innovations

Focusing on innovation in the global cruise industry

Cyber security - is the cruise industry ready?

Special Report

International Cruise Ship Industry

INTERNATIONAL
CRUISE SHIP
INDUSTRY
Focusing on innovation in the global cruise industry
www.cruise-ship-industry.com

At the beginning of this year, the major cruise industry associations jointly issued a set of guidelines on cyber security on board ships.

Conor Byrne

Predominantly aimed at raising awareness of the risks and offering guidance on assessing operations, many cruise companies are having to revisit, or in many cases develop, their methods for preventing security breaches. And with good reason, as the threat of cyber attacks has undoubtedly increased in this ever more connected world, said Conor Byrne, Director, ICE ICT, the author of this article.

Cruise ships are under increasing pressure to keep customers connected throughout their journeys across the seas. This means a constant flow of information and wi-fi systems being accessed by a deluge of different devices at any given time. Naturally the more devices and people accessing data, the higher the risk on board.

What is a cyber threat?

Every device that is connected to a network, whether private or public, is open to attack by a cyber criminal. Devices can mean the phones and tablets your passengers are using to check their emails, etc, but it can equally mean software, or even completely virtual.

The UK Government estimates the cost of cyber crime for the financial year 2015/16 as £21 bill to business, of which £9.2 bill involves the loss of IP. In the same period, it estimates cyber crime costs the Government £2.2 bill and citizens a total of £3.1 bill.

When you bear in mind that the National Fraud Intelligence Bureau believes that only 1% of all fraud attempts are reported, the impact is clearly huge.

When it comes to the cruise industry, there are three very different areas for concern. One is about cyber security threats against your company, with hackers accessing your data, the second is threats to customers on board your ships and finally is the threat to the ship's control systems.

The motivations for a cyber attack can vary, but normally a cyber criminal will be looking to do one of three things:

1) Extort,

2) Steal,

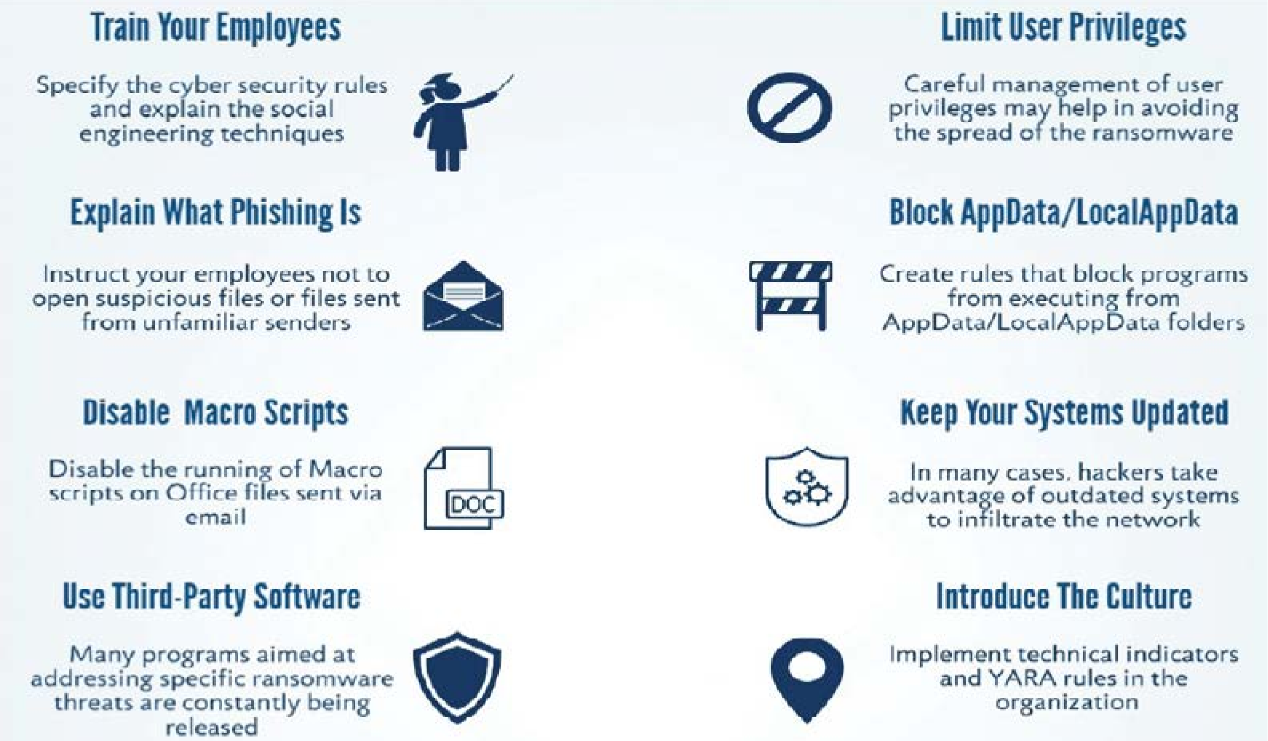
3) Control.

Extort - These cyber attacks are most commonly in the form of Ransomware attacks and Crypto Locker viruses. A victim's files will get encrypted and the attacker will demand money to unlock them.

Steal - This type of attack is the most widely reported, with bank account or credit card details stolen and used to carry out false transactions. Phishing emails are getting all the more sophisticated and it is becoming all too easy for people to accidentally fall victim to this type of attack.

Control - Control is probably the most serious threat. It has not yet gathered momentum, however, I believe we will see a prolific rise in attacks of this nature and the consequences could be extremely serious for every type of company.

For the cruise industry, it is especially a concern given the fact that ships are by their very nature an isolated network of control devices and information technology. If an attacker were to gain control of a ship, the consequences would undoubtedly be extremely serious.



Train Your Employees

Specify the cyber security rules and explain the social engineering techniques

Explain What Phishing Is

Instruct your employees not to open suspicious files or files sent from unfamiliar senders

Disable Macro Scripts

Disable the running of Macro scripts on Office files sent via email

Use Third-Party Software

Many programs aimed at addressing specific ransomware threats are constantly being released

Limit User Privileges

Careful management of user privileges may help in avoiding the spread of the ransomware

Block AppData/LocalAppData

Create rules that block programs from executing from AppData/LocalAppData folders

Keep Your Systems Updated

In many cases, hackers take advantage of outdated systems to infiltrate the network

Introduce The Culture

Implement technical indicators and YARA rules in the organization

Why care?

Consumer expectation means that cruise ships need to offer decent connectivity to compete in an ever-more connected world. Naturally, the ship itself also needs to stay connected, relying heavily on the connection for power management, vessel management, emergency shut down, HVAC, Navigation, etc.

These are all interconnected and remotely connected for monitoring purposes. Therefore, reducing connectivity is simply not an option, yet that very connectivity drastically increases the risk of a cyber attack.

The consequences of a cyber attack for a cruise ship would be extremely detrimental. Imagine the control scenario for example and the mass devastation that could be caused by taking control of a ship to hold it to ransom, or even cause a crash to create mayhem.

Most control systems' manufacturers are working hard to reduce the risks on the new 'Smart' ships, however, the main issues will be with older technology that does not have anywhere near the intelligence to detect and block attack that modern equipment has.

That said, very old ships are probably more secure than modern ones, as they just don't have these remotely controllable devices on board.

Cyber attacks against you as a company generally either take the form of access to your customer database, where hackers will access personal customer information, or on commercially sensitive data. Naturally, this can have a major effect on your business as it can be data that the competition can use to its advantage. It will also be likely to affect your share price if leaked, as well as often attracting a great deal of media attention.

Passengers and employees alike are also susceptible to the other types of cyber crimes. On a cruise ship there are a great deal of credit card details stored in the on board property management systems, along with the numerous credit card transactions, which take place on board ferries, registered throughout various point-of-sale locations, such as in shops, bars, and restaurants. In both these environments, even with PCI compliance, the POS devices or the PMS solutions are still open to attack.

The most common breach however, is caused by someone with legitimate access to data allowing it to fall into the wrong hands, either by sending something to the wrong person, often accidentally, or by misplacing a phone or laptop on board. Imagine the impact if they were to suffer an attack through your ship's network whilst on board. As well as the consequence for the individuals affected, there would undoubtedly be a massive impact for the cruise company in terms of negative publicity and a potential loss in revenue or even a direct cost in damages.

Imagine also if someone were to open a virus whilst on your network. There is a potential that the virus could then spread through the network and affect numerous other connected passengers.

Cyber Protection

Cyber attacks are increasingly an inevitability. However, there are measures that can be taken to drastically reduce the risk. Although it can seem daunting, it is absolutely critical that cruise companies take these steps in order to protect themselves as much as possible.

There are a number of important steps to achieve this:

1) Instigate common sense education for your employees on, for example:

a. How to spot a phishing cyber attack. According to a recent survey in the UK, nearly 60% of office workers receive phishing emails every day, however 27% don't know what phishing is.

b. Importance of changing passwords.

c. Importance of logging off.

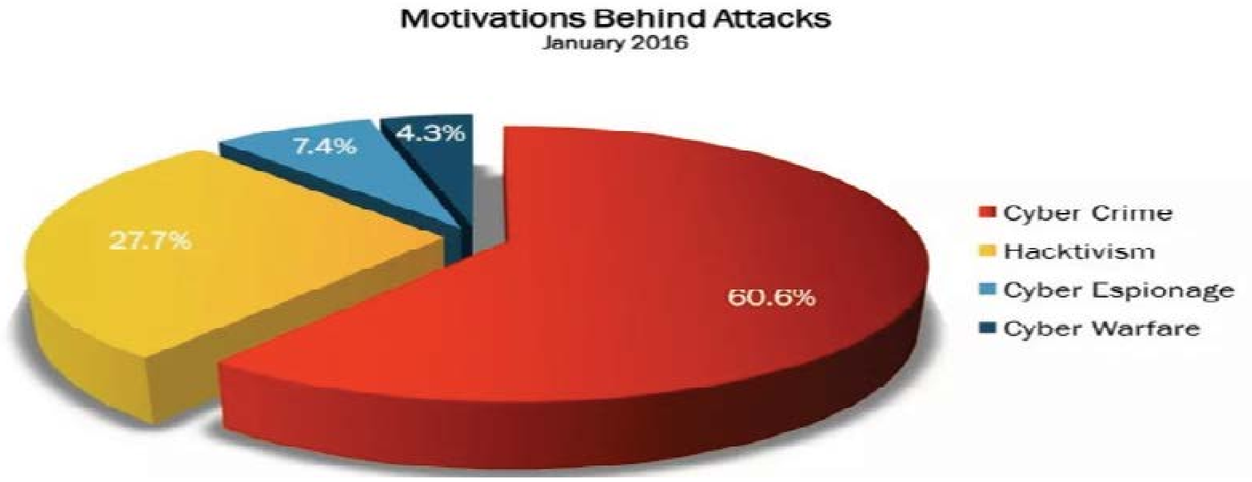
d. "read twice, send once" – make sure the email is going to the intended recipient.

2) Implement ISO27001 framework and standards.

The ISO 27001 framework can seem a bit of overkill but it is a good guide to lead you through the mire that is cyber security. It also includes a number of simple measures, such as:

a. Ensuring you have proper administration for your entire IT system. It should have role-based data access to ensure the right people within your organisation can only access the relevant information and data for them.

b. Setting up all equipment with strong password and encryption systems, including regular enforced password renewal.



c. Educating your workforce in identifying cyber attacks.

3) Educate your passengers by way of posters or information they should read when logging onto the network.

4) Harden your perimeter using penetration testing and other simulated cyber attacks. For this it is important to use experts.

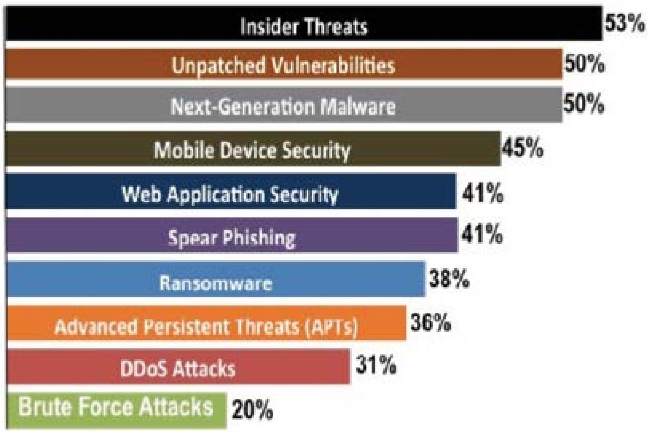
Get good advice and be aware that your IT guys are not generally experts in cyber threats. Indeed, in many cases they will have confidence in the security of what they built and will not admit that it may have vulnerabilities, which can lead to an extremely dangerous situation.

Whilst these steps will drastically reduce the risk, when talking about cyber attacks, it is not a question of "if it happens", it is more "when it happens." Cyber crime is inevitable and growing and you will at some point fall victim to it. So, as well as putting those things in place, it is also vital to know what you will do when it happens.

Putting an Incident Response Strategy in place will ensure you are ready for whatever a cyber attack may throw at you. Interestingly, whilst most companies have Business Continuity Plans in place in case of disaster, they very often don't deal with cyber security disaster.

Collaboration

There is no denying that cyber security is a massive challenge across the globe, none more so that in the cruise industry. Getting expert help and advice is vital. There is a lot of support out there, so make use of it.



At ICE ICT, we are also working with other experts and have built a consortium of specialist companies who have taken up the mantle to fight cyber attacks in the maritime industry. The group is named KOMPIRA* and the 'Identify, Educate, Detect, Protect' mission statement is supported by the consortium members whose collective skill sets and experience provide a holistic pro-active cyber security strategy.

KOMPIRA is working with Government security services, university centres of cyber excellence, police forces and the maritime community. Initiatives such as this will be crucial to resist the cyber criminals and reduce the risks for all.

*KOMPIRA – The Japanese God of Seafarers.