FS-ISAC Securities Industry Risk Group Global Cybersecurity Brief | **October 2018 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) 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.

October is Cybersecurity Awareness Month

FS-ISAC is a 2018 National Cyber Security Awareness Month (NCSAM) Champion. The annual campaign is led by the US Department of Homeland Security and the National Cyber Security Alliance (NCSA) to educate and inform consumers, small and mid-sized business, corporations, educational institutions and young people about how to stay secure and safe while connected to the internet. The first observed NCSAM was October 2004.

Stay Safe Online

During the October 2008 NCSAM, the **STOP. THINK. CONNECT.** campaign was introduced. The STOP. THINK. CONNECT. campaign provides capstone messages like "Keep a Clean Machine" and "Lockdown Your Login". As well, the content providers at STOP. THINK. CONNECT. offer a wealth of resources and tips, and documents in global languages like Spanish, Japanese, Brazilian Portuguese and Russian, in addition to English.

NCSAM 2018 Themes

- **Week 1: Oct. 1–5: *Make Your Home a Haven for Online Safety***
  Children learn basic security practices from their parents: look both ways before crossing the street, don't talk to strangers and hold an adult's hand in public. Children also need to be taught basic cybersecurity practices: the ways they use social media, adjust the

thermostat via a mobile device or shop for a toy online. Week one will review cybersecurity essentials an entire family can use to protect against cyberthreats.

- **Week 2: Oct. 8–12:** ***Millions of Rewarding Jobs: Educating for a Career in Cybersecurity***
  According to recent estimates, there will be a global shortage of 3.5 million cybersecurity professionals to fill required positions. However, there are limitless opportunities for high school and higher education students, veterans and adults looking to change careers to train in and enter a cybersecurity field. Week two will focus on ways to motivate parents, teachers and counselors to learn more about the cybersecurity field and how to best encourage and inspire students and others to seek highly fulfilling cybersecurity careers.

- **Week 3: Oct. 15–19*: It's Everyone's Job to Ensure Online Safety at Work***
  As the lines between our work and daily lives is increasingly blurred, it is more important than ever that all employees understand their role in keeping the organization secure; this is especially true when, year after year, employee social engineering attacks tend to be the primary method hackers use to infiltrate corporate networks. Week three will focus on two areas: a) cybersecurity workforce education, training and awareness and b) risk management, resistance and resilience. As well, the NCSA's *CyberSecure My Business* will help small and mid-sized businesses understand how they can protect their organization, employees and customers.

- **Week 4: Oct. 22–26*: Safeguarding the Nation's Critical Infrastructure***
  A disruption to the US critical infrastructure (e.g. food, water, financial services, power, transportation, etc.) could have dire and long-lasting consequences. While the average consumer may feel they have no control over the security or safety of these systems, Week four will highlight roles the public can play to keep it safe.

Extradition of Alleged Russian Hacker

On September 7, 2018, the US Attorney General's office for the Southern District of New York, the Federal Bureau of Investigation (FBI) and the US Secret Service announced that Andrei Tyurin was extradited from the country of Georgia. Tyurin was arrested by Georgian authorities at the request of the United States for charges arising from his participation in a massive computer hacking campaign targeting US financial institutions, brokerage firms, financial news publishers and other American companies. The hacks included the largest theft of customer data from a US financial institution in history (***DataBreaches***).

In addition to the US financial sector hacks, Tyurin also conducted cyberattacks against numerous US and foreign companies in conjunction with other various criminal enterprises operated by Shalon and his co-conspirators, including an illegal internet gambling business and illegal international payment processors. The majority of these illegal businesses exploited the success of Tyurin's computer hacking campaigns.

Tyurin, of Moscow, Russia, is charged with one count of conspiracy to commit computer hacking, which carries a maximum prison term of five years; one count of wire fraud, which carries a maximum prison term of 30 years; four counts of computer hacking, each of which carries a maximum prison term of five years; one count of conspiracy to commit securities fraud, which carries a maximum prison term of five years; one count of conspiracy to violate the Unlawful Internet Gambling Enforcement Act, which carries a maximum prison term of five years; one count of conspiracy to commit wire fraud and bank fraud, which carries a maximum prison term of 30 years; and aggravated identity theft, which carries a mandatory consecutive term of imprisonment of two years. The charges contained in the indictments are merely accusations and Tyurin is presumed innocent until proven guilty.

FS-ISAC Outreach

On September 25, 2018, FS-ISAC's Peter Falco participated on a cybersecurity panel at the Insured Retirement Institute Conference (***IRI***). Falco and other panel members discussed the importance of information sharing, as well as best practices before, during and after a cybersecurity incident. The primary target audience included firms focused in the finance industry specifically broker dealers, retirement and insurance companies.

NIST Developing Privacy Framework

The National Institute of Standards and Technology (NIST) announced plans to create a framework to guide organizations on how to protect the information of individuals using a company's product and services (***TheHill***). According to NIST's press release (***NIST***), the new framework will be based on the structure NIST has established for cybersecurity issues. The agency's goal is to develop a framework that will bridge the gaps between privacy professionals and senior executives, allowing organizations to effectively respond to challenges. The agency also announced a public workshop for mid-October in Texas to gather input on what should be included in this new framework.

A Rocking Cybersecurity Keynote, Return of the Titans and Sessions Galore All at the Fall Summit

FS-ISAC is excited to announce that Jeffrey Baxter, National Security Expert and founding member of Steely Dan will keynote the 2018 FS-ISAC Fall Summit taking place 11-14 November in Chicago. The keynote takes place on Monday 12 November.

Then, back by popular demand, you won't want to miss this year's *Tempt the Titans*! Make sure you plan to attend this member favorite. Attendees will 'vote' for their favorite early stage firm and then the top three companies will pitch to the Titans on Wednesday 14 November.

You will want to start planning your agenda today from our more than **120 sessions** and **eight tracks**. Learn more and **register today**!

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. Learn more and register (**Register Here**) for one of these upcoming sessions:

- October 24 | Federal Reserve Bank of Kansas City, MO
- 2019 Events to be announced soon

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**