Data Breach Response & Damage Control Game Plan

Privacy lapses and data breaches can occur despite your best efforts to prevent them. If prevention does fail, the imperative switches to incident response and damage control. Here's a 5-phase Game Plan for minimizing the impact of data breaches at your own organization.

Why You Need a Data Breach Response Plan

Most companies collect, use, and disclose private personal information about their employees and clients to conduct business. Allowing this data to fall into the hands of an unauthorized person can have serious consequences for not just the affected individuals but also the business that failed to keep their personal data confidential and secure. Such data breaches typically involve the theft, loss, or unauthorized use or disclosure of protected information. They may be the result of outside cyberattack or acts and omissions of a company's employees, such as where an employee loses a laptop containing client information or accesses personal data without authorization for an improper purpose.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) and provincial privacy laws require companies to take immediate actions to respond to data breaches. While the latter laws generally cover a limited range of organizations, including government agencies and healthcare companies, any company that handles confidential personal data should have plans in place to ensure fast and effective breach response. Such a plan should provide for responding to breaches in 5 phases.

Phase 1: Assess & Contain the Scope of the Breach

The first thing to do when a breach occurs is assess the nature and extent of the breach and take immediate steps to contain it. The assessment is a preliminary determination of:

- What and how much protected personal information the breach potentially compromised.
- Who and how many people the breach may have affected.
- Which of your systems the breach exposed or may have exposed and when.
- Whether any protected information has fallen into the hands of unauthorized recipients and who those recipients are.

You'll have to do an extensive investigation after you get the breach under control. But for now your focus should be on containing the immediate problem. Recommendations from the Ontario Information and Privacy Commissioner (OIPC):

- Try to contact any unauthorized recipients you've identified to arrange for the information's secure return or destruction.
- Get unauthorized recipients to provide you documented assurance that they've returned or destroyed the information and haven't retained any copies.
- Change passwords, temporarily shut down systems, and take any other actions necessary to fix identified vulnerabilities and prevent further unauthorized access to protected information.
- Suspend the access rights of any staff members who accessed protected information without authorization, pending a fuller investigation.

Phase 2. Perform Real Risk of Significant Harm (RROSH) Assessment

Once the smoke clears, step back and figure out just how big a problem you're facing. Privacy laws require regulated institutions to assess whether the harm to individuals affected by a data breach rises to a threshold known as real risk of significant harm (RROSH). Significant harm generally includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property. According to the OIPC, factors to consider in determining whether a breach meets the RROSH threshold include:

- The sensitivity of personal information involved in the breach.
- The probability that the personal information has been, is being, or will be, misused.
- Where there are steps the affected individual could take to reduce the risk of or mitigate the harm resulting from the breach.

Phase 3. Notify Affected Individuals of RROSH Breaches

If you determine that the breach meets the RROSH threshold, you must notify affected individuals as soon as feasible after the breach occurs. Privacy laws set out detailed requirements that regulated institutions must follow when providing breach notification to individuals. Companies not subject to privacy laws may have breach notification duties under other laws and/or contracts with clients, employees, or third-party contractors.

General Best Practices for Individual Notification of Privacy Breaches

If possible, notify individuals of data breaches directly via phone call, letter, email, or in person. Provide indirect notification, e.g., a prominent posting on the landing page of your company's website, only if:

- You can't determine the identities of affected individuals after taking reasonable steps to do so.
- You have good reason to doubt the accuracy, timeliness or reliability of the contact information you have.
- Direct notification would unreasonably and significantly interfere with business operations.
- Direct notification would be reasonably likely to harm the affected individuals.
- The breach affects a significantly large number of individuals making direct

notification impractical.

Whether direct or indirect, write the notice in plain language and include the following information:

- The personal information that the breach affected.
- How the personal information was affected by the breach.
- The number of individuals whose personal information was or may have been compromised.
- The circumstances of the breach.
- The cause of the breach, if known.
- The date or period of time when the breach occurred.
- The date the breach was discovered.
- The steps you're taking to contain the breach and minimize the risk of harm to affected individuals.
- The steps affected individuals can take to protect themselves, such as advising their bank or credit card company of the breach, monitoring their bank and credit card accounts for suspicious activity, and getting a copy of their credit report from a credit reporting bureau.
- Contact information for somebody at your company who can answer questions or provide additional information or assistance about the breach.

Phase 4. Provide Required Notice of RROSH Breaches to Regulatory Authorities

Government agencies and companies covered by provincial privacy laws generally have to report RROSH breaches to the provincial privacy commission and other regulatory authorities in accordance with the specific provisions of those laws. Companies may also have to provide notification of certain kinds of breaches to law enforcement, professional bodies, the Canadian Centre for Cyber Security, and other regulatory or quasi-regulatory authorities. Breach reporting may also be required under business contracts, such as agreements with suppliers of the technology involved in the breach. In all cases, be sure that the notification you provide meets all of the specific requirements of the applicable law or contract.

Phase 5. Identify & Correct Vulnerabilities

The final phase of privacy breach response is to do a thorough investigation of what went wrong. Identify the problems or weaknesses in your systems, protocols, and policies (including those relating to HR) that the breach created or exposed and what you must do to correct them to prevent a recurrence. Document and continually monitor your corrective actions and overall privacy breach response plan and make additional adjustments as necessary. Stage periodic drills or simulated exercises to ensure that everyone involved in the response plan understands and is capable of carrying out their responsibilities in a timely, coordinated, and effective manner.