Cybersecurity for FMIs

FINANCIAL INCLUSION GLOBAL INITIATIVE

NOVEMBER 2019

Welcome to the Second Edition of the FIGI Cybersecurity for Financial Market Infrastructures Newsletter

This is the second 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** 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, infrastructure and trust; 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 industry news, including developments in cybersecurity, cyber events and security breaches. We hope you find this newsletter useful and welcome your feedback.

Sincerely,
FIGI Secretariat

For any questions, comments or to unsubscribe from this newsletter please contact the FIGI Secretariat (**figisecretariat@worldbank.org**).

Managed by

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Inside this Edition

Upcoming Events	2
Recent Cybersecurity Events and Breaches	3
Cryptocurrency Corner	3
Technology Developments in Payments Security	3
Opinions, Research and Publications	4

A Regulator's Perspective

- **Bank for International Settlements (BIS):** At the Finance and Global Economics Forum of the Americas in November 2018, the General Manager of the BIS, Augstin Carstens, spoke about the the advent of new technologies in the banking sector, particularly on the use of DLT, artificial intelligence and quantum computing. He also elaborated on the challenges that arise from these new technologies and placed the focus on Central Banks to monitor and manage the risks arising from the latest technologies. In particular, he brought up issues around reliability and security, interoperability between new and existing systems, the legal underpinnings of the processes associated with the technology, and data integrity and privacy. (**Read the full story here**)

continued on page 4

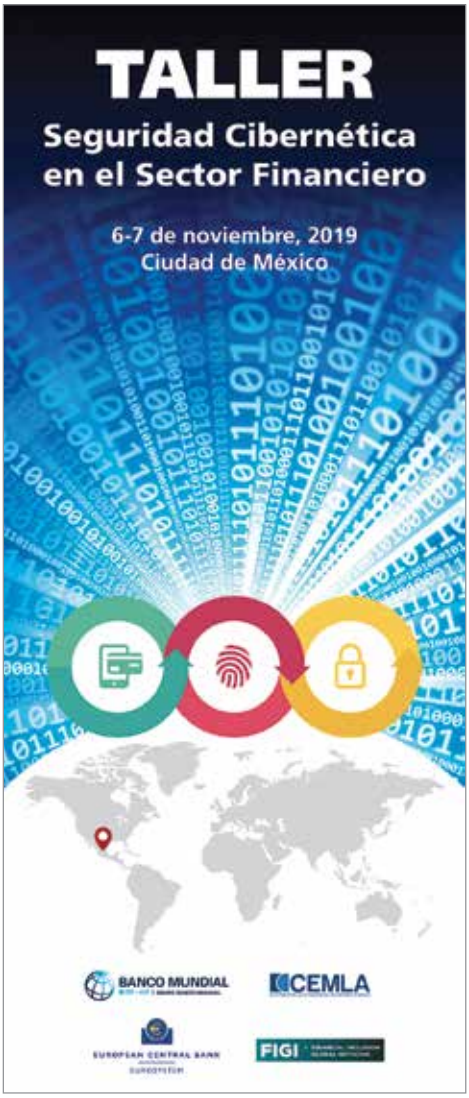
Upcoming Events

- **The Financial Sector Cyber Resilience Workshop** is taking place in Mexico City from November 6-7, 2019. The objective of this workshop is to bring together financial sector regulators, banks associations and fintech associations and learn and discuss together on how to use existing standards and foster information sharing arrangements between them that would enhance cyber-resilience in the financial sector.

  While technology brings new opportunities to the financial sector from efficiency gains to providing increased access and usage to financial services for individuals and firms it is also true that explosion of digital financial services has exponentially expanded the attack surface that criminals can exploit.

  Given the impact of these attacks to the Financial Sector, several measures have been taken to develop a framework that supports and enhances cyber resilience. The Financial Sector Cyber Resilience Workshop will explore these various approaches taken to enhance cyber resilience and share learnings as well as best practices.

  To learn more about the workshop and get access to related content, **please click here.**



- **The FIGI Security Clinic** will take place from December 4–5, 2019 at the International Telecommunications Union in Geneva to present the findings of the SIT Working Group. Topics to be discussed on the first day include: the mitigation of SS7 vulnerabilities for digital financial services (DFS), implementation of consumer authentication technologies to enhance security, security assurance framework for DFS providers and telecom operators for better risk management, and the mitigation of vulnerabilities of DFS applications based on USSD and STK. The second day of the event comprises of a series of DFS Security clinics, with topics such as the implementation of decentralized ID for DFS, tracking Ponzi schemes, and Fast Identity Online (FIDO) authentication for DFS. The target audience for these clinics includes practitioners that are actively involved in technical security implementation in the area of DFS.

  Registration is still open for this event! **Please sign up here if you are interested.**

Recent Cybersecurity Events and Breaches

- **Cloud Platform Used to Target Financial Firms:** Google's Cloud Platform was recently hacked to deliver malware via PDF decoys. The threat was detected across 42 organizations that are mostly in the financial sector, but also within governments worldwide. (**Read full story here**)

- **Bank Accounts in Ukraine accessed by Hackers:** Hackers accessed customer accounts though hacking into vulnerable computers on the Internet and infected them with Trojan malware to take full remote control of systems. The group then enabled key-logging on the infected computers to capture banking and digital wallet credentials of victims. (**Read the full story here**)

- **E-commerce websites targeted by cybercriminals:** Security researchers from RiskIQ and Trend Micro have identified cybercriminals that recently compromised nearly 277 e-commerce websites by inserting malicious JavaScript code into checkout pages that silently capture customer payment information and transfer it to the attacker's remote server. (**Read full story here**)

- **Payroll management services disrupted by ransomware:** A cloud-based payroll software company called Apex HCM was targeted by ransomware that encrypts computer files and demands payment for a digital key needed to unscramble the data. In this case, the company hired cybersecurity consulting firms to assist, however there was consensus that the best way to restore service to customers was to pay the ransom for the decryption key. (**Read full story here**)

- **Credit monitoring company found to have loophole in credit freeze process:** Consumers in the U.S. can freeze their credit files with Equifax and two other major bureaus (Trans Union and Experian). A freeze typically makes it much harder for identity thieves to open new lines of credit. However, with Equifax, this was compromised when it was found that if one does not already have an account at the credit bureau's portal, it may be simple for identity thieves to lift an existing credit freeze at Equifax and bypass the PIN with a name, Social Security number and birthday. Customers were advised to monitor their credit and create an account at the credit bureau's portal. (**Read full story here**)

Cryptocurrency Corner

- **Crypto mining service gets discontinued:** A cryptocurrency mining service, Coinhive, was discontinued in March 2018 after it was found that the company's computer code could be deployed on hacked websites to steal the computer processing power of its visitors' devices. The company also cited a drop in the value of most major cryptocurrencies as a key part of their decision to close down services. (**Read full story here**)

- **Three-layered security required for secure transactions with Cryptocurrency:** There are three main layers involved with cryptocurrency security: Coins or tokens are the first layer, exchanges between parties are the second layer, and wallets constitute the third. However, a possible compromise in the first layer will compromise the entire system, irrespective of how secure the following layers are. (**Read full story here**)

Technology Developments in Payments Security

- **DLT Security brought to voice banking:** Credit union-owned blockchain outfit CULedger has teamed up with two other companies: Best Innovation Group (BIG) and ConnectFSS, to bring distributed ledger technology security to voice banking. This will allow clients to let their members create, store and manage their identity information, which can then be referenced by any service at the credit union that needs to authenticate them. Access to that data would be controlled by the member. (**Read full story here**)

Opinions, Research and Publications

- **Network security in the cloud report:** According to a recently published report entitled "The Future of Network Security Is in the Cloud," there are benefits for digital business transformation with cloud-based, software-defined secure access, however there are also avenues for cybersecurity risk with such innovation. The report explains why businesses need to reassess their network/security architecture, how secure access service edge can enable integrated network security services, and best practices to secure digital business transformation. (**Read full report here**)

- **The rise of sophisticated phishing scams:** According to experts, phishing is now a multibillion-dollar criminal enterprise that targets consumers and businesses in increasingly sophisticated ways. Phishing attacks designed to steal funds and tax data rose 60 percent in 2018, partly because fraudsters are getting better at impersonating brands that consumers trust, such as Microsoft, Amazon and Netflix, in order to dupe email recipients into handing over login credentials that can be used to launch account takeover attacks. (**Read full story here**)

A Regulator's Perspective,
continued from page 1

- **Financial Stability Institute at Bank for International Settlements (BIS):** In his welcome address at the Financial Stability Institute's 20th anniversary conference, which took place in March 2019, the Chairman of the Financial Stability Institute of BIS, Fernando Restoy, discussed developments in financial regulation, focusing on the challenges faced by authorities in the implementation of reforms, and dealing with emerging risks to financial stability and other policy objectives. Among the main initiatives mentioned as a part of the BIS 2025 strategy were efforts to better implement global financial standards for the adoption of sound policies in the new institutional, regulatory and technological environment. (**Read the full story here**)

- **Financial Sector's Cybersecurity: A Regulatory Digest:** World Bank's Financial Sector Advisory Center (FinSAC) published the third edition of its Digest of Cybersecurity Regulations in the Financial Sector in May 2019. The latest edition includes five new jurisdictions that were not previously captured—Estonia, Ghana, Kenya, Nigeria, and Rwanda; apart from adding 40 cybersecurity related regulatory and supervisory initiatives to the existing 116. The Digest is a live, periodically updated compilation of recent laws, regulations, guidelines, and other significant documents on cybersecurity for the financial sector. (**Read the full story here**)

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).**