Bulletin | Cybersecurity, Privacy and Data Protection

April 2020

Cybersecurity and the COVID-19 pandemic

The COVID-19 pandemic and the resulting rapid adoption of remote working arrangements and technologies present new and increased cybersecurity risks for organizations of all kinds and sizes. Organizations should consider and implement, as appropriate, recently issued authoritative guidance (see Appendix) to help manage COVID-19-related cybersecurity risks. In addition, when circumstances permit, organizations should seize the opportunity presented by the pandemic to improve their general cybersecurity maturity.

COVID-19 cyber risks

Cybersecurity refers to an organization's use of various kinds of controls (based on people, processes and technologies) to manage risks of losses, costs and liabilities suffered or incurred as a result of a failure or breach of the information technology systems used by or on behalf of the organization, or other incidents that compromise the confidentiality, availability and integrity of data in the organization's possession or control. Managing cyber risks is important not only for compelling business reasons but also for compliance with various legal obligations (including obligations to protect personal information) and to avoid potentially devastating legal liabilities.

As a result of the COVID-19 pandemic, many organizations have rapidly adopted new remote working arrangements and new administrative practices, and implemented new information technologies (e.g. cloud-based productivity and collaboration tools, remote access to information technology systems and the use of personal devices/services for business purposes), often without customary cyber risk management measures or carefully negotiated contracts with vendors and service providers. Cybercriminals are taking advantage of the stresses, distractions and uncertainties caused by new work arrangements and technologies, and the fears and uncertainties caused by the COVID-19 pandemic itself, by attacking improperly configured or misused technologies, exploiting technical vulnerabilities, and engaging in various forms of fraud.

Government agencies, regulators and self-regulatory organizations have issued warnings about various kinds of new or increased cyber risks arising from the COVID-19 pandemic. For example:

- **Phishing/fraud:** Online, email, messaging and telephone scams and fraud (e.g. spoofed websites, phishing emails and social engineering scams) that impersonate government agencies, regulators, health care organizations, charities and technical support personnel, or exploit fears and uncertainties about the pandemic.

- **Technical vulnerabilities:** Exploitation of unpatched critical vulnerabilities and improper configurations of devices, hardware, software and services, including personal devices, systems and services used for remote working.
- **Video conferencing risks:** Infiltration or hijacking (e.g. Zoom-bombing) of improperly configured video conferencing sessions and conference calls, exploitation of link and file-sharing functionalities or vulnerabilities in video conferencing applications, and attacks on remote desktop applications.
- **Ransomware/malware:** Malicious distribution of ransomware and other malicious software and mobile applications.
- **Password misuse/fraud:** Use of compromised passwords and email compromise fraud.
- **Physical risks:** Increased risks of stolen or lost devices.
- **Mistakes:** Increased risks of mistakes by workers while using new technologies and procedures.

Guidance for managing COVID-19 cyber risks

Government agencies, regulators and self-regulatory organizations have issued guidance to help organizations manage COVID-19 cyber risks (see Appendix). The guidance emphasizes the three fundamental pillars of an effective cybersecurity program – people, processes and technologies. Following is a summary of some of the important recommendations:

1. People

- **Culture/awareness:** Educate and train all workers to establish and maintain a culture of confidentiality, cybersecurity and operational resiliency, including regarding remote working arrangements and COVID-19-related cybersecurity risks.
- **IT staff:** Engage and train IT staff to address increased demands, to support the use of remote working technologies and services, and to respond to COVID-19-related scams that target IT personnel.
- **Incident reporting/response:** Train all workers on the prompt reporting of cybersecurity incidents, and train relevant personnel to execute incident response plans for cybersecurity incidents involving remote working arrangements.
- **Accountability/oversight:** Ensure appropriate accountability and reporting to senior management regarding cyber risk management and cybersecurity incidents.

2. Processes

- **Remote working:** Implement processes, supported by policies/procedures, for safe and effective remote working arrangements (e.g. remote system access policies, bring your own device policies, password/credentials policies, virtual meeting/video conferencing policies, vulnerability and patch management policies).
- **Payment fraud:** Implement accounting and payment procedures to guard against payment fraud, including email compromise fraud.
- **Incident response:** Update incident response plans to include cybersecurity incidents that involve remote working arrangements and technologies, and for compliance with legal reporting, notification and disclosure obligations.
- **Physical security:** Enhance the physical security of computers/devices, digital storage media and paper documents (including the secure disposal of paper documents).
- **System access:** Periodically review and update information technology system account privileges.
- **Business continuity:** Update and test business continuity and disaster recovery plans to include remote working arrangements and related technologies and services.
- **IT procurement:** Update and implement policies and procedures for the procurement of new technologies and services, including due diligence of vendors and their products/services, testing of technologies and requirements for applicable contracts.

3. Technologies

- **Patching/updates:** Properly configure and continuously/automatically update/patch information technology systems and services (e.g. virtual private networks, Wi-Fi networks, cloud services, video conferencing services and other remote working technologies), personal computers and mobile devices, operating systems and software applications.
- **Prevention/detection:** Use properly configured firewalls, anti-virus, anti-malware and anti-phishing software, password-protected screen locks, and intrusion prevention/detection technologies on all computers and other devices, including personal devices used for business purposes. Use enhanced system monitoring and log reviews for early detection and response to cybersecurity incidents.
- **VPNs:** Use secure virtual private networks (VPNs) for remote access to IT systems.

- **Passwords/MFA:** Use robust passphrases or complex passwords and multifactor authentication for access to personal computers and mobile devices, networks (including home networks), accounts and online services.
- **Wi-Fi:** Use secure Wi-Fi networks (including home networks) with appropriate administrator credentials, user passwords and a robust security protocol (e.g. WPA2).
- **Video conferencing:** Use proper security measures and safe configurations for virtual meetings and conference calls.
- **Device management:** Use mobile device management software to set up and manage all personal computers and other devices.
- **Data protection:** Use robust encryption for data in transit and at rest. Limit or control the use of removable storage media. Create and securely store backups of important data.
- **Eavesdropping:** Disable always-listening digital assistants located in remote-working environments.

Other considerations

Organizations should consider whether they have adequate insurance for cyber risks, including risks associated with remote working arrangements and the information technology systems and devices used by remote workers. 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. See BLG bulletin *Insurance for Cybersecurity Incidents and Privacy Breaches*.

While the COVID-19 pandemic is causing enormous social disruption, economic hardship and tragic loss of life, it might also provide an opportunity for organizations to use available time and resources to improve their general cybersecurity maturity. When circumstances permit, organizations should critically assess and improve their cyber risk management practices. Government agencies, regulators and self-regulatory organizations have issued guidance to help organizations of all kinds and sizes to improve their cybersecurity maturity. See BLG bulletins *Cybersecurity Guidance for Small and Medium Organizations*; *Investment Funds Institute of Canada Issues Cybersecurity Guide*; *Cybersecurity Framework for Ontario's Electricity Industry*; and *Cybersecurity Guidance from Canadian Securities Administrators*.

Cyber risk management activities can result in sensitive communications and documents that might be subject to mandatory disclosure in regulatory investigations and litigation relating to a cybersecurity incident, unless the communications and documents are protected by legal privilege. Organizations should consider implementing a legal privilege strategy to help establish legal privilege, where appropriate, over communications and documents created during preventative cyber risk management activities and cybersecurity incident response activities, and to help avoid inadvertent and unnecessary disclosures of privileged legal advice. 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*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Appendix – COVID-19 Cybersecurity Guidance

Canada

Canadian Anti-Fraud Centre, *Bulletin alert!, COVID-19 fraud*.

Canadian Centre for Cyber Security, *Alert: Cyber threats to Canadian health organizations*.

Canadian Centre for Cyber Security, *Alert: Considerations when using video-teleconference products and services*.

Canadian Centre for Cyber Security, *Alert: Cyber Hygiene for COVID-19*.

Canadian Centre for Cyber Security, *Alert: Staying Cyber-Healthy During COVID-19*.

Canadian Centre for Cyber Security, *Alert: Staying Cyber-Healthy During COVID-19 Isolation*.

Canadian Centre for Cyber Security, *Alert: Staying cyber safe while teleworking*.

Canadian Centre for Cyber Security, *Cyber Security Tips for Remote Work (ITSAP.10.116)*.

Mutual Fund Dealers Association of Canada, *Bulletin #0816-M: Cybercriminals Currently Exploiting the COVID-19 Pandemic*.

Investment Industry Regulatory Organization of Canada, *Notice 20-0061: COVID-19 and Cybersecurity*.

United States

Cybersecurity and Infrastructure Security Agency and United Kingdom National Cyber Security Centre, *Alert: COVID-19 Exploited by Malicious Cyber Actors*.

Cybersecurity and Infrastructure Security Agency, *Alert: Enterprise VPN Security*.

Cybersecurity and Infrastructure Security Agency, *Risk Management for Novel Coronavirus (COVID-19)*.

Cybersecurity and Infrastructure Security Agency, *Avoiding Social Engineering and Phishing Attacks*.

Federal Bureau of Investigation, *Public Service Announcement, Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments*.

Federal Trade Commission, *Seven Coronavirus scams targeting your business*.

United Kingdom

National Cyber Security Centre, *Phishing attacks: dealing with suspicious emails and messages*.

National Cyber Security Centre, *Home working: preparing your organisation and staff*.

National Cyber Security Centre, *Video conferencing services: security guidance for organisations*.

National Cyber Security Centre, *Video conferencing services: using them securely*.

European Union

EU Agency for Cybersecurity, *Tips for cybersecurity when working from home*.

EUROPOL, *Safe Teleworking Tips and Advice*.

EUROPOL, *How Criminals Profit from the COVID-19 Pandemic*.

EUROPOL, *Make Your Home a Cyber Safe Stronghold*.

Australia

Cyber Security Centre, *Cyber security is essential when preparing for COVID-19*.

Cyber Security Centre, *Threat update: COVID-19 malicious cyber activity*.

Cyber Security Centre, *COVID-19: Protecting Your Small Business*.

Cyber Security Centre, *Web Conferencing Security*.

Cyber Security Centre, *COVID-19: Cyber Security Tips When Working From Home*.

Borden Ladner Gervais