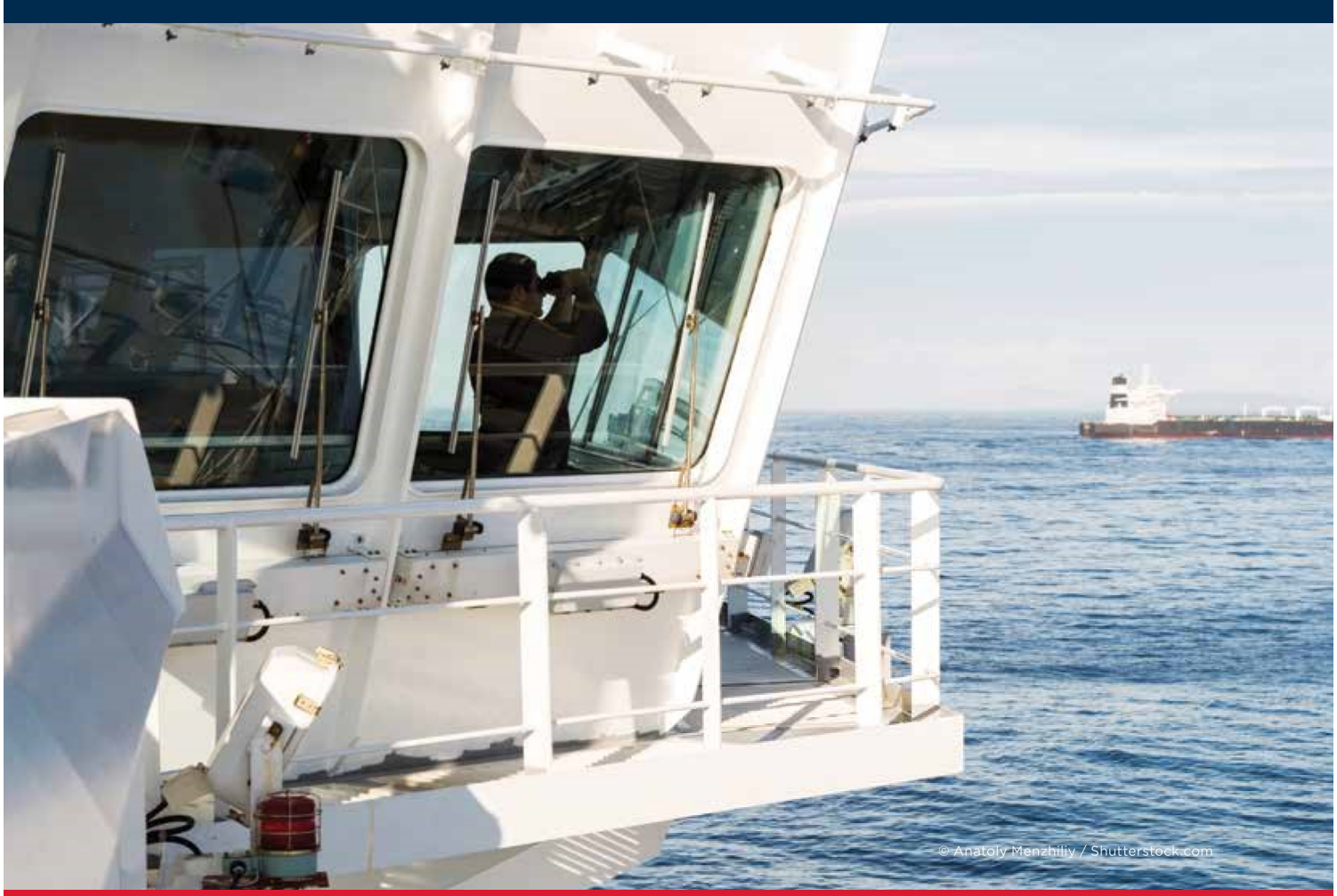


GIRDING FOR BATTLE IN THE CYBER ARENA

Early last year, the data breach investigation team at Internet service provider Verizon reported that one of its clients, a major Middle Eastern shipping company, experienced an unusual piracy incident involving the theft of millions of dollars in jewelry, diamonds and other valuables from one of its containerships. The odd thing about the theft was that the pirates were on and off the vessel in only 90 minutes, during which time they precisely targeted the few containers – out of the thousands onboard – that held the valuables. The investigators looked for company insiders who might have provided confidential shipping information to the invaders, but found instead that the data breach had an even more disquieting source: the pirates had collaborated with cyber criminals to steal data from the head office that left the ship open to a seaborne attack. Shipping's oldest enemy and its newest foe had finally joined forces.

The cyber cadre exploited a weakness in the shipping company's computer architecture to hack its content management system (CMS), the place where important documents such as ship manifests and bills of lading are stored. Using malicious software known as a 'web shell', they were able to find and download not only shipment information, but also the company's GPS vessel tracking data. They passed this along to the pirates, who then knew which ships held something they wanted, where on the ships the booty would be, and when the ship would be in a vulnerable location. Further, in resolving the issue, investigators discovered that the CMS had been compromised months earlier, and that several prior instances of apparently 'normal' piracy on the company's ships could be linked to downloaded documents.

That level of infiltration recalls a major cybercrime in the Port of Antwerp that authorities exposed in 2013. In that case, a drug-smuggling ring hacked into computer

systems controlling container movement and location, stealing data that enabled them to lose containers and send trucks to quietly pick up the boxes in which their confederates had hidden the contraband. The hack started with deceptive emails to port staff containing malicious software, which enabled the thieves to remotely access sensitive logistics data. Later, they broke into company offices and installed small data interception devices, known as key loggers, disguised as computer cabling; these record all keystrokes and, thus, all passwords and system commands. The criminals were inside the port's computer network for two years before detection.

"INTERVIEWS OF CREWS, PORT CAPTAINS, PORT ENGINEERS AND SENIOR MANAGEMENT INDICATED VERY LIMITED AWARENESS AS TO THE IMPORTANCE OR PRIORITIZATION OF CYBER AWARENESS, SECURITY, SAFETY, AND SECURITY PRACTICES."

Since then, the International Maritime Bureau has warned that shipping could become "the next playground for hackers," and at least one insurer reported discovering that what appeared to be petty-theft break-ins at shipping company offices were actually cyber espionage operations in which spyware and devices were installed on office computers.

Besides such targeted cyberattacks, there is also a growing number of reported incidents caused by normal vandalism-oriented malware floating around the Internet, like the ship that was delayed in port two days due to a virus infection in its electronic chart display and information system (ECDIS). The infection was so difficult to remove that the operator had to bring paper charts onboard in order for the vessel to get underway.

Taken together, incident reports like these indicate that cybersecurity, like safety at sea itself, involves both individual and group responsibilities. While shipboard and shoreside staff must be "cyber educated and aware" and maintain good digital safety practices, the company itself must enshrine cybersecurity in its processes and procedures to prevent malicious attacks and accidental infection.

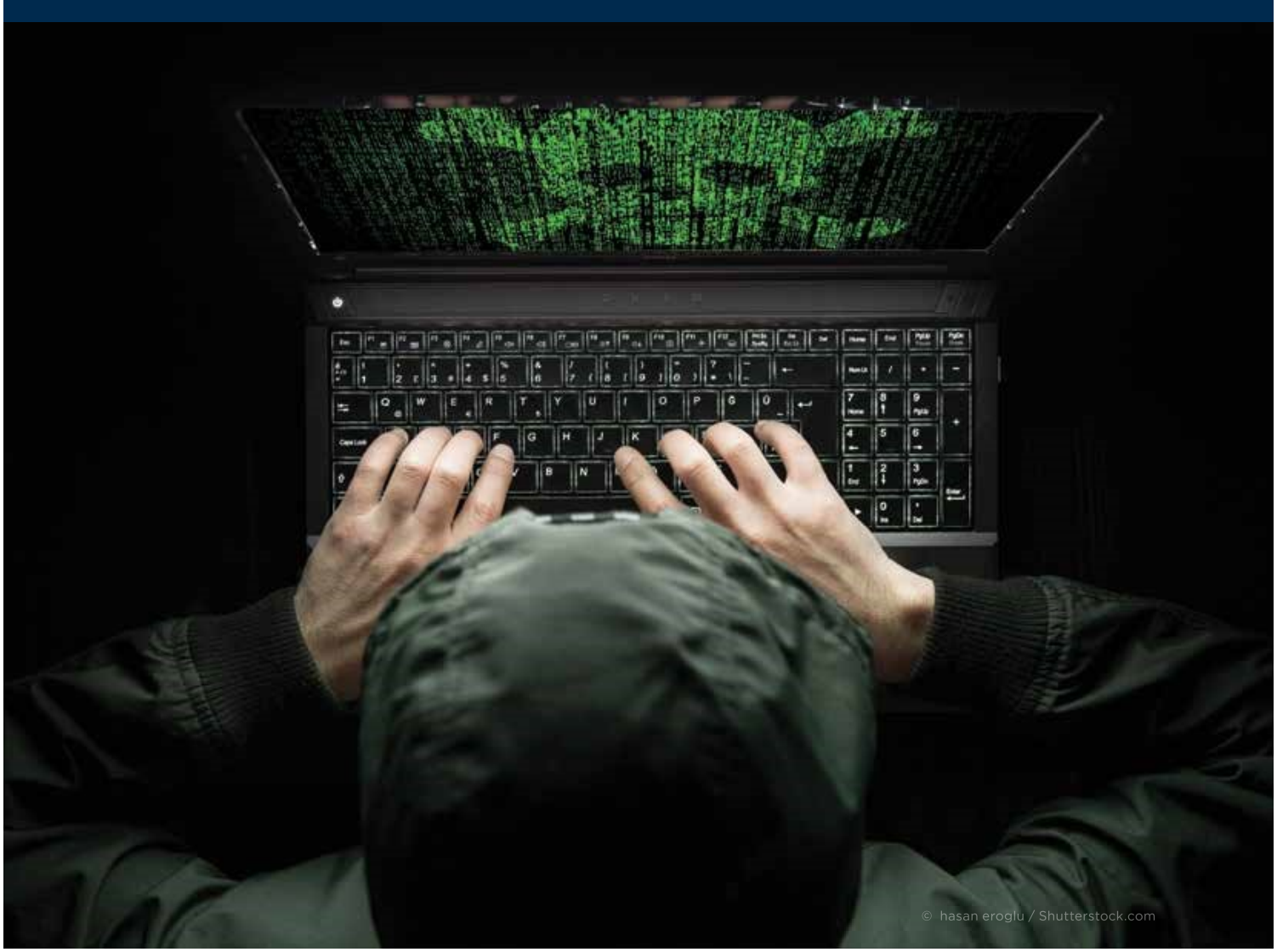
Captain Alexander Soukhanov, Vice President, USMRC

Such is among the conclusions of the Maritime Cyber Assurance research program conducted by the United States Maritime Resource Center (USMRC), a non-profit research group, and its partner, cybersecurity firm Cybrex. The ongoing effort went operational in May 2015 after partnering with the Liberian Ship Registry and shipowner group BIMCO, and has since expanded to add marine terminals to its assessments.

"Interviews of crews, port captains, port engineers and senior management indicated very limited awareness as to the importance or prioritization of cyber awareness, security, safety and security practices," says Captain Alexander Soukhanov, vice president, USMRC. "In many cases, what we discovered was determined to present a very high severity of risk."

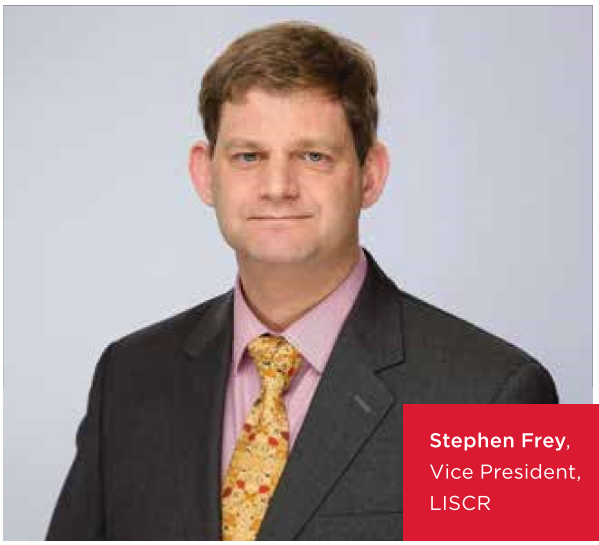
These risks raise "significant potential for disruption," he says, such as malicious takeover of engineering controls and corruption of electronic navigation charts. Some of the maritime industry's chief cyber vulnerabilities, as exposed during the research, were:

- Little to no evidence of cybersecurity policy
- Little to no cyber awareness among the crew
- Unsupported/obsolete operating systems, even in some newbuilds
- Many unpatched systems
- Many systems without anti-virus software or updated anti-virus definitions
- Unauthenticated or bypassed workstation or system access



- Dangerous modifications by crew (to software or systems) and evidence of ad-hoc networking by the crew
- Small office/home office IT infrastructure, which is inappropriate for an industrial environment
- Removable media access on shipboard PCs
- No cyber auditing occurring as a shipboard and ship management safety procedure
- Internet-connected Industrial Control Systems
- Critical systems connected to the Internet without protections or segregation
- Many systems Ethernet-connected and Internet-ready, but not protected.

One of the study's main sponsors was the Liberian Ship and Corporate Registry (LISCR), which, among other duties, identified ship operators and vessels for the assessments. During the invitation phase of the project, the organization discovered one surprising result even before any data was collected.



Stephen Frey, Vice President, LISCR

"In some cases, clients told us they had experienced cybersecurity problems already," says Stephen Frey, vice president, LISCR. Most of those incidents were what he refers to as "small issues" generated by the same "normal" menaces that computer users around

the world face every day: a computer stops working due to accidentally downloaded malware, for example, or a system develops problems because an infected device was plugged into a USB port.

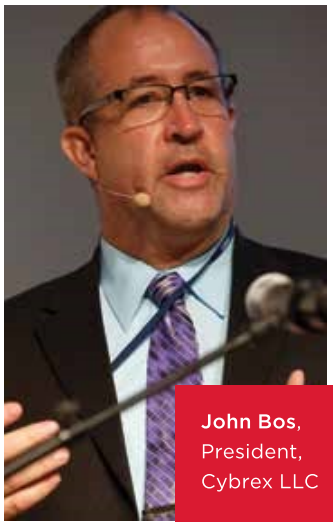
Millions of people in all walks of life engage in risky cyber behavior, such as paying bills online via public Wi-Fi, accessing secure sites on hotel desktops, opening mysterious links in e-mails and plugging thumb drives of unknown origin into their personal computers – and the potential for an unwanted cyber event increases daily. You don't even have to be online to be at risk; researchers from the Georgia Institute of Technology once demonstrated the relative ease with which a hotel iPhone charging station could be rigged to install malware onto smart devices. Threats can come at a ship from many angles.

Average risks plus special vulnerabilities mean that cybersecurity requires an expanded level of vigilance from the shipping community. Even if the problems are only minor inconveniences, malicious programs exist in such great numbers and diversity that, taken together, they represent a serious threat of disruption to vessel operations.

"These small issues can be just as damaging as a major attack; plus, they are random problems. For every malicious act, you can expect to see hundreds of random problems," Frey says, adding that a virus can board a ship as easily as it enters a home computer. "All USB ports look alike," he explains. "Chances are good that somebody on the bridge with a tablet or smart phone to charge will plug it into a USB port without looking to see if that port is part of the ECDIS or the navigation system – and without any way of knowing if the device is leaving something behind. Protection of systems onboard is pretty low right now."

According to the USMRC, the most likely infections onboard a vessel would be light to moderately disruptive events that originate in such incidental sources. Deliberate attacks or exploitation by an organized adversary appear to be less likely, simply because there is currently little evidence to suggest otherwise.

"We know of incidents where cyber sources were attributed to significant operational disruptions that delayed vessels and required lengthy restoration processes, but the origin or nature of the adversary was not determined," says John Bos, president of Cybrex LLC. "While the nature of the potential adversary is a substantial part of the risk equation, common vulnerabilities across industry sectors exist in such quantity that high adversary skills are often not necessary to achieve the desired effects. Cybersecurity and preparedness across the maritime industry is inconsistent and generally low, both afloat and ashore," he adds.



John Bos, President, Cybrex LLC

"With cyber issues, you have to continuously protect every vulnerability you discover," notes Frey. "Malicious programs can float around the Internet forever, looking for unprotected computers. This means you have to look after all the old issues as well as the new issues; with each new system you bring online, you're adding to the area, or footprint, of what you have to protect. It's a constant process in which the threats keep expanding."

All of which leads Soukhanov to suggest a few urgent first steps for shipping companies starting out on their cybersecurity journey:

- Invest in a cyber assessment now. The cost of a cyber disruption could be far beyond what you save by doing nothing, or what you spend on preparedness.
- Take responsibility for your vessels' IT and cybersecurity. Physically survey, understand and document your vessels' IT networks.
- Undergo an independent cyber research assessment by experienced professionals who understand the maritime domain and can clearly explain the potential impact of highly technical vulnerabilities to the master and CEO.
- Amend your Safety Management System with an initial cybersecurity policy for your operations. Basing this on your cyber research assessment is even better, as it will be evidence-based. Don't wait.
- Train and educate everyone, from the C-Level to the deck plates, without exception.

For Frey, the best protection is prevention through education. "Training and education in cybersafety is part of the answer to these kinds of issues – not just for the crew, but for everyone ashore as well," he says. "Another part of the equation is establishing the right safety protocols, restrictions and firewalls. Putting such protections in place is like putting locks on your door. If you leave your door poorly secured, anybody can walk in." ■