Eight Days A Week and Eight Ways to Reboot Your Cybersecurity Program; How All Firms Can Benefit From SIFMA’s New Cybersecurity Guidance

BY BRIAN RUBIN, CHARLIE KRULY AND SHANYN GILLESPIE

This article focuses on the “Small Firms Cybersecurity Guidance” recently issued by the Securities Industry and Financial Markets Association (SIFMA). While directed at “small firms,” SIFMA’s guidance can be adapted for firms of all sizes. SIFMA’s analysis is particularly important because the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) have yet to provide the industry with comprehensive cybersecurity guidance. SIFMA provides an “action item checklist” that identifies eight steps firms can take to protect against data breaches. According to SIFMA, these steps “can be implemented with relative ease and limited technical experience.” Each “action item” on SIFMA’s cybersecurity checklist is analyzed below. It is important to note that some of the issues highlighted by SIFMA have previously been the subject of SEC and/or FINRA enforcement actions, involving small and large firms alike.

1) Username and Password Protection

Brian Rubin is the Administrative Partner in charge of Sutherland Asbill & Brennan LLP’s Securities Enforcement and Litigation Team and heads the Washington, DC, litigation practice group. With more than 20 years of experience in federal securities law, first prosecuting and now defending, Brian represents clients being examined, investigated and prosecuted by the U.S. Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), other self-regulatory organizations and states. Brian previously served as NASD (now FINRA) Deputy Chief Counsel of Enforcement and was Senior Enforcement Counsel at the SEC.

Charles Kruly is a litigation associate in Sutherland Asbill & Brennan’s Washington, D.C. office. He is admitted to the New York bar and practices under the supervision of District of Columbia bar members.

Shanyn Gillespie is an associate in Sutherland Asbill & Brennan’s Washington, D.C. office.

2 Id. at 6.
3 Id.
According to a 2013 report cited by SIFMA, "76% of network intrusions and the top five methods of hacking both utilized weak or stolen credentials.14 SIFMA’s first action item is that firms apply “strict” and “robust” password security requirements, including:

- Complexity (e.g., password must use a combination of upper and lower case letters, numbers and symbols);
- Minimum length (e.g., password must be at least eight characters long);
- Regular expiration and mandatory resets (e.g., password expires after 90 days and a new password is required);
- Uniqueness (e.g., password must not contain common words and dates, and must be different from the user’s other passwords); and
- Multi-factor authentication (e.g., user must provide two of the following (a) a password or an answer to a challenge question, (b) an object or a device only the user has (like a security token), and (c) a biometric unique to the user (like a fingerprint)).

Inadequate password security has already generated enforcement actions by the SEC and FINRA, including:

- The SEC ordered a large firm to pay a $275,000 penalty for, among other things, failing to take corrective measures in response to an internal audit finding that the firm’s password protection for its proprietary trading system did not meet industry standards for “strong” password protection because, for example, the firm did not require (a) a minimum password length; (b) a complex password involving an alphanumeric/special character combination; (c) expiration of passwords after a specified period of time; and (d) automatic lockout after failed login attempts.
- FINRA fined a large firm $175,000 for, among other things, failing to protect a firm database containing non-public information by allowing the use of a generic user name (e.g., “Administrator”) and password (e.g., “password”).7
- FINRA fined a mid-sized firm $375,000 for failing to require a password to access a database, even though it contained non-public customer information and was stored on a computer with a persistent Internet connection.
- FINRA fined two affiliated large firms a combined $600,000 for, among other things, failing to have adequate password protection for their electronic portfolio management systems because they: (a) allowed employees to share usernames and passwords; (b) did not track who accessed the system and when; (c) failed to require that passwords be changed on a periodic basis; and (d) failed to disable usernames and passwords after employees left the firms.9
- FINRA fined a small firm $300,000 for, among other things, failing to enforce a requirement that passwords to access firm laptops be changed every six months through validation or mandatory password expiration.10

2) Control Administrative and Privileged Access

Like the first recommendation, SIFMA’s second action item is also intended to ensure that only authorized individuals have access to a firm’s systems and data. SIFMA recommends that firms limit access to their systems and data only to firm personnel who need such access to perform their functions.11 Thus, firms should consider:

- Mapping user access privileges by job function;
- Establishing controls to prevent unauthorized persons from accessing or altering firm systems and data; and
- Implementing controls to detect any such unauthorized activity.12

3) Application Whitelisting

SIFMA’s next action item is for firms to utilize an application “whitelist” to help ensure that only “trusted software” is executed on firm operating systems.13 (For those who think that “whitelisting” is what Tom Sawyer and his friends did to Aunt Polly’s fence, let us correct that misimpression. “Whitelisting” refers to the practice of creating a list of approved applications—the “whitelist”—and allowing only those approved applications to be executed on firm operating systems.)14 Whitelisting therefore prohibits users from executing non-approved applications on firm operating systems.15 Thus, whitelisting “flips the antivirus model from a ‘default allow’ to a ‘default deny’ for all executable files.”16 The goal of whitelisting is to prevent users from downloading malicious files and infecting firm devices and systems.

4) Anti-Virus, Email, and Website Filters

SIFMA’s fourth action item is for firms to maintain “[u]pdated anti-virus software, in addition to web security software,” and to train their personnel to exercise...

---

5 Id.
11 SIFMA Cybersecurity Guidance at 6.
12 See id.
13 Id.
15 See id.
16 Id.
“personal vigilance against suspicious emails and attachments.”17

The SEC and FINRA have brought enforcement actions against firms for failing to ensure installation of anti-virus software on firm devices:

- The SEC ordered a large firm to pay a $100,000 penalty because, among other things, its procedures recommended—but did not require—that anti-virus software be installed on registered representatives’ computers.18

- FINRA fined a large firm $450,000 based in part, on its failure to (a) require that field representatives install anti-virus software on their computers; and (b) review such computers to verify the installation of the anti-virus software.19

- FINRA fined a small firm $125,000 for, among other things, failing to implement procedures requiring quarterly reviews of computers, when such reviews would have detected the firm’s failure to install “essential monitoring software” on at least 19 employee computers.20

5) Secure Standard Operating Systems

SIFMA’s fifth action item urges firms to “[s]tandardize on trusted operating systems that meet Common Criteria.”21 SIFMA recognizes that using “unsupported or outdated operating systems” may leave firm systems and data vulnerable to attack. SIFMA cites Windows XP as an example of an “unsupported or outdated operating system[].”22 Windows XP is, according to a recent report, “comically outdated” but, nonetheless “more than a quarter of the computers connected to the Internet are still running Windows XP.”23

6) Automated Patching Tools and Processes

Sixth, SIFMA recommends that firms “[u]tilize automatic software updates and spot-check that updates are applied frequently.”24 Malware is often designed to exploit flaws in software. To combat this problem, many software companies issue updates (sometimes referred to as “patches”) on an ongoing basis to fix such flaws as they are detected. A recent example is the HeartBleed bug in OpenSSL software, which was publicly announced in April 2014 and decried as possibly the “worst vulnerability” ever detected because an estimated 500,000 websites were using OpenSSL.25 Although a patch was issued at the time of the public announcement, by late July 2014, one report found that 97% of Global 2000 organizations’ public-facing servers were still vulnerable to HeartBleed-based attacks because the organizations did not apply the patch or, more commonly, they applied the patch, but did not complete the necessary follow-up steps (e.g., replacing SSL keys and digital certificates).26 Thus, it is important to ensure that software patches are applied timely and that additional actions are taken, as necessary, to fix such software vulnerabilities.

7) Back Up Data Regularly

SIFMA’s next action item addresses the issue of data recovery in the event a cyber-attack causes the loss or destruction of data. SIFMA advises firms to use “cloud or physical external hard-drive backup systems.”27 This is not a new issue for firms; FINRA Rule 4370(c)(1) already requires that a firm’s business continuity plan address how the firm’s data is backed up and how it is recoverable.

8) Mobile Device Security and Encryption of Data

SIFMA’s final action item is for firms to “[e]nsure that mobile devices are secure with passwords and [that] data is encrypted in the event of a loss.”28 While the regulators have yet to mandate by rule or regulation that encryption is required, FINRA did fine a small firm $300,000 for, among other things, failing to encrypt data stored on a laptop.29 In that case, a laptop containing some of the firm’s “most sensitive” information (e.g., customer social security numbers and bank account numbers) was stolen from the car of an employee of an affiliated company.30 In FINRA’s view, the firm should have encrypted this data because it was “most sensitive,” it was stored on a laptop that the firm permitted to be removed from the office, and it was therefore “reasonably foreseeable” that the data was “at risk of loss or theft.”31 Firms should consider requiring encryption for mobile devices (e.g., laptops, thumb drives, BlackBerry devices, phones) to the extent they may contain non-public customer information, and they are allowed to be removed from the office.

While SIFMA’s guidance is focused on encryption of data on mobile devices, firms may also want to consider security of data stored in the cloud. A recent study by the Ponemon Institute found that more than half of the 4,000 organizations surveyed did not encrypt “sensitive or confidential data” stored in the cloud.22 While secu-
rities regulators have not yet focused on cloud security, firms should consider encrypting any non-public customer information stored in the cloud.

Firms of all sizes should consider beginning—if they haven’t already—implementing SIFMA’s recent guidance. Indeed, reports of major cyberattacks are becoming increasingly common, suggesting that it may not be a question of “if,” but a question of “when.” So, firms should remember, “let’s be careful out there.”

---


* * *