JOC.com

Cyber-attack veterans, larger maritime companies best prepared

Eric Johnson, Senior Technology Editor | Nov 13, 2018

The Jones Walker Maritime Cybersecurity Survey found that nearly three-quarters of companies that have suffered a breach or attempted breach said they are prepared for another such attack,while only 14 percent of companies yet to see such a breach said they are prepared. Photo credit:Shutterstock.com.

Larger US maritime companies and those hit by a cyber attack are more prepared than their smaller and untouched counterparts, respectively, according to a recent survey conducted by the law firm Jones Walker.

Released in late October, the Jones Walker Maritime Cybersecurity Survey found that nearly three-quarters of companies that have suffered a breach or attempted breach said they are prepared for another such attack, while only 14 percent of companies yet to see such a breach said they are prepared.

Meanwhile, every large company (those with 400 or more employees) surveyed said they are prepared for an attack. In comparison, 81 percent of midsized companies (50 to 400 employees) and 94 percent of small companies (fewer than 50 employees) said they are unprepared.

The study was based on responses from 126 respondents, surveyed in June and July. Twenty-three of the respondents were cargo owners (including containerized, bulk, and breakbulk shippers), while 28 were port operators or service providers and 75 were vessel owners or operators.

Overall, nearly 80 percent of large maritime industry companies and 38 percent of all industry respondents reported that cyber attackers targeted their companies within the past year, with 10 percent reporting that the data breach was successful and 28 percent reporting a thwarted attempt.

“Small companies are pretty much saying we haven’t been breached,” said Andy Lee, a partner with Jones Walker in New Orleans and co-author of the report, told JOC.com. Lee co-chairs the firm’s privacy and data security group.
“There’s a correlation between being aware of a breach and being unprepared for a breach. And they’re also a group that puts no budget toward it. The correlation with respondents who say there was an attempted breach is they now feel prepared. The ones who have been a victim, they now have a higher confidence level they won’t be again.”

However, Lee said further data in the study point to companies who say they're ready not being as potentially prepared as they may believe.

"When you look into their perceived impacts of the outcome of a breach, that's transparency to real readiness," he said. "It's easy to say 'yeah, I feel ready.' But if you ask about actual impact..."

Only 20 percent of firms had security audit in past year

To wit, only 20 percent of companies surveyed said they have conducted a data systems security audit over the past year, and only 42 percent said they conduct cybersecurity risk assessment annually or more frequently.

The container shipping industry has seen two high-profile attacks afflict major ocean carriers in the last 15 months. In June 2017, Maersk was hit by a virus that virtually shut down its computer networks globally, while in July 2018, Cosco Shipping dealt with an attack on its US systems.

The two incidents showed the wide-ranging outcomes of such breaches. Whereas it took weeks for Maersk to dig out from the attack on its systems, Cosco recovered relatively quickly. The divergence in outcomes can be attributed to the type of attack, how well prepared a company is to fend off such an attack, and how effective recovery plans are once an attack occurs.

Jones Walker also assessed the industry's readiness to deal with the aftermath of a breach and found most respondents lacking — even those who said they were prepared to deal with the breach. Sixty percent said they were unprepared to deal with negative public opinion, blog posts, and media reports; 49 percent were unprepared to minimize the loss of customers' and business partners' trust and confidence; 70 percent were unprepared to respond to the loss of confidential business information and intellectual property (IP); and 70 percent were unprepared to respond to the theft of sensitive and confidential information that requires notification to victims and regulators.

"They're saying 'we're not ready to answer regulators or victims, or deal with the loss of confidential information or IP," Lee said. "Those are pretty basic things to be ready for."

Lee said there's an incentive for companies to get better prepared for an attack and the aftermath of a successful attack: better underwriting or insurance premium discounts.

"If they have limited budget, resources could be dedicated to prevention in a fairly mundane way," Lee said, when asked whether companies should prioritize investment in cybersecurity prevention or recovery.

That could include keeping better track of the system logs (the data showing who is coming into system, how long they are staying there, and what they are doing). "There's a lot of data there that would give them an understanding of attack surfaces, points of vulnerabilities. They can sit down with their IT department and decide, before we go on big cyber investment, let's figure out where [we] would be attacked."

Inventory of systems

Companies should look at taking inventory of their systems. "Not a lot of companies do that," he said. "What's the aging on the system, is it patched? Is it patchable? Are you using WiFi-controlled thermostats, and [is] the thermostat password 'password'? That's a vulnerability, Internet of Things [IoT] types of security. Those are vulnerable because nobody has designed those with cybersecurity in mind."

Lee also advocated for developing a written policy for how a company would respond to an attack. "The process of thinking about your organization and how it fits within a policy and cybersecurity response plan [can] put together the team that does the responding. It would be even better if you have a team in place that has practiced a response."

In terms of budget, the Jones Walker study found 41 percent of large companies dedicate 3 to 6 percent of their IT budget toward cybersecurity, compared with only 10 percent of midsize companies. Sixty-nine percent of small companies said their cybersecurity budget is 1 to 2 percent and 28 percent dedicated no resources to it.

But 92 percent of small companies plan to increase their cybersecurity budget in the coming year, compared with 85 percent of midsize companies and 59 percent of large companies.

Another interesting wrinkle in the study: 69 percent of respondents said the maritime industry as a whole was prepared for a cyber attack, but only 34 percent said their individual company was prepared. "To me, the way they characterize their own companies is more accurate," Lee said.

Contact Eric Johnson at eric.johnson@ihsmarkit.com and follow him on Twitter: @LogTechEric.

To read the white paper: click here.