Cyber Insurance Protection for the Logistics Industry

The participants within the logistics industry have an increasing reliance on networks, cloud technology and computing systems which is exposing many to new and emerging threats.

The media is full of stories about many large businesses with household names, government departments and agencies, and SMEs succumbing to cyber breaches.

Logistics businesses are no different, they are not immune. If your business is connected to the internet, you are vulnerable to a cyber-attack. What would your business do if it was exposed to a denial-of-service attack, hacking of cargo/order tracking software or web-based warehouse management systems?

A cyber-attack could cost your business more than money. It could also threaten your intellectual property and put your customers' personal information at risk, which could severely damage your reputation.

Logistics operators should not be lulled into a false sense of security because they might be smaller businesses than say multinational carriers and therefore of little or no interest to cyber criminals. The unfortunate fact is that cyber criminals will target any business and seek vulnerabilities within their Information Technology infrastructure and exploit those weaknesses.

To highlight the issues arising from a cyber-attack, we offer the following real life case study.

MAZE Cyber-attack impacts freight-forwarding business*

The business involved in this cyber-attack is a multi-generational family run logistics business. It is largely Australian based, deriving most of its revenue from Australia, however, a small proportion of income (sub 5%) is derived from overseas.

In March 2020 the forwarder was subject to a "MAZE" ransomware attack. MAZE not only encrypts and locks down data, it also exfiltrates data, that is, copies and transfers the data to another location. A significant amount of data was exfiltrated (stolen) during this attack, around 460 gigabytes.

The perpetrators threatened to release a tranche of stolen data, and in fact published (released) 400 gigabytes.

This had a global impact for the forwarder, where numerous jurisdictions were required to be notified, including four supervisory authorities in Germany, plus relevant authorities in the UK, Sweden, Poland, Netherlands & France. In all, 10 territories were contacted.

The perpetrators were not engaged (ie no ransom was negotiated or paid) because the forwarder kept very good backups, which enabled them to become operational soon after the attack.

The forwarder's insurers immediately engaged IT forensic specialists, which allowed for instantaneous containment of the ongoing attack.

Given the aspects surrounding the stolen and published data, there were legal and privacy obligations which required significant notifications throughout Australia & overseas. This is particularly relevant with respect to the European obligations under the General Data Protection Regulation (GDPR) and the onerous reporting timeframes and penalties which can flow from not adequately responding to these obligations.

To help facilitate the GDPR response, the forwarder's insurers engaged specialist lawyers with extensive GDPR experience.

Finally, this attack generated significant media attention on the business and public relations experts were engaged by insurers to provide proactive public relations strategies.

You will note that the forwarder's insurers responded by engaging and paying for a number of specialists to assist the business at a time when it was most vulnerable.

Key takeaways from this case study:

- Keep good backups – this minimises downtime & reduces business interruption impacts;
- Data cataloguing & retention polices – understand what data the business is keeping & where it is being kept. Also develop data deletion policies for data which is no longer required;
- Overseas legal/privacy obligations – be aware if the business might be impacted. This is particularly relevant for logistics businesses where trading is undertaken overseas. There is also Australian based privacy legislation which also may be applicable;
- The quicker the incident response, the better the outcome – have in place and test a cyber incident response plan;
- Use the right incident response specialists – to move quickly to resolve issues;
- Have a proactive Public Relations strategy in place – this will manage media attention for stakeholder relationships quickly & effectively.

Why not take the opportunity to review your controls and cyber security incident response plan, which should include intrusion detection testing and gathering potential threat intelligence.

Are you confident your business would survive if it suffered a similar (or worse) cyber-attack?

Maybe not?

Cyber protection insurance is designed to help protect your business from the financial impact of computer hacking &/or data breaches.

That's why we recommend that logistics businesses consider arranging Cyber insurance coverage. Quality Cyber insurance policies are designed to help protect your business (including staff working remotely) from the financial impact of computer hacking &/or data breaches. If a cyber event emanates from a computer, laptop or other device being used at work (or at home), these policies will respond to cover the cyber event, response costs, public relations costs and any potential litigation which may arise.

There may also be business interruption issues because systems and networks may be down, meaning employees can't trade or continue with their day-to-day work.

Further, there may be contingent business interruption issues where the business's customer may be affected by a cyber event which impacts upon revenues.

These policies also include 24/7 specialist incident response teams, which is akin to Information Technology "roadside assistance" and a valuable resource in a time of crisis when urgent support is required.

Logical works closely with those businesses within the logistics industry to help them understand the unique risks they face, and work to develop a tailored risk management program to mitigate exposures and enhance cyber insurance coverage to ensure appropriate protection.

*With thanks to Emergence Insurance

Cyber insurance landscape – 2021 in Review

Last year was a stark reminder that hackers are pivoting (and succeeding) in deploying new attack strategies. There is clear evidence that they now favour targets in the supply chain industry that could provide a gateway to multiples of additional victims across numerous jurisdictions & territories, providing efficiencies to their methods. There were a wide variety of victims within the logistics industry, including ports & terminals, shipping lines, freight forwarders and transport companies. Threat actors have found this vast system of international interdependencies to be fertile hunting grounds as is demonstrated by the above case study.

Ransomware attacks continued to ravage the bottom lines of both their victims and insurance companies. Increased payment amounts may be due, at least in part, to the fact that hackers now routinely threaten to publicise their victim's most sensitive data if their six and seven figure ransom demands are not met. However, extortion payments are just one piece of the cyber claims puzzle. The latest studies have revealed that over the past year the average downtime from a ransomware attack was 23 days with average business interruption losses and other costs increasing from AUD1.1m to AUD2.6m in 2021.

What Does this mean Moving Forward?

Continued caution from cyber insurers with premiums increasing across the board, regardless of the industry sectors or size of the organisation. Organisations with best-in-class cyber security saw 50% plus premium increases in some cases. Others that lacked specific data security controls saw premiums as high as plus 100% to 300%, if they were able to arrange quotations at all. It was noted that some cyber underwriters are moving away from specific industries, including transport & logistics.

Many insurers imposed sublimits and other provisions specific to ransomware claims, which often resulted in limiting coverage to 50% of the policy limit or less. Some insurers are adding exclusionary language to specific known vulnerabilities and failure to remediate these could lead to a denial of coverage for losses attributed to them.

Whilst there were no reports of mass exodus of insurers from the market, there were clear indicators that insurers want to limit their exposure through limiting capacity. The policy limits offered during prior renewals were routinely cut to half of that amount during the 2021 renewal cycle.

As part of the growing underwriting discipline by cyber insurers, almost all asked for more details around data security control efforts. Not surprisingly, many questions focused on ransomware prevention and mitigation, with several insurers requiring ransomware supplemental applications consisting of dozens of questions to see how well organisations managed this threat.

Against this background organisations will need to understand and prepare for some uncertainty in the 2022 cyber insurance marketplace. Some organisations will likely struggle more than others, including those within the transport & logistics industry. There is little doubt that we will see a continued disciplined underwriting approach that remains very focused on data security controls, with premiums continuing their upward trend. Logistics organisations need to be wary that premiums alone should not be the barometer by which they measure the hardness of the 2022 cyber insurance market. There is a need to maintain a wide field of view of other factors, including more restrictive coverage terms, mandatory sublimits and exclusionary language specific to certain global and widespread cyber incidents which will require careful consideration. Unfortunately, in some circumstances, there will be limited (or no) choice available, meaning organisations are either unable to arrange cover or have to take what they can get.

It is clear that as insurers become even more selective & vigilant in the organisations they choose to insure, those logistics businesses who have comprehensive cyber security strategies and plans in place will not only make themselves more attractive to insurers, but it will also ensure the business is better protected and therefore less likely to be impacted and affected by cyber-attacks or cyber-crimes.

It is our experience that no organisation wants to be hacked and have to rely solely on their insurer to get them back up and running.

Remember, doing the utmost to prevent a hack from ever occurring must always be the first line of defence.

Here are some tips which may assist protect your organisation and increase its security posture:

- Create a human firewall. That is, continued awareness and training programs for team members, including phishing & social engineering threats. This is probably the most effective way of preventing a cyber-attack;

- Understand and classify your information assets and the data held. Implement a data retention policy which avoids storing data too long and in insecure locations;

- Keep business critical systems up-to-date (including software & patches) to protect, prevent and recover from any suspicious behaviour. Take regular backups of critical data and regularly test data backups to ensure they are working correctly. Keep critical backups offline, ensuring they are segregated from & inaccessible to your network;

- Assess your organisation's material risk and vulnerabilities through performing regular cyber risk assessments;

- Test and regularly update incident and breach response plans;

- Protect your organisation's passwords. They must not be easy to guess. Consider using password managers;

- Utilise Multi-Factor Authentication (MFA) within your network to create a second wave of authentications;

- Beware of public Wi-Fi. Logging on to a public Wi-Fi is one of the easiest ways to get hacked. If your team members are working remotely, it is usually safer to use VPN services, or possibly even hot spotting from their mobile phones;

- Take care with buying Information Technology, particularly peripherals. For example, we understand that cheap cables for iPhone chargers have been found to contain malware, so it is usually best to go with store/manufacturer approved products;

- Leverage monitoring capabilities and ensure logs capture useful information for incident investigations;

- Establish rigorous and regular oversight for third party outsourced services, which includes assessing third party risks;

- Determine if the Privacy Act 1988 (Cth) covers your organisation which requires preparation, response and notification obligations for eligible data breaches. You can find out more by visiting the Office of the Australian Information Commissioner website here: OAIC - Notifiable Data Breaches Web Page. Your Information Technology providers may be able to offer further guidance in that regard;

- The Australian Signals Directorate has a dedicated website, the Australian Cyber Security Centre (ACSC), which contains very useful information & step-by-step guides to assist strengthen your organisation's cyber security posture. The ACSC website can be viewed here: ACSC Website. Your Information Technology providers may be able to offer further guidance in that regard;

- Consider arranging good quality Cyber insurance. Cyber insurance doesn't reduce the risk, however, it reduces the financial impact of a cyberattack and will help your organisation recover faster.

Finally, we share below some common cyber misconceptions:

- **“Our IT systems cannot be breached”** (If large multinational corporations can be breached, SMEs must be vulnerable)
- **“We don’t transact online, so we are not at risk”** (It’s not only about transacting online. It’s about being locked out of vital IT systems & networks)
- **“Our IT employees/consultants will take care of it”** (Unfortunately, most are not experts at dealing with cyber-crime)
- **“We don’t hold valuable data”** (Data may be held which is subject to the Privacy Act 1988 [Cth])
- **“Our data is safe in the cloud”** (If the cloud is compromised, then data will be impacted)

Disclaimer: This article is general in nature and is designed to provide helpful general guidance on some key issues relevant to this topic. It should not be relied on as legal advice. It does not cover everything that may be relevant to you and does not take into account your particular circumstances and you use it at your own risk. Logical Insurance Brokers specifically disclaims any liability, whether based in contract, tort, negligence or otherwise, for any direct, indirect, incidental, punitive, consequential or other damage arising out of or in any way connected with the use of or reliance on the content of this article. It is only current as at the date of release. You must ensure that you seek appropriate professional advice in relation to this topic as well as to the currency, accuracy and relevance of this material for you.