Cybersecurity

Guarding against hack attacks

No one is immune from cyber attacks. In recent years, cyber criminals have targeted everything from multinational companies and credit card giants to towns, hospitals, schools, ports and government agencies, to name just a few. Small businesses are fair game also. One in five has been targeted and more than half of those attacked folded their tents within six months. Nor are marine-related companies out of bounds.

In 2017, containership operator Maersk fell victim to a malware attack apparently launched in Ukraine. Disruption to its operations and terminals cost an estimated $300 million. A year later criminals hacked into Australian shipbuilder Austal's data management system and stole confidential company data that they used to extort money. More recently hackers targeted a tug boat operator who inadvertently opened a virus-laced attachment. Earlier this year malware disrupted operations and production at boat builder Beneteau. These incidents are only the tip of the iceberg—and they are only those that have been made public. Most are not.

A lack of statistics on attacks and especially those that succeeded in shutting down equipment, stealing confidential data or extorting money via ransomware makes accurately gauging the overall economic impact a difficult challenge. At the 2020 RTCM panel discussion on cybersecurity, an officer from the Coast Guard Cyber Command admitted they did not know the number of attempted or successful cyber assaults on maritime assets.

Several experts contacted for this article explained that ship owners see little upside in disclosing the news that they've been hacked, so they may quietly pay the ransom and go about their business. Alerting the world that their cybersecurity guardrails were inadequate or missing altogether does little to instill confidence in current and potential customers and business partners.

That said, attempted hacks on the maritime industry that are publically known jumped by 400% since early 2020, according to Israeli cybersecurity firm Naval Dome. Company CEO Itai Sela blames the Covid-19 pandemic for a large slice of the increase. Because of lockdowns and technicians' inability to conduct servicing on board a vessel, some work is being done remotely by connecting standalone equipment to shore-based networks via the Internet for diagnostics and updating software. As we all know, casting your fate to the Internet can be a dicey proposition. Adding to the problem, Sela says, is "OEM personnel working remotely on home networks and personal PCs, which are not well protected."

Recreational boats can be targets too

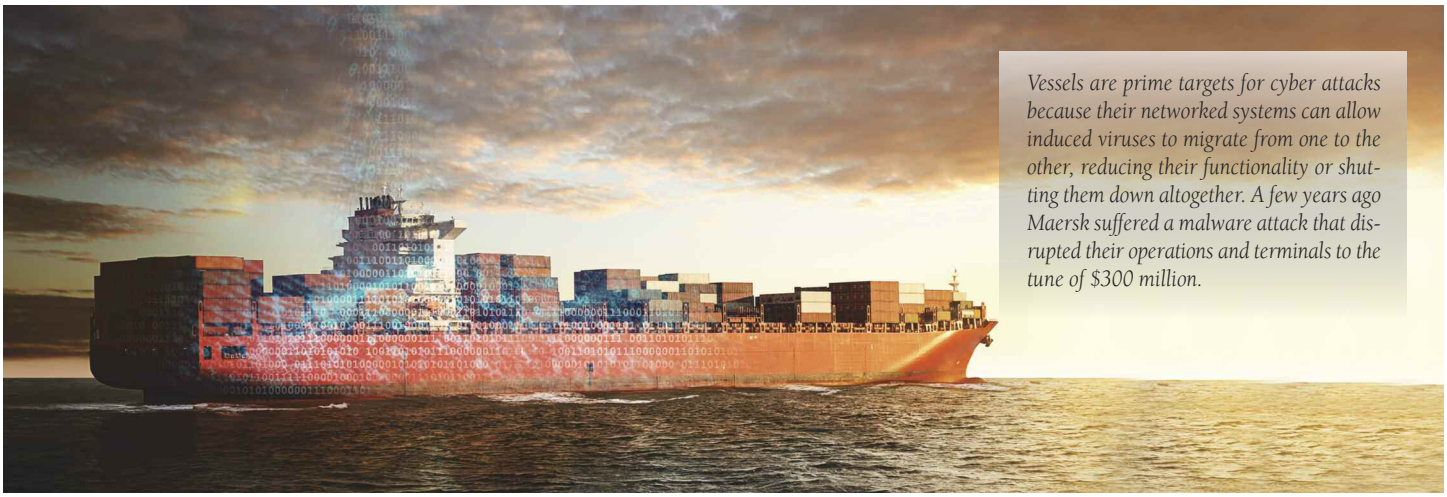
Cyber attacks aren't the exclusive province of commercial traffic. Recreational boats can be targeted also. Consider these scenarios:

A guest aboard a megayacht that is about to leave port for the Caribbean ties into the vessel's VSAT or Wi-Fi to check his email and inadvertently downloads a virus that worms its way into the monitoring and control system. That night when the boat is far offshore the bug shuts down the engines, pumps and fuel management system until a $1 million ransom is paid.

Or a disgruntled crewman plugs a thumb drive into the MFD that contains malware designed to capture and transmit sensitive data about business transactions the owner conducts while on the boat.

How about cruising up the rocky Maine coast when the locations of headlands and islands shown on the MFD are nowhere near where they should be? That's because the GPS has been spoofed by an unhinged hacker bent on running you aground.

The list goes on. There are at least a couple dozen ways that cyber attacks can and do occur, according to cybersecurity consultant



Vessels are prime targets for cyber attacks because their networked systems can allow induced viruses to migrate from one to the other, reducing their functionality or shutting them down altogether. A few years ago Maersk suffered a malware attack that disrupted their operations and terminals to the tune of $300 million.

Gary Kessler. He lists attack categories ranging from insider threats and cryptojacking (malware that takes over your computer to mine for online currencies like Bitcoin) to diddling (data alteration), phishing (emails attempting to get recipients to reveal passwords, credit card numbers, etc.) and whaling (phishing attacks targeting CEOs and CFOs). Ransomware garners most of the big news, but Kessler says phishing and other forms of malware are by far the major cyber problems. Why don't you hear about those attacks? Think of it—unfortunately—as the "new normal."

Integrated systems = vulnerability

While assaults are common in every corner of the cyber world, vessels are particularly vulnerable because of their networked monitoring and control systems. At risk are navigation, communication, mechanical and security systems. For commercial vessels those risks extend to cargo and shipping as well as port operations.

Two years ago the *Marine Link* website and others reported on an exercise by Naval Dome to show how much damage an onboard cyber attack can cause. With full knowledge and approval of the ship operator, Naval Dome first hacked into the ECDIS (Electronic Chart Display and Information System). Their approach was simply to send an email to the captain's computer, which was routinely connected to the Internet via satellite link to download chart updates.

"We designed the attack to alter the vessel's position at a critical point during an intended voyage during night-time passage through a narrow canal," the article quotes CTO Asaf Shefi as saying. "During the attack, the system's display looked normal, but it was deceiving the officer of the watch. The actual situation was completely different to the one on screen." They also were able to alter draft and water depth readings.

Naval Dome attackers then turned their attention to the standalone radar system. They were able to penetrate the radar via the Ethernet switch interface, which links to the ECDIS, bridge alert system and voyage data recorder, *Marine Link* reported.

"We succeeded in eliminating radar targets, simply deleting them from the screen," Shefi said. "At the same time, the system display showed that the radar was working perfectly, including detection thresholds, which were presented on the radar as perfectly normal."

The Naval Dome team next attacked the Machinery Control System (MCS), which was connected to the VDR (Vessel Data Recorder). For this they plugged in an infected USB memory stick.

"Once we connected to the vessel's MCS, the virus file ran itself and started to change the functionality of auxiliary systems. The first target was the ballast system and the effects were startling," Shefi said. "The display was presented as perfectly normal, while the valves and pumps were disrupted and stopped working. We could have misled all the auxiliary systems controlled by the MCS, including air conditioning, generators, fuel systems and more.

Shefi concluded that, "This type of attack can easily penetrate the antivirus and firewalls typically used in the maritime sector."

Kessler says the maritime industry overall continues to be way behind the curve in using best cybersecurity practices. It's not sufficient even at the base level of security. He points out that only 57% of maritime companies say they do any cybersecurity training. "That's appalling in any industry," he says.

The maritime world suffers from a degree of complacency along with a failure of imagination about how many types of cyber assaults are out there that can cripple their operations, says Kessler. Another big problem is a lack of information security officers at shipping companies and ports.

Companies underinvest in security precautions and defenses because they are slow to recognize how severely a breech can impact their bottom line, says Tyson Meadors of consulting firm Ex Mare Cyber. Shipping companies in particular need to develop a mindset to consider cybersecurity at every stage, from ship design and maintenance to operations.

Humans are the 'weak link'

All onboard cyber attacks essentially are attempts to break into computers, equipment, networks and systems. Most attempts don't succeed. They're fended off by increasingly sophisticated defense systems including the latest virus protection, active monitoring procedures and an assortment of firewalls. Some assaults get through, though—most with the unwitting acquiescence of owners or operators.

"Cybersecurity is not just a technical problem—humans are the weak link," says Peter Broadhurst, Inmarsat's chief of yacht and passenger vessel safety and security. Typical breaches are a crewman, guest or technician who brings an infected device aboard and plugs it into the boat's network or downloads emails and virus-laced attachments that are made to look like they came from friends or their boss.

"Some malware can't be detected by vaccine protection because it's so new," says Broadhurst. "Viruses will try to reside on a PC, server or OT (Operational Technology) and try to infect any and all systems." He recommends making sure you have effective anti-virus software and scan everything coming into your system. "A lot of people don't even know they've been breached."

Marine Electronics dealer Jon Thaw of Poseidon Electronics in Florida says he's heard about bad guys hacking into emails and changing account numbers on invoices that were sent to customers. The boat transfers money to pay for yard work and it goes into another account. Now the dealership calls to verbally confirm account numbers before initializing the transfer.

Thaw cites another example of what he calls the No. 1 threat—disgruntled employees. "The captain on a 150-foot boat did a huge refit, including an almost total crew change. The new engineer wasn't working out. Somehow he got a password from the owner and read emails that said he was about to be terminated. The owner came back and found that nothing on the boat worked—no communications, monitoring & control, AV, office systems, nothing. The engineer had wiped out everything, reset the password and walked out."

Thaw underscores the fact that there are

Tactical advice

- Make sure your satcom system isn't on the public Internet
- Check that your satcom system has its passwords changed from the manufacturer default
- Update the software on the satcom system
- Check that your ship's bridge, engine room, crew, Wi-Fi and business networks are logically separated
- Secure USB ports on all ships systems
- Check all onboard Wi-Fi networks
- Don't rely on technology
- Teach your crew about cybersecurity
- Make your technology suppliers prove to you that they are secure
- Get a simple vessel security audit carried out

Courtesy of Pen Test Partners

NMEA OneNet

OneNet Committee Chair Nate Karstens describes the new Ethernet standard's cybersecurity guardrails:

Modern networks include some significant entry points for attackers, such as Wi-Fi and the Internet. To protect against this, each OneNet device must prove that it is authorized to communicate with the OneNet network. This requires installers to pair each device to the network. Pairing is a quick process and should be straightforward once everyone understands how it works.

Beneath the surface, the pairing process is really a mechanism for distributing an encryption key to devices on the network. Once devices have this key, they encrypt all network communications using TLS v1.2, DTLS v1.2, and an IPsec protocol adapted to OneNet. The encryption algorithm is 256-bit AES operating in Galois-Counter Mode, so it automatically authenticates all messages. These are industry-standard technologies used to secure financial transactions on the Internet, so we can be confident they are highly secure.

Neither NMEA 0183 nor 2000 have built-in cybersecurity defenses.

multiple levels of cyber threats. Poseidon urges onboard electronics engineers to change all passwords every 45 days and set up five or so SSID (Service Set Identifier) levels, basically implementing new networks on the vessel. He said boat owners need to keep backups on everything and insurance polices for ransomware.

"The biggest thing we're doing is educating clients about what to look out for. All of our yachts have sophisticated firewall routers, but when it comes to high-level hacks there's no way to fully protect yourself—our government gets hacked."

Guarding the gate

For larger recreational boats and commercial vessels operating offshore, VSAT is the communications link for voice, data and accessing the Internet. "On a ship, VSAT provides the pipeline to the Internet but doesn't control what data is being transmitted to the modem and the vessel—or if it's carrying a virus," says Paul Comyns, Senior Director, Channel Sales, for Intellian. "So it's very important that anyone using satellite communication such as VSAT or Certus—or if it's Wi-Fi or LTE—know it can inflict damage on the system if they connect to a rogue website or open an email with a compromised attachment."

Comyns adds that because many ships are connected to their headquarters via a VPN (Virtual Personal Network), if a crewman using his own computer downloads a virus it can get into the vessel's network and end up in the company's shoreside network. "Additionally, many systems onboard the vessel are IP (Internet Protocol)-addressable and a virus can find its way into them and affect shipboard operations," says Comyns. "This is a very serious threat right now, and should not be taken lightly. End customers must be diligent and be sure to only use an airtime provider that can offer effective cyber protection."

Comyns stresses that systems must also have virus detection along with firewalls and mask IP addresses on the terminal. If IP addresses aren't masked hackers can search the Internet for open IPs and possibly gain entry into the system. "Most of our Network Operations Centers only allow known IP address to connect. A lot can be done to limit access to the equipment. It is not possible to hijack an antenna." Even if protections like this aren't in place, the only thing a hacker can possibly do is temporarily knock the system off the air.

Layering safeguards

Defensive equipment provided by third parties can also be good insurance. In this case, "we are usually speaking of a WAN controller/switching device (Kerio, PepWave, etc.) that controls the vessel network and also has capabilities to control what users' data access is for each WAN connection and what type of data is allowed," says KVH Superyacht Group Regional Sales Manager Steve Gorman. "Many larger yachts with more elaborate networks will also have some type of additional firewall software or device on top of that, but when dealing with our newer HTS (High-Throughput Satellite) network we have the very extensive six-level cybersecurity built into our network, so when the vessel is using the VSAT as the main WAN connection for their data communications we are not only protecting our multi-layer network but also making sure to protect the data we are downlinking back to the vessel from the shore based network."

KVH created its multi-level cybersecurity strategy a few years ago. Level one is training for commercial and recreational crews via videos, including what to do if you discover an infected file. Level two is securing the satellite network. "We do this by funneling all data from the vessel through one of our 'MEGApops' so we can monitor all data traffic and not just send it into cyberspace," says Gorman. "Firewalls are built in."

Level three is protecting the terrestrial network (earth stations). "We catch things all the time and notify the vessel. If we see something—like a Trojan attempting to transfer to a computer—we can actually stop data from coming off the vessel. Everything is checked that comes into or goes from the vessel."

Level four is installing security hardware on the boat that "prevents data from coming in and learning our network. The system notifies us that there's a potential problem with some data and we alert the vessel."

Level five is protecting Internet egress, including application-level firewalls and threat detection/blocking. The final level is incident response to address threats to the network with the goal of quickly managing and minimizing risks.

Wi-Fi protection

There are defenses that Wi-Fi users can implement as well. "We're not a cybersecurity company but we do take it seriously because we're in that connected space," says Wave WiFi's Jeff Graham. "We try to encourage protection by providing flexibility in terms of features and options. You can change the SSID and password for all of the LAN access points. We have administrative passwords that can be enabled or not. Owners can run their networks loose or tight. We provide network segregation—guest side, captain and crew side, owner side. You can also blacklist bad URLs."

Graham says the wireless security standard WPA2 is mandatory on their LAN access points to help maintain a closed network. "We also provide login code use for another layer of connected user control through a captive portal. Basic firewalls are embedded and can be enabled in all of our Wi-Fi receivers and our routers/network controllers. By default, we reject incoming connections other than those related or already established. Port forwarding is also an extended option throughout our Wi-Fi receivers and network routers/controllers."

Israeli cybersecurity firm Naval Dome conducted a demonstration that showed how easily interfaced systems aboard a vessel—commercial or yacht—can be compromised. A major concern is crew linked into a ship's Wi-Fi who inadvertently download a virus, which then worms its way into navigational and operational systems.

Another point of concern is open access Wi-Fi at marinas, which presents serious risks. "You're on a network with tons of other boats, it's tough to police," says Thaw. "Boats in Monaco and Cannes constantly find their systems hacked by paparazzi trying to find out who's onboard. They change their passwords after every charter."

New OS at every startup

A major target on any boat is somehow hacking into the MFD or ECDIS. Furuno's solution, explains Senior Product Manager Eric Kunz, is that every time one of their MFDs is switched on it loads a fresh copy of the operating system from unwritable RAM. "The system is locked down even more than your typical smartphone. It doesn't allow uploading of unregulated untested apps. Even if a hacker gets in, the next time the system starts up there's a new operating system. There's no back door like on a cell phone."

Additionally, he says, the company uses "curated apps that we test and certify. You can only get them from Furuno. Also, you'd have to infiltrate the components connected to the MFD like spoofing GPS or AIS, which is not realistic to do.

"Theoretically someone might be able to break in but it would take a major undertaking. You'd have to have specific knowledge of software that goes into a product. We're taking pretty strong measures to make sure that doesn't happen.

So far we haven't had any successful hacks into any Furuno equipment."

While Kunz doesn't consider hacking a huge issue for recreational vessels, he says there are cybersecurity concerns on the deep-sea side, where they take a different approach. "Everything goes through a gateway. With ECDIS when you download a new chart it must go through a gateway, which acts as a gatekeeper. It won't let in bad stuff."

Some advice for the cyber world ahead

Without a doubt, protecting against successful cyber assaults on vessels and related shoreside facilities is a full-time job for a team of experts that gets harder all the time as hackers grow more sophisticated. Broadhurst's advice to owners:

Understand which equipment and systems are connected on the network and can be breached. Train crews regularly about how to avoid risks and make sure guests don't bring infected devices onboard. Scan all incoming network traffic to ensure it's safe and have endpoint security in place to protect network devices. Third-party monitoring of systems that could be impacted is essential.

But despite taking all precautions, he concludes: "Nothing will give 100% security. If someone has time and motivation and resources they can probably hack in. Protection is a marathon, not a sprint. Take a long-term approach when budgeting and planning."

IMO addresses cyber risks

On Jan. 1, 2021, the International Maritime Organization's (IMO) Resolution MSC.428(98) went into effect calling on "administrations" to address cyber attack risks in existing maritime safety management systems, as defined in the International Safety Management Code.