7 Steps to Address a Data Breach

Three-quarters of organizations in the US and Europe have suffered a data breach during the past two years says a 2016 Ponemon report. The percentage is significantly higher than the number from the same survey conducted two years ago. According to the experts, it's not a matter of "if" you have a breach but "when".

Before you suffer a breach, you should know what data you have, its importance to your business and the regulations that affect it. This is critical for you to know how to respond when it's compromised. And because time is of the essence when addressing a data breach, there are a number of key steps that a company should take to minimize the associated risk.

1. Alert Security and Document

Inform your corporate security and IT departments immediately. Complete an incident report so that there is evidence of the prompt action taken to investigate and contain the breach. Describe what happened and what is being done.

2. Secure the Evidence

Secure all computers and mobile devices that could be involved in the breach. Take all involved devices offline but avoid turning on computers or devices that are off. Engage a forensics team to examine computers and devices if you don't have in-house expertise and follow their advice for securing devices and files.

3. Investigate

Whether you notify your internal investigative team or call in outsiders, it's important to act immediately to get the investigation started and the preservation of evidence under way before valuable evidence is deleted or lost. Interview everyone involved and anyone who might know anything about the breach.

4. Notify Your Customers

Notify your customers, if necessary, according to data breach notification regulations for your jurisdiction. Most US state laws stipulate that companies must notify consumers of a breach of personal information promptly and apply criminal or civil penalties for failure to notify consumers without unreasonable delay.

Recent regulations under PIPEDA govern breach notifications in Canada, which can also vary by province.

5. Mitigate Harm

Reassure affected consumers with timely and clear communication about the breach and your response to it. Outline the actions you will take, such as free credit monitoring, to mitigate any harm consumers may suffer. Consider engaging a third party company to help manage your incident response to minimize the reputational damage and your risk of lawsuits.

6. Comply with Regulations

Determine whether to alert regulators and the media and document the decision as well as any actions you take. Regulations vary depending on the type of data involved and the industry. Breaches of personal health information, for example, are subject to strict regulations. Your corporate counsel should be involved from the moment you discover the breach to determine what kinds of liability the company faces.

7. Determine Root Causes

Complete the investigation, analyze the results to determine the cause of the breach and take corrective actions to prevent data theft in your organization in the future.