Cyber 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 truth 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 business 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 logistics business, 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 business kept very good backups, which enabled them to become operational soon after the attack.

The business'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 business'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 business'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;
- 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.

There may also 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

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

- Understand your information assets and the data held within;
- Assess your organisation's material risk and vulnerabilities through performing regular cyber risk assessments;
- Utilise Multi-Factor Authentication (MFA) or 2 Factor Authentication (2FA) within your network;
- Keep business critical systems up-to date take regular backups of critical data and regularly test data backups;
- Keep critical backups offline, ensuring they are segregated from & inaccessible to your network;
- Classify your information assets and third party arrangements;
- Test and regularly update incident and breach response plans;
- Leverage monitoring capabilities and ensure logs capture useful information for incident investigations;
- Established rigorous and regular oversight for third party outsourced services, which includes assessing third party risks;
- Continued awareness and training programs, including phishing & social engineering threats;
- Arrange good quality Cyber insurance.

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)
- **"Our data is safe in the cloud"** (If the cloud is compromised, then data will be impacted)

Logical Insurance Brokers is a
division of Insurance Logic Pty Ltd.
AFSL No: 237633
ABN: 44 002 859 252

t 02 9328 3322

e team@logicalinsurance.com.au
w www.logicalinsurance.com.au

Suite 21, Level 2, 8 Hill Street,
Surry Hills NSW 2010
PO Box 103
Darlinghurst NSW 1300