Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – November 2022

US Treasury Considering National Cyber Insurance Program to Require Basic Cyber Security Measures

The US Treasury Department's Federal Insurance Office (FIO) wants to know whether a **national cyber insurance program** should require policy holders to implement basic cybersecurity measures in order to avoid creating a moral hazard. Together with the Cybersecurity and Infrastructure Security Agency (CISA) they are soliciting feedback for a report to Congress. Both agencies are interested in finding an effective cybersecurity measures to help establish a federal cyber insurance program. The efforts are based off of recommendations from the National Defense Authorization Act of 2021.

UK National Grid Chief Warns of Winter Blackouts

Due to the possibility of gas shortages, **blackouts may be imposed** between 4pm and 7pm during the colder weekdays in January and February 2023. John Pettigrew, the National Grid Chief, shared these comments during the Financial Times' Energy Transition Summit on 17 October. This follows an **agreement by EU countries** to voluntarily cut gross electricity consumption by 10% and a mandatory reduction of 5% during peak hours. Supply chain impacts due to the Russian war in Ukraine and sanctions on Russia gas have caused gas shortages across Europe. Britain relies on electricity and gas imports from European countries that import Russian gas.

Supply Chain Resiliency: Beyond Third-Party Risk Programs

Third-party risk management and supply chain resiliency are sometimes used interchangeably; however, both require **different approaches**. Business resiliency and IT resiliency have traditionally been managed separately — now, with cyber-attacks cited as the main reason suppliers go dark, it is not enough to rely on third-party risk assessments alone. IT and cyber teams, as well as the business itself, will need to speak candidly about the risk tolerance and comfort level in shutting off a key supplier when an incident occurs.

Australia Looking for Cyber Insurers to Provide Best Practices for Cyber Risk

A vibrant cyber insurance market will do more than provide financial recompense for risks that break through the first line of defense. It can also strengthen that first line, by offering clear signals and incentives to business – in the form of eligibility, pricing and sharing of insights – on best-practice standards. A **green paper** written by actuaries in Australia show how Australians are more dependent than ever on technology and cyber risk costing the county around $33 billion last year.

FS-ISAC Developments in Europe

FS-ISAC recently established a Board of Directors for European membership and has just announced the representatives, who are Daniel Barriuoso (Santander), Carsten Fischer (Deutsche Bank), Karel de Kneef (SWIFT), Beate Zwijnenberg (ING), and Jayaraj Puthanveedu (BNP Paribas). Additionally, FS-ISAC will be providing intelligence, collective defense, and cyber-resilience operations and capabilities for the **Swiss Financial Cyber Resilience Centre (FS-CSC)**.

White House Issues Statement on Cyber Efforts

On 11 October 2022, the White House issued a **FACT SHEET** on the Biden administration's efforts on strengthening America's Cybersecurity. The sheet mentions the administration's focus on improving the nation's cyber defenses, building a comprehensive approach to locking their digital doors, and taking aggressive actions to strengthen and safeguard the nation's cybersecurity, including the following:

- Improving the cybersecurity of our critical infrastructure.
- Strengthening the federal government's cybersecurity requirements and raising the bar through the purchasing power of government.
- Countering ransomware attacks to protect Americans online.
- Working with allies and partners to deliver a more secure cyberspace.
- Building the nation's cyber workforce and strengthening cyber education.

Personal Information Exposed in Microsoft Data Breach

It has been **reported by SOCRadar** that sensitive information from more than 65,000 prospective customers were exposed due to a misconfiguration on a server accessible over the internet. The information included names, email address, email content, company name, and phone numbers, as well as files linked to business between affected customers and Microsoft or an authorized Microsoft partner.

Microsoft has indicated that no customer accounts or systems were compromised, and the affected parties have been notified. They have also disputed the number of potential customers that were impacted, explaining that duplicate information was found in the exposed data.

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.