RISK INSIGHTS

WHEN A CORPORATE DATA BREACH HAPPENS: CRITICAL NEXT STEPS

Regardless of cybersecurity proficiency, no organization is safe from data breaches. That's why it's critical every business develops and documents an Incident Response Plan. Your response plan will outline steps your organization should take if you suspect data has been compromised. The quicker your business follows the plan, the better off you will be and you will be in a position to mitigate the impact the data loss will have on your business.

ACCORDING TO IBM'S 2021 CYBER RESILIENT ORGANIZATION STUDY, 54% OF ORGANIZATIONS DO NOT HAVE AN INCIDENT RESPONSE PLAN APPLIED CONSISTENTLY ACROSS THEIR ORGANIZATION.

Reviewing recent data breaches, you realize there's a wide range of targeted organizations — from global corporations to government agencies to small and medium-sized businesses (SMBs). Given the accelerating pace of data breaches, many observers caution that most companies will experience an incident at some point. The time to prepare your organization is *now*.

Building your breach response team

Key personnel must be trained and understand their responsibilities to effectively respond when a security breach occurs. By identifying and containing a breach your business can save a lot of money and negative consequences.

When developing a data breach response plan, activities across all teams should be coordinated to reduce the chances of unintentional errors.

IT and Security personnel should continuously assess the company's data security gaps and train on how to detect vulnerabilities and apply necessary security measures. They are also the first responders for the containment and remediation of a breach. According to IBM's 2021 Cost of a Data Breach Study, it took an average of 287 days to identify and contain a data breach. Companies that identified a breach in less than 200 days saved more than $1 million on average compared to those that took over 200 days.

The **Legal Team** may need to work alongside IT, depending on the severity of the breach, to identify legal obligations and provide advice.

Human Resources will serve as the frontline for communicating with employees, especially if their personnel information was breached. They may also help equip employees with resources and best practices for further protecting themselves and their families (both before and after a reported security incident).

The **Communications Team** is accountable for notifying those impacted, as well as the press. They must work together with the Legal Team to make sure communications are timely and accurate. This approach can help to minimize the possibility of government-imposed fines from regulations such as Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), or foreign regulation if you have customers outside Canada.

The Personal Information Protection and Electronic Documents Act (PIPEDA) dictates the notification requirements of your business. The law requires that you report any breach of security safeguards that pose a real risk of significant harm (RROSH) to an individual. The chances for litigation and fines can be diminished as your business becomes familiar with these requirements. Being timely with your notification also promotes an honest demeanour, helping protect your business' reputation and helping reduce possible customer turnover.

Developing a breach communications plan

As a reputable company, you are responsible for notifying law enforcement, other affected businesses, partners, employees and customers of the potential information disclosed. Post data breach communications may include explaining how the incident occurred, what information was compromised, what actions have been taken to remedy the situation and how your business intends to protect affected individuals.

It's important to note that authorized spokespersons should be identified and prepared with answers, such as a formal Q&A document. In addition, be prepared for inquiries to surface via phone calls, e-mails, social media and the press. Keep your communication honest and timely, as this can help you maintain strong relationships with your customers.

Training and awareness

For your Incident Response Strategy to be effective, employees should periodically practice with simulated breaches. If an event does occur, response team members should be familiar with the processes within the plan and ready to jump into action. When executing your plan, keep a keen eye on potential roadblocks and improve the framework with every rehearsal.

Making your Data Breach Response Plan a routine can help your organization be better prepared for an actual breach.

3 PROACTIVE TIPS FOR TODAY'S DATA BREACH ENVIRONMENT

1. **Be prepared**
   Don't wait until a breach occurs to create your response plan.
2. **Protect your employees, customer and partners**
   Consider arming your business and its stakeholders with identity protection tools as an added layer of defense.
3. **Practice makes perfect**
   An actual breach should not be the first time your team goes through your business' Incident Response Plan. Prepare by practicing.

For more information on making your business safer, contact your broker or visit us at **www.northbridgeinsurance.ca**.

[4051-001-ed03E | 05.2023]

Northbridge® Insurance | CYBERSCOUT® A TransUnion® Brand