Monetary Authority of Singapore Revises Guidelines to Combat Heightened Cyber Risks

On 18 January, the Monetary Authority of Singapore (MAS) **published** revised Technology Risk Management Guidelines to address emerging technologies and shifts in the cyber threat landscape for financial institutions (FIs). The revised guidelines focus on the cyber risks associated with the growing use of cloud technologies, application programming interfaces (APIs), and rapid software development. The MAS set out two enhanced risk management strategies for FIs: to establish a robust process for the timely analysis and sharing of cyber threat intelligence within the financial ecosystem, and to conduct or participate in cyber exercises to stress test defenses by simulating cyber-attacks. Additionally, there is guidance on the roles and responsibilities of the board of directors and senior management. According to the MAS, "the board and senior management should ensure that a chief information and a chief information security officer, with the requisite experience and expertise, are appointed and accountable for managing technology and cyber risks."

NSA's 2020 Cybersecurity Year in Review

The United States National Security Agency (NSA) published their **2020 Cybersecurity Year in Review**. Information included a focus on Covid-19 vaccine development encompassing cyber threat intelligence and safeguarding intellectual property.

Egregor Operators Arrested in Ukraine

Individuals who are suspected to being affiliated with the Egregor ransomware have reportedly been **arrested in Ukraine**. The arrests were announced on 12 February 2021, by French radio station **France Inter**. The French police had launched an investigation this past fall because of attacks against domestic organizations and worked closely with the police in the Ukraine as well. The radio station reported that the arrested individuals had allegedly provided hacking, logistical and financial support for Egregor. Since the arrests, Ergegor's infrastructure appears to have **gone dark**.

Rampant Password Reuse Continues to Jeopardize Organizations

While organizations strive to educate their employees on the importance of strong passwords, **data shows** that roughly 76 percent of employees at the world's largest organizations are still reusing passwords across personal and professional accounts. Many employees do not understand how stolen passwords may impact an organization; education on this matter is paramount on the premise that reused login credentials provide criminals with easy access to corporate systems and networks. Organizations should constantly update their database of breach data to ensure their IT teams are able to keep corporate accounts safe.