Cyber Risks & Liabilities

January/February 2023

2023 Cybersecurity Trends

Each year, new technologies emerge, and with them come cybercriminals finding new ways to infiltrate accounts and devices. To combat these attacks, it's important to be aware of new cyberattack trends and know how to ensure that your organization is as secure as possible. The following are some of the cybersecurity trends to know for 2023:

- **Improved remote security for employees**—With many more employees working from home, organizations will be making cybersecurity from a distance even more of a priority. Organizations may also consider investing more in training for employees to make sure they are up to date on how to keep their devices secure.
- **Artificial intelligence (AI)**—AI is becoming more integrated into our everyday lives. While it can provide convenience, it can also equip hackers with a new way to obtain personal information. To combat these attacks, you should make sure threat detection systems are enabled on AI devices, which can notify admins of a data breach. It's also a good idea to be cautious about what types of information AI devices have access to.
- **Mobile devices**—Two-thirds (65 per cent) of Canadians used a mobile banking app in 2021, up from 56 per cent in 2018. This number is expected to continue to grow, and as a result, hackers using smartphone viruses and malware to access financial accounts will also increase.
- **Cloud vulnerability**—As companies continue to utilize cloud-based storage, they also need to be vigilant about monitoring and updating security measures to protect against data leaks.
- **Cybersecure company culture**—Another way organizations are improving their cybersecurity efforts is by ingraining it into their company cultures. This can be done through frequent cybersecurity trainings, informational emails and occasional IT phishing simulations to test employees. By constantly educating employees on cybersecurity, you can keep it top of mind.

By understanding cybersecurity trends, you can enhance the process of protecting your organization and employees against cyberthreats.

Case Insurance Brokers Inc.
336 Millwood Road
http://www.caseinsurance.ca

Case
INSURANCE BROKERS

Self-evaluate Current Cybersecurity Practices

New cyber risks and cybercriminal techniques can be overwhelming and even scary to imagine. It can help to review your organization's cybersecurity efforts and find any gaps that may exist.

Consider asking yourself and your team the following questions to evaluate your business's current cybersecurity practices:

- Is cybersecurity training part of onboarding?
- Are employees reminded of cybersecurity best practices periodically?
- Is multifactor authentication enforced on devices and accounts?
- Are there procedures in place for detecting data breaches and informing the appropriate team members?
- Is there a response plan in place for cyberthreats?
- Is your cyber insurance policy up to date?
- Is important data backed up in multiple locations?

Contact us for more resources relating to cybersecurity best practices.

Primary Cyber Risks to Know

The Canadian Centre for Cyber Security (Cyber Centre) recently released its annual National Cyber Threat Assessment, which outlines current cyber risks that individuals, organizations and critical infrastructure providers should be aware of. The report includes five cyberthreat activities that are becoming increasingly more likely to affect Canadians. Moreover, these threats are some of the primary drivers influencing 2023 cybersecurity trends.

Considering educating yourself and your team on the following five cyber risks:

1. **Ransomware continues to be a major threat.** In the past 12 months, 63.3 per cent of Canadian organizations were affected by ransomware, according to CyberEdge's 2022 Cyberthreat Defense Report. Ransomware is one of the most disruptive forms of cybercriminal activity, and it continues to become more advanced as criminals aim to increase their profits.
2. **Cyberthreats put critical infrastructure at risk.** Cybercriminals have been purposely targeting important federal organizations because they are more likely to act fast and pay ransoms to avoid being shut down.
3. **State-sponsored cyberthreats are becoming more common.** State-sponsored cyberthreats from countries are becoming more common. They often target organizations and their databases for their own financial gain.
4. **Misinformation is being used to create distrust online.** Cybercriminals have been producing fake content using machine-learning technologies to make it easier to create and harder to detect. The Cyber Centre predicts that misinformation, disinformation and malinformation will continue to increase over the next two years.
5. **New technologies create more opportunities for cybercriminals.** New digital assets, such as cryptocurrency, are becoming yet another target for cybercriminals.

Contact Case Insurance Brokers Inc. for more cybersecurity updates and resources.