Preparing Your Credit Union for New Digital Privacy Laws

By Danny Timmins, CISSP

Canadian credit unions will need to critically assess not only their own cyber security practices, but also have a plan to monitor and manage the ever-increasing number of third-party technology providers they rely on every day to provide services and products their members and owners demand. Changes to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) increase the already significant consequences of a data breach. With many of these rules already in place as of November 1, 2018, those who have yet to align the new framework with their pre- and post-incident planning face potentially irreversible financial and reputational damage.

KEY TRENDS

According to Cisco's Global Cloud Index, 59 percent of all cloud workflows will be delivered as software-as-a-service (SaaS) by the end of 2018. Credit union digital transformation is no different. As workloads and sensitive member / employee data are moved to third parties, the impact of the new digital privacy laws no longer focus just on your credit union. This new legislation will require you to take responsibility for both privacy and security provided by your cloud providers.

KEY CHANGES

Among the most notable and consequential changes to the existing legislation is the introduction of mandatory breach reporting – which outlines an organization's responsibility to report any data compromise that has the potential to cause 'real risk of significant harm' to federal regulators and affected individuals. Also, the Act increases responsibility of organizations to maintain records of every data breach they experience for a minimum of 24 months following the attack.

Determining Harm

While more specific information will follow as the regulations mature, organizations will need to be vigilant in gauging the extent to which any breach that causes humiliation, damages an individual's reputation or relationships and including where it leads to identity theft. Other factors to consider include the likelihood stolen information could be misused and the degree of suffering or stress that an individual could experience from learning their information was compromised.

Reporting to Regulators

Organizations which experience a data breach must now submit a formal written report to the privacy commissioner which comprehensively details when the incident occurred, the circumstances of the breach itself, what personal information was (or was at risk of being) compromised and the number of affected individuals.

Reporting to Affected Individuals

Individuals whose information was (or was at risk of being) compromised, must also receive timely notice from the affected organization detailing the circumstances of the breach, timeline and what information is or was at risk.

Moreover, the affected organization must also communicate what they have done to reduce the risk of harm to the individual, what the individual can do themselves to reduce their risk of harm and who they can contact to get more information about the breach.

CONSEQUENCES

As cyber incidents become increasingly frequent and sophisticated, so are the consequences of a breach. Organizations must already be prepared to navigate the costs of addressing, containing and eliminating the threat – along with managing the ongoing legal and reputational damages. With this new legislation comes the potential for significant fines as well.

In fact, under the new compliance regime, the privacy commissioner has far-reaching powers to investigate whether organizations have sufficiently met their reporting and communications obligations. If organizations are unable to demonstrate they adequately responded to a breach or maintain comprehensive records, they could face fines between $10,000 and $100,000 per offense, though the financial impact caused by reputational damage may be even more severe.

HOW TO PREPARE

You may understandably have concerns around the costs and challenges of meeting these new regulations. However, this also presents an opportunity to build (or rebuild) your cyber security compliance structure around a clear regulatory framework and eventually to establish an information security management system. While being prepared to communicate the details of a potential breach is paramount – a robust cyber security program remains the best strategy for avoiding ever having to do so.

Addressing the following areas now can help you reduce the likelihood of a breach, minimize the scope of data compromise and prepare to act swiftly to contain, communicate and resume operations following a cyber security incident:

Information Collection, Usage, Storage and Disclosure – Keep up to date an inventory of what information you collect about your members, employees, contractors, customers and stakeholders. Consider:

- Is this information necessary for your business objectives?
- Do you have a readily accessible privacy policy documenting how you collect, use, share and protect personal information and data?
- How do you share personal information with internal and external audiences? Do you have the right security measures and policies in place to prevent a potential compromise across every touchpoint?

Security Safeguards and Procedures – Take an objective view of your current cybersecurity infrastructure to determine which threats your organization is most likely to encounter and whether you are prepared to face them. Ensure you have clear directions for handling sensitive information and effective organization-wide communication.

Internal Policies, Practices, Systems and Records – Breaches are most likely to occur at your weakest points. Ensure you protect your whole organization by systematically reviewing all hardware, software and networked devices for alignment with your cyber security safeguards and procedures.

Cyber Security Training – With phishing and other social engineering attacks on the rise, ensure all employees are aware of their role in preventing a breach, understand their role in protecting sensitive information and know when, how and to whom to report suspicious activity.

Incident Response Plan – Your organization needs clear and actionable steps for what to do in the event of a cyber security breach. Review your incident response plan to ensure it offers clear direction for how to contain, pacify and eliminate a cyber attack; provides a list of internal and external contacts and when to reach out to them and describes what information to report and to whom. If you don't have an incident response plan, now's the time to implement one.

Cyber Security Insurance Coverage – Insurance can be a helpful tool to offset the financial costs of a potential data breach, but it's important to understand what your policy covers, whether your level of coverage is sufficient and whether your organization's cyber security infrastructure is adequate to meet your policy guidelines.

MNP CAN HELP

Whether you need assistance aligning your reporting and documentation processes with the new PIPEDA regulations, require a comprehensive review of your cyber security infrastructure or are interested in fully-managed service option – MNP's Cyber Security team can help protect your credit union from a growing list of digital threats.

About MNP

MNP is a leading national accounting, tax and business consulting firm in Canada. We proudly serve and respond to the needs of our clients in the public, private and not-for-profit sectors. Through partner-led engagements, we provide a collaborative, cost-effective approach to doing business and personalized strategies to help organizations succeed across the country and around the world.

For more information on digital privacy laws, contact:

Danny Timmins, CISSP
National Cyber Security Leader
T: 905.607.9777
E: danny.timmins@mnp.ca

Eugene Ng, BComm, CISSP
Cyber Security Leader, Eastern Canada
T: 647.202.6241
E: eugene.ng@mnp.ca