Cybersecurity Bulletin

July 2019

Managing Insider Risk – Recent Best Practices Guidance

Employees and other insiders are a major security risk. A significant portion of cybersecurity incidents are caused or facilitated by the affected organization's insiders, whether acting inadvertently or intentionally. Organizations should assess their insider risk management program for compliance with recent best practices guidance, and ensure that their insider risk management program complies with applicable law.

Insider Risk

Studies consistently indicate that a significant portion of cybersecurity incidents and data breaches are caused or facilitated by a current or former insider (e.g. a director, executive/manager, employee or contract worker) of the affected organization or its business partners. The Verizon *Insider Threat Report* concludes that 20 percent of all cybersecurity incidents and nearly 15 percent of all data breaches in the Verizon *2018 Data Breach Investigations Report* resulted from "insider and privilege misuse" by individuals within the affected organization.

An organization's insiders present significant risk because they have authorized access to the organization's information technology systems, special knowledge of the organization's valuable data and security practices, and a greater window of opportunity for misconduct. Those circumstances can enable an insider to engage in misconduct that is harder to detect and remedy, and results in more harm, than external attacks.

Insiders can cause or facilitate a cybersecurity incident or data breach inadvertently (e.g. due to mistake or manipulation by other persons) or deliberately for various motives (e.g. financial gain, malice or enjoyment). Regardless of whether an insider's actions are inadvertent or deliberate, the results can be the same – potentially devastating harm to the organization and potentially significant liabilities by the organization to individuals and organizations harmed by the incident. For more information about insider risk and rogue employees, see BLG bulletin *Insider Risk Management and Rogue Employees*.

Best Practices Guidance

Effective insider risk management requires a risk-based, multi-functional approach by an organization's various departments and disciplines (e.g. human resources, legal, physical security, and information technology) to deter, prevent, detect and respond to cybersecurity incidents and data breaches caused by insiders. An organization should carefully hire, educate, train and disengage insiders, and establish and implement administrative, technological and physical security policies and procedures to protect the information technology systems and data of the organization and its relevant business partners, and to monitor and verify compliance.

Best practices guidance for managing insider risk has recently been issued by Carnegie Mellon University's CERT Division, Verizon and Public Safety Canada. Following is a summary of each guidance document.

CERT – *Common Sense Guide to Mitigating Insider Threats*

In December 2018, Carnegie Mellon University, Software Engineering Institute's CERT Division issued its *Common Sense Guide to Mitigating Insider Threats, 6th Edition*. The guide details twenty-one recommended best practices for managing insider risk: (1) know and protect your critical assets; (2) develop a formalized insider threat program; (3) clearly document and consistently enforce policies and controls; (4) beginning with the hiring process, monitor and respond to suspicious or disruptive behavior; (5) anticipate and manage negative issues in the work environment; (6) consider threats from insiders and business partners in enterprise-wide risk assessments; (7) be especially vigilant regarding social media; (8) structure management and tasks to minimize insider stress and mistakes; (9) incorporate malicious and unintentional insider threat awareness into periodic security training for all employees; (10) implement strict password and account management policies and practices; (11) institute stringent access controls and monitoring policies on privileged users; (12) deploy solutions for monitoring employee actions and correlating information from multiple data sources; (13) monitor and control remote access from all end points, including mobile devices; (14) establish a baseline of normal behavior for both networks and employees; (15) enforce separation of duties and apply the principle of least privilege; (16) define explicit security agreements for cloud services; (17) institutionalize system change controls; (18) implement secure backup and recovery processes; (19) close the doors to unauthorized data exfiltration; (20) develop a comprehensive employee termination procedure; and (21) adopt positive incentives to align the workforce with the organization.

For most recommended best practices, the guide identifies the organizational groups involved in executing each recommendation, and lists "quick wins and high-impact solutions" to help organizations accelerate their insider risk management program.

Verizon – *Insider Threat Report*

In March 2019, Verizon published its *Insider Threat Report* to provide a "data-driven view" of insider risk, illustrated by real-life case scenarios, and to recommend countermeasure strategies for a comprehensive insider risk management program. The report identifies and illustrates five insider personalities: (1) the careless worker (misusing assets); (2) the inside agent (stealing information on behalf of outsiders); (3) the disgruntled employee (destroying property); (4) the malicious insider (stealing information for personal gain); and (5) the feckless third party (compromising security).

The report details eleven recommended countermeasures for insider risk: (1) integrate security strategies and policies; (2) conduct threat hunting activities; (3) perform vulnerability scanning and penetration testing; (4) implement personnel security measures; (5) employ physical security measures; (6) implement network security solutions; (7) employ endpoint security solutions; (8) apply data security measures; (9) employ identity and access management measures; (10) establish incident management capabilities; and (11) retain digital forensics services. The report contains a number of recommended tasks for each countermeasure. The report emphasizes that an insider risk strategy must focus on two factors – assets and people. The report encourages organizations to address the "most impactful situations" (i.e. high-value assets and areas of highest risk), rather than just applying blanket coverage, to improve the effectiveness of their insider risk management program.

Public Safety Canada – *Enhancing Canada's Critical Infrastructure Resilience to Insider Risk*

In April 2019, Public Safety Canada's Critical Infrastructure Directorate issued *Enhancing Canada's Critical Infrastructure Resilience to Insider Risk* to provide Canadian critical infrastructure organizations with guidance on what constitutes insider risk, and recommendations on how to monitor, respond to and mitigate insider risk. The report details eight recommended security actions: (1) establish a culture of security; (2) develop clear security policies and procedures; (3) reduce risks from partners and third party providers; (4) implement a personnel screening life-cycle; (5) provide training, raise awareness and conduct exercises; (6) identify and protect critical assets; (7) monitor for, respond to and mitigate unusual behaviour; and (8) protect data. The report contains a number of recommended tasks for each security action. The report concludes: "Organizations must … be vigilant and resilient; continuously monitor the threat landscape; meticulously plan for response and recovery activities; and implement measures to protect against incidents".

Comment

Organizations should evaluate their insider risk management program in light of recent best practices guidance, and make appropriate improvements with an emphasis on protecting the organization's high-value assets and areas of highest risk.

When establishing and implementing an insider risk management program, organizations should be mindful of legal compliance requirements. For example:

- Performing background checks and screening (including reviewing social media activity) of individuals, as part of hiring/engagement process or during the course of employment, implicates compliance with privacy/personal information protection, labour/employment and human rights laws.
- Designing and implementing IT system policies and procedures implicates compliance with privacy/personal information protection and labour/employment laws.
- Monitoring IT system use and other work-related activities implicates compliance with privacy/personal information protection and labour/employment laws.
- Testing incident response plans, and responding to cybersecurity incidents and data breaches, implicates compliance with privacy/personal information protection and labour/employment laws, and collecting and maintaining evidence of breaches and remediation activities implicates laws regarding the admissibility of evidence.

Timely legal advice can assist an organization to effectively address legal compliance requirements. In addition, the involvement of lawyers in certain insider risk management activities (e.g. assessing relevant policies/procedures and conducting testing/training activities) and in responding to cybersecurity incidents and data breaches is necessary to establish legal privilege over communications regarding those activities. For more information, see BLG bulletins *Cyber Risk Management – Legal Privilege Strategy (Part 1)*, *Cyber Risk Management – Legal Privilege Strategy (Part 2)*, *Legal Privilege for Data Security Incident Investigation Reports*, and *Loss of Legal Privilege over Cyberattack Investigation Report*.

Organizations should also consider whether they have appropriate insurance for residual insider risk. The cyber insurance market is evolving rapidly. At this time, there is no standard form language used in cyber insurance policies, and there can be significant differences in the coverage provided by similar kinds of policies. For those reasons, organizations should obtain appropriate advice regarding cyber insurance. For more information, see BLG bulletin *Insurance for Cybersecurity Incidents and Privacy Breaches*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity Law Group assists clients with legal advice to help manage cyber risks and to respond to data security incidents. Information about BLG's Cybersecurity Law Group is available at **blg.com/cybersecurity**.

BLG Cybersecurity Group – Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Kevin L. LaRoche	Ottawa	613.787.3516
David Madsen	Calgary	403.232.9612
Ira Nishisato	Toronto	416.367.6349

blg.com | Canada's Law Firm
Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

This document provides general information only, and does not constitute legal or other professional advice. Readers are encouraged to obtain legal advice from a competent professional regarding their particular circumstances.