WHEN CYBER ATTACKS

Is your yacht safe?

By Jenny Sniffen

Cyber security threats are nothing new to the yachting industry. And even though the industry is beginning to become more educated about cyber security risks, it still has a way to go. It's no secret that a yacht owner is a wealthy individual. Some owners are well-known or high profile, some politically exposed, and some controversial. When you combine that with the increasing volume of technology on board, and the sheer amount of information and data being processed, a yacht can become a prime target for cyber security attacks.

Many yachts are vulnerable to attack because they have prioritized IT performance over security.

Despite all of this, it's important to "keep risks in perspective," cautions Malcolm Taylor, head of cybersecurity for G3 Good Governance Group. While owners are likely worried about someone stealing their boat as a result of talk about hacking yacht navigation systems, "What they should really be worried about is what people are stealing out of their pockets [through other cyber-related crimes,]" he says. In fact, Will Thomson, co-founder and CTO at CDS Marine, explains that a yacht doesn't even need to be involved in a targeted hack for its data to be accessed. "Simply by being connected online puts the vessel and the data it holds at great risk," he says. "These risks need to be understood and managed correctly, therefore making them no different to any other land-based business."

WHOSE RESPONSIBILITY?

Although cyber security-related concerns have been passed down to ETOs by default, it generally depends on the vessel's size. "On the vessel I work on, the ETOs are very involved on the cyber security side," says Jason Robertson of Robertson ETOs. "We've designed and implemented the network, we do all the Cisco phones, and we completely block and do everything internally." Another ETO says that since his yacht's audit, "[cyber security] definitely has become a responsibility for me over the past year."

In light of this, however, it's important to understand that historically speaking, ETOs generally would not have an IT background because their license is strictly electrical. As a result, this role would tend to fall on the Information Technical Officer (ITO). But, that being said, having an IT background does not translate to being an expert in all things IT. "Even within the world of IT, there are different disciplines," explains Scott Molloy of Just ETOs, who also has a background in IT. For instance, "Someone who can program systems and manage the onboard servers well is not necessarily the best at network security. Networking is a specialist discipline itself within IT," he says.

While there are ETOs, ITOs, and AV/IT engineers in the industry who possess the required skills to address cyber security concerns on board, as a whole, there's a huge shortage in the industry. "Many yachts do not have a dedicated electronic engineer, let alone an IT specialist on board," says Molloy, and even if they do, they are typically only found on larger yachts. As a result, many are unaware of the risks they are exposed to because they fail to have sufficient threat protection in place. In order to have "true cyber data and privacy protection, you need to have the experience, knowledge, and skills to properly address and prepare for it," Thomson says. "There is more to cyber security than simply installing and configuring a firewall, antivirus, and an occasional application of updates and patches."

Unfortunately, without a "qualified ETO/ITO on board who's up to date on current security standards and how to implement them, a yacht can face the very real danger of having its data stolen or held for ransom," says Matt Bingham, CTO of Azuz IT. Because many yachts lack the specialized skills and experience on board to guard against cyber threats, there is a strong argument for utilizing external companies ashore. "Crew cannot be expected to safeguard systems if they don't have experience," says Molloy. Embrace the expertise.

ILLUSTRATION: PIXABAY (TOP); FREEPIK

INVEST IN TRAINING CREW

By investing time and money into training crew, cyber security risk awareness can evolve. Knowledge and training are key; however, not enough yachts are aware of potential cyber security risks. "Ninety percent of the crew I speak with are oblivious to the gaping security holes they have on board," Bingham says.

"The weakest part of most yachts' cyber security plan is the human element," says Tom Frankland, director of JWC Superyachts. It doesn't matter how secure your systems are or whether you have the most state-of-the-art technologies protected by the newest firewalls and market-leading monitoring software, "if there are vulnerabilities among crew or passengers, then it's very possible criminals could find a way into your network," adds Taylor.

However, as Frankland explains, basic cyber security awareness and training across the industry means that the industry can better defend against the risks through the collective knowledge of all crew and shore-based staff. Additionally, Robertson points out that some yacht management companies also have begun to recognize the value of cyber security training by specifically requesting that ETOs take a cyber security course to be more aware of the threats and to implement best cyber security practices on board.

While there is no official requirement for courses yet, there is a UK Government Communications Headquarters (GCHQ)-accredited and MCA-recognized course titled "Maritime Cyber Security Awareness." This course covers "current and emerging cyber security threats for yachts. It is designed to be easily accessible through an online training platform and can be undertaken by crews whilst at work. It is refreshed quarterly to include any new threat vectors and methods to ensure the crewmember stays current and understands how to avoid being caught out," says Frankland. In addition to this course provided by JWC Superyachts, Malcolm Taylor explains that G3 also has an e-learning course and offers one-on-one training centered around both the yacht experience as well as the cyber security element.

COMMON VULNERABILITIES

Many yachts are vulnerable to attack because they have prioritized IT performance over security. "They want the technology to work first and foremost without realizing that they need to aim at security in parallel," Taylor says. But it's important to be aware of the common industry cyber security vulnerabilities – you don't want to be the one responsible for the IT network that led to the boss's information being stolen.

Some of the most common threats are "typically weaknesses in the ship's own network design and operation. Correct system design, operation, and onboard procedures are key," says Molloy. Accordingly, Wi-Fi networks, weak passwords, passwords that are not regularly changed, and passwords that are left stuck to computer screens are all vulnerable to attack. "Poorly configured and secured Wi-Fi networks that clearly broadcast the yacht name and the network they give access to, is probably not the smartest move," Thomson points out. For example, "Password" or "MYYACHT1" on network "M/Y BLUE" may not be good choices. Additionally, because "yachts broadcast a large wireless signal, which allows guests to access the Internet from anywhere on board, an attacker with an amplified wireless signal could access this network from hundreds of meters away, remaining completely undetectable," says Bingham.

Ransomware, malware, and phishing also are common issues on yachts. A ransomware attack could occur when a crewmember downloads a virus that self-installs, causing irreversible damage. When this happens, "Essentially, your entire file system is encrypted, [which means] you cannot access any data, including back-ups," Bingham says.

Malware-based attacks "are used to disrupt normal computer operations, gather sensitive information, and can aim to have back-door access to onboard systems," says Frankland. "Phishing emails are looking to get an unsuspecting crewmember to divulge personal details, usernames, and passwords, and where possible, credit card details through often credible, but replicated false websites."

If a yacht lacks a centralized administrator or does not have one at all, this also can make it vulnerable to cyber attack. "Some yachts don't have any type of IT support or professional involved at all," Bingham says. "This can lead to catastrophic results in terms of confidential information."

Another concern relates to personal devices, such as computers and mobile phones, because these devices do not have adequate threat protection software. "Proper design and management of VLANs and access control lists (permissions between VLANs) are crucial. Crew personal devices should have Internet access only on board. These 'unsafe' devices are often compromised by any manner of malicious software. If they have zero access to the rest of the onboard network, they cannot affect it," says Molloy. "Operationally, I'd say the majority of yachts have unsafe personal devices connected to the wrong part of the onboard network. Not enough people understand."

Browsers and unencrypted emails can also pose an immediate danger. "Almost everybody on board utilizes the Internet connection and, more often than not, will come across a website that may cause a threat," Bingham says. "If appropriate anti-virus/web filtering solutions have not been introduced, a program is able to self-install and spy on passwords, networks, and even hijack the computer itself." Additionally, when emails with sensitive information are not encrypted, attackers can intercept and read these emails.

"The larger the yacht, the more crew it will employ, the more data it will hold, and the more reliance it will have on communications and connectivity," says Thomson. "It only takes one click

"The weakest part of most yachts' cyber security plan is the human element."

PHOTOGRAPHY: (BOTTOM) MATEJMO/ISTOCK; (MIDDLE) FREEPIK of an email or a visit to a known website that has been compromised and you're redirected to a malicious site. Who knows what could then happen."

PHOTOGRAPHY: MARK O'CONNELL

IMPROVING THE INDUSTRY

While the industry has been slow to embrace the need for cyber security, it's now beginning to do so. Both the implementation of the changes to the General Data Protection Regulation requirements and the IMO's new guidelines focusing on cyber security risk management will likely ensure that the yachting industry catches up quickly.

As Taylor explains, through awareness, assessment, and protection, the industry will improve its cyber security defense. Acknowledgment that the industry is not immune to cyber security threats and acceptance that there is an issue in the industry is at the heart of awareness.

Yachts also need to perform an assessment to see where they are vulnerable. "An audit should be part of all vessels. They should have a technical consultant come on board to do an IT audit and vulnerability test to ensure that vessels are actually adhering to best practice to ensure a secure infrastructure and secure network," explains Robertson. "Far greater attention needs to be placed on how systems communicate and interconnect on board, how they are used and accessed, and by whom and for what purpose. Know what data you hold, where it is, who has access to it, and highly important, monitor the systems," Thomson says. Once a yacht's IT system has been assessed, it's important to take the steps necessary to mitigate any vulnerabilities. This may include designing better technology solutions to address security concerns, providing better training for crew, or maintaining better governance, policies, and procedures.

"One particular element we [have] yet to come across on any yacht is a well-drilled and understood 'cyber' incident response process and the adequate controls and protections placed around access to the sensitive, personal information yachts hold on crew, guests, and owners," says Thomson. Additionally, following the premise of the IMO's guidelines on cyber security, "A risk management layered approach needs to be taken alongside well-written policies and procedures, which are then enforced using strong technical controls, solutions, and monitoring. Cyber security is an ever-changing animal and as such, constant improvements, assessments, and monitoring will be required," he adds.

"[Yachts] will never be one hundred percent protected. There is no such thing as one hundred percent secure, nor is there a one-size-fits-all shiny box, tailor-made 'just for yachts' solution that will cure all ills," says Thomson. "In order to protect against the threats and risks, you need to know what they are [and] identify those risks and threats. This not only includes internal systems, etc., but outside factors, too. For example, the owners – are they high-profile and well-known? Could they be of 'interest'? When these and other factors are understood, they can then start to be managed and mitigated where possible." Ⓓ