FS-ISAC Securities Industry Risk Group Global Cybersecurity Brief | **April 2019** | **TLP: WHITE**

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), the International Council of Securities Associations (ICSA), the Financial Services Institute (FSI) and the Insured Retirement Institute (IRI).

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.

Making History – Annual Summit Keynote

For 20 years, FSISAC has set the bar for cyberthreat information sharing. At this year's Annual Summit, our opening keynote speaker, Brad Meltzer, will share ways in which we can maintain high standards and improve information sharing well into the future. By walking us through the legacies left by noteworthy historical figures and events, this New York Times bestselling author and host on The History Channel will illustrate how FS-ISAC can and will uphold its position as the cyberthreat intelligence leader for another 20 years and beyond. Our closing keynote is Rob Joyce, Senior Advisor for Cybersecurity to the Director of the National Security Agency (NSA) and former Special Assistant to the President and Cybersecurity Coordinator at the White House. **Register** for the Annual Summit, 28 April-1 May in Orlando.

FED Chairman: Cyber-risks and Resiliency Primary Focus

In a recent "60 minutes" interview (***CBS***), US Federal Reserve Chairman Jerome Powell expressed concern for cybersecurity threats and attacks. He noted that cyber is a major focus of financial institutions and the Federal Reserve system itself given a 'the worst case scenario' involving a successful cyber-attack on a firm, financial market, utility or payment system. He revealed that there has never been a time when he thought the Fed was doing enough in light of the increasing risks even though the Federal Reserve devotes considerable amount of time and resources to protect the Fed, financial institutions, and markets. Powell stressed the need to examine how to make institutions and utilities resilient against any type of cyber-attack and build redundancies around them. While this is an unusual

admission by a Fed Chair, it certainly shows a shift in the Fed's position, underscoring the importance of identifying the ever-growing and changing cyber threat landscape affecting the sector.

New Malware Targets Multiple IoT Devices

A new variant of the Mirai malware, responsible for creating a vast IoT botnet, has been spotted in the wild, incorporating a brand-new array of 11 exploits. In addition, the new variant of Mirai includes new credentials to use in brute force attacks against devices. The variant appears to be targeting different embedded devices like routers, network storage devices, NVRs, IP cameras, and in popular enterprise devices such as WePresent WiPG-1000 Wireless Presentation systems, and LG Supersign TVs. (***SC Magazine***). Firms using any type of devices that are vulnerable to this exploit should contact the device manufactures for recommendations and updated software patches.

Latest Survey Shows Firms Failing in Cybersecurity

Results from the 2019 Deloitte Future of Cybersecurity survey show comprehensive cybersecurity measures to be a difficult undertaking for many enterprises, that either provide a false sense of security or inadequate protections applied to systems within the organization (***Tech Republic***). Respondents of the survey included 500 C-suite executives who oversee cybersecurity at companies with $500 million (USD) or more in annual revenue. The survey found three primary challenges that firms face in implementing strong cybersecurity measures. Those challenges include:

1. Inability to better prioritize cybersecurity risk across the enterprise
2. Lack of management alignment on priorities
3. Lack of adequate funding

The survey also showed a mismatch in how IT approaches security. The survey found 85% of respondents are reporting they use Agile or DevOps for application development, but DevSecOps ranks 11% among cyber-defense priorities and investments.

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. For example, FS-ISAC conducted its second European cyber-range exercise in Zurich on March 1. The cyber-range exercise simulated a ransomware attack leveraging artificial intelligence. FS-ISAC partnered with UBS for an exercise that convened CISOs, CIOs, heads of security and security analysts from 14 leading financial services and trade associations from across Europe to take part in a WannaCry-style attack on a simulated bank network.

Upcoming Cyber-Range Exercises

- July 25, 2018 | Federal Reserve Bank of Chicago | **Register**
- August 22, 2018 | Federal Reserve Bank of St. Louis, MO | **Register**

See ***FS-ISAC Exercises*** for additional details.

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**.

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