ROGERS INSURANCE LTD.

THE TOP 5

CYBER INSURANCE MYTHS DEBUNKED

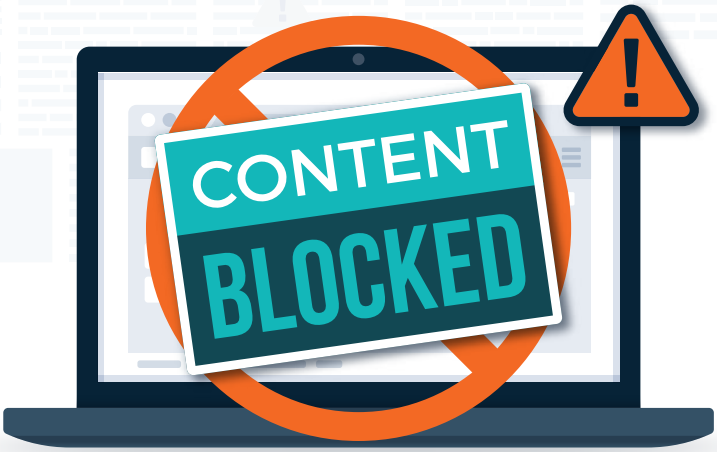
Cyber risk is one of the hottest topics in insurance. However, as it is still a relatively new and emerging concern, it can be made unnecessarily complex by industry jargons, buzzwords of the day, and a lack of standardization in policy wordings. As such, many companies find themselves confused about how cyber risk insurance actually works and are skeptical about whether it makes sense for their business to purchase a policy.

To clear up the confusion, here are five of the most common misunderstandings that businesses tend to have about cyber risk insurance and how to overcome them.

MYTH 1

"WE DON'T NEED CYBER INSURANCE. WE INVEST IN IT SECURITY..."

Vulnerability and Risk Are Two Different Things



This might be the single most common objection to purchasing a cyber risk insurance policy.

Heavily investing in IT security systems doesn't necessarily protect large corporations from cyberattacks.

While it is true that clients who invest heavily in IT security may be less vulnerable to certain types of cyberattack than organizations which invest very little, they still run the risk of exposure. Cyber threats are rapidly evolving, and cyber attackers find new ways to access networks every day.

Think of it this way, you have theft coverage on your home insurance policy even though you have high quality locks on your doors.

No amount of IT security can completely eliminate human error.

According to IBM, 95% of successful cyberattacks are incidents that occur as a result of a human error. Technology can reduce the possibility of an employee accidentally clicking on a malicious link in an email, but it can't eliminate that risk completely.

THE SHORT ANSWER

No matter how much a company invests in IT security, it will never be 100% secure. The purpose of an insurance policy is to respond in the event that the worst happens.

MYTH 2

"WE OUTSOURCE ALL OF OUR IT, SO WE DON'T HAVE AN EXPOSURE..."

Outsourcing Your IT Doesn't Eliminate Your Liability

Using a third party for IT might change your exposure, but it doesn't eliminate it.

Protecting clients' personal data is always the sole responsibility of the organization entrusted with the data, not a hired third party.

Outsourcing your organization's data storage to a third party doesn't eliminate your responsibility for your clients' private data in case of a confidentiality breach. As the party entrusted with clients' data, your organization bears full responsibility for all the regulatory actions that may arise as a result of the data breach. To avoid the detrimental effect of such actions on your company's finances and reputation, you must ensure that the service contract you sign with the third party IT provider clearly states that the hired service is required to indemnify you (the customer) the cost of loss of or liability for compromised data in case of a data breach.

Organizations' critical business operations can suffer as a result of a third party system failure.

Many businesses rely on third parties for business critical operations. Should those providers experience a system failure, it could have a catastrophic effect on the company's ability to trade, resulting in a business interruption loss and additional costs incurred to continue trading.

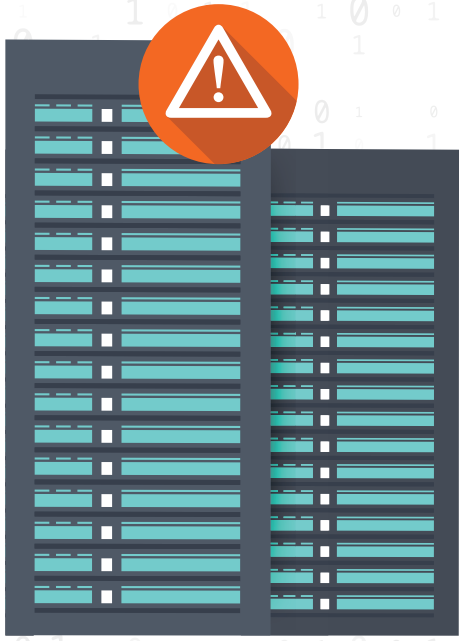
THE SHORT ANSWER

Even if you outsource your IT, the chances are you're still liable. Assuming you'll be successful in claiming back damages from a third-party is a risky gamble.

MYTH 3

"WE DON'T COLLECT ANY SENSITIVE DATA, SO WE DON'T NEED CYBER INSURANCE. . ."

Cyber Risk Insurance Is About Much More Than Privacy Risk and Data Breach



Funds transfer fraud and system damage or business interruption as a result of ransomware are two of the most common sources of cyber claims.

Cyber criminals use fraudulent emails or conduct social engineering over the phone to carry out fund transfer fraud.

In many cases, fraudsters pose as a senior executive appearing to give urgent instructions to junior employees to wire funds to and from a business bank account. Many of the victims of these losses hold next to no sensitive personal data.

The freezing or damaging of business-critical computer systems can sometimes be a much bigger problem to organizations than data theft

In 2017, the WannaCry and NotPetya ransomware outbreaks crippled many organizations within the manufacturing and logistic industries, costing some of them almost $2 billion CAD due to operational disruptions and turnaround drops.

THE SHORT ANSWER

Any business that relies on a computer system to operate, whether for business-critical activities or simply electronic banking, has a real cyber issue.

MYTH 4

"CYBERATTCKS ONLY AFFECT BIG BUSINESSES. WE'RE TOO SMALL TO BE A TARGET. . ."

Smaller Organizations Are Low Hanging Fruit for Cyber Criminals

Small businesses that lack the resources necessary to invest in IT security or provide cyber security training for their staff have become an easier and more attractive target for cyber criminals.

Attacks against smaller organizations are now so frequent that they are no longer newsworthy.

A recent Verizon report found that 58% of victims were categorized as smaller businesses. Claims data from Canada's largest insurer of Cyber Risk shows that the majority of fund transfer fraud claims come from small-to-medium sized businesses.

THE SHORT ANSWER

Cyber criminals target the most vulnerable companies, not just the most valuable.

MYTH 5

"CYBER RISK IS ALREADY COVERED BY OTHER LINES OF INSURANCE. . ."

Standalone Cyber Risk Insurance Fills the Gaps in Other Traditional Insurance Products, Which Only Offer Partial Coverage at Best

Property, crime, and professional liability are three of the most common lines of insurance assumed to include some type of cyber risk coverage, but they often fall well short of the coverage found in a standalone policy.

- **Property insurance policies offer a narrow, add-on data restoration coverage that includes only some form of sub-limit for data restoration costs and no expertise to deal with a claim involving data theft or damage.**
- **Crime insurance policies have only recently started to give coverage for social engineering attacks, but those policies are generally quite broad and lack the onerous terms found in a traditional crime policy.**
- **Some professional liability policies offer limited coverage for suits arising from data theft, but they don't cover any of the costs associated with responding to an event.**
- **Standalone cyber risk insurance policies offer a broad coverage that is also purpose-built for true cyber exposure. Most importantly, they provide access to an incident report service and bring a level of expertise to handle cyber events effectively and efficiently with minimum disruption and financial impact to the business.**

THE SHORT ANSWER

Some overlaps exist (as they do with all lines of insurance), but traditional insurance policies lack the depth and breadth of standalone cyber risk coverage and won't come with experienced cyber risk claims and incident response capabilities.