The first 48 hours: responding to a data breach

OSLER

Your organization's initial response to a data breach is critical in determining the long-term impact the incident will have on your business. The immediate steps you take after the breach can set the tone for the response and influence how smoothly your organization can move forward from the event.

When you have a data breach – the top 5 priorities

1

CONTAIN

Take immediate steps to identify and contain the breach

- IT measures
- Security measures
- Personnel measures

Assemble breach team

- Engage Privacy, Legal, Communications and IT Resources
- Identify Breach Coordinator

Do not compromise ability to investigate

- Preserve metadata and follow the trail
- Retain, segregate and preserve documentation without alteration
- Involve external counsel and/or investigation team

2

INVESTIGATE

Preliminary investigation

- Engage forensic team
- Assess cause and scope of the breach – do we own it?
- Maintain chain of custody on evidence
- Establish protocols for protecting privilege
- Identify Universe of Potentially Affected Individuals and Businesses
- Assess Exposure

Longer term forensic investigation

3

COMMUNICATE

Immediate response

- Consider Statutory Obligations of Notification
- Assess whether a RROSH has Occurred – "A Real Risk of Significant Harm"
- Internal communication
- Strategy for dealing with reputational issues
- Strategy for external communications

Longer term outreach

4

NOTIFY

Notification to regulators

- Privacy Commissioners
- Police
- Professional or other regulatory bodies

Notification of individuals

Notification to stakeholders

5

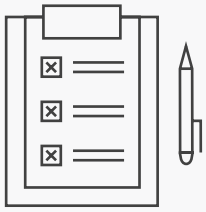
REMEDIATE

Steps to remediate harm to parties

- Steps to Recover Data
- Steps to Prevent Further Publication/Disclosure
- Availability of Credit Monitoring
- Consider Offers of Compensation
- Plan Strategy for Private/Class Action Litigation

Best practices – The key elements of an incident response protocol

The key elements of breach preparedness:



- The establishment of a workable protocol and reporting structure
- The identification of service providers and other key stakeholders
- The implementation of steps to protect confidentiality and privilege
- The availability of insurance
- The value of tabletop preparedness testing

The OPC's Commentary on LinkedIn's data breach response in 2012:

> *"Its commitment to remediation clearly flowed from the top, with senior management authorizing a* ***'Code Red' response that rendered the breach the top priority for the organization and triggered an immediate deployment of resources to deal with the breach****. … LinkedIn, like many organizations, could have had better safeguards for information to begin with. But when we looked at the company's breach response in the face of a cyber-attack, we found the organization had demonstrated due diligence and accountability"*

© Copyright 2016 Osler, Hoskin & Harcourt LLP. All rights reserved