Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – October 2021

October is Cybersecurity Awareness Month

Since 2003, October has been a month recognized as Cybersecurity Awareness Month – a month filled with cyber content designed to raise cyber awareness amongst US citizens, as well as small, medium, and large organizations. FS-ISAC recognizes the importance security and technical practitioners play in supporting and protecting your institution's financial and information assets. FS-ISAC has put together a program of events and activities that will kick-off each Tuesday in October that we believe will be an opportunity to supplement your knowledge and obtain up to 12 CPE by participating in all the following:

- **October 5** - Understanding & Leveraging the ISAC & sectors cyber resources
- **October 12/14** - Capture the Flag (CTF) event "Break the Bank" from a Red Team perspective
- **October 19** - Anatomy of a Range and value in building muscle memory
- **October 26**- Anatomy of an Attack and value of ISAC framework in action

To register, connect to the FS-ISAC website and select the '**Register Now**' button

On Prem Databases Could Be Vulnerable

After a five-year study, researchers found that nearly 50% of on-premise databases globally are vulnerable to attack, showing that they have at least **one unpatched vulnerability**. The study consisted of 27,000 scanned databases globally that showed 56% of those CVEs are rated 'high' or 'critical' in severity, which indicates that routine patching is being ignored by many firms. The **report published last week** also found that the average database contains 26 unpatched CVEs, some of which have left databases open to an attack for three or more years.

LockBit 2.0 – A Surge in Recruitment Leads to Increased Ransomware Attacks

LockBit, a Ransomware-as-a-Service (RaaS) gang known for writing and distributing its malware through affiliates, has reinvigorated its presence in building out a new affiliate program. Evidence to back this shows LockBit's activity is roughly six times more active than other groups. LockBit grew by utilizing their infrastructure to advertise future affiliates, who take on additional responsibilities as well as receive payment directly from victims. Roughly 20.8% of financial firms have been affected by ransomware

Securing Wireless Devices in Public: Guidance Issued by NSA

The National Security Agency (NSA) recently released **"Securing Wireless Devices in Wireless Settings"** , their Cybersecurity Information Sheet, to assist the National Security System (NSS), Department of Defense (DoD), and Defense Industrial Base (DIS) with the focus on remote workers wireless devices to **identify potential threats and minimize risks**. Bluetooth, public Wi-Fi, and Near-Field Communications (NFC), a short-range technology, are the main culprits that allow cyber actors to infiltrate wireless devices. NSA lists techniques used to target each technology while providing recommendations on how to safely use devices while in public spaces. This report allows users to understand the risks of open Wi-Fi spaces while allowing them to educate themselves to securely work remotely.