Cyber Crime and the Shipping Industry

Modern Shipping is under threat from non-traditional risks.

With the international shipping industry estimated to carry over 90 percent of today's world trade, the temptation for criminals has never been greater. Savvy criminals around the globe are exploiting cyber vulnerabilities to perpetrate a wide range of crimes — from longstanding physical ship-related dangers like piracy and smuggling to more recent financial-related frauds like the diversion of payments.

The challenge for ship owners is even more complex because cyber criminals are targeting diverse facets of the shipping industry. For example, there was a well-documented case of drug smugglers subverting an IT system at a major port in order to facilitate the smuggling of contraband in containers.

The rise of targeted piracy and drug smuggling reflects how criminal organizations have become more sophisticated. They will seek detailed intelligence on potential targets and will use modern technology to source information and data to assist in their planning and execution of criminal ventures. Drug traffickers, drug and people smugglers, pirates and fraudsters of all stripes are taking every opportunity to gain information that they can turn to their advantage.

While shipping and logistics companies are expert at maritime transport, they may not have the same experience with IT security. It will be essential to invest time, effort and capital into security measures to ensure these cyber risks are appropriately managed. Companies leave themselves open to great danger when they do not take into account all the potential risks and loopholes when designing and implementing their company-wide cyber security strategy.

Risks posed by technology

Over the past five decades, computer controls have been integrated into innumerable operational and business processes across diverse industries, including the shipping industry, resulting in considerable improvements in safety, accuracy and profitability. There is another side to the digital revolution, however, and in the absence of appropriate protection and loss prevention measures, the increased reliance on technology for even the most basic operations can leave a business exposed to business interruption or, in a worst-case scenario, continuity failure.

Cyber security threats today are increasing in variety, frequency and sophistication — be it from a Trojan USB stick that introduces malware aimed at acquiring sensitive commercial information… an email with detailed vessel itineraries sent to a large group of unknown people… the full-scale subverting of a company's IT system… or the potential compromising of Automatic Identification System (AIS) and Electronic Chart Display and Information System (ECDIS) systems on board ships. The number of potential risk scenarios is significant and keeps growing. Fraudsters employ whatever hacking technology works, often tailored to specific targets of opportunity.

Some organizations may be more at risk than others depending on the type and value of data they store. However, experience has shown that hackers will generally gravitate toward the low-hanging fruit of victim networks that are more easily breached. As such, it is essential that companies prepare for, and expeditiously address identified vulnerabilities.

Dangers to Shipping can come in many different shapes.

Risks posed by insiders – carelessness or intentional?

The internal cyber threat is also significant and should not be underestimated, making it urgent for companies to be fully aware of what information they have on their systems, who has access to it, who is accessing it and why. A recent Kroll analysis of client cyber cases across all industries found that 51 percent of breaches were tied to insiders. In many cases, these were not solely malicious people with a company axe to grind, although they are often part of the problem. Employees with the best of intentions may still be careless; data is mishandled and files are disposed of improperly. And even the most sophisticated employees can be tricked into divulging confidential information or authorizing what turns out to be a fraudulent disbursement.

Employees or business associates can also be duped into revealing key information. The most common tactics are phishing or spearfishing emails. The goal is to get victims to open attachments or click on links in an email. While the phishing approach is more scattershot, spear phishing generally focuses on specific people within an organization. Attackers might comb social media sites such as LinkedIn or Facebook to impersonate senders who are either well-known to recipients or otherwise considered trustworthy. Once the victim opens the attachment or clicks on the link, the sender is free to introduce malware, ransomware or key loggers or gain credentials to access confidential information.

While the idea of outsiders taking over critical operational controls may keep management up at night, employees or other insiders like contractors and suppliers often pose a more immediate and equally serious risk. Whether they are negligent, malicious, or unwitting accomplices in a fraudster's scheme, insiders can be the conduit for information coveted by criminals.

Bribery and extortion are other ways that criminals can get insiders to acquire and pass on information that is essential for protecting the safety of the crew and cargo. Disgruntled workers can also betray valuable data for spite or money. A typical internal fraudster's traits may or may not be spotted by the trained eye — e.g., previous offenses, a gambling addiction or financial problems.

Risks in Shipping

Be it a problem on the shore side or on board the vessel, shipping companies may be vulnerable to data theft, fraud and even pirate attack if key personnel carelessly or deliberately act against the company's interest. Following numerous piracy attacks in West Africa as well as South Asia, it has become increasingly clear that some incidents may have been facilitated or assisted by persons who are meant to work for the ship-owner. Organizations such as ReCAAP have started to warn about the risk of crew involvement. Additionally there has been a reported incident of an Insider on the shore side assisting in an attempt to divert freight payments to illegitimate bank account details through apparently "legitimate" emails appearing to originate from the ship-owner to counterparties.

HOT TIP : The humble and traditional telephone : it is an important tool against Fraud.

Skuld P&I Club has found on a number of occasions that frauds could have been detected and perhaps even prevented if a simple phone call had been made to verify the details of a purported legitimate email message.

Good staff training against fraud includes awareness of how useful it can be to make that call and check out the alleged contact.

Combine its use with a rigorous countercheck policy.

How to guard against the risk

There are warning signs that an employee might be committing cyber crime. Some of these signs include working odd hours without authorization; disregarding company policies about installing personal software or hardware; taking short trips to foreign countries for unexplained reasons; buying things they can't afford; and taking proprietary or other information home in hard copy form and/or on thumb drives, computer disks, or email.

However, you can't let your guard down when an employee leaves the company, voluntarily or involuntarily. Strict termination procedures should be in place to ensure that all network access privileges are terminated immediately.

Likewise, just as a company employs security guards to monitor the parameter of a building, check IDs, log who enters and leaves, and watch security monitors, or on board a vessel implement the ISPS Code regulations, the same precautions should be taken for data. For example, if an employee is logged in from her work computer and the same credentials are used to log in from an external location, a red flag should immediately appear.

Likewise, if an employee is uploading or downloading a large amount of data for the first time, those responsible for data security should be alerted.

Other recommendations include:

1. **Educate staff about the need for IT and information security.** Develop guidelines for the use of email and safe custody of sensitive information. Consider who actually needs to be copied in to emails and who should have vessel itineraries. Also, where possible, avoid sending messages to third party "group email" addresses.

2. **Establish clear guidelines on the custody of key information.** Pirates and smugglers often appear to act on the basis of precise information as to vessel movements and cargo on board.

3. **Integrate elements of both physical and logic security to protect your data**. These should also be fully integrated into business continuity/disaster recovery plans and regular staff training.

4. **Secure your supply chain.** Suppliers and contractors are a risk because often, they have intimate knowledge of your operations as well as access to key information systems. Alternatively, they can unwittingly introduce malware where their systems intersect with yours.

5. **Establish the extent of insurance required** so that your business has specific cyber coverage if required. This may include cover for business interruption and increased costs incurred as a result of any cyber crime event. The use of a third party insurer is one way to mitigate against the financial impact of cyber crime.

6. **Conduct a cyber-risk assessment.** Engage a qualified expert to conduct penetration testing and a thorough review of security protocols to determine what kind of data you hold; where that data is and where it goes; and what processes are utilized and why. Of the hundreds of such risk assessments Kroll has conducted, there has never been one in which security measures could not be improved.

7. **Establish continuous digital monitoring** so that your information technology staff — in conjunction with your teams in legal, operations, marketing, finance, etc. — will know what is going on in your networks at all times. In the event your system is compromised, this will help isolate exactly what happened and when, which in turn will aid in recovery efforts.

8. **Work with partners who have knowledge of the risk landscape.** It is not enough to take all precautions for current risks; you must also keep up with emerging threats and situations. While you might consider hiring dedicated staff to monitor emerging threats, this can prove not only costly, but also ineffective simply because these resources tend to get compartmentalized or “silo-ed,” such that certain risks can fly under the radar.

9. **Integrate data security/cyber risk with cyber policies** and breach response and preparedness plans. The simple fact is that no one is immune to an attack. Unfortunately, without a preparedness plan, decisions can be made that inadvertently compromise evidence and make your job immeasurably harder

when trying to resolve matters. These plans should be constantly evolving and rigorously tested.

10. **Be actively involved with local law enforcement.** This will give your IT team and management an opportunity to engage with law enforcement outside of an event and learn more about current and emerging risks as well as best practices to combat them.

What to do when fraud is suspected

Whether it stems from a disgruntled employee, a mole planted by an organized crime gang or a sophisticated hacker, when an information security issue is discovered, the proper response depends on first ascertaining:

- When did the security breach occur? Is it still happening?
- Where did it originate — internally or externally?
- How and why did the incident occur? For example, did a malicious intruder exploit network access privileges to steal your data for financial gain, or did an employee accidentally disclose sensitive information via email?
- What was compromised — intellectual property, personal data, network operations, etc.?

To avoid spreading malware throughout the network or destroying the trail of evidence, the organization and its IT department should not try to “fix” a suspected problem on their own without the assistance of experts. Experienced cyber security investigators are skilled in conducting interviews and retracing the behavior of people who had access to protected information. Likewise, computer forensics and data recovery specialists help ensure no digital evidence is overlooked and assist at any stage of a digital forensics investigation or litigation.

Because time is of the essence when a breach is uncovered or suspected, establishing a relationship with an incident partner before a cyber attack occurs ensures you will have the experts of choice available to respond immediately to your situation.

Conclusion

Whether large or small, specialist or global player, everyone in the shipping industry will benefit from a greater awareness and preparedness to deal with the challenges of modern IT-assisted fraud in the 21 century.

Clouds on the Horizon, Singapore East Anchorage

By

Colum Bancroft is a Managing Director of Greater China, based in Hong Kong. Colum has extensive experience assisting clients on local and multijurisdictional issues in areas such as asset-tracing and recovery; family, partnership, shareholder, and other business disputes; anti-money laundering; and fraud and corruption investigations. Having lived in Asia for more than 20 years, he has a strong understanding of the Greater China market, and has advised clients across a multitude of industries including shipping and logistics, construction and manufacturing; property development; technology; financial and professional services; hospitality and leisure and more.

Kroll is the leading global provider of risk solutions. For more than 40 years, Kroll has helped clients make confident risk management decisions about people, assets, operations, and security through a wide range of investigations, due diligence and compliance, cyber security, physical and operational security, and data and information management services. Headquartered in New York with more than 55 offices across 26 countries, Kroll has a multidisciplinary team of nearly 2,300. For more information, visit kroll.com

Visual Material Source : Skuld

For further information, Members are asked to contact the Association: lossprevention@skuld.com

Christian Ott

Vice President Head of Claims, Skuld Singapore Branch

Loss Prevention and Recurring Claims Team Leader