Most companies decline to talk about cyber penetrations, but sharing the nature of such attacks can benefit the entire industry.

How to Play Smart Defense

Brunswick Corp.'s $85 million loss has cybersecurity experts urging all companies to fortify vulnerabilities

Questions continue to swirl about the nature of the cyberattack that shut down some operations at Brunswick Corp. for as long as nine days this past summer. Officials at the company — whose brands include Mercury, Boston Whaler and Sea Ray — have said only that the "IT security incident" disrupted its propulsion/parts and accessories segments in particular, and had a major impact on its Navico Group electronics division.

There is no doubt, though, that the Brunswick episode was significant. CEO David Foulkes told investors that the incident cost Brunswick as much as $85 million, an amount that dwarfs the $4.45 million that IBM says is now the average cost of a data breach worldwide.

The Brunswick incident was also at least the second cyberattack in as many years on a major marine industry company. In summer 2022, Bombardier Recreational Products reportedly had to shut down production at four manufacturing sites worldwide for about a week. That incident was described in various reports as a ransomware attack, which happens when hackers deny a company access to its own data while demanding a ransom. With BRP, cybercriminals reportedly gained access through a supply-chain attack, which means accessing a company's systems through one of its trusted third-party vendors.

Brunswick and BRP both declined requests to speak with [*magazine name deleted]* about what types of vulnerabilities were exploited within their companies. Brunswick vice president of communications Lee Gordon said, "We made a few comments during our earnings call on July 27, but that's the only time we are going to do it." BRP manager of global public relations Mélanie Montplaisir said that "for confidentiality reasons, we do not grant interviews on this topic."

Most companies routinely decline to comment about such incidents, sometimes citing ongoing internal or law-enforcement investigations, says Gary Kessler, author of *Maritime Security: A Guide for Leaders and Managers.* But, he adds, in the big picture of cybercrime and the recreational marine industry as a whole, that type of corporate secrecy is unhelpful.

"One of the things we're lacking in the industry is really good information-sharing about vulnerabilities, and rippling it down to everybody in the industry," Kessler says.

Understanding the Problem

Kessler has an Ormond Beach, Fla.-based consulting and training business, and has worked on cyber issues with organizations ranging from the Coast Guard to the National Marine Electronics Association. He urges small-business owners who are trying to wrap their brains around cybersecurity to first learn the difference between threats and vulnerabilities.

Threats can be anything and are everywhere: hackers pulling a widespread scam from a foreign country, opportunistic information thieves, ransomware crooks specifically targeting a company for certain types of data. *Cybercrime Magazine* says threats are so widespread that this year's worldwide cybercrime damages are likely to total $8 trillion, an amount that, if it represented a national economy, would be second in size only to the United States and China. The World Economic Forum now lists cybercrime as the planet's eighth-highest risk, just below failure to adapt to climate change.

Trying to understand and address all the threats is the wrong way for company leaders to think about cybersecurity, Kessler says. Instead, executives should think about their own company's vulnerabilities, which are specific, internal and controllable.

A vulnerability can be as simple as the lack of a fence around a warehouse filled with products. It can be computer software that employees are using without an update that the company knows is needed but has failed to install. A vulnerability is a physical or digital point of access that can be located and then made less accessible to criminals.

"It's sort of nice to know what the current threat landscape looks like, but I need to know about the vulnerabilities in the systems that I'm using," Kessler says.

The lack of information about which vulnerabilities cybercriminals exploited at Brunswick and BRP is frustrating, Kessler adds, because it leaves other company owners unable to fortify their own defenses. This is especially true, he says, in cases where the smallest marine companies are using the same products and systems as bigger organizations, right up to the biggest cargo and cruise-ship companies.

"The same vulnerability that I might find

PHOTO: WHO IS DANNY - STOCK.ADOBE.COM

on *Odyssey of the Seas* might also exist on a yacht. In many cases, we're using similar equipment," Kessler says. "Navico is being used by the military, law enforcement and my fishing buddy down the street. All of them need to know if there's a vulnerability in a Navico system."

Cybersecurity Tips

Mark Oslund, director of standards for the National Marine Electronics Association, shares Kessler's views about the threat landscape in general. "Think of it as a whole subculture that lives beneath the city," he says. "Eventually, somebody comes up out of it and grabs you."

For that reason, the NMEA's OneNet standard for data interfacing and networking has a feature that's intended to address known vulnerabilities. This is different from previous standards, such as NMEA 0183 and NMEA 2000. "It's our best effort," Oslund says.

On a connected boat, all of the engines, displays — pretty much any device or piece of equipment that needs to communicate — plugs into a CAN bus network. The previous NMEA 2000 standard for that network let people trace devices that acted up and then unplug them. The newer OneNet standard employs the same principle, Oslund says, but in a higher-bandwidth way that allows for more data to be transmitted and received.

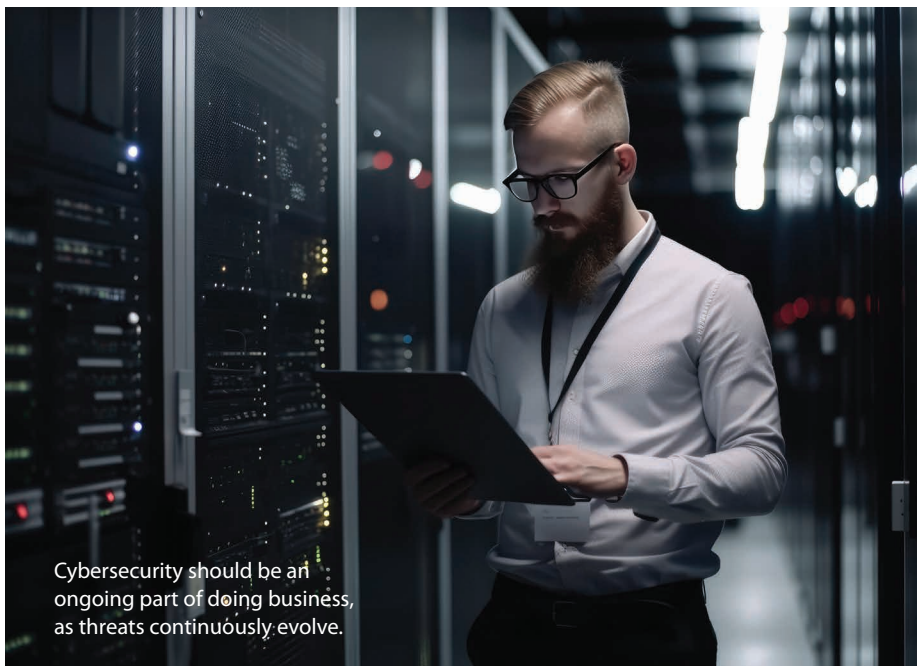
And unlike its predecessor, OneNet can tell which devices plugging into the network are trusted according to OneNet protocols. Unrecognized devices that anybody tries to plug in can't get access, he says.

"That's a form of mitigating the risk of somebody plugging in a bad-actor device, something that's going to take all the data off your network and send it to some basement in some foreign country," Oslund says.

In other words, it's a way to fortify against a known vulnerability. Kessler says all kinds of marine business owners — be they boatbuilders, dealers, marketers or anything else — can do many things to protect against other known vulnerabilities, for boats and products and for the companies in general.

First, he says, companies must ensure that all systems are up to date. If any software requires an update, install it. "When the patches come out, it's very, very important to apply those patches," he says. "It means somebody is fixing something that they found."

Another way to protect against known vulnerabilities is to have everyone in the company use strong passwords, and to have everyone use individual passwords for access to a system. "If you have a generic password and something happens, you don't actually know who's logged on," he says. "And the passwords should not be hanging on a sticky note off the monitor. We need good passwords. Don't use the same password on every system."

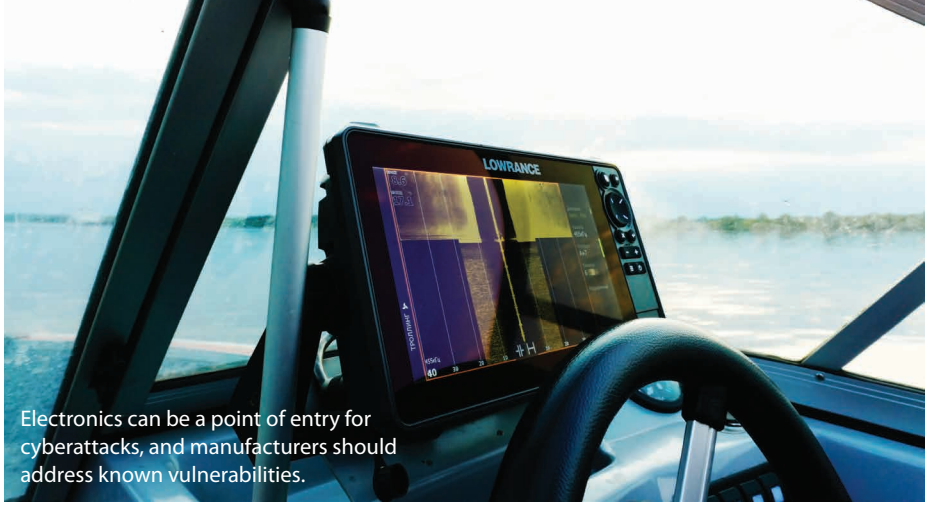


Cybersecurity should be an ongoing part of doing business, as threats continuously evolve.

PHOTO: NATTAWAT - STOCK.ADOBE.COM

Companies also need to educate their staffs about social engineering, which is when bad actors deceive and manipulate people into divulging confidential information. This can happen via email, phone, text — pretty much with any form of communication.

"When we get an email from somebody, and they say, 'Hey, listen, can you pay this $8,000 invoice, but don't use my normal bank account, use my alternate bank account, and by the way, I'm using my



Electronics can be a point of entry for cyberattacks, and manufacturers should address known vulnerabilities.

personal email today because corporate email is down,' it may sound reasonable," Kessler says. "But you should pick up the phone before you send any money."

Oslund says that where boatbuilders and manufacturers of parts and accessories are concerned, a good step is to use only OneNet-certified products. Beyond that, boats and products can be built in ways that strategically block bad actors from hopping on board a vessel and accessing systems that contain sensitive data. Make it difficult for a random person on a boat to, say, plug a flash drive into a device's USB port. "You can put systems behind a locked cabinet," Oslund says. "Limit the physical access to plug something in."

Oslund also says manufacturers and service providers can think about how they're getting data off boats and back to shore for remote-monitoring systems. Questions to consider include how valuable the information in transit might be to a hacker, and whether it's wise to transmit that information at all. There's a big difference, he says, between bank account numbers and data about how much fuel is on board.

Yet another step manufacturers can take, Oslund says, is to seriously vet anyone who is hired to work on connected products and systems. He directs people to the NMEA website, which has a searchable database of certified installers. "That subcontractor is just as important as the guy who's doing the gelcoat," Oslund says. "If you're hiring for marine electronics to ship data off the boat, you need to be able to trust the person's advice."

Kessler says trusted third-party advice and services are also helpful with malware software, e-commerce platforms and anything else where cybersecurity expertise is required. One exercise that he recommends is having a cybersecurity expert make sure all routers and other connections to the internet are secure, especially with so many employees now working remotely.

"Like everybody else in the world, I have a home office with internet in the house," Kessler says. "It would be worthwhile to somebody running a business to make sure somebody who really knows what they're doing takes a look at their router, their firewall connection. Do you need to be paying for 24/7/365 network monitoring? Maybe, maybe not, but you should have somebody looking at your setup and periodically reviewing it."

Overall, Kessler says, a key task for executives is to think routinely about vulnerabilities and how to fortify them. Discuss these vulnerabilities not just within a company's four walls, but also with any vendors the company uses. Make sure the vendors are taking cybersecurity seriously, too.

And, he adds, don't think about cybersecurity in terms of ROI. "There is no return on investment. You can't figure out your return on events that didn't happen," Kessler says. "I tell people to think about the return on negligence. Brunswick lost $85 million. Are they going to go out of business? No. But how much money can you afford to lose and stay in business?"

The goal, he says, should be to make a company and its products a less-attractive target. Fortify as many vulnerabilities as possible, even as the overall threat landscape continually changes and grows.

"You're not going to be able to fix all the problems, and even if you do fix them all today, by tomorrow, you won't be 100% because the landscape is always changing," Kessler says. "This is not something you do once and walk away from it. You want to pay attention to it." ■

PHOTOS: DMITRY - STOCK.ADOBE.COM