

Mitigating Cyber Risk in the Trucking Sector

Business Law | Corporate & Commercial | Corporate Law | Cybersecurity | Transportation and Logistics | Trucking

6 September 2023

As the transportation, logistics, and supply chain sectors increasingly shift towards the adoption of artificial intelligence, automation, and the implementation of digital infrastructures - which include connected technologies and cloud-based storage solutions - so too does the risk of cybersecurity attacks and breaches of privacy.

The transportation sector in particular carries a unique scope of what is termed “cyber risk” given the complex latticework of supply chain and logistics in which it operates. Ordinarily, this includes the multitude of actors, such as shippers, brokers, intermediaries, steamship lines, rail, and other carriers, to which they face pressures from and obligations to.

The risk is particularly enhanced for small businesses, who often lack the resources, training, and personnel when compared to their larger counterparts.

The cybersecurity of any business requires serious consideration, given the increasingly complex lines of attack used by modern attackers, as well as the potentially catastrophic consequences of an attack, which can include large extorted payouts, fatal reputational damage, and loss of customer and brand confidence, all of which affect without question can affect the bottom line.

An introduction, this article will focus on the two most common cyber attacks faced by business across the trucking sector, which can be categorized into the two following categories: (i) ransomware; and (ii) phishing.

Ransomware

As the name suggests, ransomware is an extortionary software designed to lock a user or organization access to their computers, servers, or devices. Ransomware locks these devices and demands a ransom payment in exchange for returned access.

Many affected businesses wrongfully believe that simply paying the ransom represents the path of least resistance when it comes to regaining access to their devices. This misconception lies at the root of the attack and only serves to improve its effectiveness.

In practice, a ransomware attack usually looks like an employee opening a seemingly harmless email or link contained within an email, with the user then being “locked out” followed by a message demanding payment in exchange for resumed access. These incidents are known as “single-extortion” attacks.

However, as is usually the case with crime, ransomware attacks have become increasingly complex, with some attackers implementing “double-extortion” (i.e. adding the threat of stealing a victim’s data and posting it online) or even “triple-extortion” (i.e. adds the additional threat of using the stolen data to attack or harass a business’s customers or business partners, which in this case, can include any number of entities along the supply chain)

Phishing

By contrast, phishing is a type of attack specifically geared towards the theft of sensitive personal or financial information.

Phishing messages usually take the form of an email, phone call, text message, or other form of message on a social media platform from an attacker who is posing as a reputable person (i.e. President or CEO of the business) or entity (i.e. bank, law firm, etc.), and tries to trick the user into clicking a malicious link or download malicious software (or malware, as it’s more commonly known), so as to entice the user to share sensitive information, such as a social security number, bank account number, or credit information.

Phishers often use public sources of information, such as LinkedIn Facebook, Twitter, and company directories to gather their target's personal details, work history, interests, and activities, which taken together are used to craft a highly targeted, believable message.

Preventing Cyber Attacks

Here are four simple steps a business can take to protect itself from cybersecurity breaches:

1. Consider hiring an accredited IT security professional

Hiring an IT security professional, preferably one with industry-recognized certifications (such as an Certified Information Security Manager, or "CISM"), who can assess risks, implement effective governance, and proactively respond to incidents, is a great first step to strengthening the digital front line.

2. Provide proper education and training to employees

Given that employees are the biggest risk factor, it is critical that they be provided with routine training with respect to identifying and reporting suspicious online activity.

With the workforce becoming increasingly remote, proper training becomes all the more important.

The culture and resources of a business are unique and so too should the training regimen be when it comes to cyber safety and risk prevention. However, it is generally recommended that routine training regimens include: the common techniques used by attackers, the typical characteristics of harmful or suspicious messages, the consequences of a breach, and how to properly report a suspicious incident when faced with one in real time. "Test breaches", as they are termed, are a particularly effective learning tool.

3. Know obligations should a breach occur

There is no strategy that is 100% effective in preventing a cyber breach. A business can do everything right and still fall victim to an attack.

As such, a business should have an emergency response plan in place, which includes an emergency contact list including insurers, legal counsel, and law enforcement authorities at the top of that list.

The *Personal Information Protection and Electronic Documents Act*, which applies trucking corporations and indeed to all private sector organizations across Canada, also makes it mandatory for organizations to do the following: report to the Privacy Commissioner of Canada any security breaches involving personal information which poses a real risk of significant harm to individuals; notify the affected individual(s) about those breaches; and to maintain records of all said breaches.

4. Get cybersecurity insurance

Cybersecurity insurance is designed to support and protect businesses from cyber risk.

Specifically, cybersecurity insurance can offer protection against financial losses caused by incidents such as phishing, online extortion, and identity theft.

Some insurers offer cyber insurance as an "add on" to an existing policy, but businesses are also generally able to purchase this coverage separately.

In many instances, cybersecurity insurance also offers the added benefit of providing coverage for network repair, legal claims, and even public relations services in some cases, to help rebuild trust from the customer base.

Cybersecurity insurance in today's digital marketplace is a must, no longer just a "nice to have". A PDF version is available to download [here](#).

(This blog is provided for educational purposes only, and does not necessarily reflect the views of Gardiner Roberts LLP).



Author



Jamal Rehman



Bay Adelaide Centre — East Tower
22 Adelaide Street West, Suite 3600
Toronto, ON M5H 4E3

Phone: 416.865.6600
Fax: 416.865.6636
contactGR@grllp.com