FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Securities Industry Risk Group **May 2017**
Global Cybersecurity Brief **TLP: WHITE**

FS-ISAC Collaborates 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 Advisory of the International Council of Securities Associations (ICSA).

The information provided in this Monthly Newsletter highlights Cyber Security 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**).

Colorado Has Proposed Cyber Regulations for Advisors and BDs

Proposed changes to the state of Colorado's securities laws may require financial advisors and broker dealers to protect clients' electronic data from cybercriminals (**InvestmentNews**). The proposed rule (**Colorado Proposed**) will call for firms to have written policies and procedures for protecting customer data.

Proposed Rule 51-4.14(IA) will affect investment advisors stipulating, 'reasonably designed to ensure cybersecurity' and perform a yearly cybersecurity risk assessment (**RIA**). The rule also lists seven factors the Colorado Division of Securities may consider to help determine where an investment advisor firm's policies and procedures are 'reasonably designed to ensure cybersecurity'. These factors include the size of a firm; its relationship with third parties, its written policies and employee training; the security of devices used to access sensitive information; security protocols for data in transit or at rest (including electronic communications), and how the firm mitigates the risk of lost or stolen devices that contain sensitive information.

Rule 51-4.8 focuses on broker-dealers whose obligations are to protect data stored or transmitted online. Similar to the rule for investment adviser firms, it also discusses the factors considered by the Colorado Division when determining where a broker- dealer' policies are adequate.

Based on these proposed rules, and the rules set in New York State, it is likely that other states will issue cybersecurity requirements as well.

NIST's National Cybersecurity Center of Excellence (NCCoE) Nearing Completion of Access Rights Management Project

The Financial Services sector team is wrapping up the Access Rights Management for Financial Institutions project, and anticipates releasing a draft version of the National Institute of Standards and Technology (NIST) Special Publication Practice Guide in May. The Financial Services sector team has completed integration of the components and is in the process of conducting functional testing. The Practice Guide document will contain three volumes: Volume A - Executive Summary; Volume B - Approach, Architecture, and Security Characteristics; and Volume C – "How To Guides". The team appreciates the valuable feedback they've received from the financial sector community, and looks forward to additional comments and input.

As mentioned during a call last month, the NCCoE participated in the FS-ISAC Annual Summit in Orlando on April 30 - May 3. NCCoE hosting two tables during the Opening Breakfast and arranged one-on-meetings with individuals who were interested in learning more about the work of the NCCoE. The NCCoE's financial services sector group plans on speaking to Securities Industry and Financial Markets Association (SIFMA) For more information, please contact Susan Prince at **susan.prince@nist.gov** or **financial_nccoe@nist.gov**.

Quick Summaries of Financial Sector Projects

> **Access Rights Management – Learn how to control** who can obtain access to information and resources with a cohesive and secure identity and access management system. To find out more about this project, by clicking **here**.
>
> **IT Asset Management** - Make software changes and network breaches more easily identifiable. To find out more and download the NIST Cybersecurity Practice Guide 1800-5, by clicking **here**.

Ultimately, the NCCoE projects result in a publicly available NIST Cybersecurity Practice Guide—a description of the practical steps needed to implement an example solution that addresses these existing challenges to help industry understand the possibilities to improve cybersecurity within their organizations.

Shadow Brokers Group Releases Exploits

In April, the hacker group known as Shadow Brokers released the key to unlock an encrypted cache of tools alleged to belong to the Equation Group, which security companies attribute to the US National Security Agency (NSA). The archive contained over 300 MB of data, including firewall exploits, hacking tools and scripts that targeted a number of security products. This is the fifth set of exploits made available to the public since August 2016. Of note, researchers quickly identified tools for scanning SWIFT systems. Many media outlets also reported on the documents released that allege the NSA had gained access to a number of Middle Eastern banks. This, however, has been denied by SWIFT and EastNets.

The main concern for financial institutions is the threat of new, advanced cyber tools used to exploit Windows operating systems which are publicly available for any cybercriminal or actor to use. FS- ISAC, however, views the risk of harmful exploitation as low as Microsoft announced that it has patched the vulnerabilities pertaining to its software.

FS-ISAC Information on a EU General Data Protection Regulations

On May 8, the FS-ISAC hosted an Expert Webinar Series on the impact of the European Union's General Data Protection Regulation (GDPR) on how financial firms must handle personal data, and its influence on how financial institutions may share intelligence with other institutions. The GDPR, which goes into effect on May 25, 2018, aims to strengthen and harmonize data protection requirements for individuals that reside in European Union (EU) countries. The GDPR impacts financial institutions that do business in the EU. To prepare FS-ISAC members for the new regulation, the FS-ISAC's European Legal and Regulatory Working Group issued a paper in 2016 on how to create a more consistent and streamlined incident/fraud reporting framework in the EU.

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.

Thank you,

Peter Falco and Richard Livesley

pfalco@fsisac.com rlivesley@fsisac.com

If you have any questions about this report, please contact the **FS-ISAC**.

Financial Services Information Sharing Analysis Center **www.fsisac.com**