Data Security Incident Response Plans — Some Practical Suggestions

December 02, 2016

A comprehensive and suitable data security incident response plan and a trained incident response team are fundamental parts of an enterprise risk management program. Nevertheless, recent surveys indicate that most organizations either do not have a suitable data security incident response plan or have not implemented an appropriate testing, training and exercise program. This bulletin provides some practical suggestions for creating and implementing a data security incident response plan.

Data Security Incident Response Plans

(a) Overview

A data security incident response plan (an "IRP") is a written plan, comprised of instructions, procedures, protocols and guidelines, designed to enable an organization to respond to, and recover from, various kinds of data security incidents in a way that minimizes resulting harm, reduces recovery time and costs and allows the organization to benefit from lessons learned.

In this context, "data" means any kind of written, printed or electronic document, record or data owned by, or in the custody or control of, the organization (including data transferred by the organization to a service provider for processing or storage), and "data security incident" means any kind of unauthorized access to, or collection, use, disclosure or deletion of, data or any other unauthorized event that affects the availability, confidentiality, integrity or security of data. For example, a data security incident might result from an attack by a cybercriminal, a stolen or lost device or physical file, a misdirected email, an innocent mistake or malicious misconduct by an employee or contractor, a software defect or hardware failure or an operational break-down.

In many circumstances, an organization may be under a legal obligation – imposed by statute (e.g. personal information protection laws), contract (e.g. contractual confidentiality and data security obligations) or generally applicable common law or civil law (e.g. a duty of care) – to have an appropriate IRP. In those circumstances, failure to have an IRP may expose the organization and its directors and officers to potentially significant financial liability and other adverse consequences.

(b) Practical Recommendations

Following are some practical recommendations for an IRP:

- Basic Requirements: An IRP should identify the incident response team members (both internal personnel and external advisors and consultants) and their respective roles and responsibilities, and set out the procedures they should follow to respond to and recover from a data security incident, to assess and mitigate the business and legal risks resulting from the incident and to take appropriate measures to prevent the same or a similar incident in the future. The IRP should cover all phases of a data security incident response – discovery (initial assessment and team activation), containment, recovery, post-recovery investigation and post-incident review and report.
- Actionable/Practicable: An IRP should be a short, simple document that specifies reasonable tasks and achievable outcomes, assigns accountability to specific incident response team members, and provides guidance and advice to help the incident response team make important technical, business and legal decisions in a timely manner. An IRP should be practicable and flexible for use in various scenarios and circumstances, and should recognize the need for incident response team leaders to use reasonable, informed judgment when deciding how to respond to an incident. An IRP should include pre-determined but flexible procedures (known as "playbooks") and checklists for various kinds of incidents and guidelines for important decisions.
- Best Practices/Guidance: An IRP should be consistent with current best practices and guidance issued by relevant regulators and self-regulatory organizations. For recent examples, see BLG bulletins *Guidance for Defending and Responding to Ransomware Attacks* (November 2016), Cyber Risk Management – G7 *Cybersecurity Guidelines for the Financial Sector* (October 2016), *Cyber Risk* Management – New York State Regulation for Financial Institutions(September 2016) and Cyber Risk Management – Regulatory Guidance from the Canadian *Securities Administrators*(September 2016).
- Legal Compliance: An IRP should be consistent with applicable laws (including laws of general application and relevant sector-specific laws) in each relevant jurisdiction (e.g. jurisdictions where the organization is located and jurisdictions where customers are located) and obligations imposed by the organization's contracts and commitments (e.g. the organization's privacy policy).
- Legal Advice and Legal Privilege: An IRP should mandate the involvement of legal counsel throughout the incident response process and should specify procedures to establish and maintain legal privilege protection for legal advice and technical investigations conducted for legal purposes. For more information, see BLG bulletin Cyber Risk Management – Legal Privilege Strategy – Part 1 and Part 2 (July 2016).
- Internal Communications: An IRP should include procedures and protocols for communications among incident response team members and for communications between incident response team members and other organization personnel, so that those communications are effective, secure and confidential even if the organization's standard communications systems are compromised by the incident.
- Record Keeping: An IRP should include procedures and protocols for the incident response team's creation of secure and confidential records regarding the incident and related response activities for use by the team while responding to

the incident and to enable the organization to comply with legal record retention and breach notification requirements.

- Evidence Collection: An IRP should include a protocol for the incident response team's collection and preservation of physical and electronic evidence (e.g. system log files and surveillance tapes) for use in regulatory investigations and legal proceedings. The protocol should enable the organization to establish the authenticity, reliability and trustworthiness of the evidence.
- Notification and Information Sharing: An IRP should include guidelines for determining whether, when and how the organization should give notice of a data security incident to affected individuals, organizations, regulators (e.g. privacy commissioners), law enforcement and other persons (e.g. insurers). Those guidelines should reflect the organization's data incident notification obligations under statute, contract and generally applicable common law and civil law. For more information, see BLG bulletin Cyber-Risk Management – Data Incident *Notification Obligations* (October 2015).
- Review: An organization should review its IRP on a regular basis to ensure that the IRP is consistent with the organization's current circumstances, satisfies applicable business, technical and legal requirements, and reflects lessons learned from previous data security incidents and the organization's testing, training and exercise program.

Testing, Training and Exercise Programs

An organization should have a testing, training and exercise ("TT&E") program to help ensure that the organization's IRP is up-to-date and the organization's personnel and information technology systems are in a state of readiness, so that the organization is able to respond to data security incidents in a timely, effective and lawful manner.

In many circumstances, there may be a legal requirement, imposed by statute, contract or generally applicable common law or civil law, for an organization to have a TT&E program. In those circumstances, failure to have a TT&E program may expose an organization and its directors and officers to potentially significant financial liability and other adverse consequences.

An effective TT&E program requires careful planning and continuous effort. A TT&E program should include tests of the information technology systems required to execute the IRP, training of incident response team members and other relevant personnel, and exercises based on scenarios of simulated data security incidents to enable the incident response team to simulate the execution of the IRP. An organization should conduct TT&E events periodically, and should properly document TT&E activities for future reference and use as evidence in investigations and legal proceedings.

For more information about TT&E programs, see BLG bulletin *Cyber Incident Response Plans – Test, Train and Exercise*(May 2016).

Legal Considerations

The preparation and execution of an IRP and a related TT&E program usually present important legal issues, including compliance with record retention, notification, reporting and disclosure obligations, privacy/personal information protection laws, labour/employment laws and evidence laws. An organization should involve legal

counsel in the preparation and execution of an IRP and a related TT&E program so that the IRP and TT&E program comply with applicable laws and satisfy applicable legal requirements, to help ensure that appropriate documentation is created to prove due diligence and reasonable business judgment, and to enable the organization to claim legal privilege protection for legal advice and technical investigations and assessments conducted for legal purposes.

By:

Bradley Freedman

Services:

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749