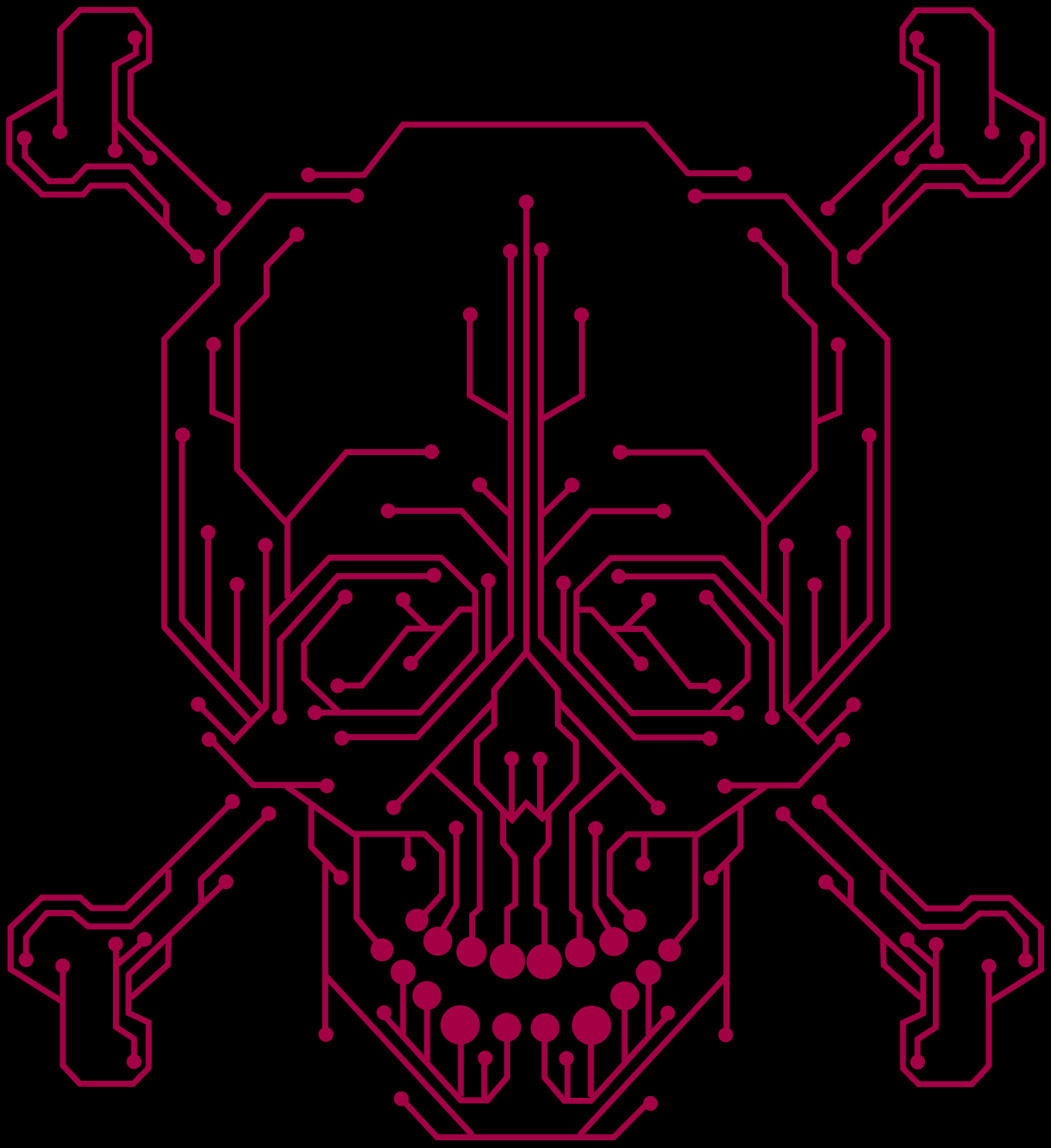

STREET SMART I.T.

The latest knowledge on cyber security for your yacht.

– ZEB ROBIN OF BOND TECHNICAL MANAGEMENT

Stories from the Wild West or of pirates on the high seas may not seem to have much in common with today's modern information technologies, however, in many ways this is indeed the state of the internet and computing in general. Cowboys today wrangle botnets instead of cattle, and ships of gold have been replaced with servers full of valuable data. Perhaps most importantly though, just as with the old frontiers, law enforcement in this new electronic wilderness has become largely irrelevant, and the responsibility for protection falls on the individual and organisation. On board superyachts, and indeed in the world at large, there is a need for owners and operators to improve their information technology (IT) and computing 'street smarts'.

All too often we see IT risks being downplayed or outright ignored; some have only taken the issue seriously after being damaged in some way. And in the yachting world, some companies unfortunately operate on the premise that in the land of the blind, the man with one eye is king. Here, I provide a way to think about IT security that cuts through the IT jargon. Although the principals will always require specialised skills to implement, they are actually simple common sense.

LAYERS OF SECURITY

Safe computing today has evolved far beyond anti-virus and spam blocking. Indeed notions of password strength are completely irrelevant given the fact that there exists various malicious software and processes (like key loggers, Trojans, "man in the middle" attacks and "zero day exploits"). We don't want to incite panic, but you should know that this stuff is real. With so many ways for criminals to enter the modern network and monetise their ill-gained access, only a layered approach to security can both resist illicit activity from the outset and minimise the damage potential should compromise occur.

THE PHYSICAL

One wouldn't expect a yacht's engines or ballast pumps to operate reliably if they weren't designed well, installed professionally and well maintained. However, in IT systems we see time again that corners are cut and poor or unplanned infrastructure is installed. We can't stress enough that 'managed' network hardware is needed which both supports modern security features and is centrally manageable. As they say, cars are useless without roads and freeways.

Just as you would pull up the passerelles at night or install tender tracking on the water toys, also make sure your IT system has intuitive means for the crew to disable or enable the various possible paths to the internet and consider asset tracking and recovery products for laptops and smart phones. WI-FI security is also worth considering as the access key to join a wireless network is not for security, it's simply for joining the network. Make sure there is another layer of authentication, which can be centrally revoked so that if your wireless pass phrases are shared, you aren't giving away the keys to the network.

Lastly, remember the number one rule of computing: If the bad guys can touch it, half your battle is already lost. Control access to your servers and take administrative access and passwords seriously. Key loggers (software that records everything typed into a computer keyboard) can quietly be installed in a variety of ways to collect your every keystroke. Stolen laptops and smart phones often end up with data harvesting hackers where disks are scanned for any data that can be monetised; there are various ways to mitigate these risks which are worth looking into.

ACCESS CONTROL

Each yacht manages its door keys, be they physical or electronic card readers, and great care is always taken to ensure that access to areas of the yacht is controlled. The same is sadly not always true in the digital domain. Make sure that all employees have only the privileges they need to be productive in their work, and establish clear policies to revoke privileges from all systems should employees one day leave. Be reasonable with employee passwords; 'a three strikes your locked' rule on logging in is infinitely better at denying brute force attacks than even the most complex and impossible to remember pass-key. Super complex passwords look pretty silly when they end up on Post-It notes stuck to employee monitors.

Recently, we assisted a customer who needed forensic help in analysing a case whereby a former crew member had accessed the vessel from shore via the WI-FI and used passwords that he had been given over the course of his work to maliciously delete dozens of hard drives on board which made the entertainment system work. Ship records thankfully were not targeted, but the fact is that it would have likely been possible if the crew member had been crazy enough to try. There are systems available that enable the network to be aware of all hardware that is attached to it using unique identifiers and allow users to be allowed or revoked access based on proper credentials. The credentials and WI-FI access can then easily be deactivated should an employee part ways with the vessel: it's no harm, no foul.

If something is broken on board, one likes to know who did it and what the circumstances were. Therefore, don't let employees share passwords for accessing important systems. Give everyone private logins to shared resources so that you have a degree of accountability if things ever go pear shaped. In general, your IT system should be able to tell you after the fact who accessed a system, when, and what it is they did.

OBSCURITY AND CONFIDENTIALITY

Superyacht crews generally do not place trust in shady strangers standing dockside, and certainly wouldn't allow people aboard without reason and pre-approval. However, many IT systems are left wide open to the internet with inadequate hardware and incomplete security configurations to ensure that access is controlled and malicious motives are kept in check. Firewalls are popular and fantastic tools to deny unauthorised external access but they do nothing to mitigate danger if an intruder is already in your network. For this reason the modern IT arsenal also includes security appliances that give added controls to what traffic is allowed, often in conjunction with bandwidth management tools that allow a yacht to make the most of limited internet access by prioritising important traffic and blocking undesirable traffic. Don't want your crew using bit torrent to steal movies? It's easy if you have the right hardware at the outset with knowledgeable staff to configure and maintain it.

We haven't yet met an owner who is willing to let the public know the location and travel plans of their vessel. Indeed, obscurity is a great defense against undesirable attention from all corners. However, we hear time and again of crew posting sensitive information on sites like Facebook for the world to read. While the above mentioned security appliances are fully capable of completely blocking access to any arbitrary website, this heavy handed type of approach is a) likely to upset crew and b) possible for reasonably savvy crew to circumvent by using encrypted VPNs and proxies.

FIREWALLS ARE POPULAR AND FANTASTIC TOOLS TO DENY UNAUTHORISED EXTERNAL ACCESS BUT THEY DO NOTHING TO MITIGATE DANGER IF AN INTRUDER IS ALREADY IN YOUR NETWORK.

Better perhaps is to teach crew up front the importance of discretion and make sure people are aware of the consequences of their actions on social networking sites. The same hardware that blocks sites can also log access, so consider allowing crew freedom with the awareness that yachts are private vessels and the list of sites visited can be monitored. The message is clear: behave. Facebook, despite the newspaper headlines, hasn't really changed crew behaviour. People have shared sensitive info in the past via telephones and email – it's just that sites like Facebook make sharing to a wide audience so easy that it seems to blind users to the ramifications of what they are doing.

INDIVIDUALS: TRAINING AND AWARENESS

To crew on a yacht, safety training is nearly universal with the most important jobs on board requiring extensive education and certifications. Crew are further taught to be aware of strangers on board, and specialty security staff are often hired to provide physical protection if required. However, in this age of data theft and social engineering computer attacks, we'd like to make the argument that it is worth extending these same ideas into the IT realm.

Every IT system needs someone who administers and controls access, just as the skipper decides whom steps foot on board. Does this administrator

verify the identities of people before he resets their passwords? Does he ever put user names and emails into the same email or does he know to split the path? The point here is that all the high-tech hardware in the world is useless if it isn't properly administered and operated day to day with sound procedures.

EVERY I.T. SYSTEM NEEDS SOMEONE WHO ADMINISTERS AND CONTROLS ACCESS, JUST AS THE SKIPPER DECIDES WHO STEPS FOOT ON BOARD.

GOVERNMENTAL OVERSIGHT

Sadly, our yachting analogy ends here. In the real world, you can make mug shots, collect fingerprints and review security camera footage, but in the digital domain things are not as straightforward. The fact is that if an attack on your infrastructure is successful, there likely won't be any recourse available.

Systems do exist which can provide the analogous functions of a real world security system in the IT domain, but here one must weigh the value of what you are protecting as costs go up quickly both in terms of installation, and operations. These security systems often require dedicated staff to manage and extensive configuration to develop to the point of being worthwhile, and they always shift the trade off away from ease of use towards high security.

SUMMING IT ALL UP

For most real world IT systems, investing in a pragmatic layered approach to security with good procedures, trained staff and sound system design will resist malicious activity and mitigate harm from a successful intrusion to the point where only rogue or tricked insiders could cause serious damage and disruption. We have implemented several security and IT policies on vessels that at the very least have provided improved security from a technical and operational perspective. The rest then remains up to the staff on board and the management company or organisation to help maintain good habits and vigilance. This then brings us to the last similarity between IT and the physical world, and possibly the most vital part of the equation: all systems, be they IT or otherwise, require the establishment of good teams filled with trustworthy individuals. ▣

FOR MORE INFORMATION SEARCH FOR BOND TECHNICAL MANAGMENT AT:
WWW.THESUPERYACHTOWNER.COM