How your ship has probably been Cyber Attacked already

A feature article by

George Ward

ECDIS Ltd Project Support
Corporate Member of IAIN

You have either been hacked... or just didn't know you have been hacked.

I predict that the first catastrophic maritime cyber incident will not be the result of a direct attack on a specific, safety critical piece of equipment. It will be the result of an infection on a random PC, perhaps through an unassuming email to a crew member, whose PC is either connected to the vessel's internal super highway or he transmits the infection internally whilst it lies dormant. Crypto locker, or Ransomware software (used by thousands of hackers) are easily available to download on the dark web. Neither of them may necessarily attack the equipment they infect; they can lie dormant and infect connected equipment when nobody expects. You have been warned. Watch the video link at the end of this article to see an attack on maritime equipment in real time.

Cyber-attack is the current buzzword. It is known by some as an industry killer and even as the potential cause of the next world war, but thought by others to be a myth. So where does the maritime industry stand in all of this?

In the main, but certainly not universally, the maritime industry has a dismal record in its slow and painful transition from paper and analogue methods of operating shipping to new innovative technologies when compared to industry rivals like aviation. But why is this and how could it affect cyber security in the maritime arena? Or, have some seafarers not even evolved enough to be talking about it yet, let alone implementing new cyber procedures on board ship. We have all met that Captain who is nervous about the machines on his ship.

Whilst the maritime industry does not seem to have been strategically targeted in terms of the vessels themselves, there is now plenty of talk of accidental or naive seafarers accepting a generic phishing email that goes on to attack their computers.

Major corporations like Google and Yahoo have released statements stating that they were deliberately hacked. The question is what will be first for the

maritime industry, the deliberate or strategic hacking of an individual ship, or a shipping corporation as a whole?

There has been a call for cyber specialists to come and provide solutions to the very real potential dangers facing the industry that could not only damage reputations but cause disruption to trade worth billions of pounds. Not all is lost though, as long as we can move the industry forward to cope with the digital world we live in today.

Cyber Security was a hot topic in 2016 – but now we are in 2017 and the seafaring community are becoming more aware of what could potentially happen. There is a real threat of cyber activists starting to gain access to, and changing, sensitive ship's data from our onboard equipment and thereby disrupting a vessel's operation such as changing its route to cause a grounding or infiltrating the systems of a digitally controlled engine room and causing an alarm to remain mute whilst an engine fails, or even catches fire, due to a 'manual' override by the hacker.

With more and more companies looking for insight into how to stop attacks from occurring, the main area of concern is the lack of security awareness by both companies and employees as they have been taken aback by the swift rise in the level of threat to the industry from cyber security; almost non-existent just a few years ago to today's high alert. It is expected that shipping companies and independent vessels could be next on the list for major cybercrime activity as it is, as yet, mainly unexplored territory for hackers who are only now starting to realise its huge potential as a target. Attacks now have the capability to obtain sensitive ECDIS, AIS and GPS data, to name but a few, so it is vital that the correct procedures and processes are in place to prevent the worst from happening.

The scary part: 51% of US adults suffered some kind of data security incident between December 2015 and December 2016. In 2015 there were 781 reported major company data breaches in the US alone due to cyber-attacks which, combined, cost companies $400 billion. These are only the reported data breaches. Sadly, there is often an element of sweeping the issue under the carpet in all industries. So, this total will continue to rise if the maritime industry, where the proportion of those of digital native age is far lower, does not adapt to ever changing technology and the major security threats it brings with it. Overall, the cost of cyber-attacks in 2019 is predicted to be a colossal $2.1 trillion.

The key issue, alongside a lack of awareness by employees and users of operating systems, is the development speed of technology. This digital age of

super computers, 4D printing and nanotechnology is like no other and is proving to be self-accelerating. That is to say one technology is put into operation while the next generation, more powerful and innovative, is being produced, thereby creating an always expanding, developing and aggressive cycle. But, due to the speed of production, this process can lead to an unstable, insecure and untrustworthy platform, as it is not able to keep up with ever changing threats.

After years of this development, technology companies are starting to adapt to this issue by trying to manage security flaws within the software by developing and applying software updates weekly, while changes to future developments can help manage the constantly increasing cyber-crime threat; until the next global threat takes place or takes over.

Some maritime software manufacturers have used a physical security method of locking out their systems in order to intercept physical security threats altogether. However, ironically, this increases the complexity of applying security software updates. This restriction can complicate a shipping company's decision to have an integrated bridge system due to issues with synchronisation and communication between different software manufacturers. This can also mean that only specialised engineers and trained software technicians are allowed to apply updates, thereby causing additional issues. Restrictions like these could mean that your system is 80% more susceptible to cyber threats.

First off, the solution is simple; but it will cost you, which no one likes unless it is absolutely necessary and unavoidable. Some companies feel that cyber security is important enough to invest in. Nevertheless, you will watch multiple companies become complacent and unconcerned about the real threat in the water, until it becomes a reality, and their organisation comes grinding to a halt.

In reality, if you spend as much on coffee as you do on cyber security measures, you will be hacked. It is alleged that almost every company in the world has already been hacked, or if not, will be soon. The Director of the FBI, James Comey, had the following to say on Chinese hackers: '*There are two kinds of big companies in the United States. There are those who have been hacked by the Chinese and those who don't know they've been hacked by the Chinese*.'

This is the world as it is and therefore we need to change with it, not be ten steps behind.

First, we know the industry is struggling from sector to sector, but cyber-attacks will only make it worse, so the first move is to ensure that everybody is educated in cyber security awareness. Preferably starting from the top and

working down so the entire seafaring community can spot a cyber-attack and know what action to take in response.

Experienced educational companies exist that offer in-depth, classroom-based courses in the subject of cyber security. ECDIS Ltd. also offers the first maritime-based cyber security awareness course with the aim of bringing the industry up to speed. Elements of all the company's BTM*, BRM** and even ECDIS courses now include cyber-attack prevention and awareness modules.

Countless companies are missing the correct procedures when it comes to security. A robust IT security policy is highly recommended, as this allows employees and users of all IT equipment to be clear as to how company data and information should be used on IT equipment. It is not just small companies either that struggle in this war against cyber activists. Large corporations are also at major exposure risk, primarily due to not having a dedicated IT and security team.

It is recommended that a company appoints a cyber security chief to implement and respond to all cyber security related issues or system flaws that may be found. This is so that one person has ultimate responsibility for implementing and maintaining all cyber security measures within the company thus ensuring consistency of approach.

Cyber security attacks are incorrectly thought of as attacks that occur just over the internet due to the wrong security measures being taken. However, lack of physical security can also be a major factor in incidents of industry changing attacks.

During the 20th century a majority of attacks occurred due to people not taking the correct measures to keep IT equipment safe, another reason why we need everyone to be aware of what is coming. It really is as easy as someone coming into your reception and asking you to print off a copy of their CV from a USB stick, which is actually infected with multiple viruses. This could ultimately allow someone else to have complete control of your business's entire network and thereby, most likely, destroy it.

In summary, cyber security is not an issue that we can ignore. It may not yet be heard of as providing a direct threat toward our vessels, but this will come in time when noticed by any cybercrime activists who either want to damage the industry or cause major damage to infrastructure or even human life. It can be averted.

Many, if not all, shipping companies have some form of internal networked server that allows all of their computers to communicate and send and save files between them and, therefore, also connect to the internet. So, with the improper procedures in place, it could be easy for anyone keen to infect an auxiliary piece of equipment that connects to a primary equipment. Think of the random software updates that happen every day, for example to an engine room sensor test, or to the bridge's digital anemometer, that may appear non-safety critical, but they are connected to safety critical systems. We often concentrate and develop robust procedures purely for the few safety critical pieces of equipment, but the attack will take place on a tertiary system that is connected to it.

Readers may be interested in watching the YouTube clip below to see a live attack on standard maritime equipment: https://www.youtube.com/watch?v=kigKU6eEpOQ

*BTM Bridge Team Management.
** BRM Bridge Resource Management.