International Journal of Hyperconnectivity and the Internet of Things
Volume 3 • Issue 1 • January-June 2019

Disrupting the U.S. National Security Through Financial Cybercrimes

Calvin Nobles, Cybersecurity Policy Felow, New America Think Tank, Washington, DC, USA

ABSTRACT

The U.S. financial sector is the bedrock of the economic health and strategic advancement. As a critical infrastructure, the financial sector continuously faces cyber-attacks and other nefarious activity. The financial sector is undergoing a technological explosion and forcing banks and financial institutions to implement cutting edge technologies. Even though technological breakthroughs are yielding competitive advantages; consequently, the same technologies are more prone to cyber-attacks stemming from technologically-induced vulnerabilities. The integrative and hyperconnected state of the financial industry and the domestic and global financial ecosystems are highly centralized and vulnerable to sophisticated cybersecurity threats, human factors, social engineering, credit card fraud, and online banking schemes. Any attempts to degrade, disrupt, or deny vital services and transactions in the financial industry could be conceived as an infringement and blockade of the U.S. global powers.

KEYWORDS

Cybercrime, Cybersecurity, Financial Technology, Human Factors, Information Technology, National Security

INTRODUCTION

The growing network complexity and proliferation of devices could lead to widespread vulnerabilities in civilian infrastructures and U.S. government systems..... (Director of National Intelligence (Borghard, 2018))

The Director of National Intelligence and agency directors from the National Security Agency, Central Intelligence Agency, and the Federal Bureau of Investigations recently testified to Congress that malicious cyber activity conducted by adversaries is concerning to the U.S. national security and the top security priority for the

DOI: 10.4018/IJHIoT.2019010101

Intelligence Community (Borgard, 2018). Malicious threat actors, in the form of nation states, terrorists, cybercriminals, and hacktivists continue to interrupt the U.S. financial sector, which is the nation's bedrock (OFR, 2017; Borghard, 2018). The U.S. banking system amassed $17.4T in assets and $164.8B in 2017, which supported the most diversified banking and financial industry ("The Financial Services," n.d.). Degrading or disrupting the U.S. financial sector will lead to financial instability (Borghard, 2018) not only in America but across the globe because the domestic and international financial ecosystem is interconnected and susceptible to cybercrimes. Defying the U.S. national security threatens the sovereignty and democracy of our nation. Sixty-four percent of Americans and more than 2 billion online users have had their sensitive information compromised (Lewis, 2018). An FBI official postulated that cybercriminals target the U.S. due to the amount of information stored on our systems, networks, devices, and in the data centers (Palmore, 2019).

The growing dependence on information communication technology requires financial institutions to leverage information systems and platforms with known cyber vulnerabilities in which cyber-attacks originate from poor system designs and substandard quality control (Clark, Berson, & Lin, 2014). Given that private organization's design information technologies, these entities are just as much involved in securing the U.S. financial sector as the government (Clark, Berson, & Lin, 2014). Loughery (2013) asserted that Congress has failed to conjure any legislation leading to efforts to curtail cybercriminals targeting of the U.S. financial sector and other critical infrastructures.

The U.S. financial industry is the nation's underbelly to building and maintaining a healthy and thriving economy. Carter (2017) asserted that financial services is the fastest-ascending market in cybersecurity as indicated by a 67% increase from 2013 to 2016. Cybersecurity spending in the U.S. is forecasted to hit $68B between 2016 to 2020 (Carter, 2017). Financial services firms are paying $18M per cyber-attack compared to $12M paid by other industries; consequently, financial firms are attacked 300 more times than other domains (Mirchandani, 2018). Banks are predominantly targeted with denial of service (DoS) attacks, spear phishing, and malware as 90% of financial institutions reported observing ransomware as another viable attack vector (Mirchandani, 2018). While hacktivists attempted the most attacks on financial entities at 80% with a 1% success rate, were less effective than cybercriminals who had a 20% success rate; however, nation-sponsored cyber-attacks had the highest success rate at 98% (Mirchandani, 2018).

To counter the threats to our 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, promote 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 are other tactical-level strategies to prevent cyber-attacks. The purpose of this critical analysis is to explore the