Cyber Risk Management – Insider Risk

written by vickyp | February 29, 2016

People are a major security risk. Most cybersecurity incidents originate from, or are facilitated by, a current or former insider of the victim organization. To manage insider risk, an organization should use a multi-disciplinary program and implement administrative, technological and physical security policies and practices to protect the IT systems and data of the organization and its relevant business partners. Legal advice is essential to address the legal challenges presented by insider risk management.

WHAT IS INSIDER RISK?

Studies consistently confirm that a majority of cybersecurity incidents originate from, or are facilitated by, the victim organization's current or former insiders (e.g. executives/managers, employees and contract workers, whether permanent or temporary, full time or part time, and similar individuals working for business partners) acting maliciously or inadvertently. IBM's *2015 Cyber Security Intelligence Index* reported that 55 percent of all cybersecurity incidents were carried out by insiders.

Insiders present significant cyber risk because they have privileged access to the organization's information technology (IT) systems (i.e. no need to circumvent perimeter-based security), special knowledge of the organization's valuable data and security practices and a greater window of opportunity for misconduct. Those circumstances often enable insiders to engage in misconduct that is harder to detect and remedy, and results in more harm, than external attacks.

Insiders can intentionally cause cybersecurity incidents for a broad range of reasons (e.g. financial gain, anger/revenge, recognition/power, adventure/thrill, love/jealously, curiosity, extortion/blackmail and ideology). Insiders can also cause or facilitate cybersecurity incidents as a result of carelessness or error (e.g. easy-to-guess or stored-in-plain-sight passwords, lost devices, erroneous disclosure of sensitive information or inadvertent activation of malicious email attachments) or manipulation (e.g. through fraud/deception or coercion) by other insiders or outsiders.

Regardless of whether an insider's acts are malicious or inadvertent, the results can be the same – potentially devastating losses and liabilities to the organization (e.g. direct financial losses caused by theft, fraud or business disruption; investigation, mitigation, remediation and litigation costs; loss to stakeholder value; harm to reputation and relationships with consumers, commercial customers and business partners; disclosure of confidential information; loss of competitive advantage; civil liabilities and regulatory penalties) and potentially significant liabilities on the part of the organization's directors and executives.

MANAGING INSIDER RISK

Insider risk management is more than an IT problem. An effective insider risk management program requires a risk-based, multi-functional approach by an organization's various departments and disciplines (e.g. senior management, human resources, procurement, risk management, IT, physical security and legal) to deter, prevent, detect and respond to cybersecurity incidents caused by insiders. Insider risk management requires an organization to carefully select, educate, train and disengage insiders, establish policies, procedures and systems for use of the organization's IT systems and data and monitor and verify compliance. Following is a summary of some fundamental components of an insider risk management program.

- **Engagement:** An organization should exercise appropriate, lawful due diligence (e.g. background/security checks, screening and interviews) when hiring/engaging insiders. An organization should require an insider to contractually agree to comply with the organization's relevant policies and procedures, many of which should apply both during and after the term of employment/ engagement, and give legally valid consent to the organization's monitoring/enforcement programs.
- **Policies/Procedures:** An organization should conduct periodic threat risk assessments to identify and prioritize its cyber risk requirements. The organization should then establish and implement documented, clear and simple policies and procedures for use of the organization's IT systems and data (e.g. data security and confidentiality policies, bring your own device policies, privacy policies, physical security procedures and incident response plans) that are suitable for the organization's identified requirements and help insiders safely and effectively use the organization's IT systems and data. An organization should also consider establishing financial and other incentives to compliance with those policies and procedures.
- **Education/Training:** An organization should educate and train its insiders, during onboarding and on a continuous basis afterwards (including through periodic reminders and refresher training), so that insiders understand the organization's cyber risk management policies and procedures and are able to safely use business and personal IT systems and services (e.g. websites, email, instant messaging and social media), take appropriate precautions at work, at home and while travelling to protect themselves and the organization against cyber risks, and identify, understand, resist and respond to cyber threats (e.g. phishing, fraudulent emails, social engineering scams and recruiters) and data security incidents.
- **Security:** An organization should implement appropriate administrative practices and physical and technological systems (e.g. IT system and data access controls based on data classification and least privilege access, user and device authentication and physical security measures) to secure and limit privileged access to the organization's IT systems and data, and to detect and prevent unauthorized access to those systems and data. An organization should strive to achieve a reasonable and lawful balance between enablement and control.
- **Monitoring/Verification/Enforcement:** An organization should lawfully monitor (including by using appropriate technologies) and routinely test for compliance

with the organization's cyber risk management policies and procedures by all insiders (including senior executives/management), and reasonably enforce those policies and procedures in a manner consistent with applicable law. An organization should consider enhanced monitoring during high-risk periods (e.g. first and last months of an insider's employment/ engagement). Insiders should be encouraged to be vigilant and promptly report suspect behaviour by other persons and all actual and reasonably suspected cyber risk incidents involving themselves or other persons.

- **Disengagement:** An organization should follow appropriate, lawful procedures when disengaging an insider, including cancelling passwords, terminating access to the organization's IT systems and data, retrieving the organization's assets (e.g. computing and storage devices and physical security access devices), deleting the organization's data from the individual's personal computing devices, conducting exit interviews and providing reminders of ongoing legal obligations, and reviewing recent (e.g. past 90 days) IT system and data use for unusual behavior.
- **Incident Response Plan:** An organization should have a comprehensive, practiced and tested incident response plan that includes procedures for dealing with insiders who are suspected of having caused or contributed to a cyber security incident.

RISKS PRESENTED BY BUSINESS PARTNERS

An organization's relationships with business partners (e.g. subcontractors, suppliers, service providers and collaborators) can exponentially increase the number of insiders and significantly change the nature and magnitude of insider risk. Organizations often provide business partners with access to, or possession or use of, the organization's IT systems or data. As a result, business partner relationships pose an inherent risk of additional insider threats to the organization's IT systems and data.

For those reasons, an organization's insider risk management program should include relationships with all of the organization's business partners, and should address risks presented by business partner personnel who have access to or use of the organization's data or internal or external IT systems. In other words, for the purposes of insider risk management: (1) an organization's insiders should be considered to include all individuals, employed or engaged by the organization's business partners, who have direct or indirect access to, or use or custody of, the organization's IT systems or data; and (2) an organization's IT systems should be considered to include all external IT systems that are owned or operated for the organization by a business partner (e.g. a cloud service provider or other provider of outsourced services, such as payroll and benefits service providers) or used by a business partner to provide services to the organization.

Insider risk management practices that an organization follows regarding its own personnel and internal IT systems and data should be extended to the organization's business partners and their personnel and IT systems. For example, an organization should: (1) exercise appropriate due diligence when selecting a business partner, with particular consideration to the business partner's cyber risk management practices and experience; (2) include in contracts with business partners detailed provisions requiring compliance with appropriate cyber risk management standards and allocating responsibility and liability for cybersecurity incidents; and (3) monitor and verify compliance with those requirements.

LEGAL CONSIDERATIONS FOR INSIDER RISK MANAGEMENT

Managing insider risk presents various legal challenges, including ensuring that risk

management practices are legally effective and comply with applicable law. For example:

- Performing background checks and screening of individuals during the hiring or engagement process implicates compliance with labour/employment and human rights laws.
- Designing and implementing IT system and data use policies and procedures implicates compliance with privacy/personal information protection laws and labour/employment laws, including rules regarding changes to terms of employment that can constitute constructive dismissal.
- Monitoring IT system use and other work related activities implicates compliance with privacy/personal information protection laws and labour/employment laws.
- Testing incident response plans and responding to cybersecurity incidents implicates compliance with privacy/personal information protection laws, labour/employment laws and laws regarding evidence and legal privilege.

Timely legal advice can assist an organization to effectively address generally applicable legal requirements and ensure compliance with laws specific to the organization or its activities. The involvement of lawyers in specific risk management activities (e.g. incident response plan testing and responding to cybersecurity incidents) might be necessary to enable the organization to effectively assert legal privilege over sensitive communications for the purpose of seeking legal advice or preparing for litigation.

Article by Bradley J. Freedman