5 transformation-driven cybersecurity considerations

Many newcomers launch a business in Canada as part of the process of maximizing new opportunities. But on their road to recovery from the pandemic, all businesses face unique dilemmas.

This includes substantial and entirely necessary investments in digital transformation. However, tight budgets are making such endeavours difficult if not impossible. Businesses continue to struggle with pivots like adopting new digital platforms, shifting their corporate model to resolve supply chain disruption and enabling a remote workforce.

The inability for businesses to quickly adopt technologies that support digital transformation processes, including identity-based segmentation, virtual desktop interfaces and full-stack cloud, is hindering their ability to adequately address new threats and even to test new security systems and protocols.

"Now more than ever, it's imperative to remediate risk exposure and vulnerabilities within an organization's existing systems – optimally from the get-go," urges cybersecurity expert Nishant Srivastava, cyber security architect and field expert at Cognizant, an IT solutions and services firm for which he's focused on designing and implementing Identity and Access Management (IAM) solutions. "Biggest threats should get highest priority, of course, but the magnitude or even likelihood of a threat should not be the sole consideration. Organizations should also look at other forms of value that new technologies can bring."

Nishant Srivastava is a cybersecurity expert.

The senior-level IAM, governance and cyber risk authority offers key digital security vulnerabilities businesses need to be mindful of given increased digital dependency amid the pandemic. Heed these best practices to help keep your company – and customers – uncompromised.

Consumer-facing app gaps. For consumer-facing web applications, some of the biggest security threats include path traversal, cross-site scripting (XSS), SQL injections and remote command execution. Of course, protecting customer data is an utmost security concern and breaches abound. One of the biggest challenges to address these kind of issues lies with lacking human resources. There is a lack of trained and skilled security staff in even the most sophisticated of regions, which is cultivating a gap in cybersecurity skills across the globe. It goes without saying that employee training and investing in highly-qualified staff are among the best ways to establish, maintain and uphold security levels of consumer facing apps. Rifts, however small, can induce excessive damage and losses.

eCommerce exposure. Online delivery businesses that are aware of security risks would be wise to introduce more secure logins, automatic logouts and random shopper ID verification and are preventing shoppers from swapping devices when ordering. Such measures will help thwart breaches that expose customer names, credit card information, passwords, email addresses and other personal and sensitive information.

Companies selling goods or services online also should not launch without a secure socket layer (SSL) connection. It will encrypt all data transfer between the company's back end server and the user's browser. This way, a hacker won't be able to steal and decode data even if he or she manages to intercept web traffic.

Another useful strategy is to enforce password limitations. Passwords should be as complicated as possible with a combination of symbols, numbers and letters.

Investing in a tokenization system is worthwhile because any hacker who accesses the back end system can read and steal sensitive information, which is held in the database as plain text. Some payment providers tokenize cardholder information, which means a token replaces the raw data so the database then holds a token rather than the real data. If someone steals it, they can't do anything with it because it's just a token.

Ransomware recourse. Ransomware threats are escalating, which is why those doing business digitally should enforce a multi-layer security strategy that incorporates data loss prevention software, file encryption, personal firewall and anti-malware. This will protect both a company's infrastructure and its endpoint.

Data backups are key because there's still a mild chance of a breach even with all of the aforementioned security solutions in place. The easiest and most effective way to minimize cyberattack damage is to copy files to a separate device. This very reliable form of backup makes it possible for people to recommence work as usual with little to no downtime, and all their computer files intact, should an attack occur.

Gone phishing. Gmail blocks over 100 million COVID-related phishing emails every day, but more than 240 million are sent. That means less than half sent via Gmail alone are blocked. Experts cite imposing limits on remote desktop protocol (RDP) access, multifactor authentication for VPN access, in-depth remote network connection analysis and IP address whitelisting as some of the best strategies to maintain security. In addition, businesses should secure externally facing apps like supplier portals that use risk-based and multifactor authentication – particularly for apps that would let a cybercriminal divert payments or alter user bank account details.

Shielding teleconferences. The shift to remote work after the pandemic hit has given cybercriminals more and more opportunities, directing their focus on the tools people use for work. It's important that people recognize their vulnerabilities, particularly while they work from home. Among these are hacked videoconference passwords and unprotected videoconference links, which criminals can use to access an organization's network without authorization. Many people who work from home do not use secured networks, unknowingly and unintentionally. Many are just not aware of the risks.

Forbes Business Council member Merilee Kern, MBA, is an internationally-regarded brand analyst, strategist and futurist who reports on noteworthy industry change makers, movers, shakers and innovators. She is founder, executive editor and producer of The Luxe List as well as host of the Savvy Living TV show. Connect with her at www.TheLuxeList.com and www.SavvyLiving.tv / Instagram.

To avoid online teleconference security issues, meetings should always be encrypted. This means a message can only be read by the recipient intended and that the host must be present before the meeting begins. There should also be waiting rooms for participants. Screen share watermarks, locking a meeting, and use of audio signatures are additional recommendations.

When asked what his best advice would be to tweak security for a workforce that's predominately working remotely, Srivastava says that companies should start by analyzing the basics like those specified above against the backdrop of a wide range of ever-escalating and evolving threats. "Employees should use dual-factor authentication and make sure apps, mobile phones and laptops are updated and that available patches and updates are always installed," he says. "They should certainly be wary of all information requests and verify the source. These even include unexpected calls or emails seemingly from colleagues."

Srivastava also pointed out that insiders at the CIO Symposium in July 2020 agreed that the pandemic packed years of digital transformation into just a few weeks. The use of third parties emerged as a major security concern to take into account. For instance, some employees abroad were unable to move their computers to their homes, so employers rushed to supply them with new equipment. In the process, some of it was not set up correctly thus compromising security. Companies should have done more to determine whether individuals were using technology properly, such as if employees were sharing work devices or using their own personal equipment.

On the plus side, the shift toward working from home sped up multi-factor authentication adoption. This is a great opportunity that today's digitally-driven businesses should take advantage of.

In short, Srivastava advocates taking a zero-trust approach. "It might sound harsh, but this is the idea that you can't trust devices, people and apps by default," he says. "Everything needs to be authorized and authenticated. Users should always verify and never trust, and businesses should act as if there has already been a breach and work to shore up weak links in the security chain. Finally, businesses should give access to information and data to as few people as possible – and wholly ensure those who do have access are appropriately trained to recognize when a red flag presents."

By employing all or even some of the advice above, businesses can continue to thrive as the digital transformation age unfolds – and do so more confidently all around.

– Merilee A. Kern

How to save money during a pandemic

We all know setting some funds aside for an emergency and life goals is important. But it can be hard to do, especially during a pandemic. Fortunately, there are saving strategies you can try even when you're not raking in a ton of cash.The first step is improving your financial literacy so you can feel confident about tackling your savings and money goals. Here are some other tips to consider:

Pay yourself first. Many people have trouble saving because there is no money left by the time they pay everything else. One solution is to pay yourself first. That means taking money off the top of each paycheque to put into your savings account. After that, take care of your bills and other needs.

Make your money grow. You probably already know that your debt gets bigger because you pay interest on it. The same idea applies to saving accounts and plans, but you get the interest. The amount you save grows. Let's say you put your money into a savings account or plan where you get 5 per cent interest. For every $100 you save in a year, you'll get an extra $5.

Check out government programs. The Canadian government has set up special savings plans to help your money grow more quickly. Depending on your goals and life stage, a Registered Education Savings Plan, Tax-Free Savings Account or Registered Retirement Savings Plan might work for you.

You can learn more about these government-approved savings plans and boost your money skills from ABC Life Literacy Canada's Money Matters program. It's a free introductory financial literacy program for adult learners that offers online courses and workshops. Learn more and access free workbooks and activities at abcmoneymatters.ca.

– News Canada