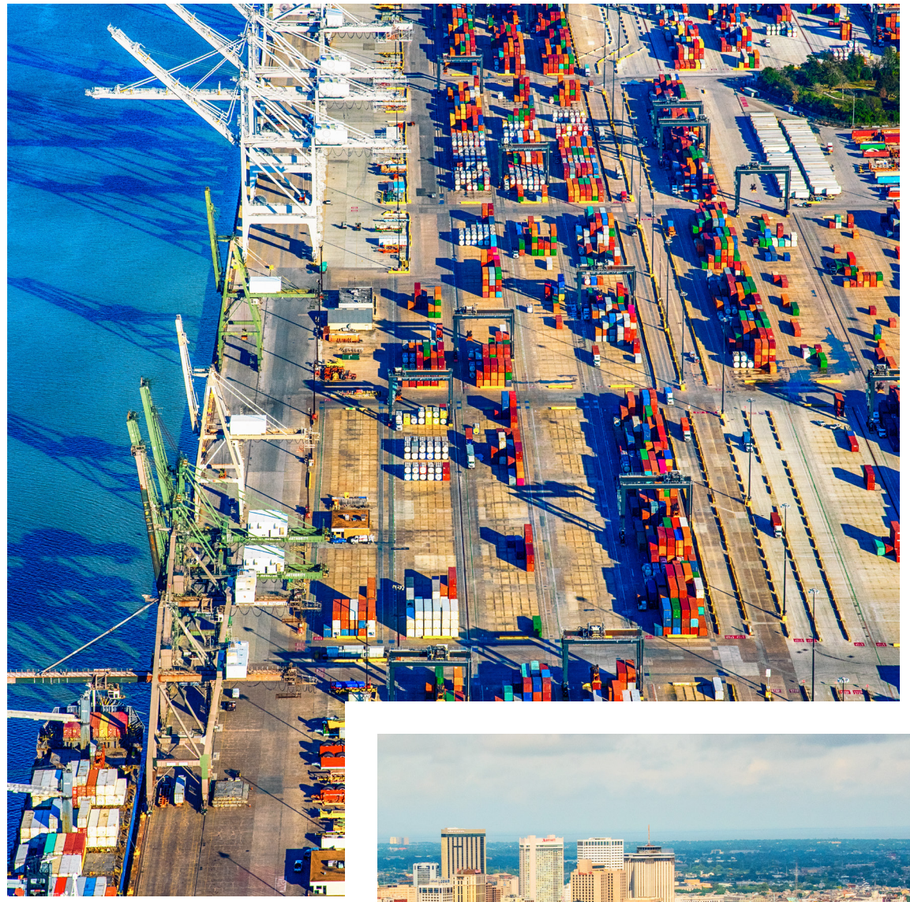
Port and terminal owners and operators are responsible for the cyber hygiene of their operations.

Because these port and terminal facilities present attractive targets to cyber-threat actors, Jones Walker LLP has selected this sector for the third installment in our series of infrastructure-focused cybersecurity surveys. This iteration follows two other critical infrastructure-directed surveys that examined the maritime industry as a whole (2018) and the midstream oil and gas sector of the energy industry (2020).

Our 2022 survey of 125 senior US port and maritime terminal executives looked at cyber preparedness and data security threats facing facilities responsible for handling the vast majority of the goods that move into, out of, and across the United States by water. In developing the survey, we drew on CISA's evaluation of port facility cybersecurity risks,[6] which include the following key areas of concern: facility access; terminal headquarters (data); terminal headquarters (ransomware); OT systems; positioning, navigation, and timing; and vessels.

These survey results delivered useful information about the port and maritime terminal sector's current state of preparedness, stakeholders' readiness to withstand or respond to threatened or actual cyber attacks, and the specific steps being taken to increase organizations' cyber resilience.

Ultimately, it comes down to motives, means, and opportunity: increasing those of the ports and maritime terminals that need fortification and decreasing those of threat actors. We hope you will find the following information useful and encourage you to use this survey as a tool in assessing — and enhancing — your organization's cyber readiness.



Several Takeaways Emerged

1

Confidence Is High in a Threat-Rich Environment

Ninety-five percent of port and terminal respondents said that they believe that their industry is prepared for cybersecurity threats, and 90% reported that their own facilities and organizations are similarly prepared to withstand a cyber-breach incident. However, this confidence may be misplaced: 74% of respondents indicated that their systems or data had been the target of a breach or breach attempt within the past year. **Page 14**

2

Take a Clear-Eyed View of Potential Threats

Port and terminal respondents' perceptions of potential threat actors and vectors aligned with recent reporting on the sources and types of cyber incidents that are occurring more broadly throughout multiple industries. In practice, however, the actual path of any given cyber attack or breach can be complex and involve multiple actors, vectors, attack surfaces, and vulnerabilities. Port and terminal operators must soberly assess their own vulnerabilities and risks to develop an effective cybersecurity strategy. **Page 25**

3

Make a Plan, Test the Plan, Update the Plan

Stakeholders must view cybersecurity as an ongoing process of normal operations. While 73% of respondents indicated that they have a written incident response plan (IRP), only one in five confirmed that their IRP had been reexamined and updated within the past year. Given the speed with which cyber threats evolve, vigilant planning is critical to lowering exposure to unnecessary risk. **Page 34**

4

People + Communication Are Key

At its core, cybersecurity is a human challenge. Cybersecurity plans must be implemented via proper training, effective communication, and a strong network of industry participants, trusted outside advisors, and public-private partnerships. While 57% of the blue-water respondents conducted cybersecurity training annually or more frequently, only 25% of the brown-water respondents met the same standard. Across the board, many ports and terminals have not implemented low-cost, high-impact tools such as encryption or collaborated with other organizations to share information and develop mutually beneficial cyber hygiene practices and cybersecurity strategies. **Page 44**

We hope you find this report on the state of cyber preparedness within the ports and terminals sector of the maritime industry useful. Please contact Andrew R. Lee, Hansford (Ford) P. Wogan, James A. Kearns, Ilsa H. Luther, or with any thoughts and questions.

Survey Methodology

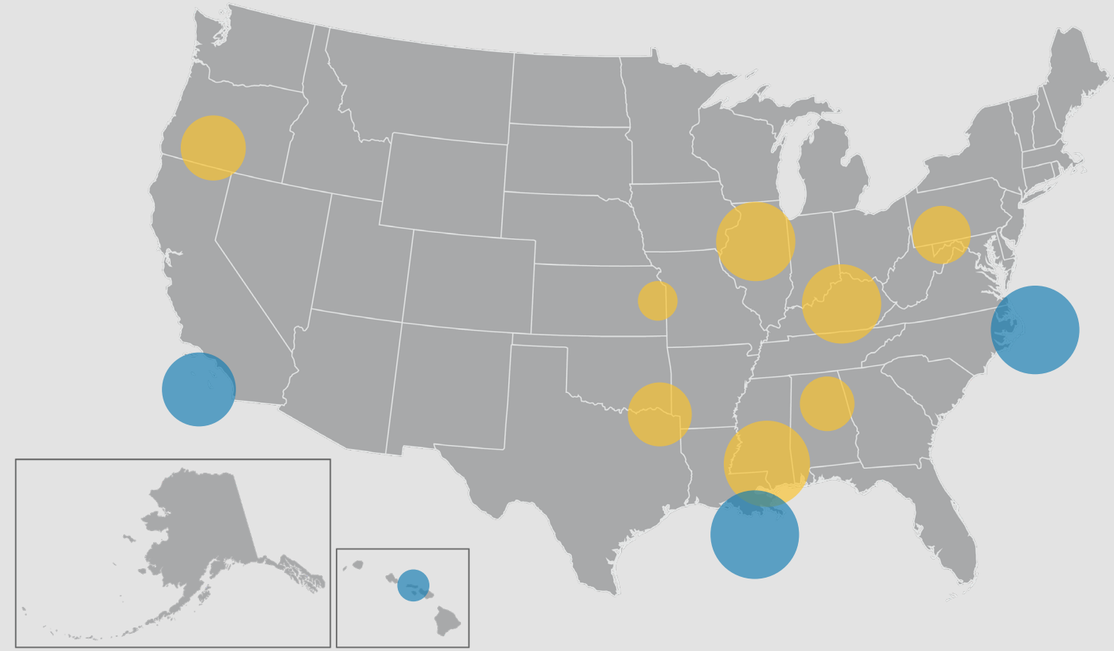
Sector: Blue- and brown-water ports and terminals in the United States
Survey Dates: May 2 to May 22, 2022
Number of Respondents: 125 key executives

Our online survey included questions that explored the following:

- Attitudes and perceptions toward cyber threats and risks
- History of actual and attempted data breaches
- Threat management and readiness
- Business operations, security training, and audits
- Strategic planning
- Security frameworks (including prevention and response plans and policies and technical platforms)
- Cyber insurance and industry collaboration

Questions that allowed for multiple answers are noted with an asterisk (*).

Location



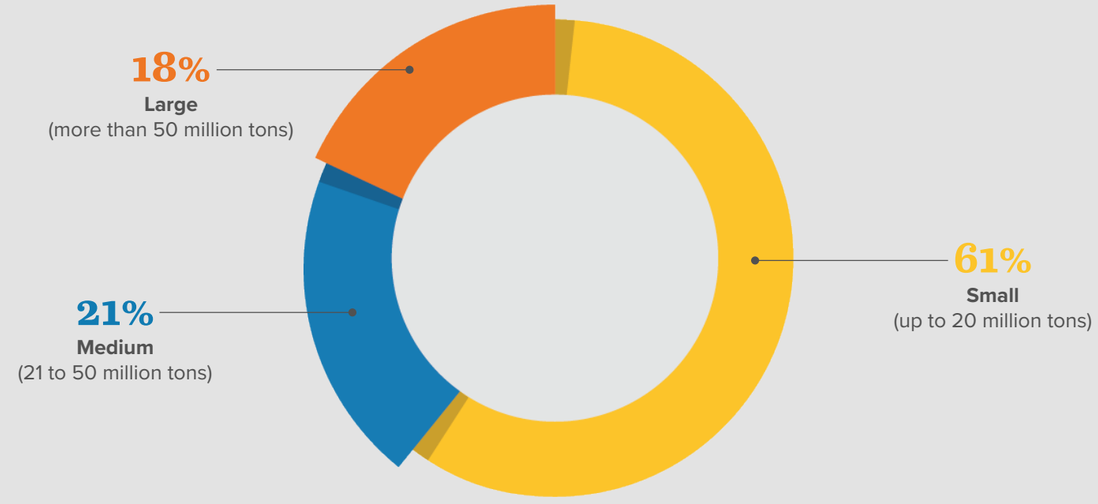
Blue-water facilities
40% (sited on Atlantic coastal waters, the Gulf of Mexico, Pacific coastal waters, and islands)

Brown-water facilities
60% (sited in non-coastal areas of the eastern United States, the Illinois, Mississippi, Missouri, and Ohio river basins, the Arkansas-White-Red rivers basin, Pacific Northwest rivers, and Southeast rivers)

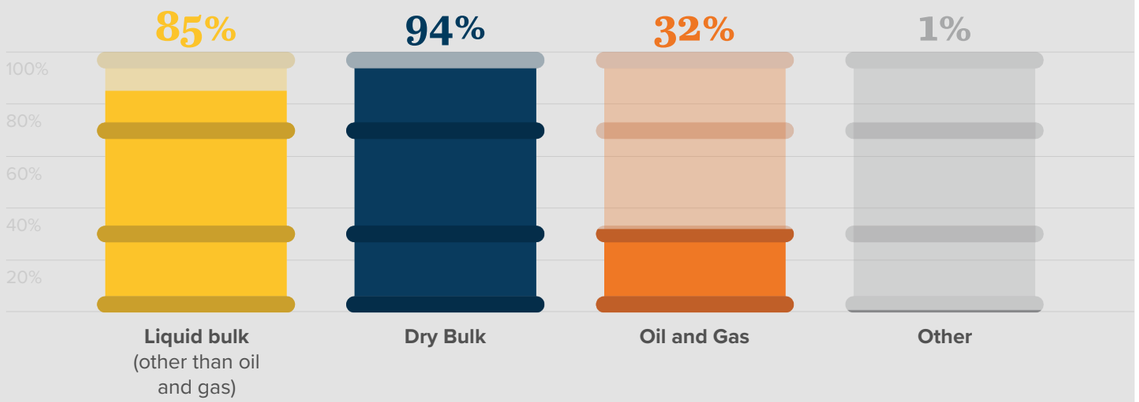
Except where noted, the responses to the survey were generally consistent across blue- and brown-water facilities.

Survey Methodology

Average annual tonnage handled over the past three years

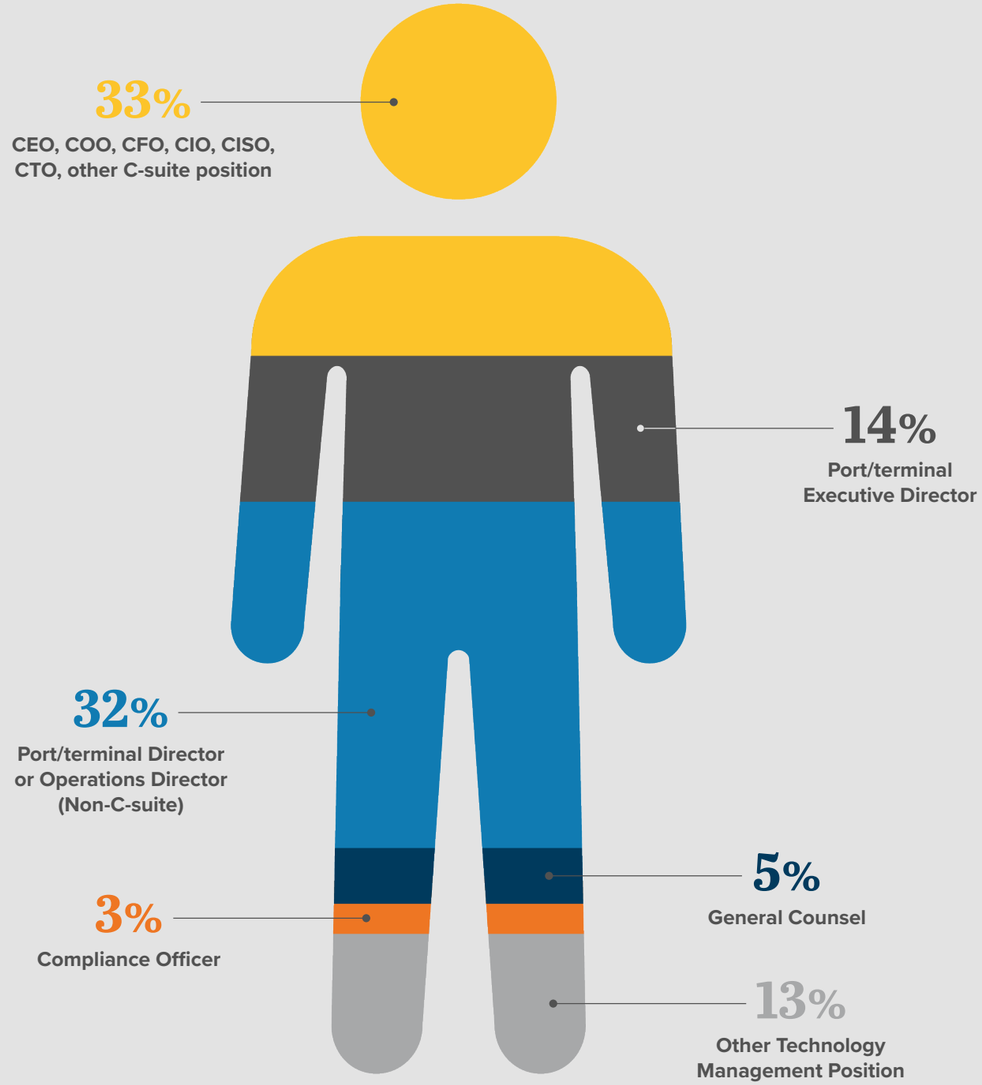


Types of commodities handled*



More than half (51%) of the blue-water respondents to the survey handle oil and gas; only 19% of the brown-water respondents handle these commodities.

Respondent position



01

Takeaway

Seventy-four percent of respondents indicated that their systems or data had been the target of a breach or breach attempt **within the past year**.

Confidence Is High in a Threat-Rich Environment

An overwhelming majority (95%) of port and terminal respondents indicated they believed that their industry is “very” or “somewhat” prepared for any cybersecurity threat. A similarly large majority (90%) reported that their own facilities and organizations are “very” or “somewhat” prepared to withstand a cyber-breach incident.

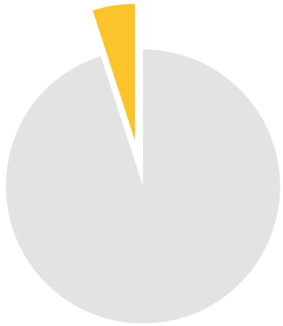
Despite this level of confidence, keeping pace with the increasing prevalence of cyber attacks remains a significant challenge. Seventy-four percent of respondents indicated that their systems or data had been the target of a breach or breach attempt within the past year.

Cybersecurity Confidence Is High

Compared to our 2018 and 2020 cybersecurity surveys, which polled maritime industry and midstream oil-and-gas stakeholders, respectively, 2022 respondents reported greater confidence in the cybersecurity preparedness of the ports and terminals sector as a whole and within their own organizations.

How would you describe the overall level of cybersecurity threat preparedness of US ports and terminals in general?

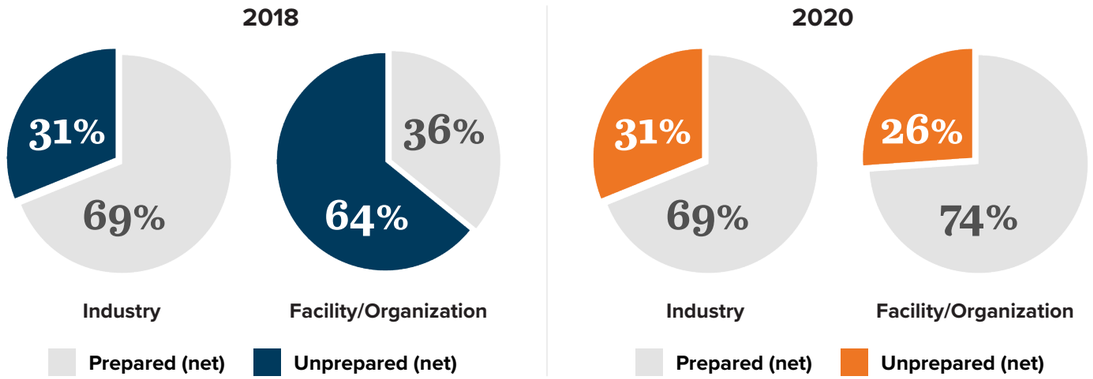
Prepared (net)	**95%**
Very prepared	72%
Somewhat prepared	23%
Unprepared (net)	**5%**
Somewhat unprepared	5%
Completely unprepared	0%



Overall, how prepared is your facility and organization to withstand a cyber-breach incident?

Prepared (net)	**90%**
Very prepared	50%
Somewhat prepared	40%
Unprepared (net)	**10%**
Somewhat unprepared	10%
Completely unprepared	0%

These answers contrast sharply with those of the 2018 and 2020 respondents: Only 69%, in both surveys, were confident that their particular industry was sufficiently cyber ready.



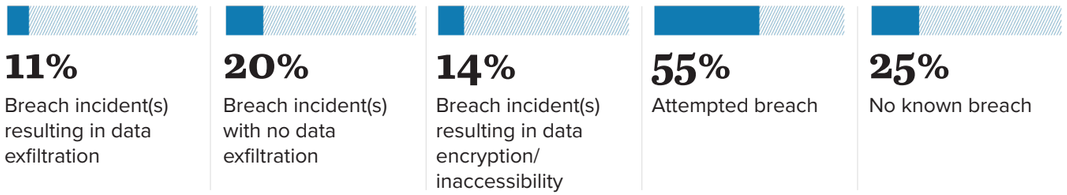
Significantly different regulatory schemes, an increasing emphasis on cybersecurity, and a rising number of actual attacks could explain this higher reported sense of preparedness within the maritime ports and terminals sector. As law-enforcement officials, government regulators, industry leaders, insurers, and media and news outlets pay increased attention to cybersecurity threats, businesses have more information and tools at their disposal to defend themselves against bad actors.

Of note is the fact that maritime operators (the focus of our 2018 survey) are not generally subject to the same federal regulatory requirements that apply to ports and terminals that handle most of the country's maritime cargo. Rather, these ports and terminals are considered MTSA-regulated facilities, meaning they are required to maintain a Facility Security Plan (FSP), which is subject to USCG review, and a Facility Security Assessment (FSA) that assesses and documents potential vulnerabilities associated with these facilities' computer-based systems.

Attacks Are an Ongoing, Real-Time Concern

Ports and terminals may be able to justify a higher sense of cybersecurity confidence; however, *preparedness* for, *prevention* of, and *response* to cyber incidents are very different things. While respondents expressed confidence in their state of preparedness, a majority indicated that their systems had been hit with actual cyber attacks.

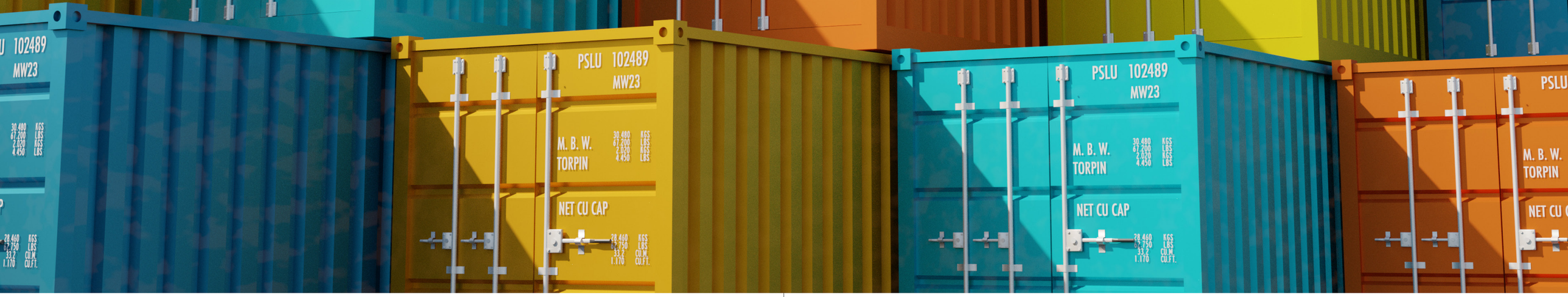
Within the past year, in what way(s) has (have) your facility's systems and/or data been compromised?*



This finding mirrors other industries. The manufacturing and mining sectors, for example, have seen significant increases in cyber attacks of multiple varieties, including denial of service (DoS), credential theft, and ransomware.[7]

Despite the high rate of attacks, the number of survey respondents who reported losses from breach incidents was surprisingly low. Eleven percent of respondents indicated that an attack in the prior year resulted in data exfiltration, 14% reported that an attack resulted in data encryption and/or inaccessibility, and 20% noted breaches without any actual data loss.

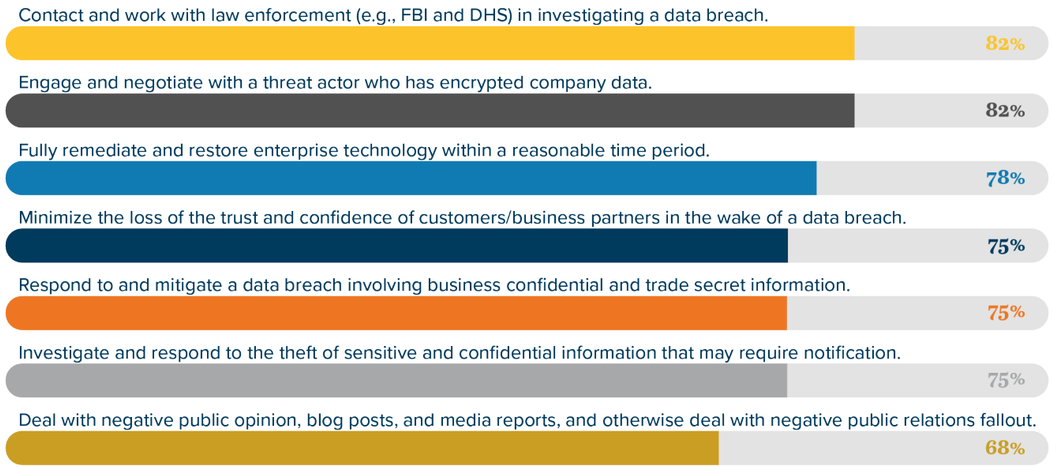
Measured according to tonnage handled, ports and terminals vary considerably. But threat actors appear to be malevolently egalitarian when it comes to size. More than half of stakeholders in every category reported that they have been targeted: large (57%), medium (54%), and small (55%).



After the Attack: Law Enforcement Cooperation, Disclosures, and Lessons Learned

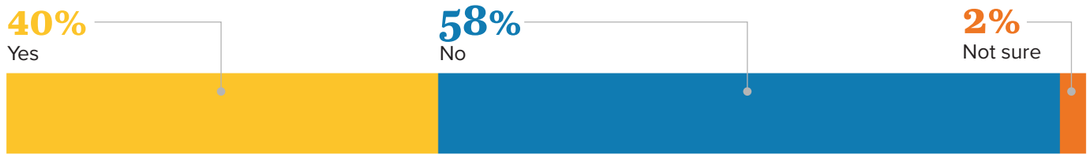
When asked about mitigation actions they were prepared to take in the aftermath of a breach incident, 82% of respondents indicated a willingness to work with law enforcement in investigating the attack. A similar percentage expressed willingness to seek help outside their organizations during the incident response and mitigation phase.

My facility/organization is prepared to ...*



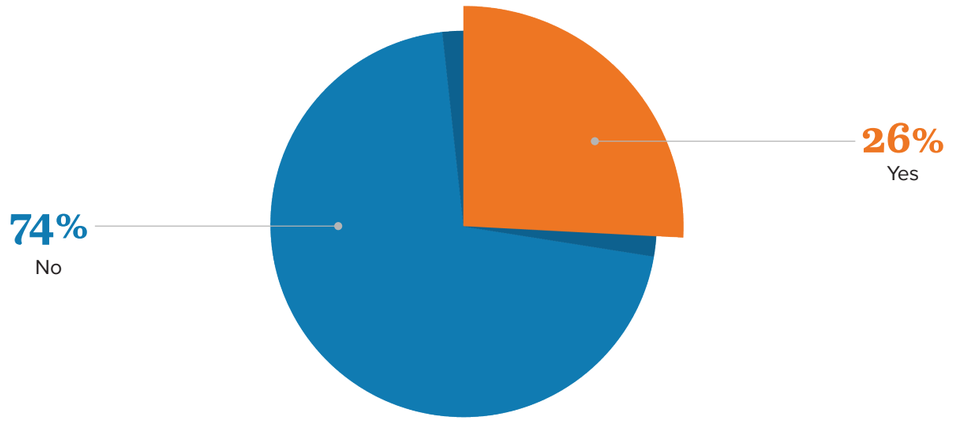
However, of the respondents who reported that their facilities had actually suffered a data breach, only 40% engaged with law enforcement during the post-breach investigation phase.

Did you engage with law enforcement (e.g., FBI or DHS) in an investigation of the data breach?



An even smaller percentage of respondents reporting a breach indicated that they had made additional external disclosures of the breach.

Was the data breach disclosed outside the company other than to law enforcement?



This lack of reported law enforcement engagement and low rate of outside disclosures following actual cybersecurity breaches are consistent with what law enforcement and other agencies have said is happening. The US Senate Homeland Security Committee emphasized the need for increased reporting of cyber breach incidents: **"When more data is collected, the federal government will be in a better position to assist existing and potential cybercrime victims with prevention, detection, mitigation, and recovery."**[8]

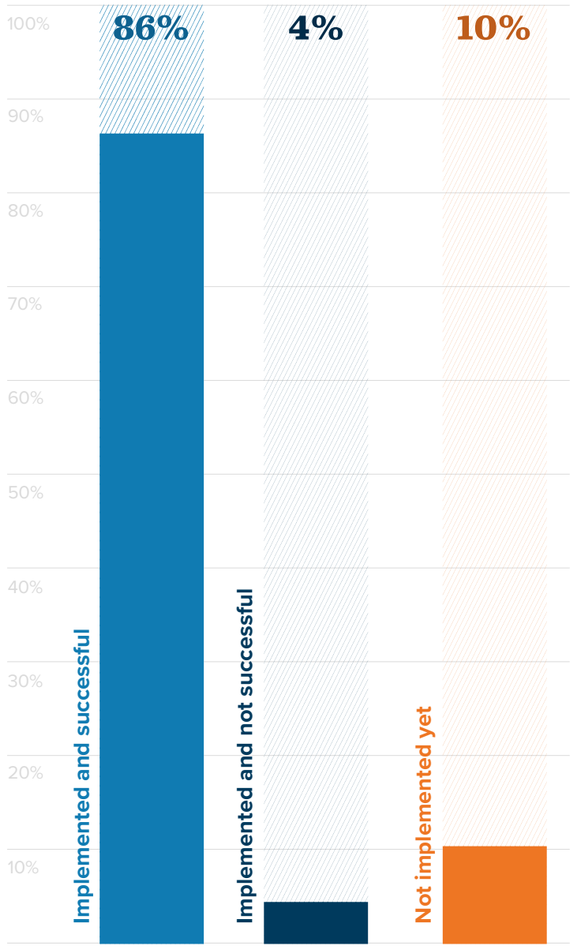
Marine facilities need to be aware, however, of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) that was enacted in March 2022. CIRCIA requires CISA to develop and implement regulations requiring a company that operates in one or more of CISA's 16 critical infrastructure sectors to report covered cyber incidents and ransomware payments to CISA within 72 hours of the company's reasonable belief that a cyber incident has occurred and to report ransom payments within 24 hours after a payment is made.

These new authorities are regulatory in nature and require CISA to complete mandatory rulemaking activities before the reporting requirements go into effect. CIRCIA mandates that CISA develop and publish a Notice of Proposed Rulemaking (NPRM), which will be open for public comment, and a Final Rule. CIRCIA also requires that CISA consult with various entities throughout the rulemaking process, including risk management agencies in CISA's critical infrastructure sectors, the Department of Justice, other appropriate federal agencies, and a soon-to-be-formed DHS-chaired Cyber Incident Reporting Council. As of the date of our report, this work is underway. Each facility should consult its legal counsel for the latest developments in this process.

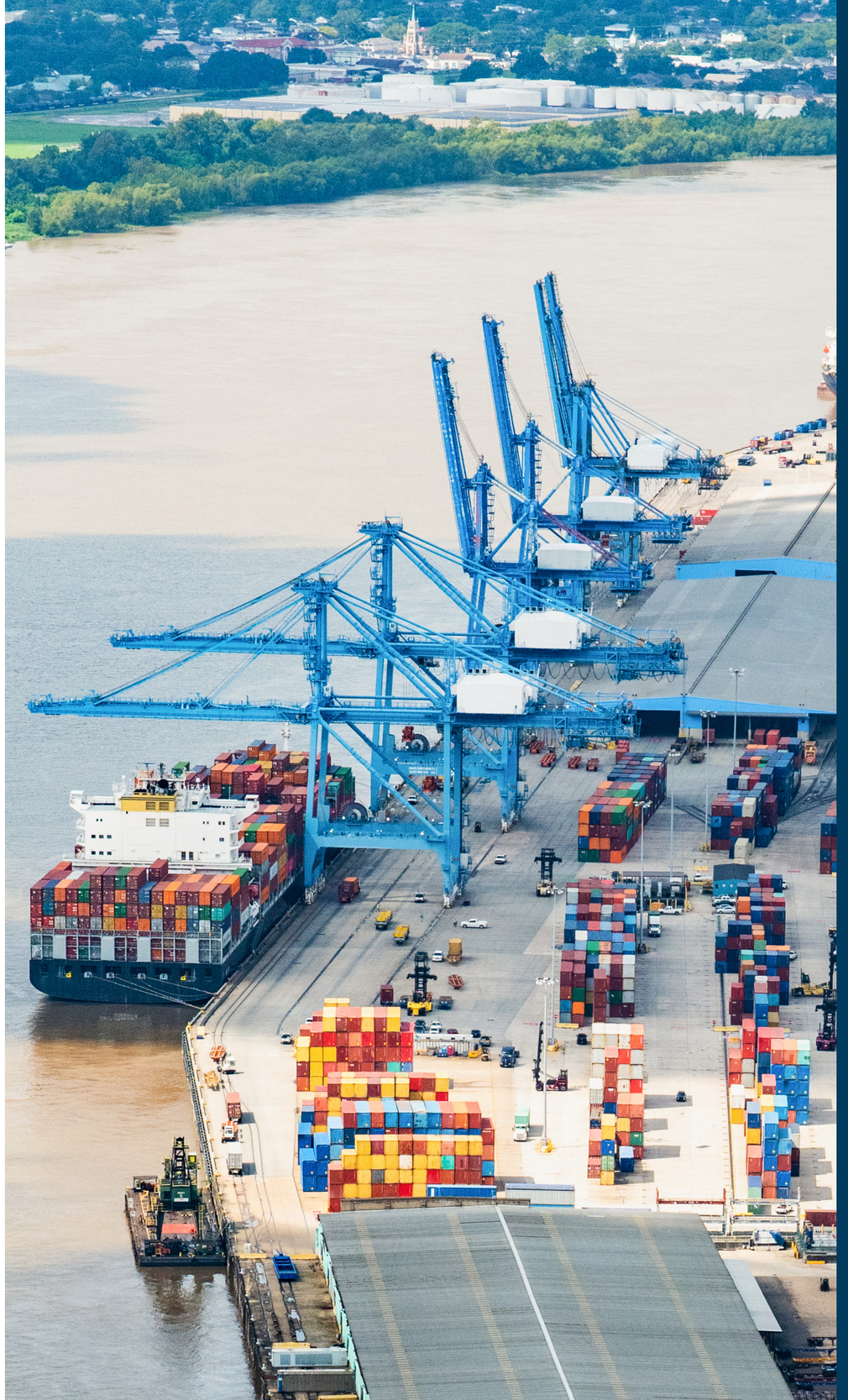
Transparency and information sharing, specifically with local and federal law enforcement agencies, as well as relevant cybersecurity cooperatives, can be of benefit to both the cyber-attack victim and to the broader industry. Such disclosures can let others who have been victims of such attacks know that they are not alone and serve as a warning against complacency for potential victims in the industry.

Eighty-six percent of respondents reporting a cybersecurity breach took post-breach action that they deemed successful.

Thinking about the cybersecurity breach(es) your facility experienced in the past year, were post-breach preventive measures implemented and successful?



This underscores the notion that, while a breach or intrusion event might be seen as a failure of policies, procedures, or defensive technologies, it is nonetheless important to view a cyber attack as a learning opportunity.



Best Practices

While port and terminal operators report that they are taking action to increase their cyber resilience, this is not the time to ease vigilance against such threats. Attacks are on the rise and growing in sophistication. **The rapid evolution of cyber threats should be matched with coordinated action.** Organizations should work closely with information security experts, industry associations, skilled legal counsel, and government cybersecurity-focused agencies to share information and refine defensive measures.

Our nation’s maritime transportation infrastructure is critically important to the US economy and to the health, safety and welfare of the public. To ensure safe and reliable port operations in the face of increasingly complex infrastructure systems and threats to cyber and physical security, our nation’s port authorities and operators must remain vigilant, fully informed and prepared, including through education, training, planning and collaboration, as further outlined in the 2022 Ports and Terminals Cybersecurity Survey.

Tom Smith, Executive Director,
American Society of Civil Engineers

02 Takeaway

Survey participants identified **“lone wolf” hackers and organized crime groups as the top threat actors** menacing the ports and terminals sector...

Take a Clear-Eyed View of Potential Threats

“The good news is that we actually know how to solve these problems. We can fix cybersecurity ... I have never seen such near unanimity and awareness ever before.”[9]

Glenn S. Gerstell, Former General Counsel,
US National Security Agency

Threat Actors and Threats: Perceptions (Mostly) Align With Reality

Survey participants identified “lone wolf” hackers and organized crime groups as the top threat actors menacing the ports and terminals sector, with nation-state affiliated groups a close third. Still, 35% listed internal staff and employees as a threat. These figures line up with findings in the broader economy.[10]

This perception also aligns with stakeholder experience. Of the respondents who reported being victims of cyber breaches, 64% indicated a solo threat actor/hacker was responsible, while 32% identified an organized crime group.

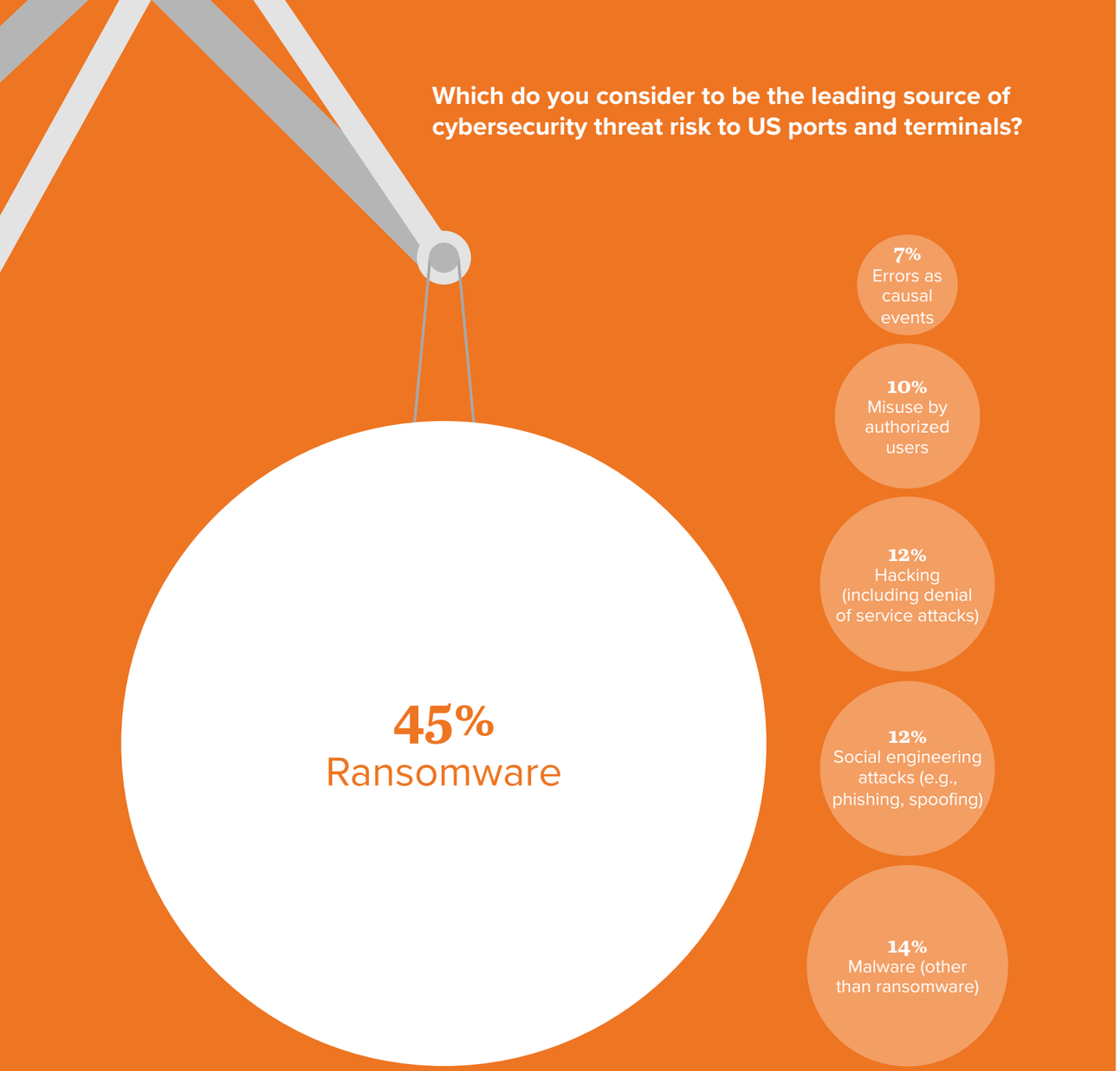
Which of the following do you consider to be the leading cybersecurity threat actors targeting US ports and terminals?*

- Solo threat actors/hackers (including vandalism, not for social or political ends)
- Organized crime groups
- Nation-state affiliated groups
- Internal/employees
- Activists/hacktivists

What type of threat actor(s) was responsible for the system compromise?*

- Solo actor/hacker (including vandalism, not for social or political ends
- Organized crime groups
- Activists/hacktivists
- Nation-state affiliated
- Internal/employees
- Unsure

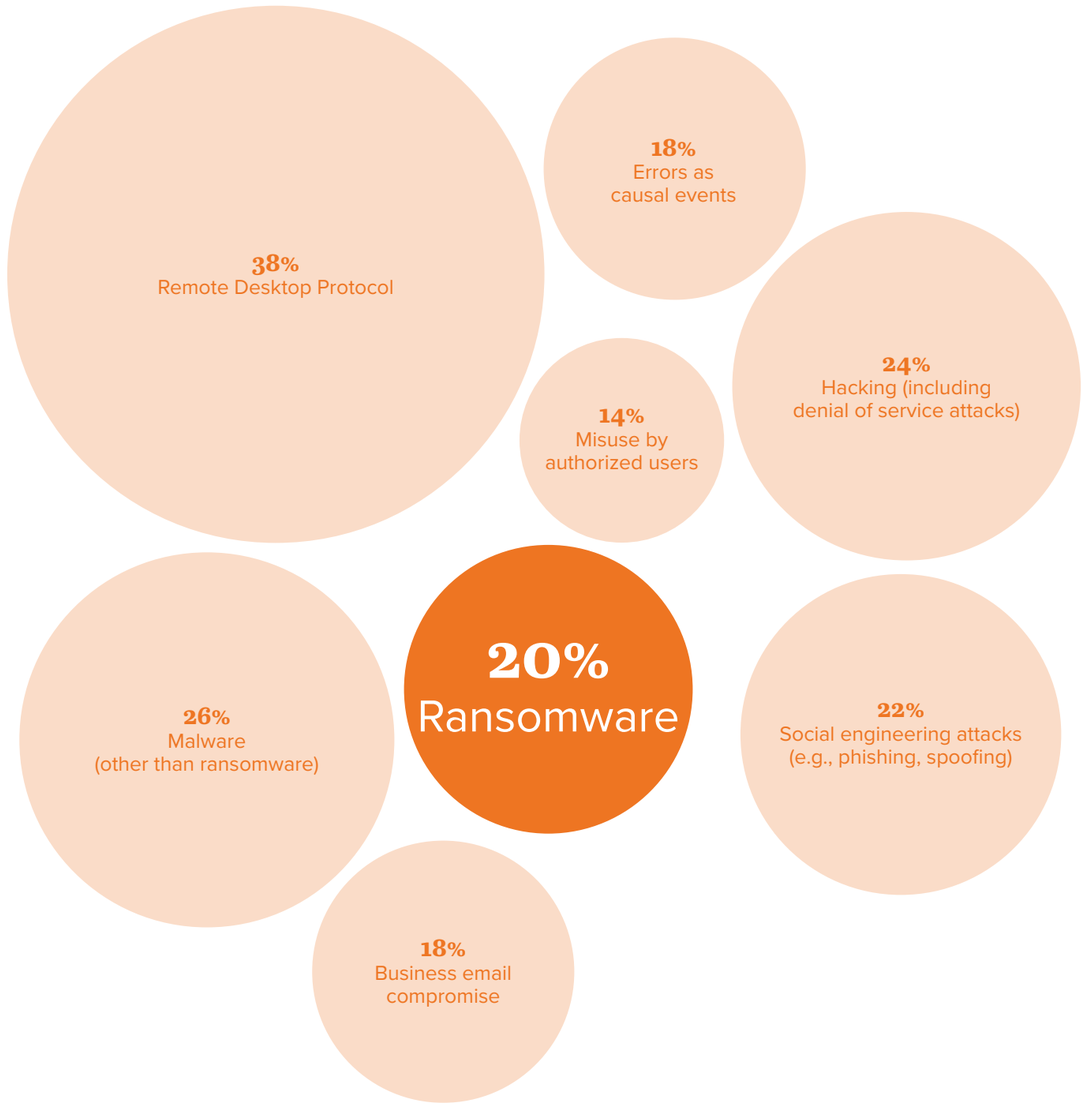
Which do you consider to be the leading source of cybersecurity threat risk to US ports and terminals?



45% **Ransomware is the primary cyber-threat concern**, according to a plurality of respondents.

Fear of ransomware appears to be outpacing actual ransomware events, as only 20% of respondents whose organizations had actually been victimized by a cyber attack listed ransomware as the primary attack vector. (However, the responses given to the following question should be considered in light of the under-reporting of ransomware attacks that law enforcement agencies suspect is taking place, as discussed below.)

What was the nature of or the type of attack that resulted in the compromise of the facility's system?*



The actual path of any given cyber attack or breach can be complex and involve multiple actors, actions, vectors, and vulnerabilities. Threat actors may chart a path that starts with a phishing email or stolen credentials. Once inside, the actor may remain in the network for a lengthy period of time, exploring the network for valuable assets, designing social engineering or data exfiltration exploits, or ultimately launching DoS or ransomware payloads. In order to implement appropriate mitigation measures, a diligent post-breach investigation is critical.

Let's Talk About Ransomware

Ransomware is a particular flashpoint for law enforcement, government officials, and industry groups. According to recent reports, ransomware involvement in data breaches rose by double digits in just the last year.[11, 12] And the data analytics firm Chainalysis reported that US businesses sent more than $1.3 billion in ransom payments to hackers in 2020 and 2021.[13]

The vastness of the problem is still unknown. The FBI has indicated that reports of ransomware events are "artificially low," while CISA estimates that only one in four ransomware incidents are reported. Meanwhile, these agencies indicate that approximately three-quarters of 2021 global ransomware payments likely went to Russian or Russian-government-controlled criminal enterprises. As CIRCIA is implemented by CISA, there is likely to be greater transparency of ransomware events and the extent to which ransom payments are being made.

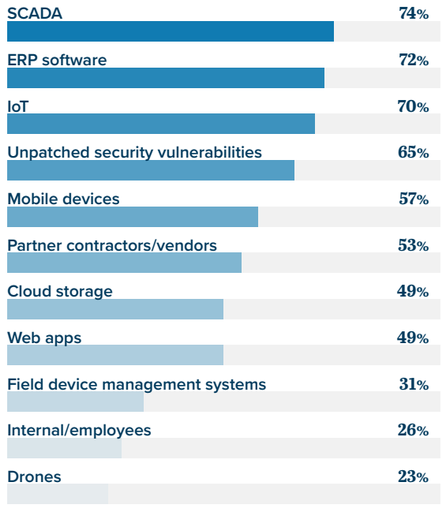
Top Vulnerabilities: Control Systems, ERP, and IoT

As facility digitalization spreads and technologies grow more sophisticated and widespread, the list of top perceived vulnerabilities for port and terminal platforms is likewise expanding.

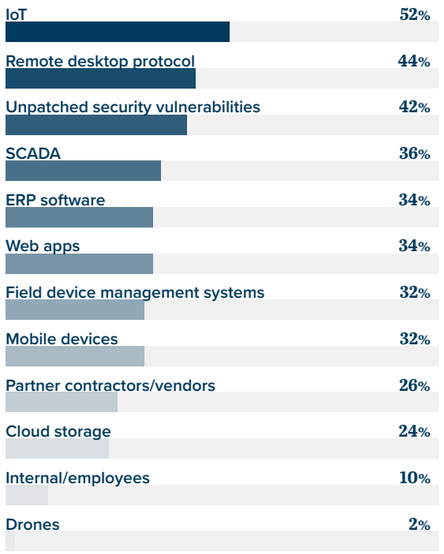
Port and terminal stakeholders saw supervisory control and data acquisition (SCADA) systems, enterprise resource planning (ERP) software, and Internet of Things (IoT) devices as attack surfaces of particular concern.

Respondents' descriptions of actual data breaches tracked their ranking of top cybersecurity vulnerabilities. The subset of respondents who reported suffering a breach listed IoT, remote desktop protocol (RDP), unpatched software, and SCADA as the top attack surfaces.

Which of the following do you consider to be the cybersecurity vulnerabilities of US ports and terminals?*



What vulnerabilities were involved in the data breach?*



"The Jones Walker team brilliantly highlights how the ever-changing cybersecurity world is affecting marine ports and terminals. Threat actors are continuously improving their attack techniques and simply having a Cyber Incident Response Plan and Cybersecurity Policy is not enough to protect your data. As Jones Walker highlights with this survey, ports and terminals need to regularly practice their cybersecurity plans through testing, tabletop exercises and outside assessments from lawyers and consultants who are investigating cyber-attacks on a daily basis."

Heather Hughes, VP Engagement Management, Stroz Friedberg, LLC, an Aon Company

Best Practices

Assessments of threats and vulnerabilities must be data-driven. **Port and terminal operators should consult with cybersecurity professionals and other experts to identify key areas of concern for their particular facilities**, utilize all available data to assess possible attack surfaces and vectors, study ways to address vulnerabilities, and take action to address them.

03

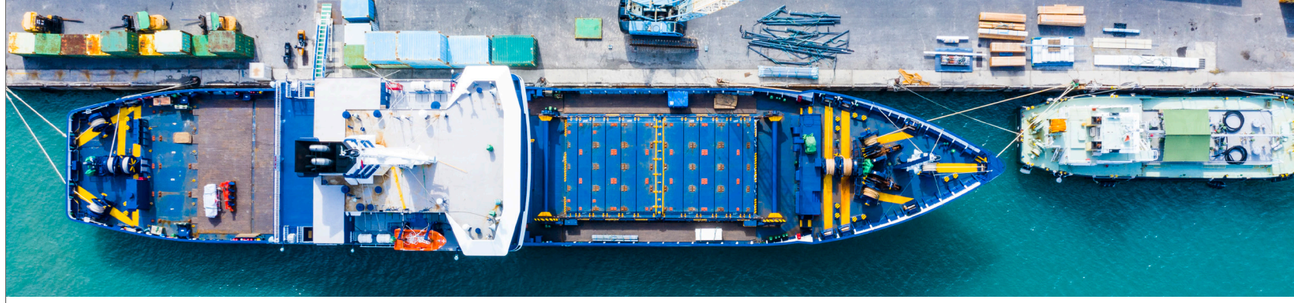
Takeaway

Make a Plan, Test the Plan, Update the Plan

Port and terminal respondents reported a high level of cybersecurity planning. Nearly three-quarters (73%) indicated that they have in place written IRPs and cybersecurity plans separate from their USCG-reviewed and approved FSPs, and 23% reported that their cybersecurity plans are incorporated into their facility strategic or security plans.

But having a plan and having a plan that works are two different things. To be effective, stakeholders must ensure that facilities' plans are practical, sufficiently detailed and comprehensive, and updated and tested frequently.

> And because no risk is static, stakeholders must view cybersecurity as an ***ongoing process of normal operations***.

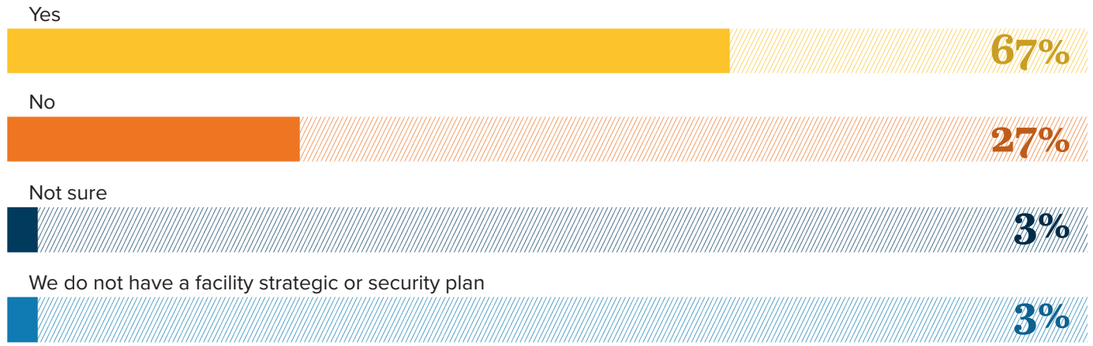


A successful cyber-resilience program is an essential component of a facility operator's risk-management plan. Each organization must first identify, evaluate, and mitigate cyber-related risks. These procedures must be incorporated into internal written policies. And because no risk is static, stakeholders must view good cyber hygiene as an *ongoing process of normal operations*. This requires establishing and following a regular schedule to **1)** review cyber risks, **2)** reevaluate the need for mitigation measures, and **3)** ensure personnel comprehend and are able to follow good cyber practices.

Cybersecurity Plans Are Mostly Present, but in Various Forms

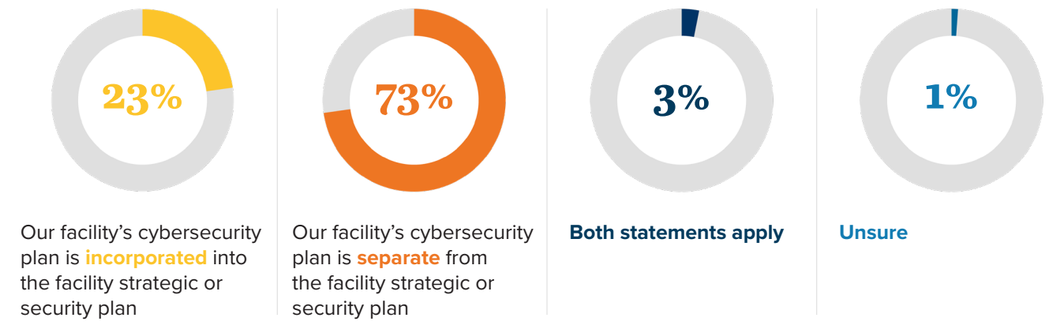
Two-thirds (67%) of facilities and organizations in the US ports and terminals sector address cybersecurity in their facility security plans.

Is cybersecurity addressed in your facility's/organization's strategic or security plan, such as a facility security plan reviewed and approved by the US Coast Guard under its MTSA regulations?



However, 73% of respondents noted that the cybersecurity plan is a separately maintained instrument.

Which of the following statements best describes how cybersecurity is incorporated into your facility's strategic or security plan?

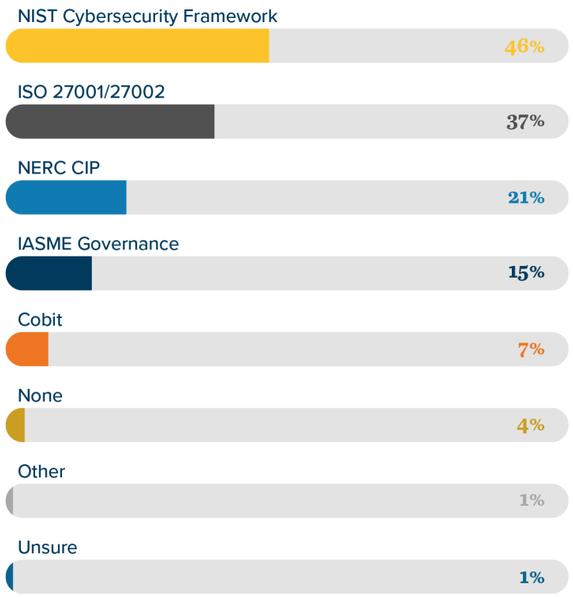


Survey respondents indicated that the development and maintenance of the cybersecurity plan is most often delegated to IT department leadership: 85% reported that the chief information officer (CIO) participates in their facility's cybersecurity plan and 75% noted that other IT staff and cybersecurity personnel are also involved. A majority (55%) also said that the chief executive officer (CEO)/president participates in the plan. Beyond that, however, other C-suite executives, boards of directors, and officers had significantly lower rates of involvement.

Who participates in your facility's cybersecurity plan?*

Virtually all respondents reported that their port or terminal's cybersecurity compliance plan follows a formal cybersecurity framework, or a combination of more than one framework. Nearly half (46%) have implemented the US Department of Commerce National Institute of Standards and Technology (NIST) Cybersecurity Framework.

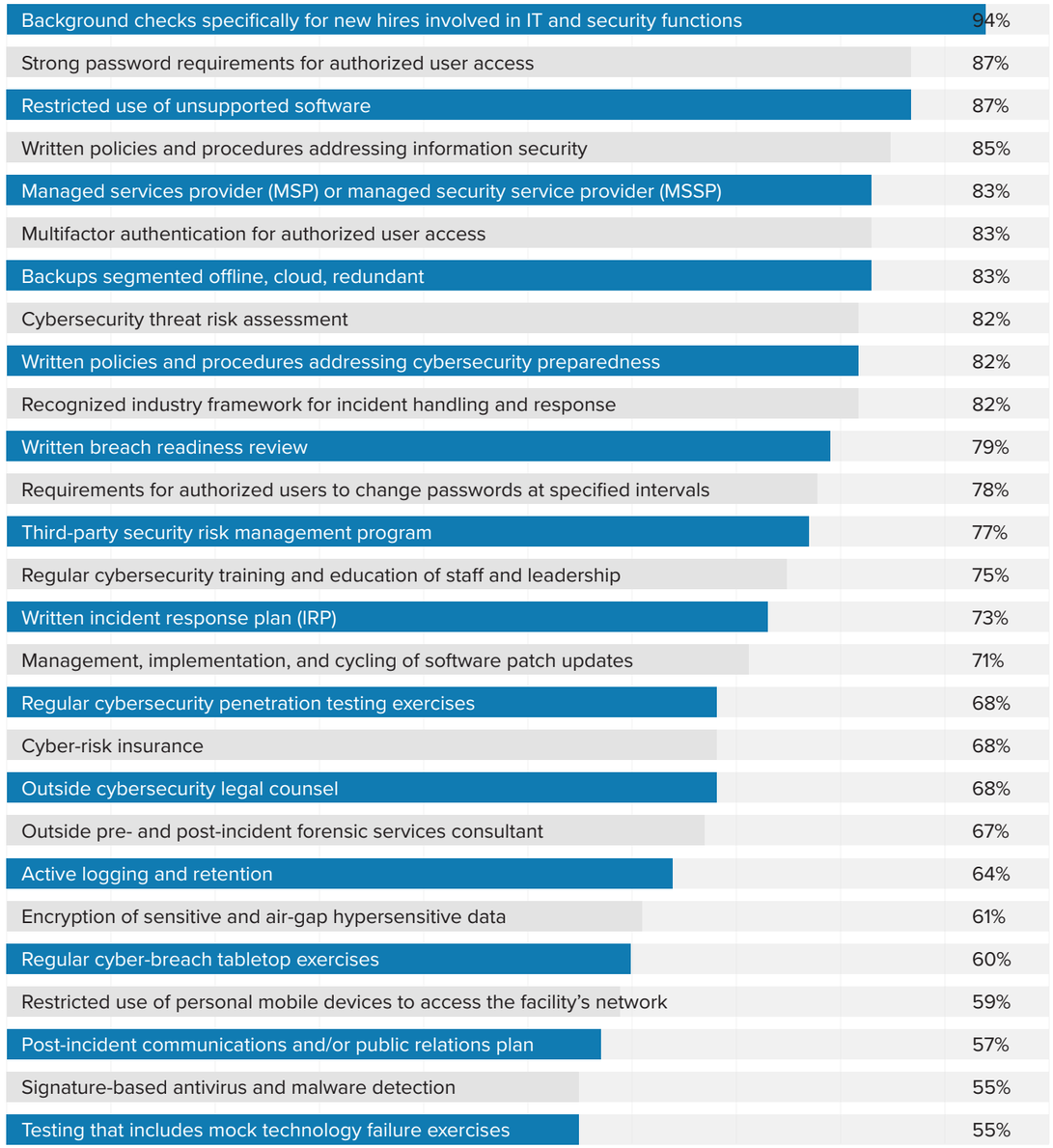
Which cybersecurity framework does your facility use?*



> Cybersecurity remains pivotal in maintaining confidence in a stable and independent IT infrastructure to support the movement of goods through America's coastal and inland waterway system. Now more than ever, our nation's ports and terminals must stay vigilant against cyber-attacks by testing our own system and policies, and trying to stay one step ahead of bad actors.
>
> **Dennis Wilmsmeyer,**
> Executive Director, America's Central Port

Respondents also indicated that their organizations have implemented a range of other measures to enhance cyber resilience, including important actions such as routine background checks, strong password requirements, and multifactor authentication for authorized user access.

The following is implemented at my facility:*



The Plan Is There — but Is It Strong and Updated?

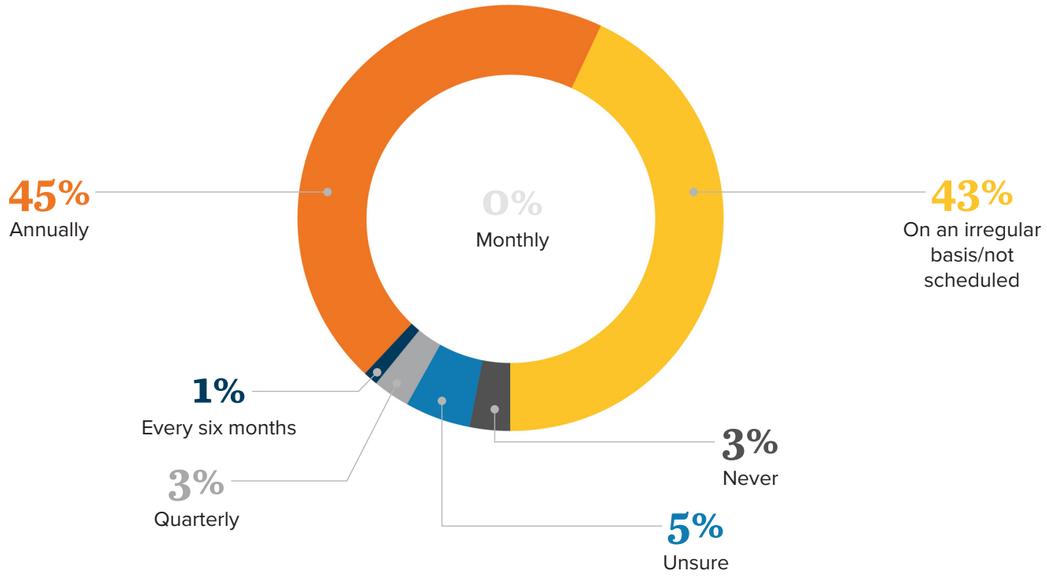
A well-designed plan is a necessary first step in achieving better cyber resilience. But a plan is really no more than a theory until it is tested, updated, and communicated — and tested again. Without this rigorous, reiterative process, the plan's effectiveness will remain unknown until it is put into action, at which point it will be too late to make adjustments if it is not up to the task.

In our survey, while 73% of respondents reported having a written IRP, only 21% confirmed that their IRP was reexamined and updated within the past year. Meanwhile, 28% of those who confirmed having updated their IRP at some point indicated that the review and revisions had occurred more than two years ago.

How recently did your facility update its written incident response plan?

Tabletop exercises (TTX) are aimed at testing the effectiveness of an organization's training. Well-designed and -implemented TTX test the operating environment to determine how the organization would respond to hypothetical challenges. The exercises can reveal challenges, consequences, capability gaps and, consequently, vulnerabilities. In our survey, more than half (51%) of respondents with an IRP reported that their facility conducted IRP TTX irregularly, not at all, or were unsure of the schedule.

How frequently does your facility conduct IRP tabletop exercises?

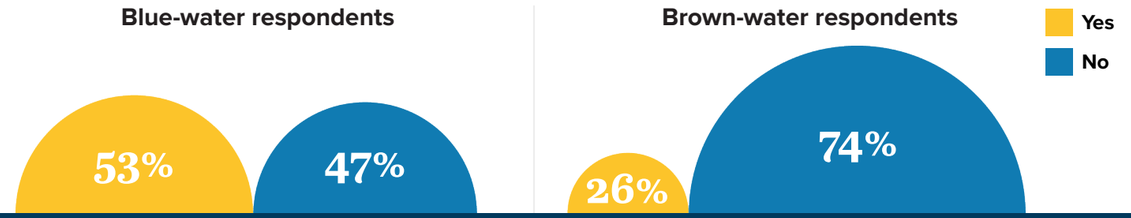


A cybersecurity risk assessment is primarily designed to help a facility assess operational cyber risk, i.e., the extent of the threats inherent in the entity's systems. Our survey found that 72% of ports and terminals reported conducting cybersecurity risk assessments at their facility at least once a year.

How frequently does your facility conduct cybersecurity-risk assessments?

Fewer respondents indicated that their organizations have taken more active steps to prepare for a cyber-breach event, specifically by undergoing a data security systems or breach-readiness audit in the 12 months preceding the survey. Between sea and river ports, 53% of the blue-water respondents reported that they had undertaken such a review, but only 26% of the brown-water respondents had done so.

Within the past year, has your facility undergone a data-security systems or breach-readiness review or audit?



Best Practices

Cybersecurity plans are useful only to the degree that they have been updated and tested. Testing can require resources, skill sets, and a level of objectivity that may force an organization to look outside for help. Consider engaging independent, skilled outside parties to conduct comprehensive tests of your cyber readiness, IRP, and information-security plan, and to provide actionable guidance and a roadmap for improvement.

04

Takeaway

People and Communication Are Key

At its core, cybersecurity is a human challenge. To have practical, positive impacts, cybersecurity plans must be implemented via proper training, effective communication, and a strong network of like-minded professionals, businesses, trusted outside advisors, and public-private partnerships.

At its core, cybersecurity is a **human challenge**.

The Jones Walker 2022 Ports and Terminals Cybersecurity Survey found that only 24% of brown water ports and terminals required staff to participate in annual training.

As an association dedicated to fostering mutual support among our members, we were also concerned to learn from the Jones Walker survey that only 25% (one quarter) of the respondents still do not collaborate with others in the industry to improve cybersecurity efforts. It seems so obvious that one way to thwart cyber attacks is to share best practices and to collaborate with each other across our industry. Industry associations like IRPT are ideal for this, especially for the smaller facilities along our nation's inland waterways.

Aimee Andres, Executive Director
Inland Rivers, Ports and Terminals, Inc.

Training Must Match the Threat

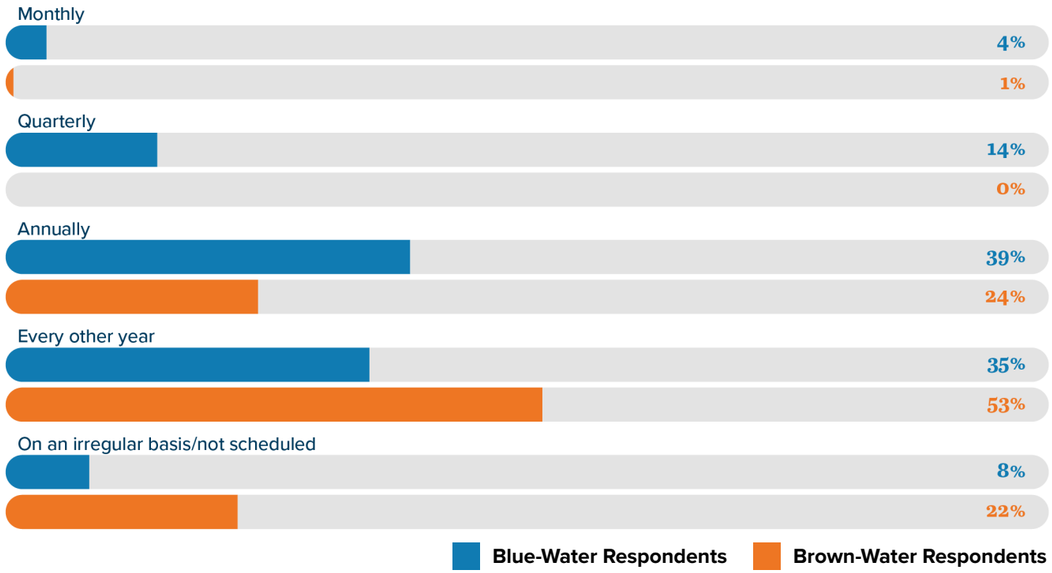
Although the marine industry has a long history of success in risk management, cyber threat actors represent a different kind of menace. They are sophisticated, constantly evolving, and highly motivated.

Despite their sophistication, however, some of the most important defenses are among the simplest to implement and manage. Strong password-management protocols, restrictions on the use of unsupported software and personal mobile devices, and robust training can establish a solid, frontline defense, which in turn can be supplemented by higher-level, technology-based solutions where resources allow.

Regular, effective employee training is particularly critical to a successful risk-mitigation strategy. Cybersecurity training should be provided on an annual basis, at a minimum, and more often for key employees whose responsibilities include managing highly sensitive data or systems. Without regular instruction and reinforcement, learning fades quickly.

When asked about the frequency of cybersecurity training, there was a significant difference between the responses of blue- and brown-water facility stakeholders. This annual standard was met by 57% of the blue-water respondents, but by only by 25% of the brown-water respondents.

How often is your facility's staff required to participate in cybersecurity training?



Work With Reputable Vendors That Embrace Cybersecurity

It is important to identify and engage top-quality cybersecurity trainers. In our survey, 54% of participants indicated that they engage third-party service providers to conduct cybersecurity training. However, some of these providers offer such training as an add-on to higher-value (from their perspective) IT services and are not fully qualified to deliver effective offerings. Buyer beware: Individuals with responsibility for engaging outside providers should work with experienced cybersecurity counsel to identify vendors with real expertise.

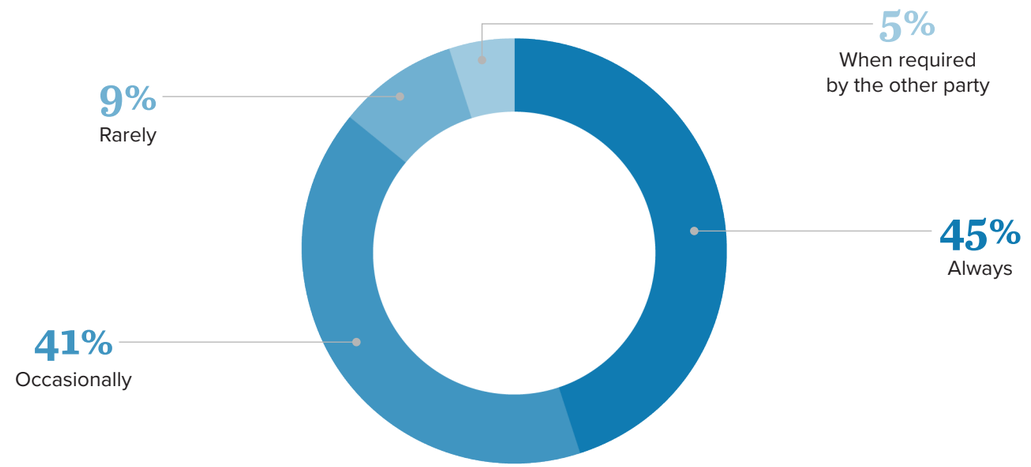
How has your facility executed staff cybersecurity training?

Third-party providers should maintain their own — and comply with others' — strong cybersecurity policies and standards. This applies not only to IT vendors but also to banks and other financial services providers; payroll services, human resources, and other outsourced-services providers; suppliers; and more.

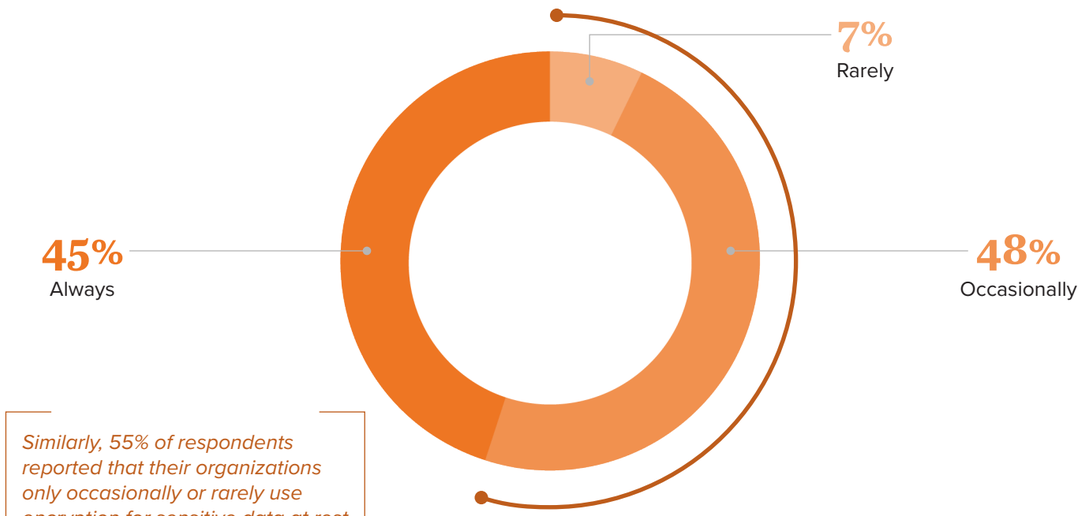
Encrypt Sensitive Communications and Information

Encryption is another relatively simple tool that can add layers of security to sensitive communications. While its use is not necessary in all situations, 55% of survey participants reported that their facilities use encrypted communications systems for sensitive communications only occasionally, rarely, or when required by other parties.

Does your facility use encrypted communications systems to transmit sensitive information?



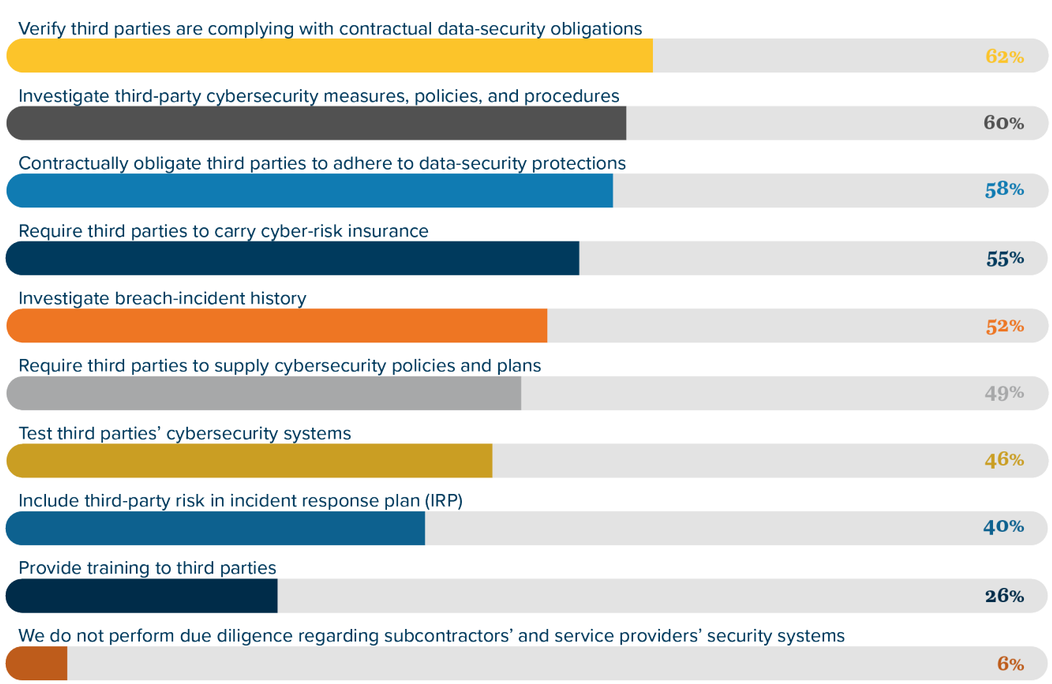
Does your facility encrypt sensitive information that is at rest and/or stored?



Similarly, 55% of respondents reported that their organizations only occasionally or rarely use encryption for sensitive data at rest.

Given the many points of entry and vulnerabilities associated with connected systems and information exchange, ports and terminals should investigate and verify that their outside vendors have high-quality cybersecurity defenses and processes in place. Our survey indicated that there is room for improvement in this area.

Which of the following actions, if any, does your facility take when choosing and performing due diligence regarding subcontractors' and service providers' security systems?*



Collaboration Is Critical

The appropriate response to a cyber breach will depend on the unique circumstances of the attack, the volume and type of data that has been exfiltrated or corrupted, and other factors. A one-size-fits-all breach response would likely fit none of these circumstances.

Businesses can, however, collaborate proactively with partners to help identify risks and develop shared strategies to deter bad actors. Government agencies, trade associations, and public-private organizations are focused on helping businesses — and critical infrastructure stakeholders, in particular — improve cyber readiness. These organizations not only provide training and resources but also act as a clearinghouse for updated, real-time information that can help raise awareness about imminent threats and provide strategies and tactics for minimizing risk.

These groups cannot, however, share what they don't know. Effective collaboration requires each participant to contribute to the conversation.

Encouragingly, a majority of our survey respondents reported that they work with other participants in this sector or with relevant agencies to study ways to reduce exposure to cyber attacks.

Does your facility formally collaborate with other port and terminal facilities to study ways to reduce risks to cybersecurity in the ports and terminals industry?

Does your facility collaborate with other organizations and agencies, such as the Information Sharing and Analysis Centers, the Cybersecurity and Infrastructure Security Agency (CISA), and the Cyber Command of the US Coast Guard, to study ways to reduce risks to cybersecurity in the ports and terminals sector?

This last result suggests that even facilities that will not be required under CIRCIA to disclose to CISA cyber incidents and ransom payments will continue to collaborate with the agencies that are seeking to provide cyber protection.

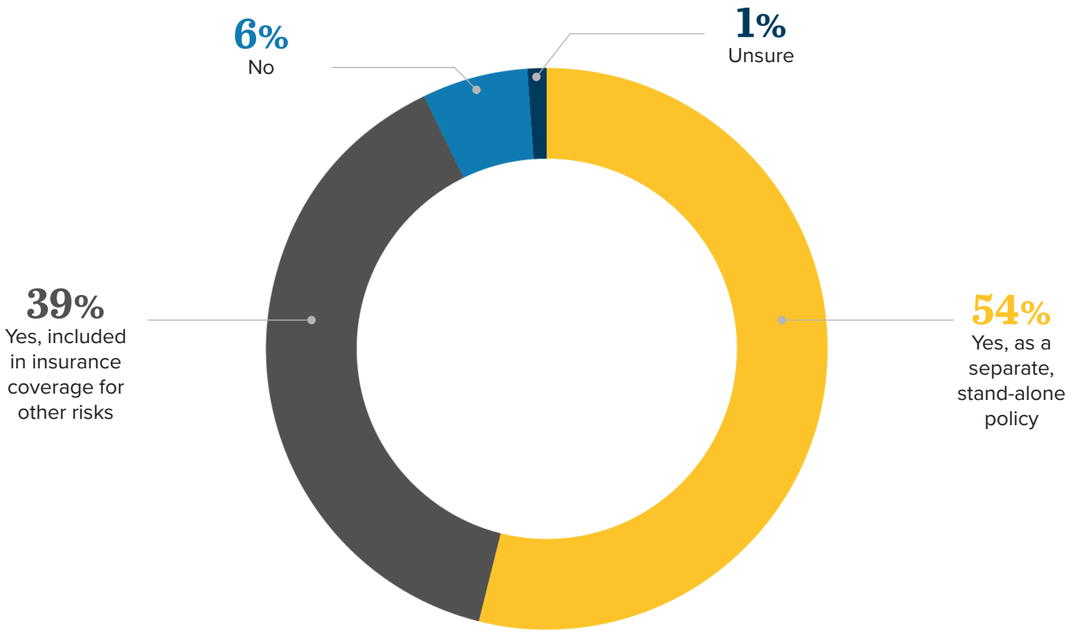
Identify Reputable Cyber-Insurance Providers — and Check Policies Carefully

Securing cyber insurance has long been an important protection for businesses. While insurance cannot prevent a breach from occurring, it can provide a breach victim with much-needed resources to carry it through a cyber attack and help speed its recovery.

The process of applying for cyber insurance can provide an opportunity to conduct what is, in effect, a cybersecurity assessment, as insurers are giving increased scrutiny to applicants' cyber resilience during the underwriting process. Also, despite its importance, cyber insurance can be an imperfect solution if it isn't obtained with care and expert advice.

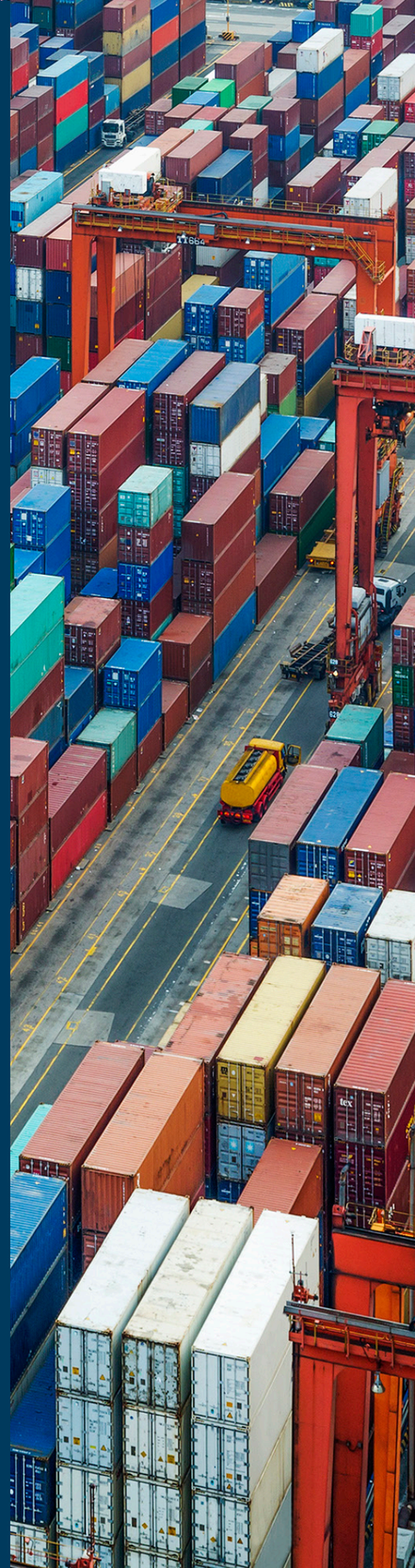
In this challenging environment, nearly all of our survey respondents indicated that they have sought out and obtained some form of cyber insurance.

Does your facility have cyber-risk insurance coverage?



Best Practices

Make employee cybersecurity training a top priority, today. **Help employees understand that they are more than just the organization's first line of defense — they also have a direct, personal stake in preventing data breaches, ransomware attacks, and other cyber threats.** Outside vendors should have a similar commitment to cybersecurity and be willing to update and improve their own preventive and response measures to match their clients' expectations. Identify and collaborate with industry groups that promote and research cybersecurity best practices. Work with legal counsel to identify, procure, and maintain effective cyber insurance, making sure that its coverages meet expectations.



05

Conclusion

Motive, Means, & Opportunity: Accelerating Cyber Resilience

Given the rapid growth of cyber attacks and our reliance on technology, every organization should consider itself a target. This situation is complicated by the fact that we are operating in uncertain times — the disruptive, ripple effects of the COVID-19 pandemic, war in Eastern Europe, and other geopolitical events have further exacerbated the chance of cyber threats.

As key components of the nation's maritime-critical infrastructure, however, the ports and terminals sector faces an elevated level of risk. In this context, achieving and maintaining cyber protection is both necessary and can seem daunting: The technologies can often be complex, threat actors are highly motivated and skilled, and the cost of protecting an organization's data and systems may appear steep.

These challenges require that we all pay greater attention to cyber-based threats. Port authorities and operators, in particular, must make difficult decisions and give priority to cybersecurity readiness while also managing supply chain disruptions, rising costs, labor shortages, and other pressures.

As this survey has demonstrated, port and terminal leaders are committed to protecting this essential element of our nation's transportation infrastructure.

We also hope that this survey shows that those who are responsible for cybersecurity at their facilities need not walk the path of cyber readiness alone. By collaborating with other stakeholders, government agencies, industry groups, and law enforcement, ports and terminals have the means and the opportunity to fortify against and repel cyber threats. Resources and tools abound — many at little to no cost — that can help organizations achieve a higher level of cyber resilience and prepare to respond against cyber attacks.

We encourage readers to use this survey when taking stock of their facilities' cyber readiness and to identify areas where they can make a positive difference in their information- and operational-security technology.

For more information, please contact Andrew R. Lee, Hansford (Ford) P. Wogan, James A. Kearns, Ilsa H. Luther, or your Jones Walker attorney.

Additional Resources

IAPH Cybersecurity Guidelines for Ports and Port Facilities, International Association of Ports and Harbors, July 2, 2021

Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.1), International Maritime Organization, June 14, 2021

Cyber Strategic Outlook, United States Coast Guard, August 2021

"Protecting Critical Infrastructure," Cybersecurity & Infrastructure Security Agency

"Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, April 16, 2018

Cybersecurity Supply Chain Risk Management (C-SCRM), National Institute of Standards and Technology

Cyber Risk Management for Ports: Guidelines for cybersecurity in the maritime sector, European Union Agency for Cybersecurity (ENISA), December 2020

Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities, Navigation and Vessel Inspection Circular No. 01-20,

Footnotes

[1] "Fast Facts: Ports," National Oceanic and Atmospheric Administration, last modified July 29, 2022, https://coast.noaa.gov/states/fast-facts/ports.html.

[2] *Ibid*.

[3] "Critical infrastructure" is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195c(e) (the USA PATRIOT Act). Congress has designated the transportation systems sector (including the maritime mode subsector) as one of 16 critical infrastructure sectors established by federal policy. *See* 42 U.S.C. § 5195c(b)(2).

[4] "Cyber-attacks on Port of Los Angeles have doubled since pandemic," BBC News, July 22, 2022 https://www.bbc.com/news/business-62260272.

[5] *IAPH Cybersecurity Guidelines for Ports and Port Facilities*," Version 1.0, International Association of Ports and Harbors, July 2, 2021, https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf, p. 8.

[6] "Port Facility Cybersecurity Risks," Cybersecurity and Infrastructure Security Agency, December 2020, https://www.cisa.gov/sites/default/files/publications/port-facility-cybersecurity-risks-infographic_508.pdf.

[7] *Data Breach Investigations Report*, Verizon, https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf.

[8] *Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns*, United States Senate Committee on Homeland Security & Governmental Affairs, March 22, 2022, https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report.pdf, p. 2.

[9] "Inside the plan to fix America's never-ending cybersecurity failures," *MIT Technology Review*, March 18, 2022, https://www.technologyreview.com/2022/03/18/1047395/inside-the-plan-to-fix-americas-never-ending-cybersecurity-failures/.

[10] Verizon DBIR, p. 11.

[11] Verizon DBIR, p. 27.

[12] "The State of Ransomware 2022," Sophos, April 27, 2022, https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/. Two-thirds of respondents to one survey reported being ransomware victims in 2021, a doubling of the previous year's tally.

[13] "Hackers Nabbed $1.3 Billion in Ransom Over 2 Years, a New Report Says," Bloomberg.com, February 10, 2022, https://www.bloomberg.com/news/articles/2022-02-10/hackers-nabbed-1-3-billion-in-ransom-over-2-years-report-says.

[14] *Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns*, p. 2.

[15] *Ibid.*, p. 2.

About the Authors

Andrew R. Lee

Andy Lee is head of the firm's privacy and data security team and is a partner with the firm's Litigation and Corporate Compliance practice groups. He advises clients regarding US state and federal privacy and data security requirements, as well as global data protection laws and cybersecurity risks, planning, response, and remediation. Andy is a Certified Information Privacy Professional/United States (CIPP/US), International Association of Privacy Professionals. A trusted resource to the media on the topics of data privacy, cybersecurity preparedness, and data breaches, Andy has been quoted in *Bloomberg*, the *New York Times*, the *Wall Street Journal*, and other publications.

D: 504.582.8664
alee@joneswalker.com

Hansford (Ford) P. Wogan

Ford Wogan is a partner in the Maritime Practice Group. He represents clients on various litigation and commercial matters, including transportation-related contracts and agreements, contractual and indemnity disputes, and property damage and personal injury claims. He has also written and presented on numerous cybersecurity issues as they relate to the maritime industry.

D: 504.582.8164
fwogan@joneswalker.com

James A. Kearns

Jim Kearns is special counsel in the Maritime Practice Group with a focus on maritime transactions. In his more than 30 years of practice, Jim has represented owners, operators, and financial institutions (as both lessors and lenders). He also has experience with port and vessel financing programs administered by the US Maritime Administration, including the Port Infrastructure Development Program, Title XI loan guarantee program, and the America's Marine Highways Program. Jim also has experience with financings program administered by the US Maritime Administration such as the Title XI loan guarantee program, the America's Marine Highways Program, and the Port Infrastructure Development Program.

D: 202.203.1095
jkearns@joneswalker.com

Ilsa H. Luther

Ilsa Luther is an associate in the Maritime Practice Group and a member of the firm's Energy and Natural Resources Industry Team. She assists clients with marine transportation agreements, vessel construction agreements, and vessel purchase agreements, traditional debt financings with ship mortgages and lease financings, Jones Act compliance as well as compliance with a broad set of US Coast Guard (USCG) regulations. Ilsa also focuses on advising oil and gas and offshore wind companies through a wide range of federal and state statutory frameworks.

D: 504.582.8115
iluther@joneswalker.com