



FS-ISAC on Cybersecurity Awareness

This monthly update is brought to you by the Financial Services Information Sharing and Analysis Center (FS-ISAC) in coordination with the Securities Industry and Financial Markets Association (SIFMA), the Investment Industry Association of Canada (IIAC) and the International Council of Securities Associations (ICSA).

The information provided in this monthly newsletter highlights cybersecurity topics and emerging threats to the securities industry globally. It is intended to increase the cybersecurity awareness of an organization's end-users and to help them interact in a more secure manner.

This newsletter is not intended to replace the benefits of joining FS-ISAC's member-based organization and readers from organizations who are not already members are encouraged to ([join](#)) FS-ISAC.

FS-ISAC Board Names Steve Silberstein New CEO of FS-ISAC

Steve Silberstein has been named the new CEO of FS-ISAC by FS-ISAC's Board of Directors. Steve replaces CEO Bill Nelson, who is leaving FS-ISAC to become the CEO of the Global Resilience Federation (GRF). Bill has been an integral part of FS-ISAC's growth and expansion over the past 12 years, from hundreds of members in the US, to nearly 7,000 members in 48 countries. Steve starts on January 1, 2019. He will focus on accelerating the pace of FS-ISAC's digital transformation, modernizing the information sharing platform, producing more actionable information sharing, continuing global expansion and supporting public private partnerships. Steve previously served as CEO of Sheltered Harbor, which became an FS-ISAC subsidiary in 2016. Most recently, he served as chief operating officer of BlueVoyant, where he was responsible for technology, marketing and administration of the firm's activities around global threat intelligence.

SEC Fines Firm with a Rarely Invoked Rule

Last month, the US Securities and Exchange Commission (SEC) announced a \$1 million fine against an investment firm for its cyber security policies and procedures, which invokes a 6-year-old identity theft rule ([Business Insurance](#)). In the settlement, the SEC states that the registered broker-dealer and investment advisor violated the safeguard rule that requires every firm register with the commission to adopt written policies and procedures that address the protection of customer records.

According to the SEC agreement, one or more persons impersonating the firm's contractor representatives called its technical support line and requested a reset of three representatives' passwords for the web portal to access its customer. The firm was notified hours later of the breach although no unauthorized fund transfers or securities were executed on customers' accounts. Unfortunately, the firm did not prevent intruders from gaining access to its systems, according to the SEC.

Experts have said this is the first time the SEC has invoked the 2013 identity theft rule, and only the third time it has brought an enforcement action involving the safeguard rule. Firms should review all SEC rules and guidelines pertaining to protection of customer information and systems and ensure that they have properly updated policies and procedures as well as other testing and controls in place that meet the requirements set forth in the commission's rules.

Software Patches Address 60+ Vulnerabilities

Last week, Microsoft released its November 2018 updates to address more than 60 vulnerabilities, including zero-days and publicly disclosed flaws ([SecurityWeek](#)). The exploits found by Kaspersky lab included a privilege escalation vulnerability in Windows that has been actively exploited by malicious actors ([CVE-2018-8589](#)). This flaw allows an attacker to execute arbitrary code in the context of the local users. This issue only affects Windows 7 and Windows Server 2008 operating systems. Another vulnerability that is repaired with these updates is related to the Advance Local Procedure Call (ALPC), where an unauthenticated attacker can use it to elevate privileges and take control of a vulnerable system ([CVE-2018-8584](#)). This flaw affects the recent version of Windows Server and the Windows 10 operating systems.

Firms should review the latest information regarding these patches and apply them to systems running the above-mentioned operating systems, to secure systems and prevent any attacks utilizing the known exploits.

FS-ISAC Presents FDX to the SPARK Institute

During the SPARK Institute's three-day conference, Anne Dubon presented on the Financial Data Exchange (FDX), providing the audience with an introduction on FDX, highlighting the value of this new FS-ISAC subsidiary. Learn more about [FDX](#) and the [SPARK Institute](#).

FS-ISAC Cyber-Range Ransomware Exercises

Cyber-range exercises offer FS-ISAC members a more technical, hands-on keyboard experience that provides greater interaction and sharing between members in a way that helps raise capability, maturity levels and resiliency across the sector. FS-ISAC has partnered with ManTech to build a network environment and facilitate the event. Events for 2019 have been announced, please visit [FS-ISAC](#) for additional details.

Upcoming Cyber-Range Exercises

- January 30, 2018 | Federal Reserve Bank of Boston | [Register](#)
- February 13, 2018 | Zurich | [Register](#)
- February 28, 2018 | Online | [Register](#)
- March 5, 2018 | Toronto Exchange (TMX) | [Register](#)
- March 19, 2018 | Federal Reserve Bank of Atlanta | [Register](#)
- April 2, 2018 | Federal Reserve Bank of Cleveland | [Register](#)
- July 25, 2018 | Federal Reserve Bank of Chicago | [Register](#)
- August 22, 2018 | Federal Reserve Bank of St. Louis, MO | [Register](#)

About the FS-ISAC

The Financial Services Information Sharing and Analysis Center (FS-ISAC) helps assure the resilience and continuity of the global financial services infrastructure through sharing threat and vulnerability information; conducting coordinated contingency planning exercises; managing rapid response communications; conducting education and training programs; and fostering collaborations with and among other key sectors and government agencies. This newsletter is not intended to replace the benefits of joining FS-ISAC's member-based organization. Please consider joining if you're not already a member.

Thank you,
FS-ISAC SIRG Team

If you have any questions about this report, please contact the [FS-ISAC](#).

This newsletter contains content developed by FS-ISAC as well as links to content developed by third parties. FS-ISAC makes no claims or warranties as to the accuracy of information provided by third parties. All copyrights remain with their respective owners.

Financial Services Information Sharing Analysis Center

www.fsisac.com

© 2018 FS-ISAC Inc.



