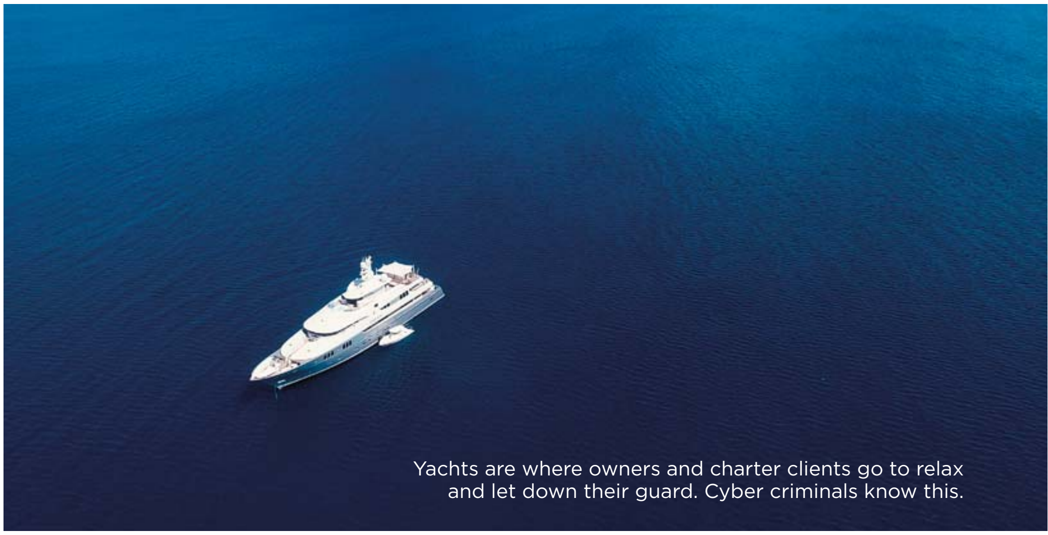
by **Michael Wills,** *CSS Platinum*

WHY AND HOW CYBER CRIMINALS TARGET SUPERYACHTS AND WHAT YOU SHOULD DO ABOUT IT

Following CSS Platinum's contribution to the Superyacht Cyber Security panel session at the Boat International Superyacht Design Festival in Cortina d'Ampezzo, Italy, in February, an Italian shipyard owner approached us.



Yachts are where owners and charter clients go to relax and let down their guard. Cyber criminals know this.

"Are cyber criminals really targeting us? Could they really do all the things you just described?" he asked. "The thing is, I am just not hearing about these attacks occurring."

"A fair question," we responded, before asking: "Tell me, if your shipyard had suffered a cyber-attack, whom would you have told?"

"As few people as possible," he responded instantly.

Herein lies the reality and the problem. In an industry as competitive as ours where multi-million-dollar transactions decisions are made on relationships and trust, cyber-attacks are not being reported for fear of the damage it will have on a company's reputation. The difficulty is that because attacks are not being reported, those yet to experience the embarrassment, pain, distress, worry and damage of a cyber-attack do not perceive it a problem.

Right now, the yachting industry is actively being targeted by multiple highly sophisticated criminal networks across the globe. Most superyachts and their owners will be the subject of "target packs" compiled on them by multiple international criminal groups. These are not tin-pot criminal opportunists; these are well financed, highly organized criminal businesses with business plans, budgets and resources available.

Where are you on the cyber-security sensitivity scale?

When considering cyber security, there are generally five groups of individuals:

- Those who appreciate the risks and proactively do something about it.
- Those who have been hacked, never want to experience the pain again and do something about it.
- Those who may appreciate the risk but consider cyber security techy, complicated and easier to ignore than try to understand.
- Those who may appreciate the risk, but do not like the thought of a cyber company crawling unfettered across their devices and networks. So, they ignore the issue. (This is not how cyber companies work, by the way.)
- Those who have no idea that they are vulnerable.

Unfortunately, cybercrime and security is here to stay and is no longer something to be ignored. Technology and artificial intelligence continue to evolve at an alarming rate and shows no signs of slowing down. This evolution coupled with the reduction in component prices and the prospect of greater connectivity and data transfer rates promised by 5G technology will result in more "things" becoming "smart", digital and automated and joining the realm of the Internet of Things. Smart things require connectivity to a network to enable them to be controlled remotely by devices. Any network connection presents an access point for a cyber-attack.

***Why* do criminals target superyachts?**

Superyachts are ripe targets, and a magnet for criminality. They are also easy targets. Yachts are where owners and charter clients go to relax and let down their guard. Cyber criminals know this and factor this into their targeting strategy.

***How* do criminals target superyachts?**

With so many systems onboard now being controlled digitally and by networks, criminals can use a cyber-attack to allow them to:

- access your emails to find information or opportunities to divert payments;
- access your onboard CCTV footage, steal the files and blackmail you;
- access your navigational systems to confuse you about your location;
- take over your propulsion systems to stop you moving out of a marina;
- make you stop at a place of their choosing;
- make you lose control of the vessel and cause environmental damage to protected reefs, or damage to marina infrastructure or other vessels and so damage your reputation.

It is important to understand that a cyber-attack is not the end goal, it is a tool to achieve a goal. For example, the goal might be theft of artwork. The criminal gains access to the vessel and the artwork via a cyber-attack that disables alarms, lights and CCTV systems onboard. Think of it as a metaphoric digital crowbar or rock through a window.

Who are these cyber criminals?

Criminals seeking to target superyachts are cunning, clever and capable of implementing elegant, elaborate and elongated strategy to achieve their ends. They are patient and, like a chess player, are capable of planning many moves ahead; with multiple contingencies should situations not unfold as they intend.

To do this effectively, however, they need to gather good information in order to formulate a winning plan. As a result, criminals will target as many potential sources of information associated with a superyacht or its owner to build the fullest picture (or target pack) of an opportunity. This will include owners, their family, their guests, the crew, shore staff, family office staff, marina staff, engineers, brokers, insurance advisors, legal advisors, yacht management companies, corporate services providers and any other individual or company who connects and holds information on the superyacht or its owner.

> *Right now, the yachting industry is actively being targeted by multiple highly sophisticated criminal networks across the globe.*

Thinking of it as peeling back the layers of an onion's skin to get to the center – the target, the goal. Once an individual/s have been identified, the criminal will seek to gather seemingly innocuous information, or coerce the individual directly into passing information or conducting an act that enables further information to be gathered. This could be access to the superyacht's network and/or in time, the owner's business or personal emails and files.

In order to find the right individual to trick or coerce, criminals use the internet to identify individuals and supporting businesses and target their cyber unpreparedness and weakness. Poor cyber security, online security or habits and/or misfortunate circumstances can inadvertently offer opportunity for an individual to be targeted and/or subverted. These circumstances can include:

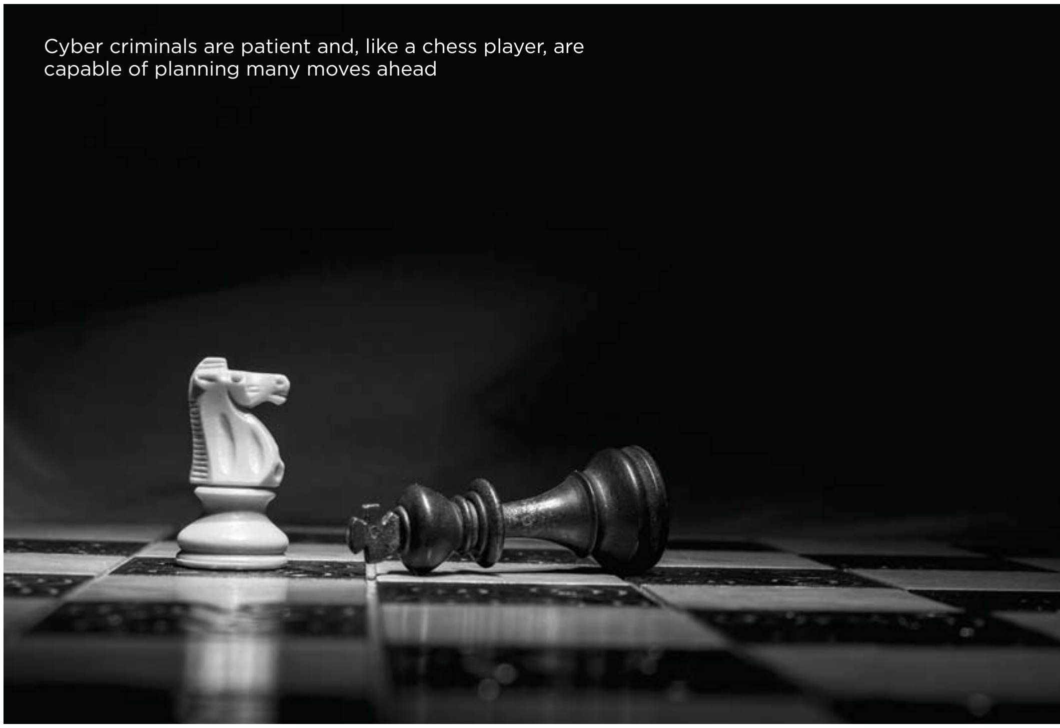
- Social media security settings not applied meaning posts are available for all to read and view.
- Inappropriate posting of pictures or comments that could identify a vessel, its owner, its route or destination;
- Poor and/or naïve electronic device usage which presents a cyber security risk by navigating to risky or insecure sites, clicking on unknown links, not regularly updating software and application update patches.
- Large debts, addictions or inappropriate use of illegal or socially taboo sites that may result in a crew member being bribed and/or coerced into providing information on the yacht and owner or carrying out an act that enables remote cyber access.
- Not knowing that personal data may have been hacked and is for sale on the Dark Web which can enable further targeting and even identity theft.

Once cybercriminals gain the access or information they require, they apply strategic patience and wait until the conditions are right and the opportunity justifies the risk. Big paydays fund the fallow targeting period until the next big payday.

A clear and present threat

Cybercrime is a clear and present threat to the superyacht and wider yachting community. Regretfully, for most it is not a case of if a cyber-attack will occur, but rather when. Addressing cyber security can be an intimidating prospect, but when vulnerabilities are addressed proportionately and coherently and governed effectively, the end result is that an owner, his or her superyacht and those that support it will be #hardtohack.

Michael Wills is co-founder and chief data officer for CSS Platinum. For further information on the company and the services it provides, including a whitepaper on the IMO's introduction of Maritime Cyber Risk Management as part of the ISM Code, please visit https://cssplatinum.com and/or email support@cssplatinum.com.


Cyber criminals are patient and, like a chess player, are capable of planning many moves ahead