In Their Own Words: How You Can Protect Your Organization from Ever Evolving Cyber Attacks

By Gundi Jeffrey

Gundi Jeffrey is an award-winning business journalist specializing in writing about the accounting profession for various publications in Canada and England. In 1985, she co-founded The Bottom Line, then Canada's only independent publication for the accounting and financial professions, serving as its executive editor.

As we all know by now, "cybersecurity" refers to any technology, measure or practice for preventing cyberattacks or mitigating their impact. It aims to protect individual and organizational systems, applications, computing devices, sensitive data and financial assets against various threats.

Advancements in many of the technologies we currently use have changed the way people communicate, bank, shop and pass the time. The growing threat of cyberattacks has made governments and industries more aware of the need to protect and defend the information and systems Canadians rely on. As a result, cyber security is growing as a recognizable discipline that encompasses multiple specialties in science, mathematics, business, social sciences and computing and engineering faculties. These are the folks who are going to help protect us from the scammers.

Among the many attacks we've come to know too well, are:

- **Phishing** – scammers sending fraudulent emails that resemble messages from reputable sources. Phishing attempts to trick recipients into revealing sensitive information or downloading malicious attachments.
- **Malware** – includes viruses, worms, Trojans, ransomware and spyware. These malicious software programs can infect systems, steal data or disrupt normal operations.
- **Ransomware** – encrypts files or locks users out of their systems until a ransom is paid. It has become a significant threat, with substantial financial consequences.

But there is nothing static about cyber security. Because this is an evolving field, organizations need relevant, practical advice that makes sense and helps them protect their information and IT assets. We decided to interview Janny Bender Asselin, Media Relations and Public Affairs, Canadian Centre for Cyber Security, Canada's authority on cybersecurity – which offers advice, guidance and information developed by its cyber experts – to see where these trends are heading and how organizations can best protect themselves.

ThinkTWENTY20: *Why has cybersecurity become so important? What has brought us to this place?*

Janny Bender Asselin: The pandemic brought on a rapid change in how we use technology. With so many of our everyday activities switching to online-first (shopping, work, school, etc.), the threat surface and our digital footprints increased, making it easier than ever for Canada and Canadians – both individually, and on a big or small business level – to be targets. Especially now, with many businesses depending on employees with home-based tools that might not be as secure as they would be at the office. All those different devices and service providers being added to the mix are potential new entry points for cyber criminals looking for financial gains or to gain access to a company's information.

One of the reasons so many of us are vulnerable is because cyber hygiene isn't part of our everyday vocabulary. Anyone with a cell phone, email address, social media or who browses the internet is susceptible to falling victim to a cyberattack – even the savviest cyber security expert. And keeping up with technology doesn't always feel straight forward, or it feels like it slows us down, which means the average Canadian is less likely to incorporate it. If we think "it can't happen to me" and do nothing about it, then yes, we can be very vulnerable. It's important to understand that it's no longer a matter of "if" but rather "when" we might face some form of cyber incident, and that implementing simple tools and layers of security into our day to day digital-lives makes us less vulnerable.

Our day-to-day "real life" security habits are second nature now: We don't leave our home or our car without locking the doors, so why would we leave a phone, computer or sensitive account without a strong password or PIN? We often have physical security systems in place too, so why not have multi-factor authentication (MFA) on our banking apps? It's just a new reality we need to adapt to and use some simple tools, and soon it is as second nature as hitting the lock button on a car door.

Because cyber security is an evolving field, organizations need relevant, practical advice that makes sense and helps them protect their information and IT assets.

ThinkTWENTY20: *It appears that the expanding IT landscape (cloud adoption, remote work, connected devices) provides more opportunities for cybercriminals. How do each of these developments provide those opportunities?*

Bender Asselin: All of these new connected devices are additional entry points for cyber criminals. The tools cyber criminals and threat actors use for malicious cyber activities are more readily available than ever, and at very low costs. Cyber tools that were once available only to nation-state actors, are now available to a growing set of cybercriminal organizations and other

non-state actors. This makes staying on top of cyber security, as well as new and developing threats, a challenge and a priority. We talked about not leaving the house without locking the front door, If we want to keep up with that analogy, the now tools available to cyber criminals mean that, even if the front door is locked and properly secured, they can find the basement window that was left unlocked instead. Threat actors and cyber criminals are always looking for "back door" vulnerabilities in just about every digitally connected product, and are quick to exploit them.

That's why we urge our industry partners to build in security from the start. We joined our partners across the Five Eyes alliance and beyond to advocate for information technology manufacturers to use secure-by-design and secure-by-default principles in developing their products. The guide emphasizes the need to shift the burden of cyber security risk away from the customer and instead encourage technology manufacturers to design safe products that are secure by design and by default.

Cybercriminals have shifted their tactics, placing more resources into targeting larger and more financially lucrative targets. This is called Big Game Hunting.

ThinkTWENTY20: *What are some examples of the most serious recent cybercrimes you have heard of too date? And how did they succeed?*

Bender Asselin: Though we can't comment on specific incidents, it is important to remember that all instances of cyber crime and cyber incidents are serious. Some may be a blip on the radar of a large enterprise, but the same event could be catastrophic for a small or medium organization. Every company has a different tolerance threshold, and it is important to be ready in case of the worst-case scenario whatever that may be.

In our National Cyber Threat Assessment 2020 report, the Canadian Centre for Cyber Security (Cyber Centre)'s research determined that small and medium organizations are most likely to face cyber threat activity in the form of cybercrime, which can have immediate financial,

operational or privacy implications. They often target human vulnerabilities as well as technical ones. Cybercriminals typically cast a wide net, not usually against specific targets, seeking a financial profit.

While the threat to individuals and small and medium organizations from ransomware remains, other cybercriminals have shifted their tactics, placing more resources into targeting larger and more financially lucrative targets. This is called Big Game Hunting (BGH). This means very carefully targeting large enterprises that cannot tolerate disruptions and are likely willing to pay large ransom amounts to restore their operations. Should the company not pay the ransom, they still have the company's information – which often contains personal data for individuals – which they can then turn around and sell on the dark web and still reach their financial objective.

ThinkTWENTY20: *This topic is very relevant to financial professionals, such as accountants, both in industry and in practice. What can they do to prepare for cybersecurity threats?*

Bender Asselin: In general, everyone and every organization should be aware of the basic things they can do to keep themselves as safe and secure as possible. Following our Basic Cyber Hygiene 101 for all Canadians is a great start:

1. Patch and accept updates to your software and electronic devices.
2. Practice good password etiquette. Use strong and unique passphrases or passwords.
3. Use multi-factor authentication, whenever this option is available.
4. Be on guard for phishing (and spear-phishing) messages.
5. Store your data securely and know your back-up procedures.

Since cybercriminals take advantage of technical and human vulnerabilities, the best way to safeguard your organization against the risk posed by vulnerabilities and other cyber threats is to apply cyber security best practices. While it may not be possible to entirely eliminate cyber threats, businesses and organizations can significantly reduce their risk and be better prepared by taking a few important actions, starting with:

Business leaders need to consider that their personal reputation could be at stake if their clients' information is compromised.

- **Provide security awareness training for employees**: Email phishing is the most common method that threat actors use to spread ransomware. Regardless of what security features are installed on someone's device, if a malicious link is opened, that device could be compromised. Therefore, it is important that employees know how to recognize phishing attempts and that there is a procedure in place for employees to report them to the organization's IT team.
- **Patch operating systems (OS) and third-party apps:** Unpatched and unsupported operating systems provide easy vulnerabilities for cyber threat actors to exploit. Be sure to keep your OS and all third-party apps patched with the newest updates.

- **Disable macros:** A number of ransomware strains are sent as Microsoft Office attachments. When a user opens the attachment, they are asked to enable macros to see the contents of the document. Once they enable macros, the actual ransomware payload will download and execute. Keep macros disabled by default, and make sure employees are aware that a prompt to enable macros can be a red flag.
- **Use least privilege:** Users should only have the minimum amount of system access required to fulfill their job duties. Restrict administrative privileges as much as possible, and ensure administrative users are required to confirm any actions that need elevated rights.
- **Back-ups:** Be sure to perform frequent back-ups and store them offline. If ransomware is planted on just one device, it can spread across your entire network quickly and covertly. Make sure your back-ups are not connected to the Internet or any local network.
- **Practice recovering:** Organizations should run a simulated ransomware event and practice recovery procedures. How long would it take you to get yourself back online? For many organizations, it takes a lot longer in practice than anticipated. These exercises can show you what to focus on to improve your recovery procedures.

ThinkTWENTY20: *And how can financial professionals help their clients to best protect themselves?*

Bender Asselin: Sharing resources and talking about cyber security is a great start. The Cyber Centre's website is a great resource for companies. Our "Get Cyber Safe" public awareness campaign has simple and practical information for individuals and small and medium-sized businesses, including a brand new Get Cyber Safe Guide for Small Businesses, which details the steps to take to protect your business from a wide range of cyber threats and prioritize IT security. It was created specifically for businesses without dedicated IT teams.

The vast majority of cyber incidents go unreported and that means we only have a partial picture of the impact cyber threats have on Canadians.

ThinkTWENTY20: *And which actions, of those, would be the most effective?*

Bender Asselin: As we like to say: security in layers. The more layers you implement, the better. The basics mentioned above are very easy to implement and will make a world of difference. Having MFA on an application or device may seem time consuming and cumbersome but think of it this way: recovering from a cyber incident will take far more time and money than waiting for a secondary form of identification will. Business leaders need to consider that their personal reputation could be at stake if their clients' information is compromised. That alone is probably worth taking the extra time to make sure you're using strong passwords and MFA.

Getting buy-in from all levels of an organization is very important. From the C-Suite at a large organization, to the individual who works for themselves, if everyone understands the true cost of a cyber incident – the time, the reputation, the recovery and the actual financial cost – it is easier to understand how the smaller actions you take to protect your accounts compound together to keep an organization safe. Everyone has a role to play, from the IT person to the CFO.

ThinkTWENTY20: *AI, especially generative AI, has been presented as both a threat and a possible cure in relation to threats. How does the cybersecurity centre view this topic?*

Bender Asselin: Generative AI is a type of artificial intelligence that generates new content by modelling features of data from large datasets that were fed into the model. While traditional AI systems can recognize patterns or classify existing content, generative AI can create new content in many forms, including text, image, audio or software code. While the capabilities of Generative AI present many opportunities, there are also cyber security concerns. For example, threat actors can craft targeted spear phishing attacks more frequently, automatically and with a higher-level of sophistication. The red flags for a phishing message, such as poor grammar, spelling errors and low-quality images or logos no longer apply. Realistic phishing emails or scam messages could lead to identity theft, financial fraud or other forms of cybercrime.

In a soon-to-be-published 2024 Public Opinion Research, our Get Cyber Safe campaign learned that:

- One-third (32%) of online Canadians use Artificial Intelligence (AI) tools, at home or work.
- Twenty-two percent of online Canadians reported feeling confident in their ability to recognize AI-generated content, such as messages, pictures, videos or deepfakes. An

additional 36% were somewhat confident. The rest (40%) were not confident in their ability to identify content that is generated by AI.

We all need to work together to ensure that Canadians and Canadian organizations are aware of the evolving cyber threat landscape, and how it is being altered by disruptive technologies like generative AI. We encourage Canadians to be vigilant of threats that AI platforms and apps can pose. It's also important to remember that these tools, platforms and apps may store and process information outside of Canada. Therefore, Canadians should know what information apps may request to access, and to be prudent with their privacy settings.

ThinkTWENTY20: *Your centre has urged the public to take steps to protect themselves against Ransomware attacks. How is this going? Are they taking up the challenge?*

Bender Asselin: This is very hard to quantify. We know that the vast majority of cyber incidents go unreported and that means we only have a partial picture of the impact cyber threats have on Canadians. To that effect, we encourage any organization that is experiencing a cyber incident to report it through the Cyber Centre's incident reporting webpage. Reporting cyber incidents as they happen allows the Cyber Centre to build a better understanding of the tactics, techniques, and procedures being used to target Canadian organizations. With that information, we can warn others and prevent more incidents.

ThinkTWENTY20: *How do you see this space evolving in the near future? What types of crimes can we expect next?*

Bender Asselin: In October 2022, the Cyber Centre released its unclassified National Cyber Threat Assessment 2023-24 (NCTA). This report highlights the key cyber threat trends facing individuals and organizations in Canada, and includes a section on how machine learning tools can be exploited. We highlighted that cyber threat actors are very likely exploiting new tools such as machine learning algorithms to enable malicious activity, such as the creation and distribution of e-mail fraud or phishing campaigns. In previous editions of the NCTA, we described how the technology to make deepfake videos portraying public figures or events was becoming more accessible to cyber threat actors and more convincing. In the latest NCTA, we note that we have continued to observe the evolution of the technology behind deepfakes and synthetic content and noted its use related to significant international events.

As Canadians adopt new technology and embrace more internet connected devices, the cyber threats will continue to grow and evolve. We continue to publish advice and guidance to help organizations be less vulnerable and more secure. We continue to work with industry partners to share threat information and cyber security best practices. For example, The Cyber Centre regularly publishes cyber bulletins and advice on our guidance page and urgent warnings on our Alerts page.