Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – August 2021

Cybersecurity Spending to Increase at Financial Services Firms

A recent **survey** with PWC UK and the CBI revealed that 70% of organizations are gearing up to **bolster their cybersecurity investments** in 2021, which is just about double the amount from 2020. Additionally, roughly 75% will work on improving their ability to detect and respond to cyber breaches while 67% of banks, insurers and investment managers will look to put more focus on their responses to new or emerging cyber threats. Financial services organizations are starting to understand investments in IT are needed more than ever to be proactive regarding the risks of internal and client breaches.

The Future of IT Security, All Thanks to the Pandemic

The **function of IT** in an organization has been to increase the productivity of users, the area that built and supported the functionality to increase productivity, all while ensuring that value was protected, resilient and completed according to best practices. Once Covid appeared and forced organizations to ensure remote work was done safely and securely, the function of IT drastically changed. Through all the endless hours of keeping business functioning seamlessly, IT now can partake in a "big reset", whereby enabling security and IT teams the chance to re-think their security systems.

US Accuses China of Cyber Espionage

The United States Department of Justice has **indicted four Chinese individuals** for alleged roles in cyber-attacks targeting intellectual property and trade secrets. The hackers who are affiliated with China's Ministry of State Security (MSS) have conducted malicious operations for the government and their gain. The attackers were part of various campaigns between 2011 and 2018, which helped steal technologies related to autonomous vehicles, high-speed railways, and aircraft. They also targeted data from genetic sequencing projects and research around diseases such as Ebola, MERS, and AIDS. The four individuals allegedly targeted organizations in the United States, the United Kingdom, Canada, Germany, Indonesia, Norway, and Saudi Arabia.

Takedown of 17 Domains Used for Business Email Compromise

Last week, Microsoft announced the takedown of 17 domains that a threat group operating out of West Africa used to **conduct business email compromise attacks**. These domains were designed to look like Microsoft sites and target the software manufacturer's O365 customers to conduct malicious activity such as business email compromise using stolen credentials to access O365 customer email accounts and then imitate customer employees all in an effort to deceive them into sending or approving fraudulent financial payments.