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.

Situation in Iran and Iraq

The FS-ISAC Global Intelligence Office is closely monitoring recent developments and escalation between the United States and Iran. On 3 January, the leader of Iran's elite arm of the Islamic Revolutionary Guard Corps, known as the Quds Force, was killed by a US airstrike in Iraq. Iranian leadership and their allies retaliated for these attacks on 8 January. FS-ISAC has engaged the US government, which continues to assess the expectation of additional proportional responses from this attack but lack insight into what form those might take. As a historical target of Iran and a symbol of economic power, US members are advised to remain vigilant to any uptick in suspicious activity. Physical or cyber-attacks could be posed against financial targets in the Middle East, the US, or its allies, as well as industries that finance relies on to operate within those same regions.

Members are encouraged to review some resources available on the FS-ISAC portal:

- *FS-ISAC Spotlight Report: Iranian Threat Actors and Campaigns*
- *Threat Intelligence Committee Threat Viewpoint - Destructive Malware*
- *Threat Intelligence Committee Threat Viewpoint - Distributed Denial of Service (DDoS) Attacks, August 2018*
- *Australian Security Cyber Centre - Password Spray Attacks: 2019-003 and 2019-004*

FS-ISAC provides a centralized hub for trusted voluntary information sharing and analysis. FS-ISAC members participate in trusted and anonymous communication channels within FS-ISAC and with other financial institutions.

SEC Releases 2020 Examination Priorities Letter

On 7 January, the US Securities and Exchange Commsons (SEC) released its 2020 Examination Priorities Letter. A number of guidelines will focus on broker-dealers and their implementation preparedness of recent rulemaking while RIA firms' policies of advising retail investors and private funds will be examined. According to SEC Chairman, Jay Clayton, the Office of Compliance Inspections and Examinations (OCIE) will conduct broker-dealer exams by looking in on market participants' readiness of Regulation Best Interest (Reg BI), which takes effect 30 June, 2020. RIA exams will target firms that have not been examined over the last several years or newer RIA firms. (Financial Advisor IQ). "OCIE's 2020 examination priorities identify key areas of risk, both existing and emerging, that we expect self-regulatory organizations (SROs), clearing firms, investment advisers and other market participants to identify and mitigate," according to Clayton. The SEC will continue their focus on the retail investor, providing more insight on the electronic trading marketplace and digital assets.

Federal Reserve Bank of New York Cyber Warning

According to new research published in a paper by the Federal Reserve Bank of New York (NYFR paper) a sophisticated cyber attack on the United States could ripple through major banks and severly disrupt the broader financial system. The report states that a cyber attack on the data or systems of any one of the five most active banks could spill over to others and affect more than a third of assets in the overall network.

According to the paper, exact estimates of potential damage varied based on the timing and location of a US cyberattack. In one of the more severe scenarios; banks hoard liquidity in response to the attack, forgone payments could amount up to 2.7 times US gross domestic product. Even banks with less than $10 billion in assets would impair significant amounts in the systems.

Data Leak Affects 250 Million Customers Over 14 Years

A report reveals that 250 million Microsoft customer records, spanning 14 years, have been exposed online without password protection. The report reveals that the same set of 250 million records were found on five different servers (FORBES). The records were customer service and support logs detailing customer conversations between the software company's support agents and customers across the world. The records spanned from 2005 to December 2019. Researchers state the data was unsecured and anyone with a web browser who stumbled across the data could easily access it. Researchers say that much of the personally identifiable information was redacted, however, information such as email addresses, IP addresses, geographical locations and other information was available. Once aware of the situation, a representative from Microsoft reported that all servers were secured within 24 hours and they are working quickly to prevent an event like this to happen again.

*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! For additional information, visit us online.

Upcoming Cyber-Range Exercise scenarios focus on Ransomware, Business Email Compromise (BEC) or Cloud Leak (NEW) attacks:

- *3 March | FS-ISAC Cloud Leak Exercise | Atlanta, GA | Register*
- *22 April | FS-ISAC Ransomware Exercise | Dallas, TX | Register*
- *16 June | FS-ISAC Business Email Compromise Exercise | Toronto, CA | Register*
- *22 July | FS-ISAC Business Email Compromise Exercise | Minneapolis, MN | Register*
- *18 August | FS-ISAC Cloud Leak Exercise | St. Louis, MO | Register*

Additional dates and locations (Boston, New York, Chicago, 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.

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

This newsletter contains content developed by FS-ISAC as well as links to content developed by third-parties.

Financial Services Information Sharing and Analysis Center

fsisac.com