Managing cybersecurity risks in the health sector
The path to securing greater public trust

Cyber attacks and security breaches have steadily increased across Canada and the world—and health organizations are seen as a leading target. In May 2017, the United Kingdom’s National Health Service faced major disruption with a significant ransomware attack. While no information was compromised, the attack postponed some operations and raised concerns about the state of cybersecurity in the health care sector.

Health care organizations are greater targets for theft than organizations in other sectors for a few key reasons. The personal health and research information these facilities hold are high-value commodities to cyber criminals. And decentralized information systems provide for greater access, putting patient care, research and privacy at risk.

In 2017, we collaborated with a sampling of Ontario health care organizations to assess their cybersecurity readiness. They were all aware of the approach we undertook and gave us permission to help them get a broader view of cybersecurity. We simulated the techniques real attackers would use to steal sensitive information, focusing on avoiding detection and monitoring. And we were able to access some sensitive information without being detected in a surprising number of cases. While steps have been taken to remediate these specific issues, the threat of new vulnerabilities is ever-present. Based on our analysis of what we discovered, we’re recommending actions organizations can take to focus their resources, be more proactive and start on the path to greater patient trust in the face of unprecedented security threats.

84% of Canadian executives in all sectors see cybersecurity and privacy skills as important to their organization. - Digital IQ 2017 - Canadian insights
Health care organizations are increasingly aware of the importance of managing cybersecurity risks. Based on our study, we recommend five actions that can be taken to translate risk awareness into improved cybersecurity.

1. **Develop a risk-informed cyber strategy**

A cyber risk management strategy should be informed by an awareness of the threats organizations face. To start, assess the threats against the facility’s digital assets and identify potential security issues. It’s important that health care organizations organize themselves by developing a clear list of cybersecurity priorities and resources required to support meaningful transformation. Use the help of experts throughout the process, if needed.

Best practices for conducting a risk assessment also include having a clear understanding of the assessment’s purpose and scope. With a proper assessment and strategy, organizations have a clear, actionable way to achieve their goals in the face of change while preserving their priorities.

2. **Actively monitor systems**

If hackers infiltrate an organization’s systems, it’s important to be able to detect their movements—and take quick action in response. But a lack of strong internal monitoring is common in health care organizations across Canada. During our in-depth assessment, we were able to uncover sensitive information from a few facilities without being detected, highlighting the need for continuous monitoring of systems for abnormal activity.

Organizations should develop playbooks and review their internal procedures to determine what alerts are generated and what procedures are used to follow up on them. This will help guide them during a potential security breach. And when working with third parties, make sure to get a full picture of the data shared with the third party—and manage any risk with contractual obligations. Good monitoring can go a long way to preventing damage caused by a breach.

3. **Improve security awareness among staff**

Health care organizations are at risk of targeted phishing attacks. During our assessment, several staff revealed their credentials through emails, and then we used these credentials to gain access to their internal network. These organizations are also vulnerable to physical intrusions, where hackers enter facilities and connect unauthorized devices to get remote access to internal systems.

Security awareness training is key in preventing employees from falling for sophisticated attacks or letting unauthorized personnel into sensitive areas. Dedicate time and resources to raise awareness, train employees and monitor their activities. Organizations should conduct regular phishing tests to detect problems, and then provide coaching.

---

Managing cybersecurity risks in the health sector 3
Discover and act on vulnerabilities

Find vulnerabilities and configuration issues before a hacker exploits them. First off, health care organizations should perform periodic vulnerability assessments on top of making sure systems are as robust as possible. Beyond that, penetration testing will help facilities spot a majority of flaws in their environments that could leave sensitive data open to attacks. A penetration test will help identify if organizations are acting on any vulnerabilities and configuration issues, so it’s important to do a vulnerability assessment before initiating a penetration test.

Engage leadership

Senior leaders must take ownership of building cyber resilience and drive the development of a cyber risk management culture at all levels. Across all sectors, only 44% of respondents in our 2018 Global State of Information Security® Survey say boards are actively shaping their organizations’ security strategies.

It’s important to establish a top-down strategy to manage cyber and privacy risks across all health care organizations. There are many stakeholders involved: boards need to set the mandate, management needs to enable its teams and teams need to do an effective job. The most secure organizations are in a position to succeed due to strong leadership and a board-level mandate around cybersecurity.

What’s next?

In the face of unprecedented security threats, it’s time to take a broader view of managing cybersecurity to help protect patients, research and privacy. Acting on these recommendations can help our health care organizations mitigate cybersecurity risks.

Contact us

Catherine Hunter
Partner, Health Consulting Leader
PwC Canada
416 687 8465
catherine.hunter@pwc.com

Richard Wilson
Partner, Cybersecurity & Privacy
PwC Canada
416 941 8374
richard.m.wilson@pwc.com

Tara McCarville
Partner, Health Industries
PwC Canada
416 869 2493
tara.mccarville@pwc.com

David Craig
Partner, Cybersecurity & Privacy
PwC Canada
416 814 5812
david.craig@pwc.com

pwc.com/ca/healthcare-cyber

© 2018 PricewaterhouseCoopers LLP, an Ontario limited liability partnership. All rights reserved. PwC refers to the Canadian member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.