Hacking the U.S. National Security Through Financial Cybercrimes

Cyber threat actors, in the form of nation states, terrorists, cybercriminals, and hacktivists aim to disrupt the U.S. bedrock (OFR, 2017) — the financial industry (Borghard, 2018). Degrading or disrupting the U.S. financial sector can lead to financial instability (Borghard, 2018); thus, making the U.S. militarily and economically vulnerable to domestic and international threats. Challenging the U.S. national security threatens the sovereignty and democracy of our nation. One internet service provider observes more than 80 billion malicious scans per day by cybercriminals searching for vulnerabilities in interconnected systems and devices (Lewis, 2018). Researchers indicate that approximately 300,000 malware variants are released every day targeting governments, businesses, organizations, and people around the world (Lewis, 2018). Cybercriminals have victimized Sixty-four percent of Americans and more than 2 billion people online had their personable identifiable information compromised (Lewis, 2018). An FBI official postulates that cybercriminals target the U.S. due to the amount of information stored on our systems, networks, clouds, and data centers (Palmore, 2019).

The financial industry experienced innumerable data breaches in 2016. As a result, information security investments in the financial industry increased by 67% (Carter, 2016). The U.S. financial industry is forecasting information security investments to total $68 billion from 2016 to 2020. Cyber threat actors unified efforts to conduct attacks on U.S. financial institutions (Carter, 2017) by offering cybercrime-as-a-service to target the financial industry (Lewis, 2017). Cybercriminals are focusing more on financial sector given the value and universal utility of
financial services organizations (Carter, 2017). The monetization of stolen records on the dark web motivates cybercriminal to target the financial institutions (Lewis, 2018).

The U.S. financial sector is building stronger defenses; consequently, forcing cybercriminals to use social engineering tactics and malware to target employees in the financial sector. The financial sector social engineering attacks increased by 58%, but more than 90% of financial services organizations employees fall prey to watering holes and social engineering schemes, which is the leading attack vector for targeting the financial sector (Carter, 2017).

As U.S. financial institutions strengthened cybersecurity defenses cybercriminals conversely increase the sophistication of attacks (Carter, 2017). The financial sector remains vulnerable to offensive cyberspace attacks from cyber threat actors; thus, attacking the financial sector is derision on the U.S. national security (Borghard, 2017). Threats against the U.S. financial industry are constant stressful to our national security.

To counter the threats to national security, the U.S. needs to improve private and public collaboration and information sharing, leverage advanced analytics, support international laws to prosecute cybercriminals, leverage artificial intelligence, conduct tabletop exercises, cyber resiliency, reduce attack surfaces at all cost, and train and exercise employees on cybersecurity awareness and social engineering tactics. Prioritizing risks, identifying cybersecurity standards for third-party partners, and enforcing strong authentication and identity management.

**Key Terms:** Critical Infrastructure, Cybersecurity, Cybercrimes, and National Security

**Session Description and Objectives:**
This presentation is a critical analysis of how cyber threat actors are targeting the bedrock of the U.S. national security through relentless attacks on our financial industry. Presentation attendees will be informed on the following:
- The disruptive nature of cybercrimes on the financial industry
- The cost of financial crimes can disrupt the financial sector and create instability
- How repeated and sustained cybercrimes will impact the U.S. critical infrastructure, economy, and national security
- The motivation for attacking the U.S. financial industry

References


