Cybersecurity for FMIs

FINANCIAL INCLUSION GLOBAL INITIATIVE

APRIL 2019

Welcome to the first edition of the FIGI Cybersecurity for Financial Market Infrastructures Newsletter

The Financial Inclusion Global Initiative (FIGI) is a three-year program implemented in partnership by the World Bank Group (WBG), the Committee on Payments and Market Infrastructure (CPMI), and the International Telecommunications Union (ITU) funded by the **Bill & Melinda Gates Foundation** (BMGF) to support and accelerate the implementation of country-led reform actions to meet national financial inclusion targets, and ultimately the global **'Universal Financial Access 2020'** goal. FIGI funds national implementations in three countries—China, Egypt and Mexico; supports working groups to tackle three sets of outstanding challenges for reaching universal financial access: (1) electronic payment acceptance, (2) digital ID for financial services, and (3) security; and hosts three annual symposia to gather national authorities, the private sector, and the engaged public on relevant topics and to share emerging insights from the working groups and country programs.

The FIGI Cybersecurity for Financial Market Infrastructure Workstream, led by the WBG as part of the Security, Infrastructure and Trust (SIT) Working Group, aims to explore compliance and best practices for cybersecurity specifically on financial infrastructures. The Workstream aims to develop a toolkit of resources and materials for awareness and education for policymakers and related and plans to further develop methodologies, standards and good practices on cybersecurity for financial market infrastructures over the course of the FIGI project.

This newsletter aims to update you on the latest developments in cybersecurity, cyber events and security breaches. We hope you find this newsletter useful and welcome your feedback.

Sincerely,

FIGI Secretariat

Managed by

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Inside this Edition

A Regulator's Perspective

- **Reserve Bank of Australia:** On July 8th, 2018, Ms. Michele Bullock, the Assistant Governor (Financial System) of the Reserve Bank of Australia, in her speech at the 5th Bund Summit on FinTech, Shanghai, spoke about the advent of Big Data analytics to generate insights into consumer payment behavior, and the increased interest in accessing data derived from these insights. With more data being stored and shared, she elaborates on the imminent need for regulators to focus on data security, and cybersecurity more generally. (**Read the full story here**)
- **South African Reserve Bank:** In his welcome address at the Innovation

continued next page

Recent Cybersecurity Events and Breaches

- **ATM Bank Servers Tricked into Spitting Out Millions of Dollars:** A joint technical alert from DHS, the FBI, and the Treasury issued a warning about a new ATM scheme being used by the North Korean APT hacking group known as the Hidden Cobra. (**Read full story here**)

- **International Banks compromised by North Korean Hacking Groups:** Researchers from the FireEye Cyber Defense Summit shared details on cyber theft attempts by North Korean hacker team, APT 38, to steal over 1.1 billion USD from financial institutions worldwide. (**Read full story here**)

- **Newegg Credit Card Hack:** Magecart, the hacking group behind the Ticketmaster and British Airways data breaches, recently victimized computer hardware and consumer electronics retailer—Newegg. Magecart managed to infiltrate the website and steal credit card details of customers by using a digital card skimmer. The skimmer inserted a few lines of malicious Javascript code into the checkout page that captured payment information of customers. (**Read full story here**)

- **Phishing scams target payroll information:** A set of social engineering (phishing) scams across the country were recently reported by the FBI's Internet Crime Complaint Center. They targeted employees' payroll credentials—by sending phishing emails designed to capture login information and access payroll information. Once accessed, the attacker would change bank account data and settings to ensure the victim did not receive suspicious alerts. (**Read full story here**)

- **GovPayNet leaks 14 million customer records:** Government Payment Service Inc. (GovPayNet), a company used by thousands of US state and local government agencies to accept online payments for traffic citations, licensing fees, bail payments, and court-ordered fines has leaked more than 14 million customer records dating back to at least six years. (**Read full story here**)

- **Google–Mastercard contract:** A report by Bloomberg revealed a multi-million-dollar deal between the tech giant and Mastercard that allows it to track what users buy offline. Neither Google nor Mastercard has publicly announced the business partnership to track retail spending. The deal is said to be a four-year negotiation, where all Mastercard transaction data in the U.S. will be encrypted and transmitted to Google. (**Read full story here**)

Cryptocurrency Corner

- **Cryptomining malware families to be on the lookout for:** Crypto-jacking activities that bleed off victims' computing power to mine for cryptocurrency have skyrocketed in recent times. While crypto-mining malware may not be calibrated specifically to steal data, campaigns carried out by these malicious tools damage computing equipment and siphon off vast amounts of electricity apart from carrying out other kinds of lateral damages. Listed below are some of the most prevalent crypto-mining malware families active today

1. CoinHive
2. XMRig
3. CroniX
4. ZombieBoy
5. PowerGhost
6. RedisWannaMine
7. Underminer
8. MassMiner

(**Read full story here**)

- **Bitcoin Core Software patches DDoS vulnerability:** The Bitcoin Core development team released an important update to patch a major DDoS vulnerability in its underlying software that could have been fatal to the Bitcoin Network, which is usually known as the most hack-proof and secure blockchain. (**Read full story here**)

- **Leaked NSA tip exploited to generate cryptocurrencies:** A software flaw leaked from the US Government has been exploited to generate Monero, Bitcoins and other cryptocurrencies. Cyber Threat Alliance released a report in September 2018, stating that detected cases of illicit cryptocurrency mining—the digital equivalent of minting money—have surged 459 percent in 2018 compared to the previous year. (**Read full story here**)

- **Extradition of Alexander Vinnik a.k.a. Mr. Bitcoin:** Alexander Vinnik, the alleged owner of the now-defunct Bitcoin currency, BTC-e, is being extradited to his homeland Russia, after the Supreme Civil and Criminal Court of Greece overruled a previous decision to send him to France or the United States. Vinnik, has been accused of operating a BTC-e cryptocurrency exchange, which was shut down after his arrest in July 2017 at the request of the US government. He was convicted of fraud for laundering Bitcoins (BTC) worth over 4 billion USD for criminals involved in hacking attacks, tax fraud, and drug trafficking. (**Read full story here**)

A Regulator's Perspective,
continued from page 1

and Cybersecurity Conference, which took place on August 28th, 2018, Francois Grosepe, Deputy Governor of the South African Reserve Bank, elaborated on how the government should focus on seeking more strategic approaches to develop dynamic, resilient infrastructure, and how the private sector should provide financing solutions and promote partnerships with the government in this regard. (**Read full story here**)

Technology Developments in Payments Security

- **WebAuthn, FIDO2 Infuse Browsers, Platforms with Strong Authentication:** A new set of standards under the banner FIDO2 offers protection against hacking, credential theft, and phishing scams in hopes to reign in an era that ends the use of passwords alone as a security construct. Two modern authentication innovations born from collaboration between the World Wide Web Consortium (W3C) and the FIDO Alliance offer cross-platform standards that enable strong authentication based on public key cryptography. (**Read full story here**)

- **Stellar–TransferTo partnership:** TransferTo has partnered with Steller.org to enhance the way money is transferred across borders. Under this collaboration, financial institutions and partners of both companies hope to benefit from the combined network coverage and the ability to leverage new technologies to send and receive money more efficiently to over 70 countries. (**Read full story here**)

- **Biometric Sensors on Payment Cards:** The Smart Payment Association believes the introduction of biometric sensors on payment cards represents a huge stride for the finance industry in eliminating fraud for issuers and cardholders, and providing additional security and identity verification to support remote or cross-border transactions. (**Read full story here**)

Opinions, Research and Publications

- **Cost of Cyber Crime Report:** According to the 2017 'Cost of Cyber Crime Study', jointly developed by Accenture and the Ponemon Institute, a better understanding of the cost of cybercrime may help executives bridge the gap between their own defenses and the escalating creativity—and numbers—of threat actors. The study explores the effectiveness of investment decisions by analyzing nine security technologies across two dimensions: the percentage spending level between them and their value in terms of cost-savings to the business. Findings suggest that that many organizations may be spending too much on the wrong technologies. (**Read full story here**)

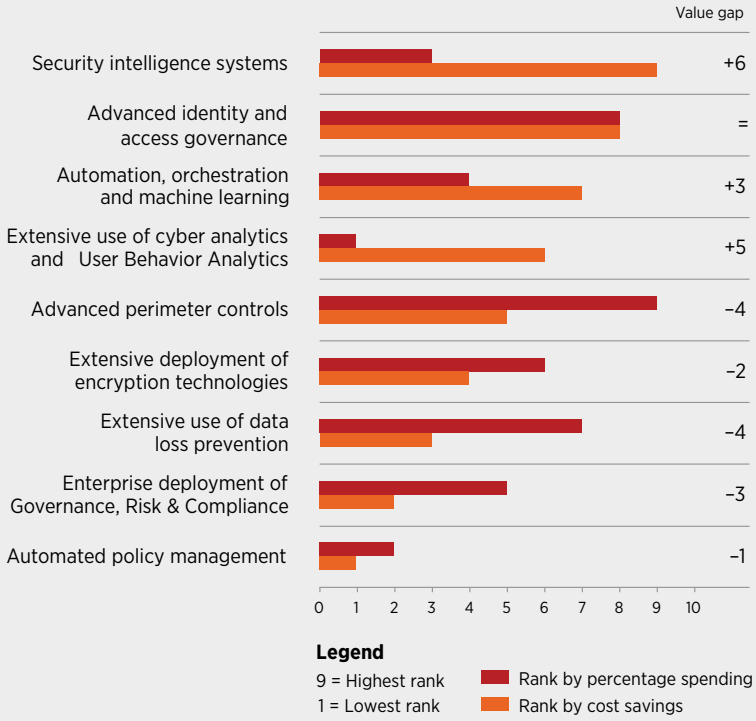
- **Cyber Analysis Experts discuss areas of focus:** A year since the infamous Equifax breach in 2017, cyber analysis experts highlight areas that organizations need to continue to focus on:

  1. Patching and configuration management
  2. Deploying encryption and tokenization
  3. Monitoring the company's data by making frequent risk assessments
  4. Finding out who has access to which data—and for what reasons
  5. Developing a public relations program

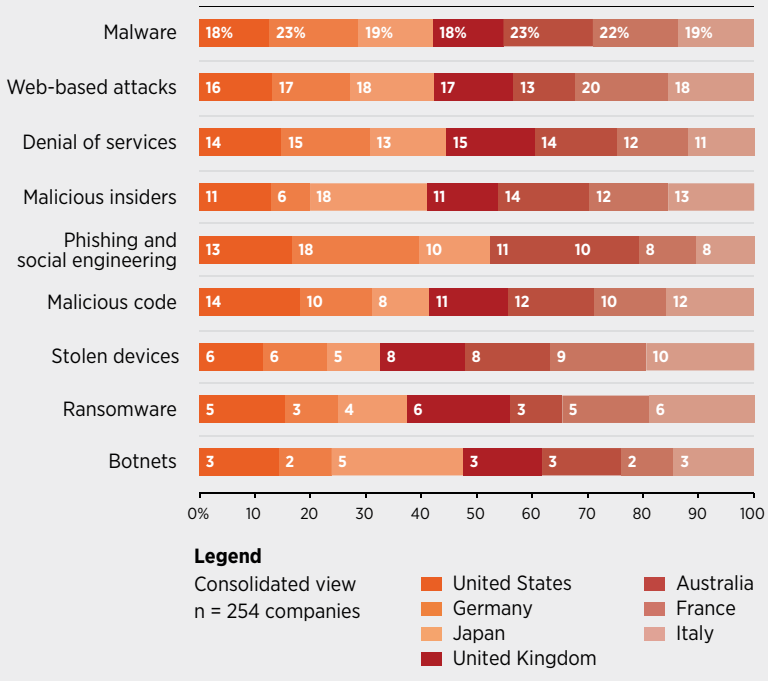
  (**Read full story here**)

THE POSITIVE OR NEGATIVE VALUE CAPS ASSOCIATED WITH SECURITY INVESTMENTS

Rank orderings by spending levels and cost savings



Percentage annualized cybercrime cost by attack type and country



FIGI Cybersecurity for FMIs Information: For any questions, comments or to unsubscribe from this newsletter please contact the FIGI Secretariat **(figisecretariat@worldbank.org)** and Renuka Pai (**rpai@worldbank.org).**