Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – November 2023

SEC's 2024 Examination Priorities

For the first time, the SEC's Division of Examinations has released their publication of their examination priorities with the start of the fiscal year. Their **2024 Examination Priorities report** details how their examinations in the upcoming year will concentrate on areas of emerging, core, and perennial risks. Throughout the report there is focus on compliance programs, business continuity plans, protecting client information, policies, and procedures for use of third-party providers, recordkeeping and retention, and continued mention of shared and branch office locations.

Their section on information security and operational resiliency focuses on:

- Third-party risk management. How you identify, address, and manage risks, and your visibility into the security and integrity of third-party products and services. Additional focus on concentration risk associated with third-party providers, and whether there has been unauthorized use of third-party providers.

- Policies and procedures, internal controls, governance practices, and responses to cyber-related incidents, with a specific mention of ransomware attacks.

- Adequate training of staff on your identity theft prevention program, and your policies and procedures for protecting customer records and information, including personally identifiable information.

There was a specific focus on Broker-Dealers and advisors, and their branch offices. Their examinations will look at practices to prevent account intrusions, safeguard customer records and information, promote cyber resiliency, and cybersecurity issues related to third parties. They will also assess your preparations to address the recently adopted rule to shorten the settlement cycle for transactions from two to one business day.

The report concludes with a section on anti-money laundering programs. Examinations will review whether broker-dealers and registered investment companies are tailoring their AML program to their business model and associated risks, conducting independent testing, have an adequate customer identification program, meeting their suspicious activity report (SAR) filing obligations, and ensuring compliance and monitoring of the Office of Foreign Assets Control sanctions.

Attackers Exploit Zero-Day on Network Devices

Threat actors are exploiting another **zero-day flaw in Cisco's** IOS XE operating system which runs a host of Cisco's networking device such as routers, switchers, wireless access points and other products. The zero-day flaw allows the malicious actor to implant a malicious backdoor. The vulnerability (**CVE-2023-20273**) allows remote access on the affected device to obtain full administrator privileges allowing a complete takeover of the system. The vulnerability affects the web user interface on the operating system through IP https server or IP http secure server commands. Cisco recommends disabling the HTTP Server feature which may act as a stop gap until a device can be upgraded.

2023 Financial Sector Threat Landscape Report

Trustwave, an Affiliate partner of FS-ISAC, has released their 2023 Financial Services Sector Threat Landscape report and it is now available ***here***. Built on data from Trustwave's 250 SpiderLabs researchers, over 100,000 hours of pen tests annually, and ongoing managed security and IR services, the report highlights the unique threats to financial institutions because of potential for monetary gain, concentration of sensitive customer data, complex and interconnected supply chains, and regulatory constraints. The report assesses the emerging impact of generative AI on security threats, analyzes attack flows specific to the financial services industry, and offers actionable intelligence and recommended mitigations for every step of the attack cycle.

CISA and NSA Share Top Ten Cybersecurity Misconfigurations

The red and blue teams at CISA and NSA recently released a **joint cybersecurity advisory** detailing the most common cybersecurity misconfigurations in large organizations and provided the TTPs that threat actors use to exploit them. They stated that these misconfigurations show a trend of systemic weakness even in mature organizations, and that software manufacturers need to embrace the secure-by-design principles. The top ten misconfigurations include: Default configurations of software and applications; Improper separation of user/administrator privilege; Insufficient internal network monitoring; Lack of network segmentation; Poor patch management; Bypass of system access controls; Weak or misconfigured multifactor authentication methods; Insufficient access control lists on network shares and services; Poor credential hygiene; and Unrestricted code execution. You can reference their advisory for mitigations of these misconfigurations.

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.