Fight Back:

Cybersecurity Strategies for Canadian Healthcare Providers

With the right strategy and controls in place, organizations can protect their sensitive information and ensure patient safety.

Virtual healthcare has broadened the provision of health services, allowing access to much-needed care across the country. Now, more than ever, expanded healthcare access has proved invaluable as current pandemic priorities overburden Canada's healthcare resources.

But since the onset of COVID-19, hundreds of hospitals across North America have experienced data breaches, ransomware and other cyber-attacks posing significant privacy threats to staff and patients. Healthcare systems are often an easy target for cyber perpetrators because they integrate with many networks and technologies with no unified security policies.

Fortunately, organizations don't have to sit in fear of the next cyber strike. By developing and deploying a high-level cybersecurity strategy targeting the vulnerable areas within an IT infrastructure, healthcare organizations can deploy industry-leading solutions and best practices that will substantially mitigate their risks.

CALIAN®

Confidence. Engineered.

Half of healthcare data breach victims (i.e., your patients) also face medical identity theft, with an average

cost of $2,500 per person.

Cyberattacks a Growing Problem in Healthcare

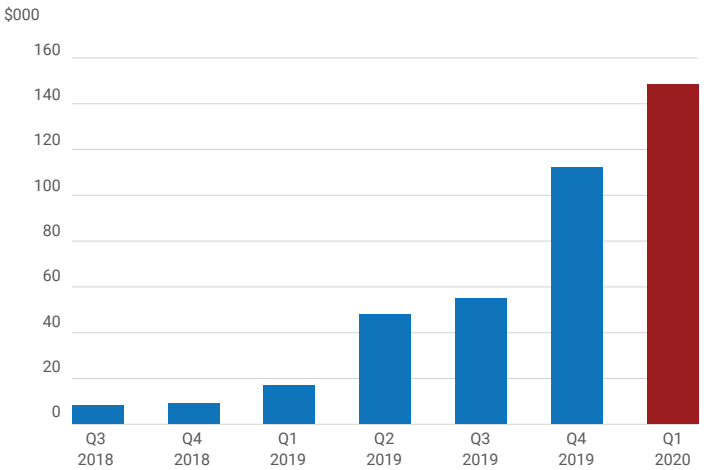
Personal impact: With sensitive personal data at stake, healthcare data breaches and ransomware attacks are among the most damaging among all industries. In Canada's most serious healthcare data breach to date, cybercriminals gained access to the personal records of patients and employees in the Eastern Health and Labrador-Grenfell Health regions of Newfoundland and Labrador's healthcare system. The exposed information included names, birthdays, addresses, email addresses, phone numbers, medical care plan numbers, names of family doctors, marital status and in- and out-patient times.

Unfortunately breaches like these are not an isolated incident in the healthcare sector; almost 50 per cent of all security breaches in Canada in 2020 were in healthcare, including hospitals. In October 2019 alone, three Ontario hospitals were victims of ransomware attacks.

Operational impact: Hospital service shutdowns during a cyberattack put vulnerable patients at risk. The cyberattack on Newfoundland and Labrador's healthcare system caused the cancellation of all non-urgent imaging and blood collection appointments—and reduced the number of chemotherapy sessions performed in the province's hospital system for weeks.

Financial impact: Cyberattacks also strip an already stretched healthcare budget. In recent years, cybercriminals have increasingly focused their activities against large enterprises that cannot withstand sustained disruptions to their networks and are willing to pay large ransoms to quickly restore operations. The average ransomware payment was approximately CA$148,700, and at the more extreme level can hit multimillion-dollar amounts.

Average ransom payment over time

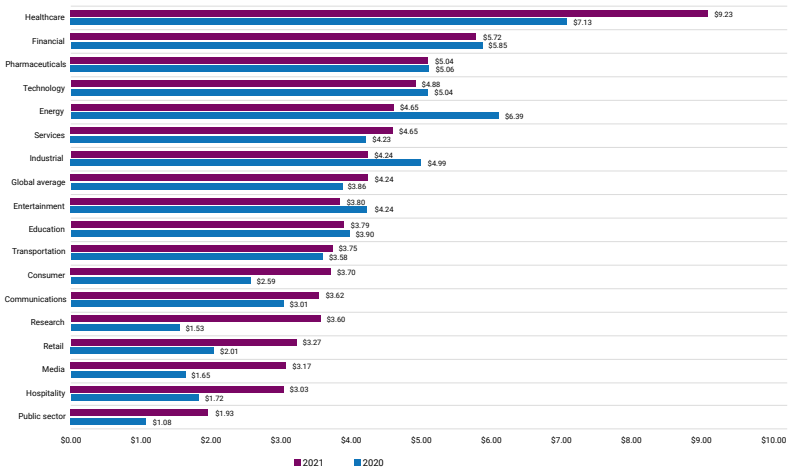


Source: Canadian Centre for Cyber Security https://cyber.gc.ca/en/guidance/threats-canadian-financial-and-economic-health

Figure 4

Average total cost of a data breach by industry

Measured in US$ millions



IBM Cost of a Data Breach Report 2021 https://www.ibm.com/security/data-breach

Globally, the average cost of a healthcare data breach in 2021 was

$9.23 million, up 29.5 per cent from the year prior.

Solid Solutions to Put Safety First

While the healthcare sector is in the business of providing patient care and not cybersecurity, every organization has an obligation to understand their security threat factors so they can mitigate risk and action safety priorities. Conducting vulnerability assessments and testing to identify risks will help your organization to develop and deploy a comprehensive cybersecurity strategy that will keep criminals and data breaches at bay. Adhering to best practices will help ensure that security protocols are adopted across an organization.

Even smaller, primary care organizations can take advantage of sophisticated security solutions and industry best practices to guard against cyberattacks.

A Step-by-Step Approach to Secure Your Organization Against Cyber Threats

1) Assess possible threats

As the healthcare ecosystem expands and evolves, more and more healthcare information is being shared among various systems. Sharing information—whether it's via cloud services, third-party partners or within your own data centres—may expose your organization to new points of access for cyber criminals. Plus, any data breaches within your institution may put the entire partner supply chain at risk. That's why it's important to assess possible threats within your organization through ransomware simulations, penetration tests and active directory security assessments to reveal vulnerabilities in your systems before threat actors do.

© 2022 Calian

"One thing we cannot overlook is that attackers may know your systems better than you do because this is their business," said Raheel Quershi, partner, Cybersecurity Risk & Advisory Services at iSecurity. Given that they are on top of exposures that organizations may not even be aware of, he says it's critical to frequently assess possible threats and conduct security tests in a non-malicious environment.

2) Develop a cybersecurity strategy

Technology solutions, while essential, will only work optimally if there is a strategy in place to deploy them. With a cybersecurity strategy, your organization can prioritize the tools and resources needed to protect assets and minimize risk. This strategy should be revisited regularly to adapt to ever-changing threats within the healthcare system. Having a proactive plan will help avoid attacks that can be detrimental to patients and your operations.

3) Implement threat intelligence and endpoint detection and response

Once a cyber attacker breaks out of that first machine or system, the goal is to stop them as soon as possible to avoid a cyber incident from becoming a much more catastrophic cyber breach. Drex DeFord, executive healthcare strategist at CrowdStrike, likens it to a healthcare trauma centre. "If you can give care to a patient within the first hour of arriving, you're way more likely to save them," he said. "The same holds true for cybersecurity."

Research conducted through CrowdStrike shows that it takes an adversary about 1.5 hours to break out of the first device and move laterally. Healthcare teams can work with security partners to develop standards that can pinpoint a breach quickly and eradicate it before the attacker can move further across a system. "What we've seen is if you can contain an attack within 60 minutes, you'll likely not fall victim to cyber criminals," said DeFord. An organization's endpoints should also be monitored continuously to compare tactics and techniques that could signal potential breaches so that immediate actions can be taken.

4) Secure your email

Email is the No. 1 threat factor when it comes to organizational breaches, with the vast majority of compromises starting with email and, unfortunately, staff members are often the weak link.

While organizations need an email gateway to weed out threat factors, they also need an in-depth analysis of these factors to determine their origin. “When we’re analyzing these email threats, we see that they are a multi-step approach,” said Erin Leonard, senior sales engineering manager at Proofpoint. That means they could be coming in with malware and then sell that information to a ransomware actor to use later. “We want to share that information with other technology vendors so that our library of threat awareness is growing, enabling us to protect you more and more.”

5) Prevent data leakage

With cloud-based data storage becoming an industry standard, healthcare organizations need to consider what security tools are needed to protect information in the cloud. Even in a managed cloud environment where sensitive information is housed, there could be users sharing this information within the organization or publicly.

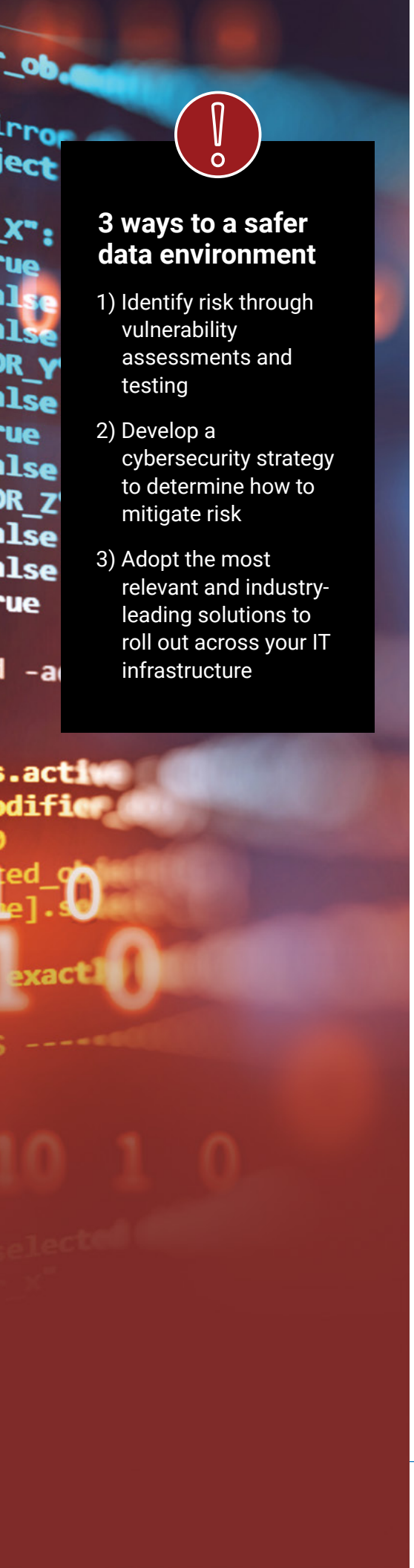
In a hospital environment there is the added threat of outside clinicians or contractors working on joint projects who are bringing in their own devices and software configurations. “We look at how much data is lost in misconfiguration, and addressing the door being left open in those environments is something we have to start thinking about,” said Damian Chung, business information security officer, Netskope. In understanding where data is going—and putting protocols in place to ensure it is not being shared inappropriately—organizations can have peace of mind in knowing they are controlling data leakage.

6) Implement multi-factor authentication and identity management

Now that the world is accessing data from various locations for virtual care, organizations need to be wary of people accessing these applications. Given that many of these outside environments have disparate identity stacks to manage all their touchpoints, security teams won’t necessarily know who is accessing data from where, which can lead to security threats.

Using multi-factor authentication or identity management can mitigate this risk. Adam Crown, group product marketing manager, Healthcare Solutions at Okta, says there are flexible and seamless authentication tools available that give organizations the ability to get risk signals from the environment and, based on those signals, ask for additional authentication as needed. “Oftentimes if it is not a risk event it allows the user to complete signal signoff,” he said. “The user experience is critical but balancing security is also top of mind.”

© 2022 Calian



3 ways to a safer data environment

1) Identify risk through vulnerability assessments and testing

2) Develop a cybersecurity strategy to determine how to mitigate risk

3) Adopt the most relevant and industry-leading solutions to roll out across your IT infrastructure

Take the First Step to Securing Your Systems

Partnering with security providers experienced in dealing with healthcare assets can help you find solutions customized to your environment to mitigate risk and protect sensitive patient information.

Don't wait until the next cyberattack to take action. Booking a cybersecurity vulnerability assessment now will get you started on securing the best security solution for your healthcare organization.

About Calian

Calian® helps people communicate, innovate, learn, stay safe and lead healthy lives with confidence. Every day, we live our values of customer-centricity, integrity, innovation and teamwork to engineer reliable solutions that solve complex problems. That's Confidence. Engineered. A stable and growing 40-year young company, we are headquartered in Ottawa with offices and projects spanning North American and international markets. Visit calian.com to learn about the diverse products, services and solutions we offer to healthcare, communications, learning and security sectors. www.calian.com

About iSecurity, a Calian company

iSecurity delivers world-class enterprise solutions that manage cybersecurity risk while addressing unique regulatory requirements and critical infrastructure. Its team is comprised of senior and fully accredited cybersecurity advisors (CISSP, CICA, CISM), enterprise architects (TOGAF, Zachman, SABSA) along with a 24/7 managed security and incident response services. www.isecurityconsulting.com

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 14,000 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. www.okta.com

About CrowdStrike

CrowdStrike provides cloud-delivered endpoint and cloud workload protection. Leveraging artificial intelligence (AI), the CrowdStrike Falcon® platform protects customers against cyberattacks on endpoints and workloads on or off the network by offering visibility and protection across the enterprise. www.crowdstrike.com

About Proofpoint

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyberattacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. www.proofpoint.com

About Netskope

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, the Netskope Security Cloud provides the most granular context, via patented technology, to enable conditional access and user awareness while enforcing zero trust principles across data protection and threat prevention everywhere. Unlike others who force trade-offs between security and networking, Netskope's global security private cloud provides full compute capabilities at the edge. www.netskope.com

CALIAN®

Confidence. Engineered.

© 2022 Calian