Issue #5 July 9, 2015

Breach Response Plans

by *Lyndsay A. Wasser*, CIPP/C, Co-Chair Privacy

Privacy breaches can occur despite an organization's best efforts to prevent them. When such incidents arise, it is important to have a response plan in place so that valuable time is not lost scrambling to assign roles and responsibilities.

Each of the privacy commissioners has issued guidelines on responding to privacy breaches. Although certain specific details vary, in general, all of the regulators recommend the four steps outlined below for responding to a privacy breach. The first three steps should be undertaken immediately following a breach, and can be implemented simultaneously, and all four steps should be addressed in every organization's breach response plan.

Step 1 – Contain the Breach

Prompt containment of any privacy breach is key to minimizing risk and potential damages. Containment can include:

- Stopping any unauthorized practices
- Steps to recover any lost information
- Shutting down any electronic system that was breached
- Revoking or changing computer access codes
- Correcting weaknesses in physical or electronic security
- Removing from the workplace any person who is responsible for an intentional breach

Step 2 – Evaluate the Risks

This step includes designating a person or team to be responsible for leading an investigation into the breach, and then evaluating the risks to the organization and individuals whose personal information may have been affected by the incident.

In evaluating the risks, the organization should consider:

- The number of individuals affected by the breach
- The identity of persons affected by the breach (e.g., employees, customers, members of the public)
- The type and quantity of information involved, including the sensitivity of the information
- Potential harm to individuals (e.g., identity theft/fraud, security risks, financial loss, humiliation or damage to reputation)
- Potential harm to the organization (e.g., risks to reputation, loss of assets, exposure to legal proceedings, fines or other regulatory penalties)
- The cause of the breach (e.g., whether the breach was intentional/malicious or accidental), including the known or probable perpetrators
- Security measures that were in place to protect the information (e.g., whether a lost device was password protected and/or whether information was encrypted)
- Whether the breach resulted from an isolated incident vs. a systemic issue
- The extent of the disclosure, including the number of likely recipients and whether there is a risk of on-going breaches or further exposure of the information

Step 3 – Notification

Internally, persons responsible for privacy compliance within the organization should be notified as soon as possible of any actual or potential breach. Depending upon the company's structure, other internal notification may also be required, including notification of senior management and/or persons responsible for managing media relations.

In terms of external notification, in Canada, breach reporting is currently mandatory under Alberta's *Personal Information Protection Act* ("Alberta PIPA") and the personal health information protection legislation in Ontario, Newfoundland and Labrador, and New Brunswick.

Alberta PIPA requires that the organization notify the Information and Privacy Commissioner (the "IPC") of any incident involving the loss of, or unauthorized access to, or disclosure of personal information, without unreasonable delay, where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure. The IPC can then require the organization to notify affected individuals.

The federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") has also been amended to require breach reporting. Such amendments have not yet come into force, but will become mandatory once the associated regulations have been enacted. Under PIPEDA, organizations will be required to notify the Office of the Privacy Commissioner of Canada (the "OPC") and affected individuals of a security breach involving personal information if the breach poses a "real risk of significant harm" to the affected individuals. Government institutions and other organizations will also need to be notified in certain circumstances. Furthermore, organizations will be required to keep a record of all data breaches (whether or not they meet the harm threshold described above), and must report all breaches to the OPC upon request. Failure to report or record a breach will be an offence punishable by fines of up to C$100,000.

In addition to the statutory reporting obligations described above, the organization should consider whether it has any contractual notification requirements. It is becoming increasingly common for organizations to require notification of any actual or suspected breach of personal information that is processed or handled by their service providers.

Finally, the organization should consider whether any form of voluntary notification is necessary or prudent in the circumstances. For example, the organization may consider notifying:

- Legal counsel, who can guide the organization through the breach management process and defend the organization against any claims arising from the incident
- Law enforcement authorities, if the breach was caused by illegal activity or could result in the commission of a crime

- Affected individuals who could be at risk of identity theft or other harm, so that they can take steps to protect themselves
- Relevant privacy commissioners, so that they can respond to inquiries or complaints that are directed to them about the incident
- Insurers, if the organization has coverage applicable to the incident
- Credit card companies, credit reporting agencies and/or financial institutions, where the incident could lead to attempted identity theft
- Union representatives, where employees' personal information is compromised
- Other relevant parties, such as professional or regulatory bodies, authorized agents, or third party contractors

Although voluntary notification may be beneficial in some circumstances, the organization should carefully consider the manner and content of such notices to ensure that they do not inadvertently cause more harm. For example, providing too much information in mass notices could lead to additional unauthorized disclosure of personal information respecting affected persons.

Organizations are encouraged to contact their legal advisor for guidance on content, timing, and method of notifications.

Step 4 – Prevention of Future Incidents

After the organization has dealt with the immediate consequences of a breach, it should turn its attention to preventing future incidents. Depending upon whether the incident involved an isolated event or systemic flaws, this component of the process may involve:

- A security audit of both physical and technical controls
- Developing procedures or implementing controls to correct systemic issues, including remediation of any gaps in security measures
- Review of and improvements to privacy policies
- Improvements to training programs
- Discipline of employees involved in the breach, where appropriate

Although the guidelines set out above provide a good starting point for organizations looking to develop breach response protocols, it is important for the organization to customize this process to reflect its unique circumstances and internal processes. Ideally, a customized breach response plan will specifically delineate roles and responsibilities in the event of a breach, so that individuals will understand the part they are expected to play if an incident occurs. Such advance planning will prevent panic and disorganization in the aftermath of a breach.

In addition, as always, even the best policy or plan will not be useful to the organization if employees are not familiar with it. Therefore, persons who are expected to be involved in the breach response process should be provided with information and training on: (1) what constitutes a privacy breach; (2) what steps to take in the event of a potential breach; and (3) the organization's response plan, including specific contact information for the person(s) responsible for leading the containment and risk evaluation process.

For more information on this topic please contact:

Toronto Lyndsay A. Wasser 416.865.7083 lyndsay.wasser@mcmillan.ca

a cautionary note