A Practical Approach to a Data Breach

Your office is inundated with inquiries about a potential data breach from executive management, they want to know the scope and potential impact to the company. Just minutes before, you were notified by the information security team of the data breach. You have limited or no knowledge of the scope, scale, categories of personal data and location of customers, clients or employees that may be at risk.

How do you respond and advise the executive team and business of the impacts? This article is based on real life experience that may assist in how to handle the internal chaos and aid in keeping your sanity.

Day One

Reply to executive management to inform that Information Security, IT and Information Governance teams partnering with the Privacy Office to investigate and analyze the breach, and advise this effort may require extensive resources, funding and time.

The Privacy Office also informs the business leaders they will lead communications to executive management, ask their teams to limit emails to include general updates and refrain from sending detailed communications, as this could create higher business risk in the event future legal action (email is always requested in the ediscovery process).

You schedule 15 minute daily briefings with executive management, typically at the end of the day and ask your CISO and CIO to provide technical updates.

Day Two to Five

Provide executive management with daily detailed updates on the scope, scale, and categories of personal data that may be at risk due to the breach. Advise that the business may be required to provide notification to customers, clients, law enforcement, or data protection authorities.

In parallel, the investigation and analysis actions to be completed during this period of time should entail:

- Quantify the tools, level of resource skills, and time necessary to complete the technical investigation;
- Identify the categories of the personal data collected and stored across the business; this will assist in the creation of a cost model to mitigate or resolve the vulnerabilities,
- Identify resources to aid in analysis of notification requirements and define the thresholds for notification (i.e. the number of individuals, geography, sensitivity of the data, and timing);
    - Engage external resources (when necessary) to provide regulatory guidance by state, country, or jurisdiction;
- Document the sources of the personal data, location of the customer, client and/or employee, and the format of the data: electronic, online or offline, or in physical records;

- Identify the potential financial fines, civil actions (business and executive), revenue risks (i.e. due to loss of use of personal data from country x), and enforcement actions such as government oversight programs; and
- The likelihood of regulatory action or possible publicity.

Week Two to Five

Provide executive management with weekly detailed updates via a concise summary of the results of the investigation and analysis. This should include the areas outlined below.

- Responsibilities of corporate communications, legal, sales, marketing, and operations;
    - Secure executive management support of the resources for developing external messaging, call center Q/A's, strategic client notifications and response resources to assist customers;
- Identify IT and InfoSec resources and technology costs to complete data breach resolution;
- Develop an overview of the applicable legal and regulatory risks and actions needed to update policies and data protection controls;
- Define the risk details:
    - Risks ranked by the importance or impacts to the business;
    - Regional specific risks, tasks, and costs of the data breach; and
    - Potential future risks, due to enactment of pending regulations or laws.
- Impacts to the timelines for the release of new or updated products and services; and
- Resources for ongoing monitoring, periodic reassessment of the regulatory environment, and level of risks for external threats;

In addition, you will need to complete applicable notifications to customers, clients, or employees and the filings to required government, law enforcement, and/or data protection authorities within this time period.

In Addition

It is highly probable during the investigation and analysis, the results provide discovery that the business has data in every corner, multiple share drives, and file cabinets which will create a need to improve your information governance program.

For assistance in executive management briefs/updates, analysis of data breach requirements, or development of customer, client, employee, law enforcement, or governmental notifications, contact Jim Keese, Privacy International, LLP at jmkeese@privacy-internationallp.com or at 720-638-5064.