Cybersecurity Bulletin

March 2019

Financial Industry Regulator Issues Cybersecurity Guidance

In December 2018, the United States Financial Industry Regulatory Authority issued a *Report on Selected Cybersecurity Practices – 2018* to help broker-dealer firms improve their cybersecurity programs. The Report provides detailed recommendations for managing common cyber risks, and includes a list of core cybersecurity controls for small firms. The Report provides guidance that is consistent with best practices recommended by Canadian financial industry regulators, self-regulatory organizations and privacy commissioners, and is useful for organizations in all industries.

FINRA and Cybersecurity

The Financial Industry Regulatory Authority (FINRA) is an independent, self-regulatory organization for broker-dealer firms doing business in the United States. FINRA is authorized by the United States Congress to protect American investors by making sure the broker-dealer industry operates fairly and honestly.

In 2015, FINRA issued a *Report on Cybersecurity Practices* to provide information about the following practices that broker-dealer firms should consider to strengthen their cybersecurity programs: (1) cybersecurity governance and risk management; (2) cybersecurity risk assessment; (3) technical controls; (4) incident response planning; (5) vendor management; (6) staff training; (7) cyber intelligence and information sharing; and (8) cyber insurance. The report explained FINRA's expectation that broker-dealer firms would make cybersecurity a priority and would devote sufficient resources to understanding and preparing for current and evolving cybersecurity threats.

In 2016, FINRA published a *Checklist for a Small Firm's Cybersecurity Program* to help small broker-dealer firms with limited resources establish a cybersecurity program. The checklist is primarily derived from the National Institute of Standards and Technology (NIST) *Cybersecurity Framework* and FINRA's Report on Cybersecurity Practices (2015), and references the *SANS Critical Security Controls for Effective Cyber Defense*.

The 2018 Report

FINRA's *Report on Selected Cybersecurity Practices – 2018* presents FINRA's recommendations for effective practices regarding five important cybersecurity topics: (1) cybersecurity controls in branch offices; (2) phishing attacks; (3) insider threats; (4) penetration-testing programs; and (5) mobile devices. The Report reminds that the recommended practices should be part of a holistic cybersecurity program, as discussed in FINRA's 2015 *Report on Cybersecurity Practices*. The Report also provides a list of core cybersecurity controls for small broker-dealer firms to be used in conjunction with FINRA's *Checklist for a Small Firm's Cybersecurity Program*. Following is a summary of some of the key recommendations in the Report.

Branch Controls

The Report explains that effective cybersecurity controls in branch offices are especially important for firms with decentralized business models. The Report details four practices for addressing cybersecurity risks at branch offices: (1) develop comprehensive and easily referenced written supervisory procedures to define minimum cybersecurity requirements and to formalize oversight of branch offices; (2) create inventories of branch-level data, software and hardware assets, and related third party services, for use in conjunction with cybersecurity risk assessments to help identify critical assets and their cyber vulnerabilities; (3) establish and maintain branch technical controls to

mitigate identified cybersecurity threats; and (4) implement a robust review program to ensure that branches consistently apply cybersecurity practices.

Phishing

The Report explains that social engineering or "phishing" attacks, which try to convince a targeted individual to disclose sensitive information (e.g. personal information or credentials) or take harmful action (e.g. clicking on a malicious link or opening an infected attachment), are one of the most common cybersecurity threats to firms and their customers. The Report warns about the increasing sophistication and quality of phishing attacks, especially carefully planned attacks targeted to a specific individual (known as "spear phishing") or to a senior executive (known as "whaling") that can be difficult to distinguish from legitimate communications. The Report provides a useful summary of the characteristics of common phishing communications.

The Report details practices to mitigate phishing risks, including: (1) develop policies/procedures to specifically address phishing; (2) include phishing scenarios in risk assessments; (3) establish policies/procedures to confirm transaction requests; (4) implement email scanning and filtering to monitor and block phishing and spam communications; (5) train staff, including simulated phishing campaigns and remedial training for staff who demonstrate risky behaviour; (6) review processes/procedures to detect and remediate a successful phishing attack; (7) implement data loss prevention practices/procedures to reduce the impact of a successful phishing attack; and (8) provide customers with resources to protect themselves from phishing attacks.

Insider Threats

The Report warns that insider threats are a critical cybersecurity risk, because insiders (i.e. individuals with authorized access to firm systems and data) are often able to circumvent controls and cause material data breaches and other significant harm to an organization. The Report explains that an effective risk-based insider threat program typically includes the following components: (1) executive leadership and management support; (2) identity and access management policies and technical controls; (3) technical controls to help identify risky activities or anomalous behavior and detect potential attacks, and data loss prevention controls to prevent the inadvertent or malicious transmission of data to unauthorized recipients; (4) training for all insiders; (5) measures (based on people, processes and technologies) to help identify potentially malicious insiders and deter intentional misconduct, and to cultivate a strong culture of compliance; and (6) a comprehensive asset inventory.

Penetration Testing

The Report explains that penetration (or "pen") testing can be an important part of a cybersecurity program. A pen test simulates a malicious external or internal attack on a firm's network to identify vulnerabilities and evaluate the effectiveness of preventative measures. The Report notes that firms often take a risk-based approach to determining the systems to be tested and test frequency. The Report encourages due diligence when selecting pen test service providers, and the use of appropriate contractual arrangements (including confidentiality obligations) with all pen test service providers. The Report notes that firms often follow established governance structures and procedures for determining when and how to address risks identified by a pen test.

Mobile Devices

The Report explains that the increasingly widespread use of mobile devices by staff, customers and service providers can present significant cyber risks, including infected, cloned or pirated applications, operating system vulnerabilities, and phishing, spoofing or rerouting calls, emails and text messages.

The Report details practices to mitigate risks presented by staff use of mobile devices, including: (1) develop policies/procedures (e.g. "bring your own device" standards) for staff use of mobile devices and for the protection of sensitive data and information; (2) prohibit staff use of a mobile device unless the device has been approved and the user has agreed to comply with applicable policies/procedures; (3) train staff; (4) require all mobile devices to comply with technological requirements (e.g. mobile device management applications, password requirements, software restrictions, and encryption and transmission controls); (5) emphasize the importance of physically securing mobile devices and reporting lost devices; and (6) enforce compliance with mobile device policies/procedures with appropriate consequences for violations.

The Report details practices to mitigate risks presented by customers' use of mobile devices, including: (1) customer education/information about mobile device risks; (2) require the use of multi-factor authentication and implement data loss prevention controls; (3) prohibit the use of mobile devices for certain activities (e.g. changes to account settings or contact information); (4) automatically terminate remote network access after a period of inactivity; and (5) secure development and testing of mobile applications.

Core Cybersecurity Controls for Small Firms

The Report lists the following "core controls" for small firms' cybersecurity programs: (1) patch maintenance; (2) secure system configuration; (3) identity and access management; (4) vulnerability scanning; (5) endpoint malware protection;

(6) email and browser protection; (7) perimeter security; (8) security awareness training; (9) risk assessments; (10) data protection; (11) third-party risk management; (12) branch controls; and (13) policies and procedures. The Report cautions that an effective cybersecurity program requires that each of those controls be considered in the context of the firm's particular business model and technology infrastructure, and in light of other relevant circumstances. The Report encourages small firms to consider other FINRA cybersecurity guidance.

Comment

FINRA's 2018 Cybersecurity Report provides a helpful summary of some cyber risk management best practices that are useful for organizations of all sizes and in all industries. The Report is consistent with cybersecurity best practices recommended by Canadian financial industry regulators, self-regulatory organizations and privacy commissioners. The Report and other FINRA cybersecurity resources were referenced in the Cybersecurity Guide recently issued by the Investment Funds Institute of Canada. See BLG bulletins *Investment Funds Institute of Canada Issues Cybersecurity Guide*; *Cybersecurity Guidance from Investment Industry Organization (May 2016)*; *Cybersecurity Guidance from Investment Industry Organization (January 2016)*; *Cybersecurity Guidance from Canadian Securities Administrators*; *New York State Cybersecurity Regulation for Financial Services Companies*; *U.S. Securities and Exchange Commission Issues Cybersecurity Guidance Update*; *Cyber-Risk Management Guidance from Financial Institution Regulators*; *Regulatory Guidance for Cyber Risk Self-Assessment*.

Many of the cybersecurity activities recommended by FINRA present legal compliance considerations, including privacy and employment law rules. Organizations should obtain legal advice to ensure that their cybersecurity practices are consistent with applicable laws. For example, see BLG bulletin *Privacy Commissioners Issue Guidance for BYOD Programs*.

Some of the cybersecurity activities recommended by FINRA could be performed by or on behalf of legal counsel, so that resulting reports and advice are protected by legal privilege. Organizations engaged in cyber risk management activities should have an appropriate legal privilege strategy to help establish legal privilege and to avoid disclosures of privileged legal advice or inadvertent waivers of legal privilege. 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*; *Loss of Legal Privilege over Cyberattack Investigation Report*. ■

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