JANUARY 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

CYBERSECURITY GUIDANCE FOR SMALL AND MEDIUM SIZE ENTERPRISES

Cyber risk management is important for organizations of all kinds and sizes. Small and medium size enterprises are increasingly being targeted by cyber criminals. In November 2016, the U.S. National Institute of Standards and Technology ("NIST") issued an interagency report titled *Small Business Information Security: The Fundamentals* to provide cyber risk management guidance for small businesses. The Report and similar guidance issued by Canadian and U.S. agencies provide useful advice for organizations of all sizes.

The NIST Report

The Report encourages small businesses to understand and manage risks to their information, systems and networks. The Report explains that information security encompasses people, processes and technologies, and focuses on protecting the confidentiality, integrity and availability of information. The Report notes that an information security program should not be limited to cybersecurity (which relates to the security of information technology devices and systems and electronically stored information), but should also include physical security, personnel security, business continuity planning, operational security and privacy. The Report explains that it is not possible for any business to be completely secure, and that an information security program should reasonably balance a business's desire for security with the business's other needs and capabilities.

The Report explains that information security risk is a function of threats, vulnerabilities, the likelihood of an incident and the potential impact of the incident. The Report summarizes a four-step process for creating a basic, risk-based information security program: (1) identify and prioritize information types; (2) create an inventory of technologies that access, process and store information; (3) identify threats, vulnerabilities and incident likelihood for each kind of information and technology; and (4) prioritize, implement and monitor information security efforts.

The Report uses the NIST *Framework for Improving Critical Infrastructure Cybersecurity* to organize some basic risk mitigation practices, procedures and activities into five categories – identify, protect, detect, respond and recover. The Report emphasizes that the recommended activities are not one-time events, but a continual, on-going process.

Following is a summary of some of the recommendations:

- **Identify:** Activities to understand resources and risks, including: identify and control individuals with access to information; conduct background checks of those individuals; require a password-protected user account for each individual; establish and implement policies and procedures for information security.
- **Protect:** Activities to limit or contain the impact of a potential information security incident, including: limit authorized access to data/information; patch operating systems and software applications on all computers/devices; use software and hardware firewalls on all computers/devices and networks; secure wireless access points and wireless networks; use email and web filters and block access to blacklisted internet sites; use encryption for sensitive information; continuously train and educate personnel.
- **Detect:** Activities to timely discover information security incidents, including: install, use and regularly update anti-malware software on all computers/devices that access information or connect to networks; maintain and monitor logs of all network activity.
- **Respond:** Activities to enable a timely response to an information security incident, including develop incident response plans for disasters and information security incidents.
- **Recover:** Activities to enable resumption of normal operations after an information security incident, including: periodically make and safely store full and incremental backups of all data stored on all computers/devices and storage media; consider procuring cyber insurance; regularly assess and improve information security processes, procedures and technologies.

The Report recommends some every-day activities and practices to minimize information security risks. Following is a summary of some of the recommendations:

- **Personnel:** Pay attention to employees and contractors, and watch for unusual activity.
- **Phishing/Social Engineering:** Be careful of email attachments and embedded links to websites. Do not disclose sensitive personal or business information (including credentials) in response to phishing and other social engineering scams.
- **Devices:** If possible, have separate computers/devices and email accounts for business and personal/home use. Do not connect untrusted or personal/home use devices (e.g. USB drives, external hard drives or hardware) to a business computer/device or network.
- **Software:** Do not download software from an unknown source.
- **Credentials:** Use strong passwords that are regularly changed (every three months) and are not re-used. Use multi-factor authentication for computers/devices or applications that access or store important information.

Additional Guidance for SMEs

The Government of Canada's Get Cyber Safe website provides useful cybersecurity resources for individuals and businesses, including the *Get Cyber Safe Guide for Small and Medium Businesses*. The Guide provides advice on how a small or medium size business can establish and manage a basic cybersecurity program, and recommendations regarding specific cybersecurity practices (e.g. web security, email security, data security, remote access security and physical/employee security). The Guide includes a simple *Cyber Security Status Self-Assessment* to help determine a business's basic cybersecurity status.

The U.S. Federal Communications Commission website provides links to useful cybersecurity resources for small businesses, including a *Small Biz Cyber Planner 2.0* and a companion *Cyber Security Planning Guide* to assist businesses to create a cybersecurity plan. The Planner and Guide provide helpful information and advice for managing cyber risks (e.g. privacy and data security, scams and fraud, network and website security, email, mobile devices, employees, incident response and reporting, policy development and management).

Comment

The NIST Report and other government guidance provide helpful advice regarding basic cybersecurity practices that is useful for all organizations. Additional cybersecurity guidance (including templates, questionnaires and checklists) is available from other regulators, government agencies and industry organizations in Canada and the United States. For example, see the following BLG bulletins: *Guidance for Defending and Responding to Ransomware Attacks* (Nov. 2016); *Cyber Risk Management – G7 Cybersecurity Guidelines For The Financial Sector* (Oct. 2016); *Cyber Risk Management – Regulatory Guidance From The Canadian Securities Administrators* (Sept. 2016); *Cybersecurity Guidance From Investment Industry Organization* (May 2016); and *Cybersecurity Guidance From Investment Industry Organization* (Jan. 2016).

Many of the practices, procedures and activities recommended by government agencies have legal implications, including compliance with privacy/personal information protection laws and labour/employment laws. An organization should involve legal counsel in the preparation and execution of cyber risk management activities so that those activities comply with applicable laws and to help ensure that appropriate documentation is created to prove due diligence and reasonable business judgment. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

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

For more information about cyber risk management and BLG's related legal services, please see the BLG website.

BLG Vancouver
1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com