Financial Institutions Looking at Substantial Cyber Attack Losses

According to a **recent survey** by the International Monetary Fund (IMF), hackers are infiltrating financial institutions at a much quicker rate, with the resulting losses totaling $100BLN. The approach utilized by the IMF varied from using actuarial science to operational risk measurement to ascertain an estimate of the total losses from cyberattacks. Depending on the severity of the attacks, losses could range from $270BLN - $350BLN.

Cybersecurity Still a Concern for SEC's CAT

The testing period for the Securities and Exchange Commission's (SEC) consolidated audit trail (CAT) has gone smoothly; however many **industry experts warn** that cybersecurity is a concern. Starting on 13 April 2020, broker-dealers were required to begin submitting data to the CAT's comprehensive database which includes trades they executed on behalf of clients, including institutional investors. Initial reporting to CAT has gone smoothly as many firms took advantage of an extended testing period.

Organizations such as the Securities Industry and Financial Markets Association (SIFMA) have raised concerns such as securing the data that is fed into the CAT system, particularly when retrieved in 'bulk download' by one of the 24 self-regulatory organizations (SRO). With people working from home during the pandemic, there is an additional security risk; this is amplified on as questions arise as to where that data is downloaded, does it remain on a corporate system or is it on the personal system of the employee working from home.

SEC Chairman Jay Clayton has asked SEC staff to prepare a recommendation on improving data security requirements in the national market system plan governing the CAT, including exploring alternatives to bulk downloading data by each SRO that would better secure CAT data.

Costs Related to Covid-19 Cybercrimes Jump

Data breaches, while continuing to make headlines, increased **273% in Q1 2020** versus Q1 2019. Cybercriminals took full advantage of the uncertainty that Covid-19 provided. Employers scrambled to set up their workforces to work from home, which also brought about new online habits for employees. The focus has now started to shift to cybercriminals focusing on stimulus payments, unemployment, Paycheck Protection Program (PPP), and benefits with no industry immune to breaches.

SEC to Develop Emerging Threats Exam Team

Late in July, the Securities and Exchange Commission created a new exam team called the **Event and Emerging Risks Examination Team (EERT)** to focus on emerging threats and current events. The EERT will be within the Office of Compliance Inspections and Examinations (OCIE) department, and will proactively engage with financial firms about emerging threats and current market events, as well as provide expertise and resources to the SEC's regional offices when critical matters arise. Working with OCIE exam staff in the regional offices, the EERT will focus on implementing OCIE exam priorities, including those identified in OCIE's annual examination priorities letter. The EERT will also work with OCIE staff to provide expertise and support in response to a significant market events that could have a systemic impact or that places investors assets at risks such as exchanges outages, liquidity events and cybersecurity concerns.

FS-ISAC Americas Fall 2020 Virtual Summit

Registration for the FS-ISAC virtual Americas Fall Summit, held on **14-15 October** is now open. Join our two-day virtual summit to stay at the forefront of these new technology trends and emerging paradigms so your firm can become a master of adaptation. Those with IntelX accounts can easily register via the IntelX, or **Register**.

Regulator Warns Member of Imposter Site

The Financial Industry Regulatory Authority has **alerted member firms** to avoid an impostor website with a similar domain name. The fake site's domain name has an extra "n," making it finnra.org, but it looks like FINRA's legitimate website and contains links to a fake registration site.

The **notice** sent by the regulator states the new imposter website, should not be confused with FINRA's real website (www.finra.org). The imposter site looks nearly identical to the actual FINRA site and contains registration links to a false site, where the possibility of bad actors could leverage false domain to send fake emails, and business email compromise (BEC) campaigns as well as sending malware.

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. Learn more at fsisac.com.