Lisa Forte, Cyber Protect Officer for the Police Cyber Crime Unit in the UK speaks to MAST on key cyber threats to the maritime industry

Lisa Forte, a Cyber Protect Officer for the Police Cyber Crime Unit in the UK is onboard with MAST's cyber awareness campaign. Lisa comments and advises on 2 key threats and the fundamentals of protecting from cyber-attacks. This article follows on from MAST's recent co-presenting on maritime cyber security with Shipowners P&I Club. A link to the webinar can be found below the article.

Tackling the cyber threats to the maritime sector

There's a plethora of information on the cyber threat to the maritime industry. It is argued that attackers could take over your guidance and positioning systems and steer your ship wherever they want. Or that attackers could hold your port to ransom by stopping all your automated processes. This is all true, and some of these complicated attacks may have already happened in some limited cases. Whilst you should devote time and attention to mitigating these potential threats, a risk assessment of the cyber landscape shows that we need to focus on the real cyber-crimes that are happening right here, right now. In my role I see the same attacks used across all industry sectors. The majority of cyber threats are indiscriminate. They don't care if you are an orthodontist or an oil carrier. As long as you have money and you have internet connected devices then you are a target.

In this article I am going to talk about two threats that you should have on your radar.

Ransomware

Ransomware attacks target companies of all shapes, sizes and locations. It encrypts your data making it unreadable and the perpetrator then demands money to release it. The most common way that it gets onto your systems is via links or attachments in emails. These emails are getting increasingly believable and difficult to spot.

What are the solutions?

1. Don't let the emails reach your users in the first place. Using methods like the DMARC protocol and having strict rules on your email filters is a great start. Staff training to spot these emails is also money well spent.
2. *"Backup early, backup often".* This is the best way to mitigate the impact of ransomware. If you have a backup you can hopefully restore all your files.
3. Plan for the worst. Even with backups you are looking at some downtime. Companies that have a business continuity plan in place for a cyber-attack are far more likely to survive an incident.

Working for law enforcement I would never advocate paying the ransom, you may not get your data back or it may be corrupted. Paying a ransom also increases the chance of being added to a list of "companies that pay" causing you to be hit again.

Insider Threat and Data Exfiltration

Do you know exactly what data you hold and where that data is located? Who can access it? One thing I see time and time again with cases that involve data exfiltration is that the staff (and directors) have way too much access. In maritime this applies both in the office and onboard your vessels. Frequently when people move roles they end up accumulating permissions to access files. This is a bad idea. Imagine that you are an attacker. You identify a target shipping company and prepare to break into their systems, grab their sensitive data and make some money. You find an account for an employee, you brute force his password and enter the network. Your next step would normally be to escalate his account permissions to access desirable files. This could take some time. Luckily this employee has access to every file, folder and system. That has just made your job much easier! Employee permissions are like keys, not everyone needs access to everything. Speak to your IT team about having a permissions audit done.

Another aspect of data exfiltration is insider threat. In the UK and the USA it is now unusual for departing employees not to steal anything when they leave - even if they are not disgruntled. If your employees can access everything they could steal everything. Another reason to go back and check the limitations on everyone's accounts! You can buy a 64GB USB stick for £20 which will store nearly 200,000 documents. That's a lot of critical information! Train

your employees to report suspicious behaviour of other staff and check unusual activities on employee accounts, should Kevin really be working from home on at 2am on a Sunday?

The fact is that you will never stop all attackers. Like with any crime, a lot of attackers will move on if the attack isn't straightforward and almost automated.

Cyber-crime is a serious threat to shipping. It is important to stay up to date with current threats, train your staff and have a plan for the attacks you are most likely to experience.

Lisa Forte is a Cyber Protect Officer for the Police Cyber Crime Unit in the UK. For any questions or to request any further guidance email lisa.forte@avonandsomerset.pnn.police.uk or https://www.linkedin.com/in/lisa-forte/

Shipowners P&I Club cyber security webinar co-hosted by MAST. To watch the recording follow this link: https://www.shipownersclub.com/shipowners-pi-club-hosts-maritime-security-webinar-recording-available/