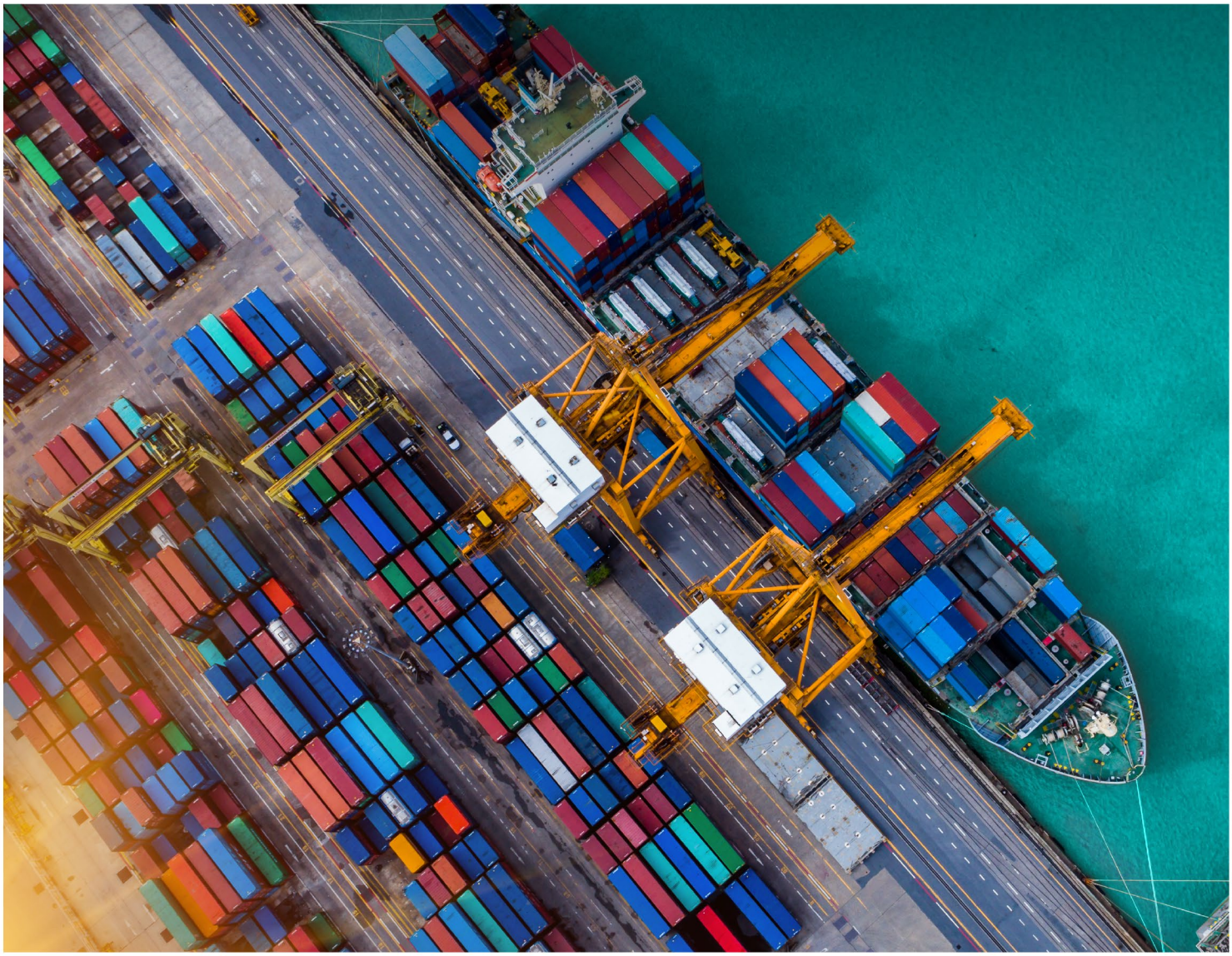
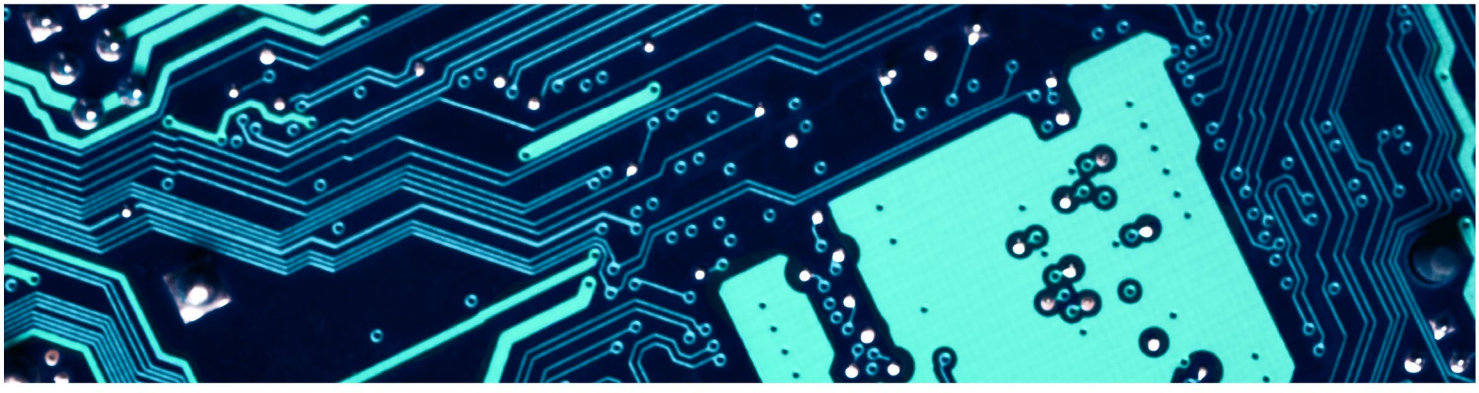
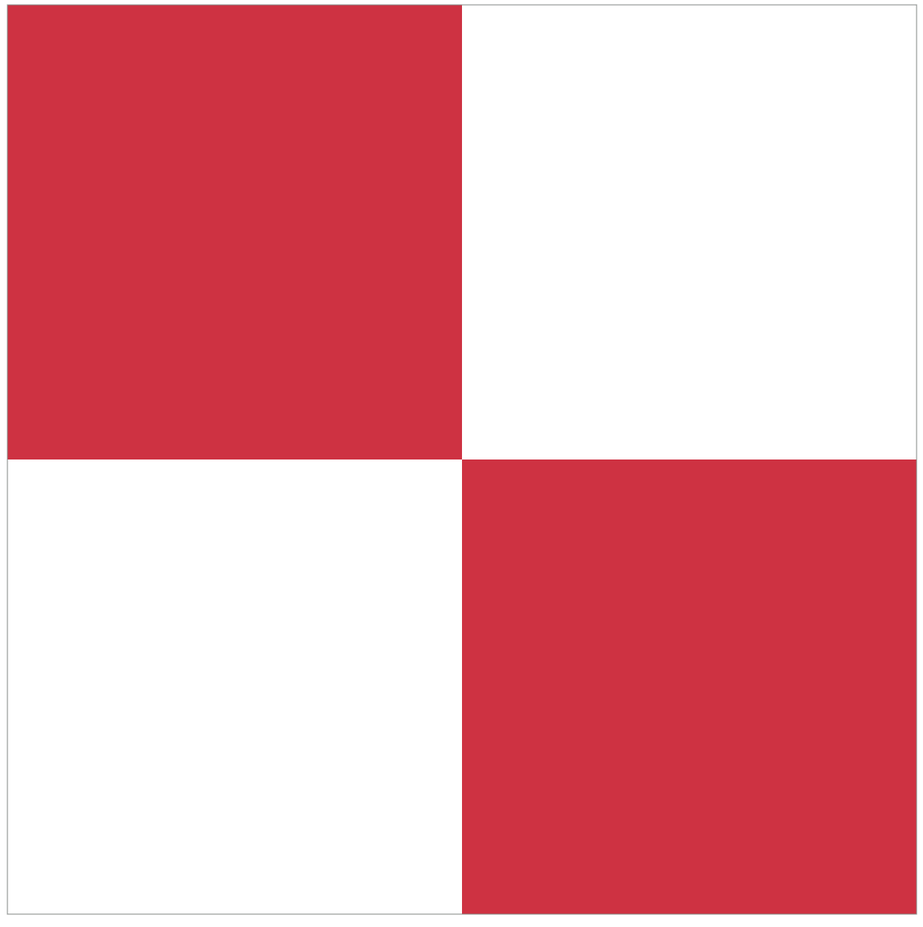
JONES WALKER



JONES WALKER LLP 2018

MARITIME CYBERSECURITY SURVEY





Contents

Introduction

With emerging markets and an ever-present focus on operational efficiency, the maritime industry is undergoing a significant technological shift, relying upon widespread connectivity, better analytics, and more accessible information to guide routing and pricing decisions. However, with increasing reliance on technology come new – and potentially grave – risks, many of which the industry as a whole is unprepared to address.

Welcome to the inaugural **Jones Walker LLP 2018 Maritime Cybersecurity Survey**. In undertaking this survey, our goals were to better understand:

1) the opinions of key executives and managers regarding cyber threats facing the maritime industry today,
2) their perceptions of overall industry cyber preparedness,
3) their views of their own companies' readiness to prevent or respond to potential cyber attacks, and
4) the specific actions or initiatives they have taken — or are planning to take — to address these challenges.

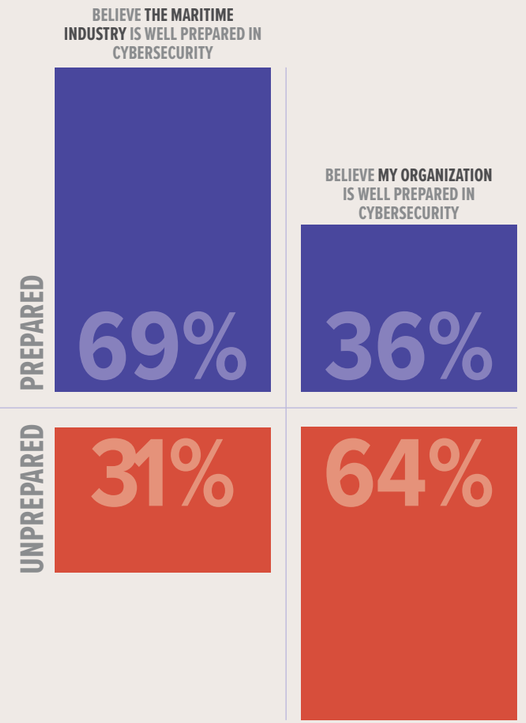
38 percent of maritime industry respondents in the United States reported that cyber attackers targeted their companies in the past year.

This whitepaper summarizes key findings from our survey of 126 senior executives, chief information and technology officers, non-executive security and compliance leaders, and key managers from maritime companies across the United States. Highlights of our survey include the following:

- Nearly two in five maritime companies suffered some form of successful (10 percent) or attempted (28 percent) data breach in the prior year.
- A majority of respondents (69 percent) expressed confidence in the maritime industry's cybersecurity readiness; however, only a minority (36 percent) believed that their own companies were prepared.
- The larger the company, the greater the sense of cyber preparedness. For example:
    - Respondents from small and mid-size companies reported that their organizations were unprepared to prevent a data breach (94 percent and 81 percent, respectively), whereas 100 percent of large companies felt prepared to deal with a data breach.
    - Most (97 percent) large companies carried data breach insurance, but only 8 percent of small companies and 31 percent of mid-size companies had any form of cyber risk insurance policy.
- Only a minority of respondents (34 percent) participate in government and industry initiatives such as the Maritime & Port Security Information Sharing & Analysis Organization (MPS-ISAO) established to educate participants regarding the risk of cyber attacks.

In addition to disclosing our survey results, our report identifies key industry risk areas and offers guidance as to where maritime organizations should consider focusing their efforts.

In the United States maritime industry, 69% of respondents believe the maritime industry is prepared in cybersecurity — but only 36% feel that their company is prepared to prevent a data breach.



The Cybersecurity State of the Maritime Union

Digital innovation and connectivity have transformed the maritime industry, and maritime companies are as technologically advanced as businesses in any other sector. Innovations and automation at ports and on vessels, rigs, and containers are dependent on complex, sophisticated computer networks, cloud services, industrial control systems, global positioning system (GPS) navigation and tracking tools, automatic identification systems (AIS), electronic chart display information systems (ECDIS), and, increasingly, adoption of a range of Internet-of-Things (IoT) devices.

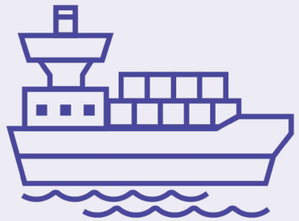
While they certainly increase efficiencies and competitiveness, rapidly evolving technologies also present significant risks. A growing list of cyber-threat incidents confirms that companies in the maritime industry are being targeted for cyber attacks, hacking, ransomware, data theft, and advanced persistent threats (APTs). Identified and suspected perpetrators range from individuals to unfriendly state actors.

Knowledge feeds understanding, and both are necessary for appropriate prevention and response. To help industry stakeholders better understand the current "cybersecurity state of the maritime union," Jones Walker — in conjunction with LUCID, a global data technology and market research company — developed and conducted our survey of cybersecurity opinion, investment, and readiness among industry participants.

Methodology

To ensure that our survey represented key sectors of the maritime industry in the United States, we included the following stakeholder groups:

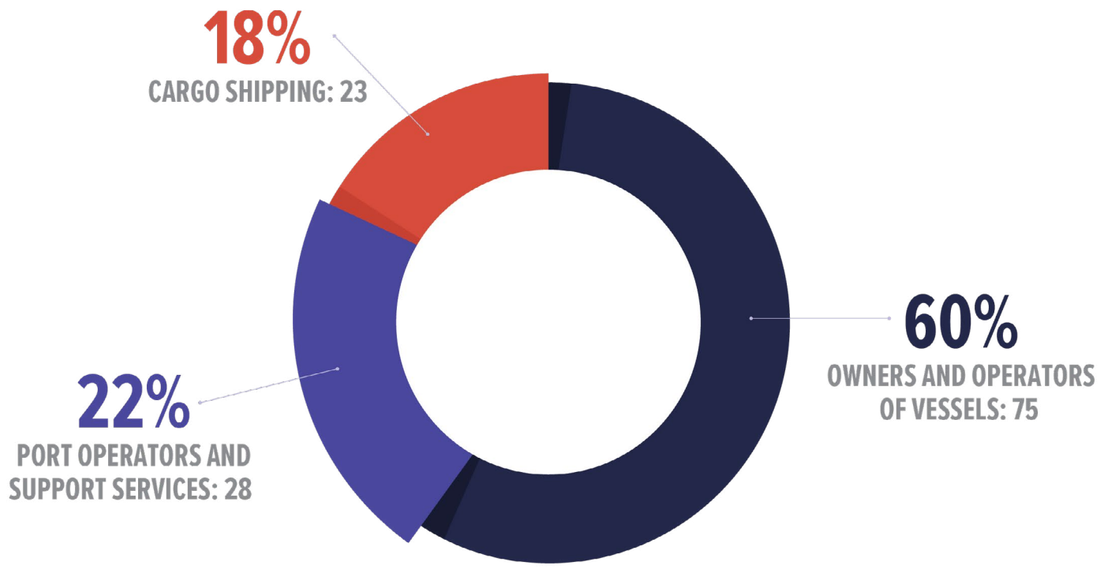
1. Vessel owners and operators of vessels, including tugboats/pushboats; cruises; offshore rigs; fishing and ecology vessels; research vessels; ferries and other passenger vessels; and yachts and pleasure craft



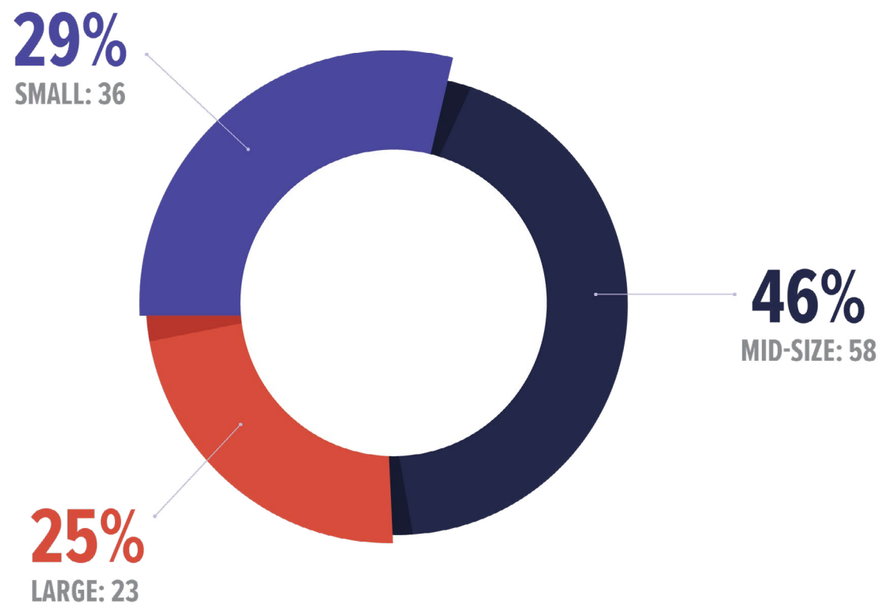
2. Port operators and support services, including terminal operators, shipyards and repair yards

3. Cargo shippers

Survey participants:



We included respondents from companies of varying sizes, categorized as **small (1 to 49 employees)**, **mid-size (50 to 400 employees)**, and **large (more than 400 employees)**.



Key Objectives

We created a list of target participants and their key executives responsible for cybersecurity and asked the executives to complete an online survey that sought input about the following areas:

- **Attitudes and perceptions** toward cyber threats and risks
- **Threat management** and readiness
- Business operations, **security training**, budget/staffing, and audits
- **Strategic planning**
- History of actual and **attempted data breaches**
- Security framework (including **response plans** and policies and technical platforms)
- **On-vessel security**

Preparedness Linked to Size of Company and History of Data Breaches

More than two-thirds of respondents (69 percent) believed that the maritime industry was somewhat or very prepared in the area of cybersecurity. Asked about their own workplaces, however, **64 percent** responded that their companies were at least **somewhat unprepared to prevent a data breach**:

	Overall, how prepared is the maritime industry in cybersecurity?	**Overall, how prepared is your organization to prevent a data breach?**
Prepared (net)	69%	36%
Very prepared	8%	4%
Somewhat prepared	61%	32%
Unprepared (net)	31%	64%
Somewhat unprepared	29%	39%
Completely unprepared	2%	26%

Our results regarding respondent preparedness appear to vary based on two factors:
1) company size
2) recent experience as a cyber attack target.

Overall, how prepared is your organization to prevent a data breach?

Nearly all respondents from **smaller companies reported that they were unprepared to prevent a data breach.** Conversely, all respondents from **large organizations said that they were "somewhat" or "very" prepared to prevent a data breach**:

	Among small companies	**Among mid-size companies**	**Among large companies**
Prepared (net)	6%	19%	100%
Very prepared	0%	0%	16%
Somewhat prepared	6%	19%	84%
Unprepared (net)	94%	81%	0%
Somewhat unprepared	22%	71%	0%
Completely unprepared	72%	10%	0%

Within the past year, to what level has your data been compromised?

Large-company respondents reported a higher occurrence of cyber attacks during the 12-month period preceding our survey — 78 percent reported having been targeted, while 83 percent of small-company respondents said that they had not been targeted:

	Among small companies	**Among mid-size companies**	**Among large companies**
Successful breach	0%	5%	31%
Attempted breach	3%	33%	47%
No breach	83%	60%	22%
Unsure	14%	2%	0%

What was the root cause of the most destructive data breach your company has experienced?

Respondents from larger companies were also more likely to pinpoint external attacks as being behind their most destructive data breaches.

	Among small companies	**Among mid-size companies**	**Among large companies**
Malicious attack (external hack of social engineering)	17%	45%	97%
System malfunction	3%	0%	0%
Internal (staff) theft or breach	11%	16%	0%
Human error (Internal)	11%	3%	0%
Unsure	36%	19%	3%
No response	22%	17%	0%

What is your company's greatest cybersecurity vulnerability concern?

When asked about their companies' greatest cybersecurity exposure, respondents from l**arge companies focused on external threats**. **Mid-size and small companies offered a more mixed assessment of current threats**, and third-party vendors did not register as a primary concern:

	Among small companies	Among mid-size companies	Among large companies
External attack threats, including ransomware and malware	22%	50%	100%
Internal bad actors	6%	9%	0%
Internal negligence	61%	26%	0%
Vulnerability	0%	7%	0%
Unsure	11%	9%	0%

Overall, how prepared is your organization to prevent a data breach?

Companies that had been targeted in a successful (10 percent) or attempted (28 percent) cyber attack during the prior year also **reported being more prepared to prevent another data breach**:

	Among companies that have suffered breach/ attempted breach	Among those that reported no breach
Prepared (net)	73%	14%
Very prepared	10%	0%
Somewhat prepared	63%	14%
Unprepared (net)	27%	86%
Somewhat unprepared	27%	47%
Completely unprepared	0%	39%

Overall, how prepared is your organization to prevent a data breach?

Respondents' assessment of their companies' cyber readiness did not vary based among industry subsectors. **All three stakeholder groups — vessel owners/operators, port operators, and cargo shipping companies — offered a similar range of responses, with shipping companies indicating slightly higher confidence in their preparedness.** Thirty-six percent of small-company cyber breach victims were unsure of the root causes of their data breaches:

	Owners and operators of vessels	Port operators	Cargo shipping companies
Very prepared	3%	4%	9%
Somewhat prepared	28%	29%	48%
Somewhat unprepared	31%	61%	39%
Completely unprepared	39%	7%	4%

Taken together, several **themes** emerged from the responses to our survey:

Despite industry leaders having a strong sense of security about maritime cybersecurity as a whole, they also report that **their own companies are unprepared to defend themselves** against or to respond to potential threats.

Respondents were **concerned about their ability to prevent cyber attacks** and their **effectiveness at managing the long-term implications** of a data breach.

The **larger the company, the more likely the respondent reported having been targeted** by cyber attackers — and the more likely the respondent reported high confidence in being prepared to defend against future attacks.

Smaller companies report fewer data-breach incidents, and those that do are less likely to be aware of the root cause. Smaller companies also acknowledge a significant lack of cyber preparedness.

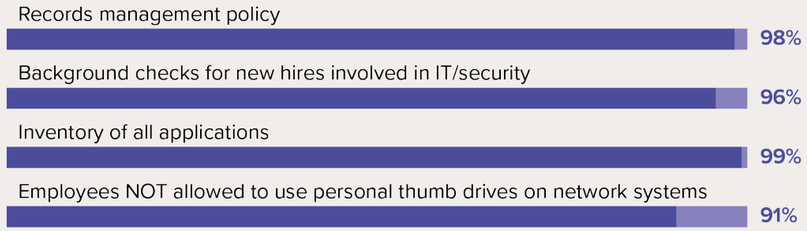
Our survey revealed that the U.S. maritime industry has **a false sense of preparedness**. While 69% of respondents believe that the industry is ready to handle potentially devastating cyber attacks, **only 36% report that their own companies are prepared**.

Cyber Preparedness Initiatives: Tools Are Many, but Users Are Few

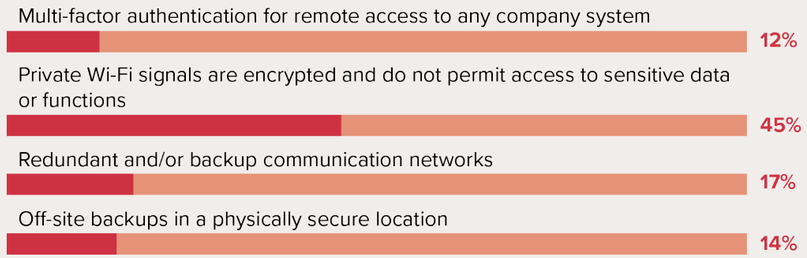
We also explored the types of technologies, procedures, and industry best practices that are being used throughout the maritime industry.

Our respondents indicated that they have largely adopted basic policies and secure-IT solutions, but they also demonstrated that there exists a real need to embrace more robust cybersecurity policies, processes, and tools.

Respondents from small and mid-size companies consistently report that basic policies have been adopted and procedures have been implemented:



However, at companies of all sizes, there are notable gaps in more sophisticated policies:



Small and mid-size companies report regular use of automated intrusion detection and diagnostic tools:

Yet companies of all sizes lack more advanced communications systems:

A **limited number of respondents reported that their companies have documented policies and established business best practices regarding cybersecurity**:

Active at your company...	Yes
Written policy governing use of mobile devices that access company networks	36%
Company's strategic plan addresses cybersecurity	21%

Very few respondents reported that their companies conduct regular testing and auditing of data systems:

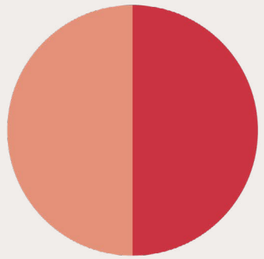
Active at your company...	Yes
Within the past year, has your company undergone a data security systems audit?	20%
Testing that includes mock technology failure exercises	12%
How frequently does your company conduct risk assessments for cybersecurity?	
Every six months	10%
Annually	32%
Less frequently than annually	8%
Never	27% (Note: the majority of small companies never conduct risk assessments)
Unsure	24%

Small companies are also **at risk due to lack of employee training on cybersecurity**:

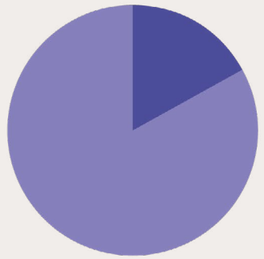
Active at your company...	Among small companies	Among mid-size companies	Among large companies
Cybersecurity training program for employees with systems access	11%	57%	100%
Require cybersecurity training for employees before granting access to company networks	6%	22%	78%
Education and training for information security staff to enhance its cybersecurity skill set	11%	55%	100%

How often are your employees required to participate in cybersecurity training?

When asked more specifically whether employees are required to participate in cybersecurity training, 100% of large companies report having cybersecurity training, but **half of respondents from small companies reported that they never require their employees to participate**:



AMONG SMALL COMPANIES
50%
DO NOT MANDATE EMPLOYEE TRAINING



AMONG MID-SIZE COMPANIES
17%
DO NOT MANDATE EMPLOYEE TRAINING

The gaps noted above are **even greater when looking at vetting, training, and compliance** among third-party vendors:

Active at your company...	Yes
Company vets a third-party provider's cybersecurity fitness as part of its due diligence analysis when acquiring products/services	25%
Provides cyber training to contractors who have access to its networks	4%
Company requires its contractors to include cyber risk management procedures	47%
Company has right to audit its contractors for conformance with cyber procedures	10%

Managing the Aftermath: When "What If?" Becomes "What Now?"

We also asked respondents to look beyond prevention and to assess their readiness to handle the long-term aftermath of such an event. In responding to the question, "How would their companies deal with a cybersecurity incident?" the **majority indicated that they were unprepared to handle the far-reaching business, financial, regulatory, and public-relations consequences of a cyber attack**:

60%
are unprepared to deal with negative public opinion, blog posts, and media reports after a data breach

49%
are unprepared to minimize the loss of customers' and business partners' trust and confidence after a data breach

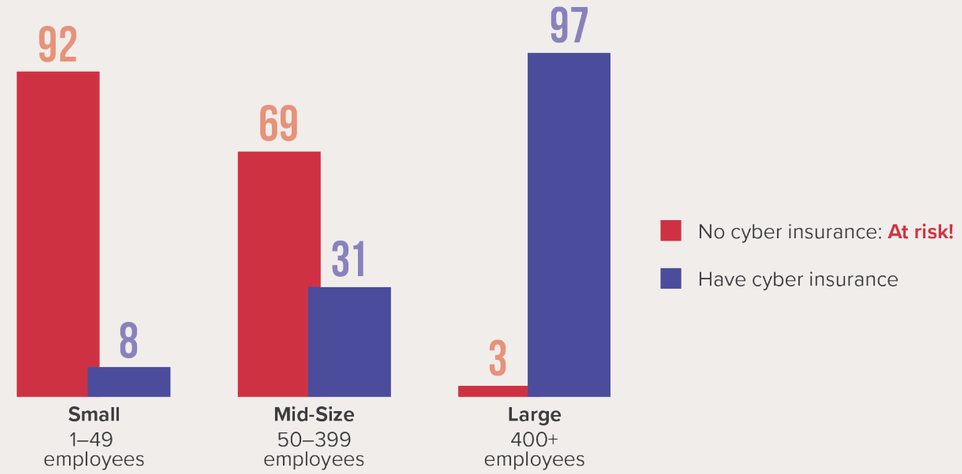
70%
are unprepared to respond to a data breach involving business confidential information and intellectual property

70%
are unprepared to respond to the theft of sensitive and confidential information that requires notification to victims and regulators

Most companies do not have a written plan in place to deal with potential incidents, with the problem most acute among small and mid-size companies.

Active at your company...	Among small companies	Among mid-size companies	Among large companies
Formal data breach incident response plan in place	0%	12%	63%
Written business continuity plan that addresses cyber incidents	0%	7%	69%
Company has a disaster recovery plan	3%	40%	97%

The **majority of small and mid-size companies also lack cyber risk insurance**, exposing them to huge potential costs:



The Future of Maritime Cybersecurity: Investment and Collaboration Are Key

The maritime industry has a well-established and impressive safety record. But when it comes to cyber threats, our study found that — particularly among small and mid-size companies — there is a considerable knowing-doing gap. The industry is not as prepared as it must be to prevent and address damaging cyber attacks.
Industry stakeholders should apply their history of establishing successful safety programs to cyber readiness planning. Company leaders can use this experience to apply a systematic and proactive approach to enhancing their cyber preparedness and data breach responsiveness.

Increase investment in cybersecurity

What percentage of your company's current budget is allocated to cybersecurity?

Currently, **cybersecurity budgets are small**, with the majority of companies spending 1 to 2 percent of overall budget on cybersecurity:

What percentage of your company's current budget is allocated to cybersecurity?	Among small companies	Among mid-size companies	Among large companies
3% to 6%	0%	10%	41%
1% to 2%	69%	83%	59%
0%	28%	3%	0%

How will your company's cybersecurity budget change in the coming year?

C**ybersecurity investment is growing**, particularly among small and mid-size companies, which seem determined to catch up to their large-company counterparts:

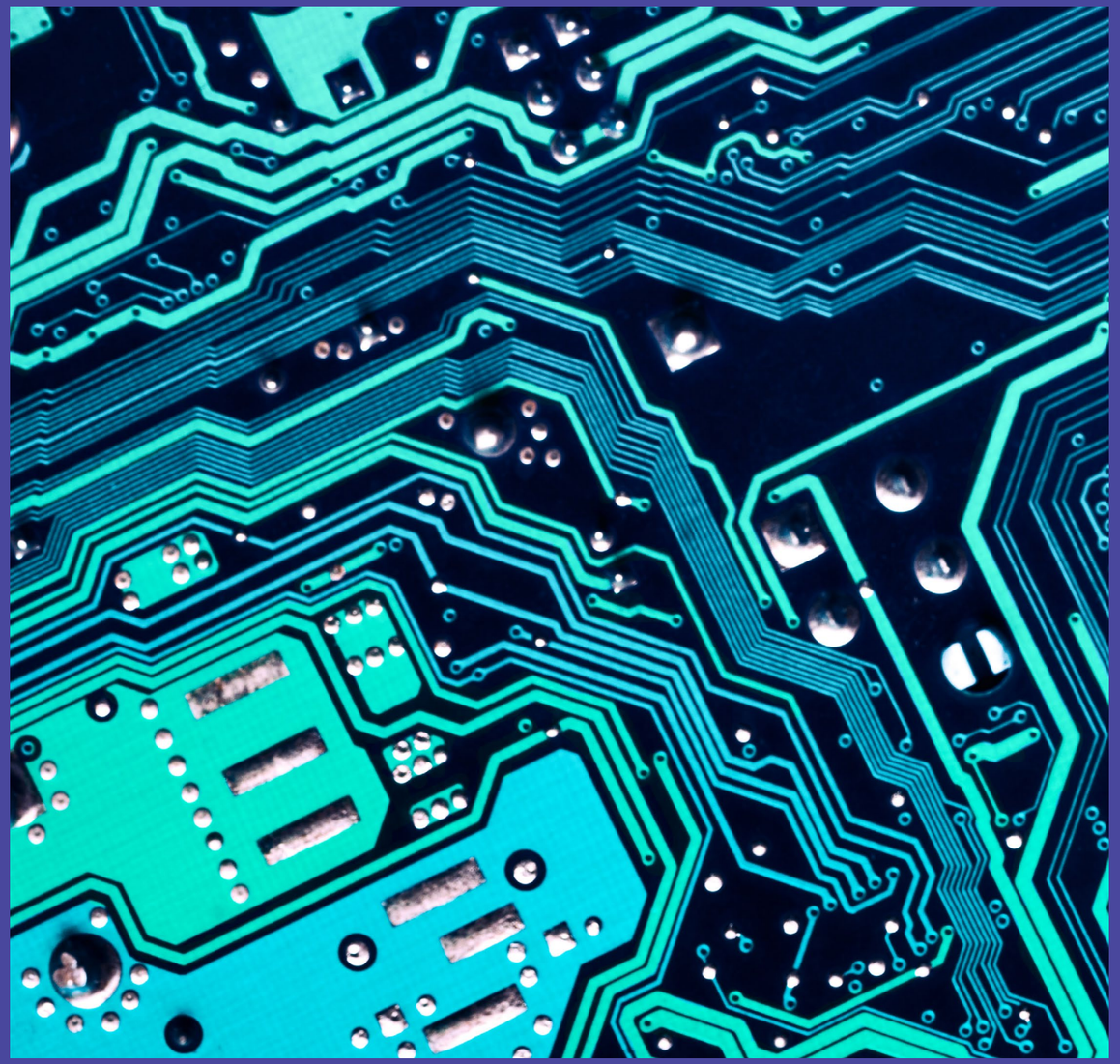
How will your company's cybersecurity budget change in the coming year?	Among small companies	Among mid-size companies	Among large companies
Increase	92%	85%	59%
No change	6%	10%	22%
Decrease	0%	2%	13%
Unsure	3%	3%	6%

Partner with other companies and organizations

Only a **small portion** of respondents **indicated that their companies are actively engaged in cybersecurity collaboration and information-sharing programs**:

	Yes
Does your company formally collaborate with others in the industry, including competitors, to study ways to reduce risks to maritime cybersecurity?	24%
Does your company formally participate in the Maritime & Port Security Information Sharing & Analysis Organization (MPS-ISAO)?	14%
Does your company participate with the Coast Guard in cybersecurity readiness training development and data breach incident response?	34%

Conclusion:
Embrace Cyber Readiness Now by Focusing on Cost-Effective, High-Impact Solutions



What does a *prepared* company look like?

Compared with companies that report deficiencies in key areas outlined in the survey's questions, prepared companies share common characteristics.

- Include **cybersecurity** as part of their **strategic plans**
- Document **cybersecurity policies and procedures**
- Provide **more training** on cybersecurity procedures
- Develop and maintain **disaster recovery, business continuity**, and **other contingency plans**
- Appoint empowered **information security and/or compliance officers**, with well-defined roles and responsibilities
- Participate in **threat assessments** and share information
- Obtain or re-evaluate **cyber risk insurance**

As noted at the beginning of our report, most respondents to our survey believe that their companies are not ready to face cyber threats and challenges, while they also believe that the maritime industry, as a whole, is prepared. We encourage you to use Jones Walker's survey as a benchmark to help your company assess and improve its cyber readiness. It is our hope that the information we have provided can help shift that balance in a positive direction: **as each stakeholder takes steps to embrace cybersecurity, so too will the entire industry**.

About the Authors

Andrew "Andy" R. Lee is a partner with Jones Walker LLP in New Orleans. He co-chairs the firm's Privacy and Data Security Group and regularly advises clients regarding cybersecurity, records retention policies, electronic discovery, and related issues. He assists in developing, implementing, and enforcing policies and procedures to ensure defensible, repeatable, and efficient processes and programs related to the security of sensitive corporate data, recovery after cyber intrusions, litigation hold procedures, and electronic discovery of data in legal proceedings and internal investigations. He maintains an active national trial and appellate practice and has been annually recognized by *Super Lawyers*, *The Best Lawyers in America*, and *New Orleans CityBusiness* for his trial work and leadership in the New Orleans legal community.

Hansford "Ford" P. Wogan is an associate in the Maritime Practice Group, where he focuses on maritime and oilfield litigation. Ford represents clients in a broad range of disputes, with a concentration on maritime personal injury/death and oilfield defense, including claims under General Maritime Law, the Jones Act, the Longshore and Harbor Workers' Compensation Act, and the Outer Continental Shelf Lands Act. Ford also handles a wide range of issues and claims involving property damage, marine insurance coverage, limitation of liability, oil pollution response and liability, environmental damage, vessel collisions and allisions, vessel seizures, and cargo and contract disputes. Ford has extensive experience litigating various matters in state and federal courts, including multiple trials at the federal level.

JONES WALKER

www.joneswalker.com