CompuVision
Manage Protect Accelerate

Insurance Cyber Security Needs

Why cyber security is a growing topic for insurance companies

Contents

Introduction

Risk is the number one equation that companies should evaluate in today's technology landscape, especially concerning the insurance industry. Cyber security is a growing topic for insurance companies due to data processing and storage for every lead managed. In addition, technology adds services and usability for customers and new areas of risk management for insurance providers.

Increases in employees working remotely, the surge in the gig economy, and the introduction and growing popularity of artificial intelligence are opening many new risks in data management and cyber security; this is especially true in the insurance industry.

In 2018 laws were put in place to try and prevent cyber security breaches from happening in the first place. These laws also mandate that companies report data breaches and inform their customers of any breach that compromises personal data.

During the year 2020 in Canada, the GDP (gross domestic product) totaled nearly $150 billion in the finance and insurance industry. At the same time, ransomware hackers demanded $1.2 million dollars to restore an insurance company's data after it was encrypted. The process of decrypting everything including servers, and desktop computers, took 15 business days in total.

A growing number of cases being reported of ransomware being used to hold computers, servers, and entire companies' data files hostage means insurance companies are looking to ensure that their privacy practices are insured by every means possible.

Everyone needs risk mitigation, insurance, and the knowledge that safeguards are in place to protect personal data.

Expertly safeguarding data that is accumulated, sorted, stored, and accessed regularly is not a small feat, and there are extraordinary measures you can take to protect yourself. However, if these measures are not taken, insurance companies that cover businesses in case of a data breach may not agree to coverage. And what is more ironic, are many of those insurance brokerages or providers are not compliant themselves.

What measures can insurance companies put in place to ensure the highest possible security measures are active at all times? How can insurance providers protect themselves from spending business days trying to decrypt data? What are the weak links in these safety measures? How do the top insurance companies protect their reputations and client data at the same time?

Data Volume and Sensitivity

It is a well-known fact that insurance companies are high-value targets for all kinds of cybercrimes. As of July 28, 2021, Canada's cybercrime statistics report states that over 40,000 cyber scams were reported, which amounted to around 30,000 victims and $105 million of loss. By July, cybercrime in 2021 has already surpassed that of 2020, which means that the crimes are becoming streamlined, and efficient.

The insurance industry demands that sensitive personal and health information be stored and searchable for any leads, especially for customers. Security measures and privacy statements assure potential customers understand each company's efforts to ensure data security.

Unfortunately, the forms and approaches for cybercrimes targeting the insurance industry are on the rise. Knowing the various forms of cybercrime can help companies limit risk and maximize warning signs or possible breaches.

Forms of cyber security issues

There are nine commonly used cybercrime approaches to gaining access to personal data; some are new fangled and require knowledge of technology. Others are old school and require a firm understanding of human behavior.

The best security measures implement a strategic plan that puts controls, warnings, and locks on all of these common areas of cyber attack entrance.

Nine most common tactics and forms of cybercrime

- Social Engineering
- Malware
- Exploit Kits
- Viruses
- Ransomware
- Trojan Horses
- Email and Phishing
- Phone Call Cyber Attacks
- Unlocked Doors

40,000
cyber scams

30,000
affected victims

$105M
dollars lost

Cybercrime Risk Mitigations for Insurance

The growing risk of becoming a victim of insurance-targeted cybercrime is indicative of a dire need for security measures that allow customers access to their data while also keeping company, personal, and sensitive data secure.

In addition, regulatory mandates and reinsurance policies also require accountability to validate that security processes are in place and being used correctly should a cyberattack occur.

The main measures for risk mitigation in the insurance industry are easily implemented and usable with ongoing training for employees and systems monitoring.

Prevention: Avoid higher risk endeavors

According to the American Academy of Actuaries, information sharing is one of the best ways to prevent and overcome the difficulties related to cyber security and cybercrime. In addition, information sharing can help insurance providers stay updated on current problems and avoid risky situations that compromise data.

Mitigation implement systems, processes, and policies for risk reduction

Increasingly companies are turning to technological systems in infrastructure that include code-based control mechanisms that can be manipulated by malicious coding. These silent cyber attacks are concerning because they can generate claims on liabilities for property, flood, general, management, and homeowners insurance, as well as cyber policies.

Implementing risk mitigation systems and updating policy wording can ensure that cybercrime does not cause profit loss. Unsurprisingly, the Bashe Attack Report suggests that losses due to silent cyber attacks could total nearly 2 billion dollars, but businesses remain underprepared.

Mitigation strategies include policies and security tactics around data. These can include but are not limited to:

- Limiting data and device access
- Regular software updates
- Setup and maintenance firewall software
- Up-to-date malware and antivirus software
- System and data backups
- Train staff in security best practice

Reinsure, redistribute risk

Reinsurance is a secondary measure; prevention, monitoring, and security measures should always be the priority. As a secondary safety net, many insurance companies outsource their coverage to other insurance companies in reinsurance. Ransom rates demanded during cyberattacks have risen by 43% since 2020.

Additionally, a few advantages of reinsurance are that some of these policies will cover the restoration in the case of an attack. A few guidelines will cover data loss, theft, and extortion. Some will include paying for a PR firm to handle damages to reputation.

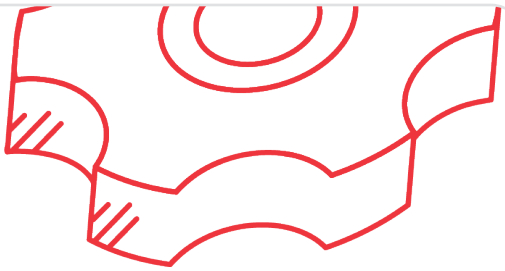
Assuming risk

The last and commonly chosen mitigation tactic is assuming risk. Did you know that any given company should be checking all devices, including mice and keyboards? Something as simple as mice can be a security risk and need to be routinely monitored?

In a world where tech is constantly changing and needing updates hiring a knowledgeable, up-to-date security company can save much time and reduce headaches by eliminating the need to research the latest news on firmware.

By not taking appropriate security measures, providers assume an ever-growing statistical risk of being a victim of cybercrime. When the average data breach can cost $3.86 million, this could mean a hefty price to pay for assuming risk.

AI and Cyber Security



Artificial Intelligence is a two-sided issue when it comes to cyber safety and data processes. Cybercriminals see the advantage of using artificial intelligence to their advantage when enacting criminal attacks.

Cyber Security specialists can flip the coin to the other side and use AI to automate and reduce the amount of work involved in preventing cyber attacks. In addition, they are potentially allowing for early warnings of repeated incoming attacks.

The first use of AI in securing networks is filtering what communications coming into the network are real and what are not. The second level of implementing AI for security purposes is the ability of AI to disable fraudulent network connections and disable the account.

Value of Trust

Trust is one of the most profitable commodities in any business relationship. The value of trust is especially true when trusting another party for coverage in a vulnerable and valuable area such as life or health insurance.

Unfortunately, the combination of sensitive data, human behavior, and physical or cyber unlocked doors is causing higher and higher amounts of cyber targeting in the insurance industry.

As an industry built on a foundation of risk mitigation, it makes sense to take all the necessary precautions to mitigate risk and prove to your clients and reinsurers that all the appropriate safety measures are in place.

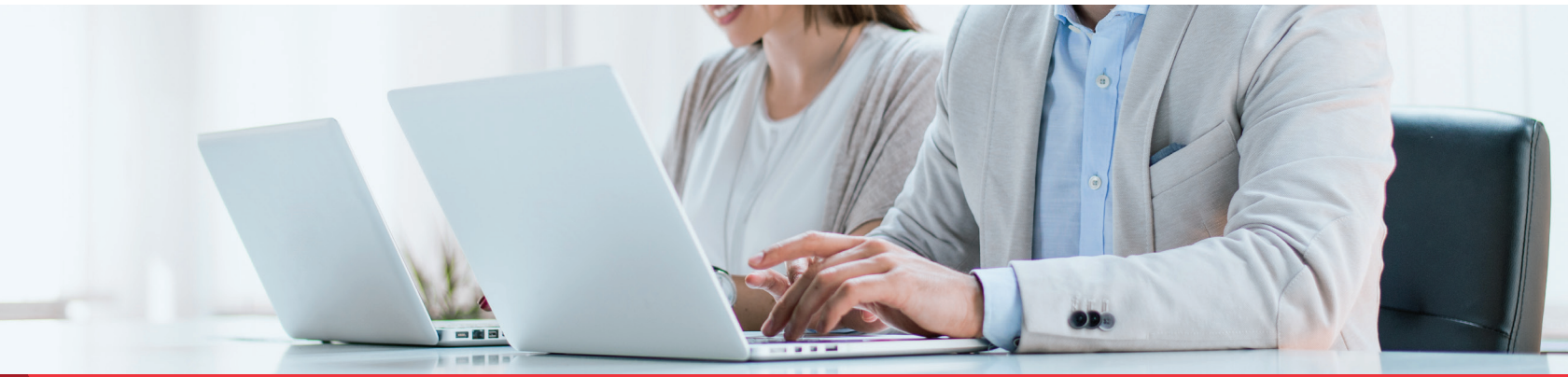
In addition, the ability to have security measures validated in cyber targeting is of great value in an industry with increasing risk.

Knowledge and experience

Actuarial statistics say that the insurance industry's risk is rising, which means that insurance costs are rising. However, a portion of the rising insurance cost can be mitigated by getting security risk assessments performed by knowledgeable and experienced professionals.

The most educated professionals will know exactly where to look for vulnerability. They will help implement access reduction efficiencies and start implementing security protocols that will show immediate benefits in risk reduction strategies.

In all actuality, improving your cyber security measures can be very easy to implement, especially when leaving the time-consuming regular checks and monitoring up to the professionals.



Conclusion

When used well in the insurance industry, technology reduces workloads, allows insurance companies to reduce paper use, and gives consumers easy access to their data.

The caveat, when used well, includes the use of intelligent data security, storage, and protections which sounds like a tremendous amount of work because it is.

However, partnering with a company specializing in security, monitoring, and cyber-attack mitigation strategies will simplify the task dramatically.

Insurance companies can save hours, days, and even weeks, by using companies that are familiar with and have help desks specifically trained to work in the insurance industry.

You can ensure cyber hygiene in all locations if you know where to find the weaknesses. CompuVision actively audits security strategies and provides a complete cyber security threat assessment which helps you understand how and where to protect your business.

To learn more, and to find out how CompuVision can protect your business now and in the future, go to: **compuvision.biz/services/protect/cyber-security**

Contact Us

Questions?

Get in touch and let us know how we can help. With offices in Edmonton and Calgary and local representation across Canada and North America, we have someone nearby ready to answer your questions.

General Inquiries and Sales: 1-587-525-7600

Email: info@compuvision.biz

CompuVision Systems

Edmonton, Canada

Suite 101, 15511 – 123 Avenue NW
Edmonton, Alberta T5V 0C3

Calgary, Canada

Suite 355, 3115 – 12 Street NE
Calgary, Alberta T2E 7J2

Houston, United States

Suite 105, 21830 Kingsland Blvd
Katy, Texas 77450

CompuVision

Manage • Protect • Accelerate