Cyber Incident Response Plans — Test, Train And Exercise

May 19, 2016

Organizations should use a testing, training and exercise program to help ensure that their cyber incident response plan is ready to effectively respond to cyber incidents.

"Give me six hours to chop down a tree and I will spend the first four sharpening the axe." - Abraham Lincoln

Organizations should have an established plan for responding to various kinds of cyber incidents in an effective, timely and lawful manner, and should use a testing, training and exercise program to help ensure that the plan is up-to-date and that relevant personnel and systems are in a state of readiness.

Cyber Incident Response Plans

For business and legal reasons, an organization should have an incident response plan ("IRP") that is suitable for the organization and addresses various kinds of cyber incidents, such as external attacks, insider misconduct and ransomware incidents. An IRP should identify the incident response team members (both internal and external personnel) and their respective roles and responsibilities, and set out detailed, pre-determined but flexible procedures (known as "playbooks") and guidance for responding to various kinds of cyber incidents, including guidance for important technical, business and legal decisions.

In many circumstances, there may be a legal requirement – imposed by statute (e.g. personal information protection laws), contract (e.g. contractual obligations to comply with the Payment Card Industry Data Security Standard) or generally applicable common law or civil law (e.g. a duty of care) – for an organization to have a suitable IRP. In those circumstances, failure to have a suitable IRP may expose an organization and its directors and officers to potentially significant adverse consequences, including statutory sanctions and financial liability for breach of contract or breach of duty.

Testing, Training And Exercise Programs

An organization should use a testing, training and exercise ("TT&E") program to help ensure that its IRP is up-to-date and its relevant personnel and information technology ("IT") systems are in a state of readiness. In many circumstances, there may be a legal requirement for an organization to have a TT&E program. Important elements of a TT&E program include the following:

- **Test:** Tests of the IT systems required to execute an IRP, including component tests, system tests and comprehensive tests.
- **Train:** Training of relevant personnel so they have the knowledge, skills and technical proficiencies required to effectively execute an IRP.
- **Exercise:** Exercises based on scenarios of simulated cyber incidents to enable relevant personnel to simulate the execution of an IRP through either: (1) facilitated discussion of their roles, responsibilities, coordination and decisions in response to a cyber incident (known as a "tabletop exercise"); or (2) execution of roles and responsibilities in a simulated operational environment in response to a cyber incident (known as a "functional exercise"). Exercises should either validate, or identify deficiencies or errors in, an IRP and assess the training and competence of relevant personnel.

An effective TT&E program requires careful planning and continuous effort by the organization's relevant internal and external personnel. An organization should conduct TT&E events periodically, including after changes to the organization's structure, IT systems or IRP, and as necessary to comply with legal requirements. An organization should properly document its TT&E activities for future reference and use as evidence in regulatory investigations and legal proceedings.

Legal Considerations

An organization's IRP should be prepared with appropriate legal advice to ensure that the IRP properly addresses important legal issues, including compliance with record retention, notification, reporting and disclosure obligations, privacy/ personal information protection laws, labour/employment laws and laws regarding evidence, and to permit the organization to reasonably claim legal privilege over sensitive communications relating to the development of the IRP.

An organization's TT&E program should be designed and executed under the direction of the organization's legal counsel, to ensure that the program satisfies applicable legal requirements and is properly documented, and to permit the organization to reasonably claim legal privilege over sensitive communications and reports relating to the TT&E program.

Comment

An organization should use a TT&E program to help ensure that the organization's IRP is up-to-date and the organization's personnel and IT systems are in a state of readiness, so that the organization is able to respond to cyber incidents in a timely, effective and lawful manner. Government agencies, regulators and industry organizations have emphasized the need for TT&E programs and issued helpful, detailed technical guidance. For example, the National Institute of Standards and

Technology's *Guide to Test, Training, and Exercise Programs for IT Plans and* Capabilities provides guidance and sample documentation for a TT&E program.

By

Bradley Freedman

Expertise

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