Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – September 2022

Suspicions Heightened for UK Banks

The National Crime Agency (NCA), headquartered in London, UK has seen a **surge in suspicious activity** by UK banks and other regulated institutions. The NCA gave an update on the activity last week. The updates show detail concerns around sanctions, breaches and money laundering and terrorist financing. The agency was originally formed to focus on organized crime but has recently been reorganized to outweigh the influence of the oligarchs. The NCA has setup a new "Kleptocracy" unit to focus on corrupt politicians and malicious actors and targeting those who have a proximity to the Russian President and his regime.

Importance of a Robust Response Plan

In an interview early this month, **Christophe Barel**, FS-ISAC's Managing Director for Asia-Pacific Region spoke about the importance of an incident response plan for a firm's **cyber resilience program**. Mr. Barel also stated how important it is for a firm to test their plans through exercises and simulations, and to 'plug the gaps and then test again'.

Minister O'Neil to significantly review Australia's cyber security strategy

Following the May 2022 Federal election, Clare O'Neil was appointed as both Minister for Cyber Security and Minister for Home Affairs on 24 June. The creation of a dedicated cyber portfolio is a first for the Australian government. In mid-August, Minister O'Neil was reportedly planning a significant review of Australia's cyber security strategy. A spokesperson for the Minister indicates that the revision will be '…grounded in sovereign capability, with a plan for the future workforce and growth of the cyber security sector, including Australian cyber SMEs. Importantly, the approach will be underpinned by engagement with industry stakeholders to develop solutions that are both innovative and practical. Minister O'Neil has not yet announced a delivery timeframe for the changes.

The Source of Most Attacks: Ransomware and BEC

According to a **recent report** published by Palo Alto Network's Unit 42 ransomware and false business emails accounted for more than 2/3 of all cyberattacks in the past 12 months. Attackers gained access to networks via three primary initial vectors; phishing, known software vulnerabilities and brute-force credential attacks. The report indicates that these three attacks totaled over 77% of all suspected root causes for intrusions. The report also states that exploits from unpatched vulnerabilities remain the leading attack vector. The continuous exploitation of known and unpatched vulnerabilities reinforces the needs for firms to ensure that their systems and software are up to date.

Patch Release for Dogwalk Zero-day

Late last month software manufacturer Microsoft released a **series of patches** including one to fix a zero-day vulnerability known as **Dogwalk**, which allows hackers to gain remote code execution in Windows. Dogwalk exploits the MSDT utility built into Windows designed to collect information to send to Microsoft. The utility makes it possible for the operating system to perform automated fixes that Microsoft labels as 'Troubleshooters'. Other fixes released include correcting a **Windows Network File System code execution vulnerability** which provides the attacker with elevated privileges to remote code execution.

Podcast: Why Regulators are Shining a Spotlight on Cyber Resilience

A series of **podcasts** published by PWC, cover the latest developments in cyber risk, resilience, and threat intelligence. Each episode is joined by special guests to give you practical insight on how to improve your cyber security and create a more resilient business. FS-ISAC's **Lucie Usher** was a guest on last week's latest episode which covered:

- What is driving cyber resilience up the regulatory agenda in sectors such as financial services, energy, and utilities?
- The key cyber risks for organizations in regulated sectors, including supply chain attacks, the growing use of operational technology in industrial operations and geopolitical unrest.
- How is the regulatory landscape evolving around cyber resilience - nationally and globally - and what does this mean for organizations?
- What organizations in regulated sectors can do to increase cyber resilience and ensure compliance, including greater information sharing, rigorous self-assessment and continuous exercising and testing.

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.