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 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**).

As GDPR Deadline Approaches Cybersecurity Concerns Increase

With the European Union's General Data Protection Regulation (GDPR) deadline less than a year away, a new survey shows cybersecurity risks have become a major concern among executives (**Business Insurance**). The global study of more than 1,300 executives, whose firms offer products or services in the European Union (EU) found that 65% now consider cybersecurity as a top risk as compared to 32% in a similar survey conducted last year.

The GDPR will apply to companies that are in control or process data of citizens of the European Union, including the United Kingdom. These companies will be required to have data protection officers/ data controllers in places. Under the GDPR, the Data Controller will be under a legal obligation to notify the Supervisory Authority without undue delay. The reporting of a data breach is not subject to any *de minimis* standard and must be reported to the Supervisory Authority within 72 hours after having become aware of the data breach (Article 33). In the event of a breach, fines could total up to 4% of a company's annual revenue.

The survey also showed that only 8% of GPDR-affected organizations are fully compliant and that 57% of organizations are in the process of developing compliance plans while 11% of companies have not started developing any plans.

Firms that operate within the EU and hold customer data should have or begin to have a plan that complies with GDPR.

Exploit Discovered in WPA2

A new discovery by the Computer Emergency Readiness Team (US-CERT) shows a crack in Wireless Protected Access 2 security Protocol (WPA2). This crack makes wireless internet traffic open to eavesdroppers and attacks (**Fortune**). This exploit may provide a new way for an attacker to install ransomware, or to manipulate data for other types of attacks. The exploit can also be used to steal information such as credit card numbers, passwords, emails, photos and other personal and sensitive information of a firm and/or user. Researchers have named this exploit KRACK, which is short fort Key Reinstallation Attacks (**Krackattacks**).

The US-CERT has issued a warning of this exploit (**Ars Technica**) as well as contacting hardware vendors in advance of their public announcement allowing them to release security updates. The US-CERT has released a list of vendors and status of updates (**US-CERT**).

Firms are advised to check the US-Cert website for vendor updates and apply these update as well as segment wireless access points from the enterprise network.

FS-ISAC Outreach

PwC published key findings from the Global State of Information Security Survey 2018 (GSISS) in a report titled "Strengthening digital society against cyber shocks" (**PWC**). FS-ISAC CEO Bill Nelson provided commentary for the report about next steps global business leaders should take in response to cyber-attacks. Bill specifically mentions the importance of information sharing, the value of simulated cyber exercises, and the roles of the Financial Systemic Analysis & Resilience Center (FSARC) and Sheltered Harbor (**SH Site**) to enhance financial sector resilience. Bill also noted that Global Resilience Federation (**GRF**) can help other sectors and communities establish information sharing capabilities.

On November 2, 2017, FS-ISAC's Peter Falco spoke to attendees at the 2017 BITS Technology Conference. Peter's presentation was titled "Mitigating Cyber Risks Through Information Sharing" which provided an over of FS-ISAC, case studies and how firms could use information sharing to combat cyber risks.

On October 25, 2017, FS-ISAC's Peter Falco participated on a Cybersecurity panel at the EZE Software's EZE Advance 2017 Conference. (**EZE**) Peter and other panel members discussed the latest developments in cybersecurity and what can be done to safeguard a firm, including accessing resources via the FS-ISAC. The primary target audience was firms focused in the asset management and alternative investment space, but discussions were relevant to other financial firms as well.

Malware Used on Taiwanese Bank Heist

Two men have been arrested by Sri Lanka police in connection with Taiwanese bank heist (**BankInfoSecurity**). The would-be thieves used malware to generate fraudulent money transfers using SWIFT messages – enough to transfer $60 million USD out of the Taiwan based bank to banks in Cambodia, Sri Lanka and the United States. News agencies report that the bank had detected the suspicious transaction and was able to recover all but $500,000.

Firms should ensure that systems are protected and vulnerabilities that could allow unauthorized access to corporate networks such as the malware be addressed. Firms should also consider

applying policies and procedures that flag money transfers that reach a certain dollar amount and require a human intervention to release the flagged transfer.

New Variant of Petya Ransomware – Bad Rabbit

On Tuesday, October 24, a new ransomware made its debut. The new strain was dubbed "Bad Rabbit" and is a suspected variant of Petya. As ransomware, it infects a computer and restricts user access to the infected machine until a ransom is paid to unlock it.

Immediately, FS-ISAC's IAT published a Cyber Threat Portal alert with indicators of compromise to notify financial institution members, Tracking ID **934711**. In their announcement about Bad Rabbit, the US-CERT reiterated its discouragement of individuals and organizations paying the ransom, as paying does not ensure access will be restored.

At this point, Bad Rabbit is making its way around Europe and Russia; however, as experienced earlier this year with WannaCry and NotPetya, new strains of ransomware can spread like a worm. Therefore, it is a good time to ensure that protections are in place at community institutions to prevent the same type of infection.

Firms are advised to review the FS-ISAC Tracking ID 934711 for indicators of compromised (IOCs), disable SMB and RDP, and educate users of this new threat. Firms should also ensure backups are running and secure, in the event they are attacked by this ransomware.

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,

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**