Cyber security and the Superyacht industry – separating fact from fiction and looking at what can be done to mitigate cyber risk.

Over the past 12 months or so a great deal has been written about the threat to superyachts and their owners from cyber criminals and cyber attacks in general. That the risk is real is not in doubt, and the IMO will implement regulations by 2020 which will provide that all vessels over 500gt will be required to demonstrate they have addressed the cyber threat.

However in this time gap between the initial scare and hype of recent times and 2020 when we will have industry parameters of how to mitigate this cyber risk, we see yacht management companies, yacht owners and crew often taking matters into their own hands.

Much less has been written about what can be done to minimise the risks, and even less that brings any sort of perspective to them. Here we ask Malcolm Taylor, Head of Cyber Security at G3, for his views.

BM Q1. **In the face of all the recent publicity, can you tell us what you believe are the top cyber security threats faced by UHNWI's and their teams?**

G3 A1. I think it's important to stand back and consider what the attackers want. Firstly, and by far the most common, they want to make money – cyber crime is their job. Secondly, and much less common, to cause mischief or harm. Now UHNWI's are de facto wealthy, and many of them lead lives which a few consider controversial even if a lot of that is rooted in envy. So, in other words, they're an almost perfect target. Added to that, and crucially, many of them live their online lives without the levels of protection afforded to big corporates – they're very vulnerable. So, the biggest threats are theft of money, of private information for sale or blackmail, and of sensitive corporate information – such as business deals. I know of cases where individuals have lost £millions and deeply personal and family information. The impact can be devastating, especially in the latter cases – private information is, in many ways, priceless.

BM Q2. **We have seen a lot of reports, not just in the mainstream media but also from experts in the shipping industry, as to the physical threats posed to vessels (e.g. disruption of navigation systems such as AIS). What do you perceive to be the threats to physical assets and is the threat as serious as it is sometimes presented?**

G3 A2. Where yachts are concerned, a lot gets written about what I would call existential threats – hacking a navigation system, steering a yacht off course, even stealing it or driving it onto the rocks,

Tel. +44 (0)20 7375 1393
Fax. +44 (0)20 7392 9529
info@bargatemurray.com
Facebook.com/bargatemurray
Twitter.com/bargatemurray
Bargatemurray.com

that sort of thing. They're frightening thoughts – but are they realistic? They are all maybe technically possible, and perhaps they're getting easier as attacks develop. But I would still ask, is this realistic? It means not only a highly complex technical attack, but also that the crew will be fooled comprehensively and not notice anything is amiss. Superyacht crews know what they are doing and many of those I've spoken to are confident they would notice an attack like this and defeat it. It's about their 'feel' for their boat and their knowledge of the sea. And finally, look at it from an attacker's point of view; why would an attacker go to all the trouble of stealing a yacht, and all the problems that would bring, when he could much more easily steal £millions? It makes no sense. So, I go back to my previous answer. The biggest threats are thefts whilst on board, and especially because the systems on most yachts are woefully under-protected.

It frustrates me sometimes that owners are being scared by these highly unlikely worse-case scenarios, and so ignoring the really very common risks. The first key to security is understanding your specific threat and then addressing it – which is very hard if people are being persuaded to look in the wrong direction, to look at the extreme yet unlikely rather than the commonplace and highly likely.

BM Q3. **What direction is the cyber security market going in, with regard to superyachts?**

G3 A3. The ISM is interesting. BY 2020, all vessels over 500gt will be required to demonstrate they have addressed the cyber threat. That will be a big change. Otherwise, technology will keep improving but so, sadly, will the attackers. Security is really risk management; understand, improve, maintain. I don't see that changing much, to be honest. Wherever there's a network, there's an attacker.

BM Q4. **Can you give us some real-life examples?**

G3 A4. We work with complete confidentiality of course, but I can give you a couple of anonymised, real-life war stories yes.

First, a family office that lost a considerable sum of money in an email scam. They received an email apparently from a family member asking for a relatively large payment to be made to a company they had used before, complete with bank account details. The office made the payment and thought no more about it. A few weeks later, they realised the payment was a fraud – and the money hasn't been seen since. This was a cyber attack – the original email was faked to look like it came from the family member. It didn't, it came from the attacker and the bank details belonged to the attackers, but the email was very credible. This is a relatively simple attack but increasingly common, and it's also relatively simple to minimise the risks. There are some technical protections available, and these attacks, sometimes known as CEO fraud, are best defeated with good policies; never accept payment requests by email even from people you know. Call them and check – and use contact details you have and not those from the actual email. Two minutes on the phone in this case would have saved hundreds of thousands of pounds and frustrated the attack.

Second, a yacht about to go on a charter when the crew discovered that ransomware was affecting all their systems – entertainment and yacht management. They were all-but immobile with no technology

at all and guests due. A well defended network would have reduced the impact massively. First, by limiting the privileges of the machines on board so the ransomware could affect only the machine it landed on – not the whole yacht. Second, by having good, regular back-ups in place such as ransomware prevents access to data by encrypting it – so a recent back up allows the system to be cleaned and the recent back-up restored, with minimal impact or data loss. Third, as we saw with the Wannacry ransomware, a good software-patching regime minimises the risks significantly. And finally, good AV and email etiquette can prevent a lot of ransomware – the AV should catch it as it comes in, but if it does get through then the crew will recognise the threat and know what to do and what not to do.

Finally, we are working with a UHNWI who had really private photographs stolen by a hacker – not intimate, but private. We've hardened their defences to minimise the risk of a repeat, and are working with their legal team on recovery. That one is really hard on a personal level – it has been devastating to the whole family. And recovery is harder than prevention – much harder.

Conclusion

In terms of legal problems that a cyber attack could create, let's look for example at an attack which might have the effect of preventing a yacht from carrying out an agreed charter (or meaning that it is delivered late). Assuming that a standard MYBA charter agreement is used, it is strongly arguable that the force majeure clause would not protect the owner in these circumstances, exposing them to financial penalties. Moreover, many insurance policies still expressly exclude losses that arise out of cyber attacks. These are clear and pressing issues for owners to consider where prevention is far more preferable than cure.

Malcolm Taylor
Prior to joining G3 as Head of Cyber Security, Malcolm was a senior officer in the British Foreign Office for 20 years. He served at GCHQ in Cheltenham, and in London and overseas in Iraq, Pakistan and Afghanistan and is expert in strategic cyber and communications security. He heads G3's UHNWI work, with a particular focus on super yachts and their owners' broader digital lives. He also provides strategic cyber security advice to senior corporate and government clients.

Email: malcolmtaylor@g3.eu
Mobile: +44 (0)7471 351 559