Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – March 2022

Cyberattacks Via Excel Add-Ins Have Excelled nearly 600%

In a **report published in Q4 of 2021**, HP Wolf Security reports that it detected a 588% increase over the quarter in attacks involving add-ins (.XLL files) for Microsoft Excel users. The report stated that users received emails with malicious .XLL attachments of links. One the recipient opens the attachment or clicked on the link, it would prompt the user to install and activate the add-in, where malicious code would be included int the xlAutoOpen function (default system location for XLL files) which will run immediately after the add-in is activated. This mode of attack is dangerous because it requires one click to install and activate the malicious code on a system. The report recommends three steps firms can follow to protect themselves from these types of attacks:

- Configure their email gateway to block inbound emails that have .XLL attachments. Some email gateways already do this because .XLL files are dynamic link libraries (DLLs), a type of file not often sent by email.
- Configure Excel to allow only add-ins from trusted publishers.
- Configure Excel to disable all proprietary add-ins.

SEC Proposes New Rules for Cyber Risk Management

The U.S. Securities and Exchange Commission (SEC) has proposed **new rules** related to registered investment advisors and business development companies on cybersecurity risk management. The **commission's proposed rules** would require advisors and funds to implement written cybersecurity policies and procedures to safeguard investors. The proposed rule changes would require advisors and funds to publicly disclose cybersecurity risks and significant cybersecurity incidents in the last two fiscal years in their brochures and registration statements.

Mitigating Ransomware in 2022

Ransomware is a daily reality for all organizations, with no regard of the business model or size. Internal commitments, starting with senior management down to a new hire, are vital in ensuring all employees remain vigilant. With ransomware being one of the top five trends in 2022, we are reminded of three ways to mitigate the risks. The first is continuous training of all employees will aide in the organization's commitment to remain on guard and become more cyber-aware. The second is while trying to stay atop of security measures, organizations need to remember that security controls largely remain within security basics. The third is chances of recovery of funds after a ransomware attack increase if there is more collaboration between organizations and regulatory agencies in developing realistic cybersecurity mandates.

2022 FINRA Examination Priorities Letter

On 9 February 2022, the Financial Industry Regulatory Authority (FINRA) published the **2022 Report on FINRA's Examination and Risk Monitoring Program** to inform member firms' compliance programs by providing annual insights from FINRA's Examinations and Risk Monitoring programs. The SRO's intent of the report is that it is an up-to-date, evolving resource library of information to firms. The report builds on the structure and content in last year's report, and adds new topics such as Disclosure of Order Routing Information. In the report, **FINRA mentioned cybersecurity** and the increase in the number of threats. They suggest mitigating cyber related risk, and firms are expected to have a process for continuously assessing cyber security risks. They also require firms to include comprehensive cybersecurity and phishing-specific courses in their annual training programs.