The State of Cybersecurity in Canada

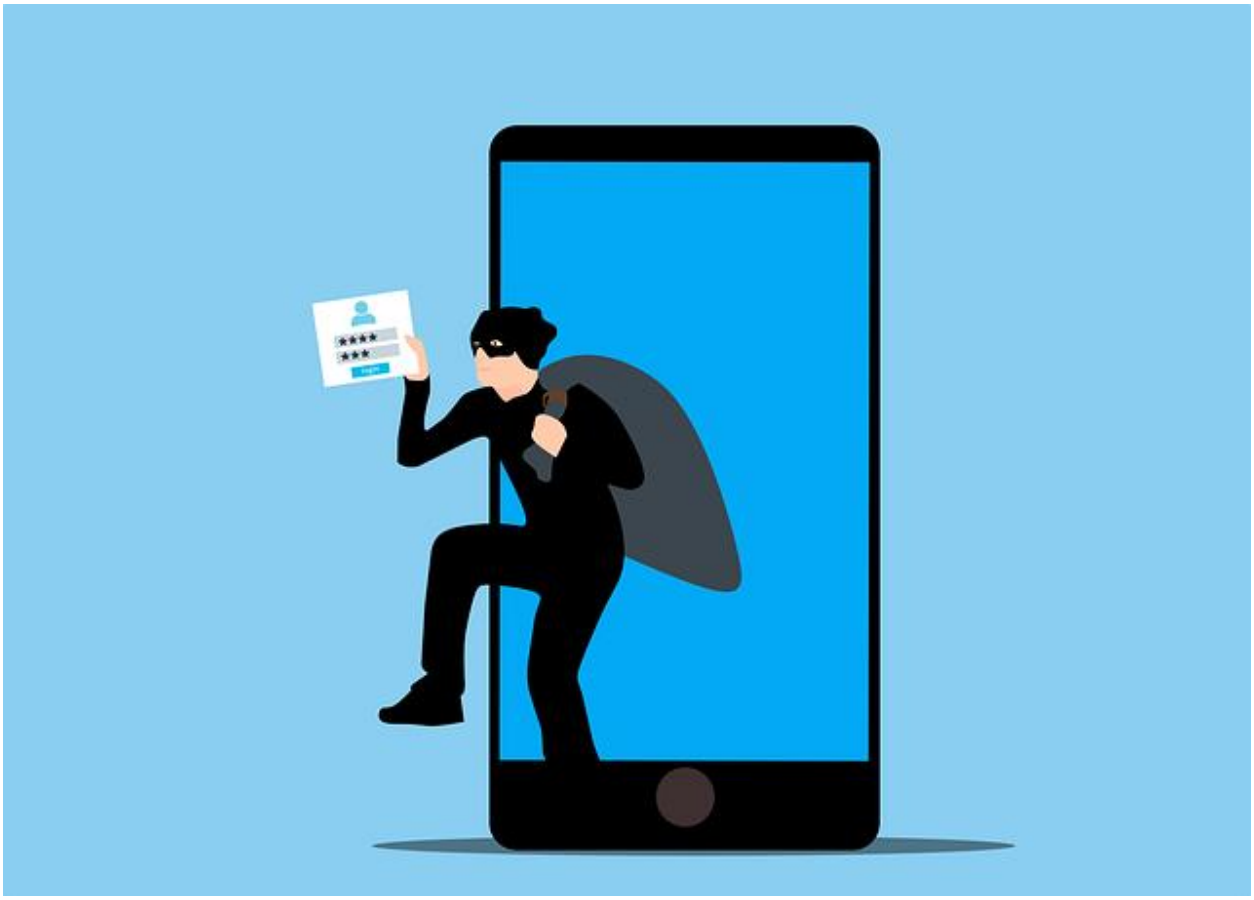
Report by Grant Thornton, summarized by Gundi Jeffrey

Grant Thornton LLP has released a report on the state of cybersecurity in Canada that provides insights on imminent cybersecurity threats and what business' can do to protect themselves. According to the report, "as businesses develop new ways to protect themselves from online attacks, cybercriminals are becoming savvier – and finding new weaknesses to exploit. It's important for businesses to be aware of cybersecurity developments to prepare accordingly."

The report addresses:

- Threats to small businesses
- Attacks on critical infrastructure
- Cybersecurity implications of AI
- Supply chain attacks

ThinkTWENTY20 has summarized the report as it contains valuable information on how organizations can prepare and protect themselves from cyberattacks now and in the future.



Smaller Businesses Under Attack

With larger organizations typically having strong controls around cybersecurity, whether in terms of training, processes or technology, small- and medium-sized businesses (SMB) are

increasingly feeling the brunt of cyber-attacks in Canada. As these businesses increasingly rely on digital infrastructure for day-to-day operations, they became enticing targets for cybercriminals seeking to exploit vulnerabilities. Phishing attacks, ransomware incidents and data breaches were among the most prevalent threats faced by SMBs. Many of these smaller Canadian businesses lacked the resources and expertise to implement robust cybersecurity measures, making them more susceptible to exploitation.

"The financial repercussions of cyber-attacks were often devastating for small businesses, with the cost of recovery and reputational damage putting their very survival at risk. The average cost of a data breach in Canada is $5.64 million$1 million more than the global average, and a Mastercard study showed that 99 per cent of victims said the cyber-breach impacted their business operations. Furthermore, the study noted that the most common effect of these cyber-breaches was the loss of customer data, and more than a third said the hack strained their relationships with vendors or customers."

As small- and medium-sized businesses increasingly relied on digital infrastructure for day-to-day operations, they became enticing targets for cybercriminals seeking to exploit vulnerabilities.

Moreover, the interconnected nature of supply chains means that small businesses often became entry points for larger-scale attacks on their partners and customers. In response to this escalating threat, industry experts and governments stresses the importance of raising cyber awareness and providing support to small businesses in enhancing their cybersecurity posture. Collaborative efforts between cybersecurity firms, governments and trade associations aimed to equip small enterprises with the necessary tools and knowledge to defend against cyber threats, empowering them to navigate the digital landscape with greater resilience and confidence.

The Weakest Link in the (Supply) Chain

According to the report, "supply chain attacks provide an indirect method for attackers to breach a target organization – by first compromising a supplier and subsequently exploiting their trusted relationships with downstream organizations, threat actors can entirely circumvent those organizations' secure network perimeter, thus avoiding the need for direct action against a target network's defenses. Many of the attacks we've seen in recent years have come via weak third and fourth parties with the methods used to provide remote access to these organizations found to be insecure. A Gartner risk report indicated that, "There were 100 times more supply chain attacks in 2022 than in 2020. This trend will only get worse – by 2025, 45% of global organizations will be impacted."

This vulnerability has led to an increased emphasis on third-party risk management. Security audits of potential external vendors and partners are becoming standard fare in the vetting process. Companies that are unable to demonstrate a solid security approach are losing

business. As a result, many companies are prioritizing employee awareness and training programs. As the threat landscape continues to evolve, collaboration and information sharing within industries and regulatory bodies have become essential to stay ahead of cyber adversaries. “The future of supply chain cyber security lies in adaptability, resilience, and a proactive approach, ensuring that businesses can thrive in the face of the ever-changing cyber threat landscape.”

Cyber-fatigue emerged as a pressing concern within the technology and security communities with the unprecedented surge in cyber-attacks, data breaches and privacy violations.

Sleeping On Cybersecurity as A Result of Cyber-Fatigue

Cybercriminals continue to look for the easiest ways to access an organization’s network or systems – the quickest and cheapest path that allows them to stay hidden under the disguise of an authorized employee. Grant Thornton saw continued growth in attacks perpetrated by social engineering, which contributed to fraud hitting all-time-high in Canada. In 2022, fraud cost Canadians at least $530 million, a 40 per cent jump over the previous according to the Canadian Anti-Fraud Centre.

The report points out that, as the scope and number of attacks increased, cyber-fatigue emerged as a pressing concern within the technology and security communities with the unprecedented surge in cyber-attacks, data breaches, and privacy violations, led to a constant barrage of security alerts, updates, and notifications for individuals and organizations alike. Additionally, the spike in attacks has seen security teams impose an overwhelming number of precautions on workers: use extremely long and complex passwords, change them every six weeks, multi-factor everything, keep your systems updated, and never, ever use insecure Wi-Fi. “As a result, there was a noticeable sense of exhaustion among users (and security professionals). The continuous stream of cybersecurity news and incidents also contributed to a desensitization to the severity of the threats, making it challenging to distinguish genuine risks from noise.”

Cyber-fatigue manifests as decreased vigilance, complacency towards security measures, and a higher likelihood of falling victim to social engineering tactics. “Addressing cyber fatigue became a critical aspect of cybersecurity strategies, necessitating user-friendly security interfaces, clear communication of risks, and efforts to strike a balance between security measures and usability. In 2022, the industry recognized the importance of not only fortifying technological defenses but also fostering a cybersecurity culture that acknowledges the impact of fatigue and empowers individuals and organizations to remain vigilant and resilient in the face of evolving cyber threats.”

Overall, the past year has proved pivotal year for cybersecurity, emphasizing the necessity for constant innovation and adaptability to protect against emerging threats in an increasingly interconnected digital landscape.

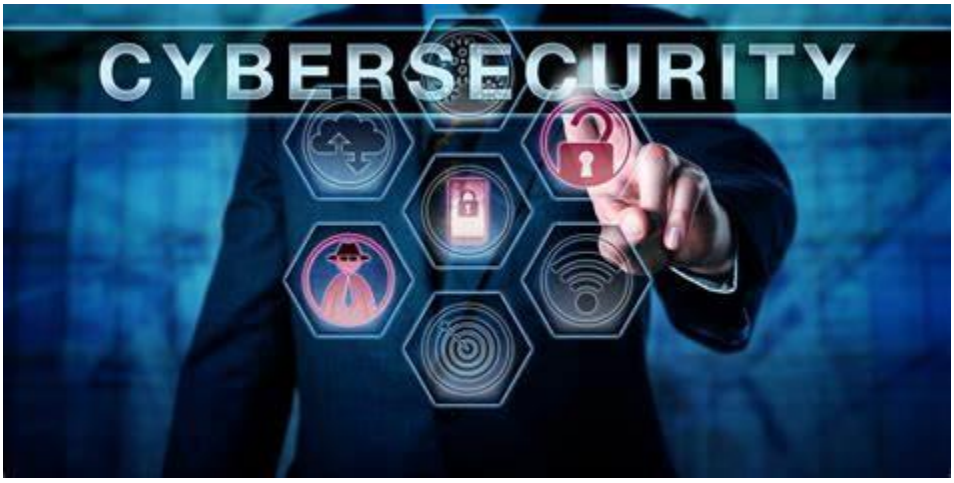
Trends On the Rise

Attacks on critical infrastructure

According to the report, cyber-attacks on critical infrastructure and Operational Technology (OT) systems are a growing concern due to their potential to cause severe disruptions and catastrophic consequences. As nations continue to digitalize and interconnect their essential services, attackers increasingly view critical infrastructure as attractive targets.

This trend has been consistently growing for years, the report says, but took on new urgency with the ongoing war in Ukraine. “Cyber warfare has emerged as a powerful tool used by state and non-state actors to achieve their strategic objectives. The conflict has witnessed an increase in sophisticated cyber-attacks targeting critical infrastructure, government institutions, and private organizations, both within Ukraine and beyond its borders. Canada is not immune to this. As a NATO member providing ongoing support for the Ukrainian government, we have been a target for attacks critical infrastructure such as our energy system. A recently published Communications Security Establishment (CSE) threat assessment noted that "…this activity is very likely to disrupt critical services for psychological impact, ultimately to weaken Canadian support for Ukraine. We assess that this activity will almost certainly continue for the duration of the war, and will likely increase as Russia's invasion efforts falter, or new support for Ukraine is announced.”

As the report points out, “the situation in Ukraine serves as an important reminder of the potential effects of cyber warfare on a global scale. It highlights the importance of enhancing cyber security measures not only for nations involved in armed conflicts but for the international community as a whole.”



Some key trends in cyber-attacks on critical infrastructure and OT in 2023 include:

- Advanced Threats: Cyber attackers are using more sophisticated tactics, techniques and procedures to target critical infrastructure. These attacks involve advanced malware, zero-

day exploits, and multi-stage campaigns that aim to evade detection and cause maximum damage.

- Ransomware Targeting Infrastructure: Ransomware attacks have evolved to specifically target critical infrastructure, such as power grids, water facilities, and transportation systems. The attackers' goal is not only to encrypt data but also to disrupt operations and extort large ransom payments.
- Supply Chain Attacks: Attackers may exploit vulnerabilities in the supply chain of critical infrastructure, compromising trusted vendors and suppliers to gain unauthorized access to critical systems and data.
- Convergence of IT and OT: As IT and OT systems converge to increase efficiency and connectivity, the attack surface for critical infrastructure expands, offering attackers more entry points into the industrial control systems.

Critical infrastructure operators are investing in state-of-the-art cybersecurity technologies, conducting regular risk assessments and prioritizing employee training to improve cyber awareness.

To counter these threats, the report says, “critical infrastructure operators are investing in state-of-the-art cybersecurity technologies, conducting regular risk assessments and prioritizing employee training to improve cyber awareness. Furthermore, comprehensive incident response plans and continuity strategies are being implemented to reduce downtime and mitigate the potential impact of successful cyber-attacks.”

Grant Thornton believes that, “as the world becomes increasingly reliant on interconnected systems, the focus on protecting critical infrastructure and OT from cyber threats will remain a top priority for both public and private sectors in 2023 and beyond.”

AI: the double-edged sword

The continued adoption of AI holds immense promise for various industries, but it also comes with significant cybersecurity implications. “AI's widespread integration in diverse applications, from autonomous vehicles and smart cities to healthcare and finance, enhances efficiency, decision-making, and user experience. However, this increased reliance on AI-driven systems opens up new attack vectors and potential risks that need to be addressed to ensure a secure digital landscape.”

The research for the report fund that one major cybersecurity implication is the potential for AI-generated cyber-attacks. “As AI technologies advance, cybercriminals can leverage them to create more sophisticated and targeted attacks, such as AI-powered phishing campaigns, deepfake attacks and automated malware generation. These attacks can be difficult to detect and respond to, as they may mimic legitimate user behavior and exploit AI-based vulnerabilities in systems. Moreover, AI-driven cyber-attacks can lead to more significant and widespread

impacts. Automated and highly scalable attacks could potentially disrupt critical infrastructure, financial markets, or even influence political processes. The use of AI by malicious actors may also blur the lines between cyber warfare and cybercrime, creating complex challenges for attribution and response."

Another cybersecurity challenge is related to the security of AI systems themselves. "As AI algorithms become increasingly complex and interdependent, they become vulnerable to adversarial attacks and data poisoning. If attackers can manipulate the training data or input to AI systems, they can lead to biased decisions, misclassification or unauthorized access to sensitive information."

Additionally, the report points out that the current shortage of skilled cybersecurity professionals capable of effectively defending against AI-driven threats is a growing concern. "The demand for AI expertise in both offensive and defensive capabilities may outpace the availability of skilled personnel, leaving organizations vulnerable to emerging cyber threats."

Collaboration between the cybersecurity community, policymakers and AI developers will be essential in order to establish ethical guidelines, standards and regulations to ensure the responsible and secure deployment of AI technologies in the years to come.

A change in the posture of cyber-insurance providers

A surge in online attacks has had a profound impact on the insurance landscape, sparking a reevaluation of business' risk management strategies and prioritization of cyber insurance as a crucial component of their overall security posture.

Notes the report, "as cyber threats continue to diversify and become more sophisticated, cyber insurance policies will likely expand to cover a broader range of risks. This may include coverage for emerging threats like AI-driven attacks, supply chain vulnerabilities, and cyber-physical risks (e.g., attacks on IoT devices impacting physical infrastructure). It may also mean offering tailored and dynamic policies where insurers may offer more customized and dynamic cyber insurance policies tailored to specific industries, business sizes, and risk profiles. These policies may be designed to adjust their coverage and premiums based on real-time risk assessments and the insured entity's cybersecurity posture."

As cyber-attacks became more disruptive and costly, insurance providers adapted their offerings to address the evolving threat landscape. But, the report points out, “the increased risk also led to a reevaluation of policy terms and premiums, with some insurers tightening their underwriting criteria to mitigate potential losses. The growing demand for cyber insurance led to an expansion of the market, with new insurers entering the arena and existing ones refining their coverage options. The year saw a greater emphasis on tailored policies, where businesses could customize coverage based on their specific needs and risk exposure. Additionally, the cyber insurance industry focused on providing proactive risk assessment and incident response services to help organizations bolster their cyber resilience.”

Cyber insurance is expected to undergo significant changes in response to the evolving cyber e. Overall, the future of cyber insurance is likely to be marked by innovation, greater risk awareness and a shift towards proactive risk management.

Even as insurance providers innovate to develop new risk mitigation products, Grant Thornton says, “organizations should also expect higher scrutiny over the maturity of their cybersecurity controls and requirements for more detailed cybersecurity risk assessments from policyholders to determine the level of coverage and premiums. Entities with stronger cybersecurity measures may receive more favorable premiums, while those with higher risk profiles may face increased costs. This could encourage businesses to improve their cybersecurity practices to qualify for better coverage terms.”

To mitigate both cybersecurity risk and the financial risk of high insurance premiums, “businesses must prioritize cybersecurity measures such as implementing robust security protocols, conducting regular security assessments, investing in employee training, and staying

informed about the latest threats and best practices in the industry. Collaboration with cybersecurity experts and leveraging advanced threat detection technologies can also help organizations fortify their defenses against the evolving cyber threat landscape."

Zero Trust

The research found that, in 2023 and beyond, the concept of zero trust is becoming increasingly vital in the field of cybersecurity. "Traditional security approaches that relied on perimeter-based defenses are no longer sufficient to protect modern, dynamic digital environments. Zero trust architecture offers a paradigm shift by assuming that no entity, whether internal or external, should be trusted by default. Instead, it advocates verifying and validating every access request and transaction, regardless of the user's location or device."

The importance of zero trust lies in its ability to address the evolving threat landscape. "With the rise of remote work, cloud computing, the attack surface has expanded, making it more challenging to establish a secure perimeter. Zero trust embraces the 'never trust, always verify' principle, reducing the risk of lateral movement for cyber attackers within a network. This model helps prevent data breaches and unauthorized access even if the attacker has already compromised one part of the system."

Moreover, the zero-trust philosophy emphasizes data protection. "By adopting encryption and tokenization, data remains secure even if it falls into the wrong hands. This approach helps businesses comply with regulatory requirements and maintain customer trust."

According to Grant Thornton, "as cyber threats continue to evolve, the concept of zero trust is poised to become a foundational pillar of cybersecurity strategies. Its adaptive, proactive, and context-aware nature makes it an essential approach to safeguard digital assets, privacy, and sensitive information in 2023 and beyond."

The Need for Robust Cyber Defenses

As the cyber threat landscape continues to evolve with increasingly sophisticated attacks and emerging technologies, says Grant Thornton, "the need for robust cyber defenses has never been greater. Organizations and individuals alike must remain vigilant, proactive and adaptable to the dynamic nature of cyber threats. Embracing advanced technologies such as AI-driven security solutions and zero-trust architectures will become crucial in safeguarding digital assets and personal information. Collaboration between industry stakeholders, governments and cybersecurity experts will pave the way for more effective threat intelligence sharing and coordinated response efforts. Furthermore, a strong focus on cybersecurity awareness and education will empower individuals to protect themselves against cyber risks. Despite the complexity of the challenges ahead, the collective commitment to cybersecurity will lead to a safer digital landscape, where innovation and technology can thrive securely in 2023 and beyond."