Cybersecurity: Guiding Principles and Risk Management Advice for Healthcare Boards, Senior Leaders and Risk Managers

Arun Dixit, Jennifer Quaglietta, Kopiha Nathan, Leo Dias and Duke Nguyen

Abstract

In recent years, the average cost of healthcare-related data breaches increased from approximately US$7 million in 2020 to over US$9 million in 2021. Moreover, breaches in healthcare have been consistently more costly than in other sectors for 11 consecutive years. With the frequency and costs of cyberattacks expected to rise, healthcare organizations must carefully plan for and identify strategies to mitigate cyber-related risks. This paper provides practical guidance for boards, senior leaders and risk managers in the development and implementation of organization-specific cybersecurity measures, with a focus on the identification, mitigation and management of risks.

Introduction

Canadian healthcare organizations have been faced with an elevated risk of cybersecurity threats, which has increased further since the onset of the COVID-19 pandemic (Canadian Centre for Cyber Security 2020). Furthermore, an increase in cybersecurity attacks has been attributed to increased activity by nation-state and cybercrime threat actors (Accenture 2021). Cybersecurity incidents in a healthcare organization can have serious and devastating consequences. They can lead to one or more types of adverse events, including service interruptions, operational and financial losses, patient safety issues and increased mortality rates, privacy breaches, potential civil action or class action lawsuits and regulatory penalties. Moreover, data breaches in the healthcare sector have been the highest for 11 consecutive years, with the average cost of a data breach increasing from US$7 million in 2020 to over US$9 million in 2021 (IBM Corporation 2022). Mitigating against a cyber breach requires increasingly digital healthcare organizations to ensure continuity of care for patients in the event of a cyber-related incident (Pina 2022). Due to the complex nature of cyber threats, security and infrastructure tools alone are not enough to protect an organization from risk as social engineering techniques can be used by threat actors to gain unauthorized access to systems. A single vulnerability can be exploited, which can cause a threat to the healthcare organization. The overall strength of an organization's defence plan is only as robust as its weakest points. As such, cybersecurity preparedness plans must reach all staff within an organization. Furthermore, as technology continuously evolves, so do the associated cyber threats and potential attack vectors. Threat actors are continuously innovating to exploit varying vulnerabilities in technology, workflows and human resources (Wilner et al. 2022). With healthcare organizations facing resource and funding scarcity for the investment, implementation, administration and maintenance of technologically advanced security solutions, seeking advice on ensuring cyber defence best practices and processes for healthcare leaders becomes increasingly important (Garcia-Perez et al. 2022).

Many factors are involved in the prevention of, preparation for and management of potential losses associated with cyber threats. Organizations must follow sound risk management strategies to ensure overall risk mitigation and resilience. Resilience can be achieved through building organization-wide cyber intelligence, expertise, partnerships and a culture of security with appropriate governance, strategy, policies and standards and controls, including appropriate information technology (IT) solutions.

Cybersecurity expert John Chambers has stated that there are only two kinds of organizations – those that have been hacked and know it and those that have been hacked and do not know it yet (Cisco Press 2016). With this urgency in mind, we present practical risk management-based strategies that leaders can adopt to help create organization-specific policies and practices.

Risk Management Principles

The risk management principles presented in this paper build on existing literature for the healthcare landscape. Several authors have presented recommendations for healthcare organizations to reduce the prevalence of security incidents through risk management practices. DeSouza and Valverde (2016) conducted a review of Canadian case studies and feedback from information security professionals to develop recommendations for organizations for reducing behavioural risk. Nifakos et al. (2021) conducted a systematic review of human factors–related literature and provided a summary of recommendations. More broadly, organizations including the Canadian Centre for Cyber Security (Canadian Centre for Cyber Security 2022) regularly provide recommendations on cyber preparedness and information regarding cyber alerts for IT professionals. Other authors have published guidance documents for Canadian healthcare organizations on risk management, including Canada Health Infoway (n.d.), Digital Health Canada (2022), HealthCareCAN (2022) and the Healthcare Insurance Reciprocal of Canada (HIROC) (HIROC 2017). This paper supplements existing work by providing a principle-based framework for guidance to leaders of Canadian healthcare organizations on the prevention of, preparation for and management of cyber risks.

Principles for Canadian healthcare organizations to consider when building organization-specific policies and practices for cyber risk management

These principles include governance and leadership; cyber risk management frameworks; risk-based management of cybersecurity; education and training; monitoring tools and technologies; and organizational cyber resiliency. A brief description of each principle is provided below.

Governance and leadership

Board oversight and corresponding senior management accountability are essential to fostering a successful cyber risk management program that effectively supports the implementation of cyber risk mitigation activities. Board oversight should, at a minimum, assign senior management accountability for cybersecurity and clearly delineate who will ensure the implementation of controls and mitigation strategies throughout the organization. A board committee can be positioned to receive regular updates from senior management or the subject matter expert on the progress and effectiveness of cyber risk management strategies. Boards can also undertake training, education and research to increase cyber literacy, understand challenges and risks faced by the organization, engage external experts regularly for updates and benchmarking and participate in informed discussions with management about critical cybersecurity exposures.

Senior management should also be accountable for the following:

- operationalizing cyber risk management activities that are mandated by the board,
- serving as an overarching enforcement body for the organization's cyber risk management undertakings,
- providing regular progress updates to the responsible board committee,
- ensuring that accountability for cybersecurity is cascaded throughout the organization from IT operational leads to all functional managers and leaders,
- preparing and critically reviewing the organization's cybersecurity incident response plan and
- keeping partners and stakeholders fully informed of the organization's cybersecurity strategy.

Several resources are available to support leaders in managing cybersecurity, including from the Chartered Professional Accountants of Canada (CPA Canada 2019) and HIROC (HIROC 2022).

Cyber risk management frameworks

Several well-recognized frameworks have been established for managing cyber risks, which can be fully or partially adopted to suit an organization's needs and business model. The National Institute of Standards and Technology (NIST 2018) cybersecurity framework addresses potential threats and risks to infrastructure and critical systems. The NIST framework applies the principles and best practices of risk management to improve the security posture and resiliency of the overall infrastructure. In addition, the SANS Institute's (2021) Centre for Internet Security Critical Security Controls framework provides a set of recommended actions focused on effective cyber defence.

The International Organization for Standardization (ISO) 27001/27002 framework provides best practice recommendations for holistic information security management system implementation standards (ISO n.d.). Adopting a cybersecurity framework can help organizations identify areas of weakness, build a road map to address the gaps and track and report the maturity level of the cybersecurity program.

Additional guidelines and checklists are available to support the development of organization-specific processes, including the *Ransomware Playbook* from the Canadian Centre for Cyber Security (2021), Cyber Loss Risk Reference Sheet from HIROC (2020) and learning modules from the Cyber Security Centre of Excellence (Government of Ontario 2020).

Risk-based management of cybersecurity

A risk-based approach can help organizations identify threats and vulnerabilities before they are found or exploited by a malicious actor, especially as new cyber threats and system vulnerabilities are constantly being discovered (IBC 2022). To effectively manage risks, organizations must keep abreast of what is happening externally and closely monitor their internal systems and processes.

Slow network performance or unusual increases in network traffic are some examples of internal environment monitoring that can lead to early identification of the emerging threat. Undertaking regular vulnerability assessments and penetration tests will also help organizations identify, validate and classify their vulnerabilities. Similarly, subscribing to security notifications, alerts and publications from vendors and trusted authorities can lead to the identification of external threats and new system vulnerabilities, such as zero-day vulnerabilities, in a timely manner.

Early identification of evolving risks can help organizations implement appropriate actions to mitigate them in a timely manner. Examples can include patching vulnerabilities, blocking traffic from selected geographical locations and others.

Education and training

State-of-the-art technology alone is insufficient to completely protect organizations against intentional or unintentional harmful actions of an end-user with access to systems, networks, devices and equipment. A 2021 report found that over 80% of cyber breaches involved a human element, including factors such as stolen credentials, successful phishing attempts or other human errors (Solomon 2022). Moreover, the average time to detect and contain a cyber breach is nearly 280 days, according to a recent report from the IBM Corporation (IBM 2022). As such, a strong organizational cyber-awareness training and education program is a critical factor for cyber preparedness.

Additional considerations for the development of a training program (Deloitte Touche Tohmatsu Limited 2019) include the following:

- A robust cybersecurity awareness training and education program should enable staff members to recognize cyber threats, such as phishing emails, malicious websites and others.
- Training programs should be conducted at more frequent intervals and tailored to specific user groups and the information they require.
- The development of success metrics can gauge completion and participation of training activities.
- Embedding cyber risk management thinking in all activities and decision making can strengthen the organization.

In the development of organization-specific cybersecurity success metrics, frameworks such as CARE (Consistent, Adequate, Reasonable and Effective), established by Gartner, Inc. (Gartner 2021), can be informative. This framework recommends organizations to consider success metrics in each of the following four categories:

- *Consistent:* Ensure that cybersecurity controls function as intended and comparably across all areas of an organization.
- *Adequate:* Ensure that controls are satisfactory according to business needs.
- *Reasonable:* Ensure that controls are appropriate given the need for maintaining security and the ability to perform business operations.
- *Effective:* Ensure that security controls and practices function as intended and provide desired outcomes.

Additional resources to support the development of technical success measures include "Building a Cybersecurity and Privacy Awareness and Training Program" (NIST 2021).

Monitoring tools, technology and activities

Tools for monitoring processes, systems and activities can help organizations with the proactive identification of potential anomalies in access patterns. Organizations may require external professional assistance to adopt holistic intrusion detection, as well as prevention and monitoring tools and activities. Early identification of potential threats and vulnerabilities will help organizations contain breaches in a timely manner and may help limit exposure and operational interruptions.

Healthcare organizations may not be able to effectively address all cyber-related risks on their own. Partnerships with other healthcare organizations and provincial and territorial bodies responsible for cybersecurity for public organizations can

lead to cost-effective cyber risk management strategies. This includes combining efforts to implement a centralized managed security service or security operations system that provides surveillance and protection software and monitoring. Smaller organizations can partner with nearby larger healthcare organizations so that resources can be pooled and applied efficiently.

Cyber resiliency

Cyber resiliency of an organization can be defined as its ability to effectively respond to, contain and manage cyber attacks or cyber-related breach events with the objective of minimizing operational impacts and associated losses. A comprehensive cybersecurity resiliency program includes formalized incident response plans, a disaster recovery plan, system downtime procedures, regular drills and testing of data recovery and appropriate cyber response education for staff and leadership teams, such as table-top exercises.

The first element of building a cyber resiliency program involves understanding the current state of an organization's cybersecurity posture. Healthcare organizations need to develop an inventory of existing assets, which may include data and their permission and sensitivity classifications; applications, software and systems; networks; and hardware to support IT infrastructure.

A comprehensive cyber resiliency program will also include strategies to prevent or minimize the loss experienced because of a cybersecurity incident. In general, cyber resiliency, cybersecurity incident management and loss prevention strategies are essential components of a comprehensive cyber risk management program. Minimum cybersecurity strategies for organizations to consider to help mitigate risk are provided in Table 1.

A Principle-Based Decision-Making Framework

When the potential for a breach or an actual breach is identified, immediate actions are required to support risk reduction and containment. By preparing ahead of time and building meaningful decision-making criteria for potential scenarios, healthcare organizations can manage difficult events and decisions more effectively.

The principles outlined in Table 2 are considerations that leaders should include when developing internal cyber risk management plans specific to their organization.

TABLE 1.
Minimum cybersecurity strategies for risk mitigation

Governance and leadership
• Regularly conduct board and senior management breach management education and simulations • Align cyber risk management with business needs and embed cyber preparedness into all organizational decision-making activities • Incorporate cybersecurity expertise into board governance
Cyber risk management framework
• Enforce multifactor authentication for user accounts • Ensure that account access provision is completed according to least privilege access, supplemented with ongoing access requirement reviews and validation • Perform regular testing of the business continuity plan and disaster recovery and system downtime procedures
Risk-based management of cybersecurity
• Establish and regularly test strategies for data retention, classification, backup and archiving • Develop internal and external contact lists of key stakeholders to notify in the event of a cyber event • Implement robust processes for evaluating vulnerabilities in new and existing technologies and applications
Education and training
• Establish policies and practices for strong and complex passwords • Conduct frequent, role-based staff training and education activities • Subscribe to monitoring services from reputable organizations and vendors to notify staff of potential breaches or vulnerabilities
Monitoring tools, technology and activities
• Implement tools to monitor for signs of potential intrusion • Implement and regularly update anti-virus, anti-malware and firewall applications • Implement patch management, including the timely application of patches and updates addressing security patches
Cyber resiliency
• Develop and regularly test cybersecurity breach incident response plans or playbooks • Adopt policies, tools and practices for SOC and SIEM • Regularly conduct simulations and debrief activities to continue to improve organizational resilience

SIEM = security incident and event monitoring; SOC = security operations centre.

TABLE 2.
Minimum considerations for the development of cyber risk management plans

Principle	Description
Containment	Have the appropriate threat isolation procedures been completed to remove or reduce the spread of ransomware?
Recovery potential	Is there any evidence to suggest that the attack was based on malware that can leave files inaccessible regardless of any containment actions?
Backups	Are recent backups of the data assets easily available? Can these backups be accessed with minimal impacts to services?
Data permanence	Consider the varying impacts of data elements that can be changed by the impacted organization or parties (such as passwords) and other data elements that cannot (such as an individual's date of birth).
Impact	Does the attack present a major critical disruption causing an inability to function safely?
Legality	Jurisdictions may have varying legislation regarding the legality of making payments in the event of a cyber breach.
Disclosure and reputational risk	Is there an obligation to disclose the attack to relevant authorities or its clients?
Limitations	What are the terms and conditions of an organization's insurance coverage?

Conclusion

As Canadian healthcare organizations continue to face increasingly frequent and complex cyber-related threats, guidance on the mitigation and response of these incidents becomes increasingly important. Organizational resilience in response to cyber threats can be achieved through a variety of approaches. What is essential is building expertise at all levels in cyber intelligence, fostering partnerships and promoting a culture of security with appropriate governance, strategy, policies and standards and controls. This paper has sought to add to the body of literature on risk management for Canadian healthcare organizations by providing advice on principle-based risk management, as well as outlining considerations for organizational decision making in the event of a cyberattack. HQ

Acknowledgement

The authors thank Catherine Gaulton, Trevor Hall and HIROC's Healthcare Safety and Risk Management team.

References

Accenture. 2021, August 4. Triple Digit Increase in Cyberattacks: What Next? Retrieved January 13, 2023. <https://www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks>.

Canadian Centre for Cyber Security. 2020, March 20. Alert - Cyber Threats to Canadian Health Organizations. Government of Canada. Retrieved June 7, 2022. <https://cyber.gc.ca/en/alerts/cyber-threats-canadian-health-organizations>.

Canadian Centre for Cyber Security. 2021, November 30. *Ransomware Playbook*. Retrieved June 7, 2022. <https://cyber.gc.ca/sites/default/files/cyber/2021-12/itsm00099-ransomware-playbook-2021-final3-en.pdf>.

Canadian Centre for Cyber Security. 2022, October 28. Information and Guidance: Cyber Security Guidance. Government of Canada. Retrieved June 7, 2022. <https://cyber.gc.ca/en/information-guidance>.

Canada Health Infoway. n.d. Infoway Works Closely with the Provinces and Territories to Develop Solutions that Protect Personal Health Information. Retrieved June 7, 2022. <https://www.infoway-inforoute.ca/en/digital-health-initiatives/privacy-security>.

Chartered Professional Accountants (CPA) Canada. 2019. 20 Questions Directors Should Ask about Cybersecurity. Retrieved January 13, 2023. <https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/information-management-and-technology/publications/questions-directors-should-ask-about-cybersecurity>.

Cisco Press. 2016, February 16. Responding to Real-World Cyber Threats. Retrieved August 22, 2022. <https://www.ciscopress.com/articles/article.asp?p=2481826>.

Deloitte Touche Tohmatsu Limited. 2019. *Deloitte Cyber Awareness Training*. Retrieved December 22, 2022. <https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/risk/Cyber-Awareness-Training-fact-sheet-October-2019.pdf>.

DeSouza, E. and R. Valverde. 2016. Reducing Security Incidents in a Canadian PHIPA Regulated Environment with an Employee-Based Risk Management Strategy. *Journal of Theoretical and Applied Information Technology* 90(2): 197–208.

Digital Health Canada. 2022. Cyber Security Resources. Retrieved June 7, 2022. <https://digitalhealthcanada.com/cyber-security-resources/>.

Garcia-Perez, A., J.G. Cegarra-Navarro, M.P. Sallos, E. Martinez-Caro and A. Chinnaswamy. 2022. Resilience in Healthcare Systems: Cyber Security and Digital Transformation [Available online]. *Technovation*. doi:10.1016/j.technovation.2022.102583.

Gartner. 2021, September 15. 4 Metrics that Prove Your Cybersecurity Program Works. Retrieved October 18, 2022. <https://www.gartner.com/en/articles/4-metrics-that-prove-your-cybersecurity-program-works>.

Government of Ontario. 2020, September 30. Cyber Security Centre of Excellence. Retrieved June 7, 2022. <https://www.ontario.ca/page/cyber-security-centre-excellence>.

Healthcare Insurance Reciprocal of Canada (HIROC). 2017, November. *Cyber Risk Management: A Guide for Healthcare Administrators and Risk Managers*. Retrieved June 7, 2022. <https://www.hiroc.com/system/files/resource/files/2018-10/Cyber-Guide.pdf>.

Healthcare Insurance Reciprocal of Canada (HIROC). 2020, September. *Risk Reference Sheet: Cyber Loss*. Retrieved June 7, 2022. <https://www.hiroc.com/system/files/resource/files/2020-11/Cyber%20Loss_0.pdf>.

HealthCareCAN. 2022. Leading Practices in Cyber Security. Retrieved June 7, 2022. <https://www.healthcarecan.ca/our-work/champion/cyber-security/>.

IBM Corporation. 2022. *Cost of a Data Breach: A Million-Dollar Race to Detect and Respond*. Retrieved December 22, 2022. <https://www.ibm.com/reports/data-breach>.

Insurance Bureau of Canada (IBC). 2022. Cyber Risks: An Increased Threat during COVID-19. Retrieved August 22, 2022. <http://www.ibc.ca/ns/business/risk-management/cyber-risk/an-increased-threat-during-covid-19>.

International Organization for Standardization (ISO). n.d. ISO/IEC 27001 and Related Standards Information Security Management. Retrieved June 7, 2022. <https://www.iso.org/isoiec-27001-information-security.html>.

National Institute of Standards and Technology (NIST). 2018, April. Cybersecurity Framework. Retrieved June 7, 2022. <https://www.nist.gov/cyberframework/framework>.

National Institute of Standards and Technology (NIST). 2021, September 21. Building a Cybersecurity and Privacy Awareness and Training Program. Retrieved December 22, 2022. <https://csrc.nist.gov/News/2021/pre-draft-call-for-comments-sp-800-50>.

Nifakos, S., K. Chandramouli, C.K. Nikolaou, P. Papachristou, S. Koch, E. Panaousis et al. 2021. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors* 21(15): 5119. doi:10.3390/s21155119.

Pina, L. 2022, February 28. Improving the Cybersecurity Posture of Healthcare in 2022. Retrieved June 7, 2022. <https://www.hhs.gov/blog/2022/02/28/improving-cybersecurity-posture-healthcare-2022.html>.

SANS Institute. 2021, May 18. CIS Controls v8. Retrieved June 7, 2022. <https://www.sans.org/blog/cis-controls-v8/>.

Solomon, H. 2022, May 24. *Human Error Tops Causes of Data Breaches, Says Verizon Report*. Retrieved August 2022. <https://www.itworldcanada.com/article/human-error-tops-causes-of-data-breaches-says-verizon-report/485343>.

Wilner, A.S., H. Luce, E. Ouellet, O. Williams and N. Costa. 2022. From Public Health to Cyber Hygiene: Cybersecurity and Canada's Healthcare Sector. *International Journal: Canada's Journal of Global Policy Analysis* 76(4): 522–43. doi:10.1177/00207020211067946.

About the Authors

Arun Dixit, BASc, M. Eng, is a digital and innovation strategist at HIROC. He is passionate about improving healthcare safety. He can be reached by e-mail at adixit@hiroc.com.

Jennifer Quaglietta, BASc, MBA, held a position as the past vice president, Performance Excellence and Information Services at HIROC, and lead system transformation in support of creating a safer healthcare system across Canada.

Kopiha Nathan, BCom, is the lead privacy compliance officer at HIROC. In this role, she leads HIROC's privacy program and oversees compliance for internal information security controls.

Leo Dias, BEng, MSc, is the director of Information Services at HIROC. In this capacity, he supports HIROC's subscribers and staff in leveraging information to create a safer healthcare system.

Duke Nguyen, Diploma (Computer Networking), is the team lead, Infrastructure and Service Management at HIROC and oversees numerous initiatives to support operational excellence in information technology initiatives.