Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – May 2020

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 Investment Industry Association of Canada (IIAC), the International Council of Securities Associations (ICSA), the Financial Services Institute (FSI), the Insured Retirement Institute (IRI), the Securities Industry and Financial Markets Association (SIFMA) and the SPARK Institute.

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.

CISA Releases v2.0 of the Essential Critical Infrastructure Worker Guidance

The Cybersecurity and Infrastructure Security Agency (CISA) executes the Secretary of Homeland Security's authorities to secure critical infrastructure. Consistent with these authorities, CISA has developed an "Essential Critical Infrastructure Workforce" advisory list in collaboration with other federal agencies, state and local governments, and the private sector. This list is intended to help state, local, tribal and territorial officials as they work to protect their communities, while ensuring continuity of functions critical to public health and safety, as well as economic and national security. Decisions informed by this list should also take into consideration additional public health considerations based on the specific COVID-19-related concerns of particular jurisdictions (**CISA**).

US Secret Service Warns on Coronavirus Email Scams

The United States Secret Service (USSS) sent an alert on 2 April notifying law enforcement officials of hackers sending emails with attachments that installs malware remotely on employee computers (**USSS**). Hackers are keen on taking advantage of organizations' efforts to keep employees informed on COVID-19 updates, with some posing as vendors, so as not to raise suspicions.

US Issues Cyber-Threat Warning Against North Korea

On 15 April 2020, the United States published a public advisory on cyber threats posed by North Korea. The joint advisory from the US Treasury, US Departments of State, Homeland Security and the Federal Bureau of Investigation highlighted the threat posed by North Korea and how to stay aware and safe (**US Cert**). The advisory warns the public about crypto-jacking and extortion campaigns, cyber-enabled financial theft, and money laundering scams. The report also suggests that the malicious cyber activities threaten the integrity and stability of the international financial system and explains North Korea is using the profits from cyber-crime to strengthen its military capabilities.

FS-ISAC Cyber-Range Ransomware, Business Email Compromise and *new* Cloud Leak 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. These popular exercises sell out quickly, so register early!

NOTE: Due to the outbreak of COVID-19, and with abundant concern for the physical health and well-being of our members and staff, as well as the staff of our cyber-range exercise partners, the Dallas Ransomware Cyber Range Exercise has been rescheduled for 23 September. We will continue to reevaluate whether a physical presence is available given that we have the option to make each of these exercises 100 percent virtual. Thank you for your understanding and cooperation.
Upcoming Cyber-Range Exercise scenarios focus on Ransomware, Business Email Compromise (BEC) or Cloud Leak (NEW) attacks:

- 16 June | FS-ISAC Business Email Compromise Exercise | Virtual | **Register**
- 22 July | FS-ISAC Business Email Compromise Exercise | MPLS, MN | **Register**
- 18 August | FS-ISAC Cloud Leak Exercise | St. Louis, MO | **Register**
- 3 September | FS-ISAC Cloud Leak Exercise | Chicago, IL | **Register**
- 23 September | FS-ISAC Ransomware Exercise | Dallas, TX | **Register**

Additional dates and locations (Boston, New York, Kansas City and San Francisco) will be added soon! Please check the **FS-ISAC Events** page where you can filter by Exercises for more dates or send questions about these cyber-range exercise events or other FS-ISAC exercises to **exercises@fsisac.com**.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. These popular exercises sell out quickly, so register early! For additional information, visit us online.

If you have any questions about this week's report, please contact the FS-ISAC SIRG.

Financial Services Information Sharing and Analysis Center

fsisac.com