Cybersecurity for FMIs

FINANCIAL INCLUSION GLOBAL INITIATIVE

AUGUST 2020

Third 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

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

A **third** of the world's population is currently under lockdown, and an estimated **300 million** people globally are working from home, including up to **90 percent** of employees in the banking and insurance sectors. This has resulted in a significant increase in the security strain within organizations. With more people logging in via personal devices to share data and teleconferencing over personal networks, the potential for breaches in security has grown significantly.

In order to manage these emerging threats in cybersecurity, it is important for FMIs to have robust cyber governance measures in place. This includes having clearly defined roles within an organization and creating a culture of responsibility among staff at all levels to ensure cyber resilience. It also involves understanding the cyber threat environment within which the FMI operates. A keen appreciation of the security landscape can help the organization better understand the vulnerabilities in its critical business functions and facilitate the adoption of relevant risk mitigation strategies. An in-depth review of these measures can be found in the ECB-WB **Cyber Resilience for Financial Market Infrastructures** note produced by the FIGI SIT Cybersecurity Workstream.

A Regulator's Perspective

Increase in Financial crime in times of Covid-19—AML and cyber resilience measures

The Financial Stability Institute published a policy brief entitled "*Financial crime in times of Covid-19—AML and cyber resilience measures*" in May 2020. The report delves into vulnerabilities opened by the covid-19 lockdown including higher risks of cyber-attacks, money laundering (ML) and terrorism financing (TF). The report shows that Covid-19-related cyber threats are increasing. For example, ransomware attacks have increased 148 percent in March 2020 over baseline levels in February 2020. Among the different sectors, the finance sector was the top target, with a 38 percent increase in cyberattacks against financial institutions.

The report also explores the responses by authorities worldwide to help financial institutions tackle these concerns more effectively. The Financial Action Task Force pointed to an increase in ML and TF risks stemming from Covid-19-related crime, including (i) increase in misuse of online financial services and virtual assets to move and conceal illicit funds; and (ii) possible corruption connected with government stimulus funds or international financial assistance. Several law enforcement agencies—at the local, national, and international level have also issued warnings related to these evolving threats. (**Read full article here**)

Essential workers in financial services list expanded in the US to accommodate security needs

The Cybersecurity and Infrastructure Security Agency (CISA) issued an updated version of their guidance on *"Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in Covid-19 Response"* in March 2020, which expands the categories of essential financial services sector workers to include those staffing data and security operations centers. In collaboration with other federal agencies and the private sector, CISA developed an initial list of essential critical infrastructure workers to help state and local officials in their work to protect their communities, while ensuring continuity of functions critical to public health and safety, as well as economic and national security. As state and local communities establish Covid-19-related restrictions, CISA is providing this guidance affirming that workers supporting financial operations, such as staffing data centers and security operations centers, are also to be considered essential critical infrastructure workers to ensure that the cybersecurity and data protection needs are met adequately. (**Read full report here**)

Different Measures Undertaken to Secure Telecommuting and Remote Workspaces

As with most cybersecurity concerns, the evolving nature of this pandemic requires creative ways to address the challenges arising from online exposure that some of the virus-tackling measures have inadvertently caused, including large-scale telecommuting among employees. Below is a list of resources discussing guidelines to strengthen cyber security while teleworking:

- **The National Institute of Standards and Technology (NIST)** *ITL Bulletin* provides guidelines on telework and remote access to help organizations mitigate security risks associated with the enterprise technologies used for teleworking. (**Read full report here**)

  NIST also produced a blog titled *'Preventing Eavesdropping and Protecting Privacy on Virtual Meetings'* to address security concerns during conference calls and web meetings. (**Read full blog here**)

- **Interpol** outlined different types of possible cyberattacks and released a set of teleworking recommendations and prevention tips. (**Read full article here**)

continued on page 3

Different Measures Taken . . .
continued from page 2

- The **Cyber Readiness Institute** produced a guidance note on 'Securing a Remote Workforce' for businesses. (**Read full article here**)
- The **National Cyber Security Alliance Covid-19 Security Resource Library** features free and updated information on current scams, cyber threats, remote working, disaster relief, and more. (**Read full article here**)
- The **Global Cyber Alliance** published tips for maintaining cyber hygiene when working from home. (**Read full article here**)
- The **Cyber Threat Intelligence League** produced a report on their technical efforts to neutralize cyberattacks and stop malicious cyber activity related to the Covid-19. (**Read full article here**)
- **Cybersecurity and Infrastructure Security Agency (CISA)** provides resources to combat cybercrime, secure networks and protect critical infrastructure from cybersecurity issues that may arise from the spread of Covid-19. (**Read full article here**)
- **CISA** *TIC 3.0 Interim Telework Guidance* provides security guidance for remote federal employees to connect securely to private agency networks and cloud environments. (**Read full article here**)
- **Boston Consulting Group** published a blog 'Managing the Cyber Risks of Remote Work' (**Read full article here**)
- **Singapore Computer Emergency Response Team (SingCERT)** published an article on proactive measures to enhance cybersecurity preparedness while working from home. (**Read full article here**)

Cybersecurity Events and Breaches

- **Government transfers—including Covid-19 impact payments—become potential targets of cyber fraud**
  The Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of the Treasury, the Internal Revenue Service (IRS), and the United States Secret Service (USSS) urged citizens to be on the lookout for criminal fraud related to Covid-19 impact payments. They cautioned about scams that use Covid-19 as a pretext to steal personal and financial information, as well as to steal the impact funds. (**Read full article here**)

- **Increase in payment fraud as a result of Business Email Compromise**
  Schemes such as phishing (fake emails to induce provision of credentials or access), vishing (telephone-based phishing) have been on the rise using COVID-19 messaging as a pretext. Hackers typically access email platforms like Microsoft Outlook or buy similar domains to access private networks and can then monitor email traffic for weeks or even months. About 80 percent of finance professionals have reported attempted fraud, and the Federal Bureau of Investigation suggests that losses have exceeded $3.5 billion in 2019. Attacks that specifically use Business Email Compromise tactics accounted for $1.7bn of 2019 losses. (**Read full article here**)
- **Mobile payment apps and government transfers targeted as Covid-19 hits developing countries**
  There has been a rise in online fraud and scams across many developing countries as they struggle to to address the health and economic impact of the pandemic. This includes scams on mobile payment apps (e.g. CashApp) and hoax emergency money offers for essential items from government agencies. There have even been false claims that the coronavirus is related to exposure to new technologies. Measures that authorities can take in response to better protect consumers include alerting people to the risks, ensuring that providers have adequate consumer complaint mechanisms in place, and coordination with law enforcement both in the country and across borders. (**Read full article here**)

- **Cyber criminals look to exploit increased anxiety levels during Covid-19**
  The National Crime Agency in UK issued a warning regarding cyber criminals looking to exploit citizens by asking for upfront fees for bogus loans, offering high-return investment scams, or targeting pensions. With more remote workers, a greater portion of the population will be vulnerable to computer service fraud where criminals can employ tactics to gain access to computers and/or divulge your logon details and passwords. It is also anticipated that there will be a surge in phishing scams or calls claiming to be from government departments offering grants, tax rebates, or compensation. The article further explores steps that can be taken to prevent falling prey to these scams. (**Read full article here**)

Cryptocurrency Corner

The cybercrime unit of the IRS prepares for a new wave of crypto-currency audits to fight tax-evasion
Officials from US, UK, Australia, Canada, and the Netherlands—collectively known as the Joint Chiefs of Global Tax Enforcement—shared data, tools, and tax enforcement strategies to identify new leads to mitigate cross-border money-laundering, tax-evasion, and cybercrime. The effort is a part of IRS's renewed focus on fighting tax-evasion and cybercrime tied to cryptocurrency, as the digital currency becomes increasingly popular. The IRS further released guidance on how virtual currency investors and their tax advisers are expected to report income from their holdings. (**Read the full article here**)

Anti-money laundering laws to apply to crypto firms
Scrutiny over Facebook and its plan to offer its proposed Libra stablecoin has led to checks being imposed on cryptocurrency operators and related firms to prevent anonymous users from engaging in criminal behavior. The head of the Financial Crimes Enforcement Network, Kenneth Blanco, announced the requirement of crypto firms to comply with existing regulation for anti-money laundering. (**Read the full article here**)

Paypal Ventures invests in cryptocurrency compliance and risk management startup TRM Labs
Founded with the aim of using cryptocurrency and blockchain to democratize access to financial services, TRM Labs is raising money to help financial institutions embrace opportunities associated with cryptocurrencies by mitigating the security risks involved. It integrates with more than a dozen blockchains, and analyses billions of virtual asset transactions to detect signs of fraud and financial crime like money laundering in real-time. Launched out of the Y Combinator accelerator last year, TRM Labs has reportedly delivered its technology to banks, brokerages, and exchanges across the US, Latin America, Asia, and Europe. (**Read full article here**)

Developments in Payments Security

Cybersecurity tactics for the Covid-19 pandemic
The pandemic has presented chief information security officers (CISOs) and their teams with two main priorities: (i) securing work-from-home arrangements on an unprecedented scale and (ii) maintaining the confidentiality, integrity, and availability of consumer-facing network traffic as volumes spike—partly as a result of the additional time people are spending at home. The article explores technology modifications, employee-engagement approaches, and process changes that cybersecurity leaders have found effective in managing risks exacerbated by the Covid-19. (**Read full article here**)

Cyber-skills firm builds cyber wargames for IT and security teams to learn from

The Immersive Labs platform uses real-time feeds of the latest attack techniques, hacker psychology and technological vulnerabilities to build cyber wargames for IT and security teams to learn from. The latest funding round comes 11 months after Goldman Sachs injected $8 million into the firm, saying its technology had helped hone the skills of the people at the front line of the investment banking company's cyber defenses and helped identify new talent throughout the organization as well. (**Read full article here)**

Opinions, Research and Publications

Economic Impact of Covid-19 on Global Cyber Security Market
The Covid-19 outbreak and resulting restrictions on daily life are highlighting the importance of digital platforms, testing their resilience, and demonstrating the power of tools that financial institutions have lacked in past crises. Online and mobile banking has grown increasingly popular, lessening the traditional role of branches. Increased digital traffic, while welcomed, could pose challenges. Bankers will need to carefully monitor systems to ensure they have the capacity to handle surging usage and safety concerns emerging from it. (**Read full article here**).

Covid-19 could hasten digital banking trend
The Covid-19 outbreak and resulting restrictions on daily life are highlighting the importance of digital platforms, testing their resilience, and demonstrating the power of tools that financial institutions have lacked in past crises. Online and mobile banking has grown increasingly popular, lessening the traditional role of branches. Increased digital traffic, while welcomed, could pose challenges. Bankers will need to carefully monitor systems to ensure they have the capacity to handle surging usage and safety concerns emerging from it. (**Read full article here**).

Global Banks model doomsday ransomware scenario
Financial institutions and government agencies across the globe

continued on page 5

Opinions, Research and Publications
continued from page 5

participated in a cybersecurity simulation in November 2019 to test their responses to a wave of ransomware attacks on the financial sector. The closed loop simulation included securities firms, banks, asset managers, FS-ISAC, and financial market infrastructure providers of all sizes from Australia, Canada, Europe, Hong Kong, India, Malaysia, Japan, Singapore, and the US. The tests centered around a fictional ransomware attack on a too-big-to-fail bank in the US, before moving to take down a similar-sized institution in Asia and the UK. Organizations participated from their own locations to further enhance the realism of the simulation and make use of real-world communication systems like email and phone. The results showed that no single actor from the federal government, to an individual firm had the resources to protect markets from cyber threats on their own. (**Read full article here**)

Protecting against cyberthreats while maintaining business continuity

The main challenge for chief information-security officers and cybersecurity teams is to protect their institutions while enabling operations to go on without interruption. For example, cybersecurity teams at companies that provide web-based services to consumers must adjust their security programs to match scaled-up operations while securing a massive shift to work-from-home tools. At the same time, it should be possible for security-team members to look after themselves and their families during a health crisis. This article expands on four principles to address some of these concerns: focusing on critical operating needs, testing plans for managing security and technology risks, monitoring for new cyberthreats, and balancing protection with business continuity. (**Read full article here**).

Why collaboration is key to cybersecurity in financial services

For many financial services institutions, competitive advantage lies in the ability to move large volumes of data between public and private cloud services and applications in an agile manner. This can place a security strain on an industry which constantly needs to find new ways to protect itself and its customers. According to IBM's 2019 Cost of a Data Breach Report, the average total cost of a data breach in the UK is upwards of $3.85m. Investing in the right tools like firewalls, security tokens, or anti-virus programs can play a big role, but there is also a need to explore how organizations can collaborate rather than compete to create safety in numbers—by sharing knowledge, spotting threats and developing solutions faster. Furthermore, in the age of Open Banking, collaborative efforts can ensure a consistent security posture across the broader data ecosystem. (**Read full article here**)

Kenya adopts a data protection law to bolster tech investments

Safaricom's M-Pesa mobile money has been operational in the region for a while, but due to limited regulations on data protection, external investors have been less forthcoming. Under the new law in Kenya, violations of data privacy can result in hefty fines and jail time apart from being investigated by an independent office. The lack of safeguards against data privacy had also been a hinderance to digitizing the identity records of citizens, which was slowing down the provision of services. This law is likely to facilitate the process of enhancing Digital IDs in the region as well. (**Read full article here**)

The Compliance Officer's plan for recovery in the Next Phase of Covid-19

With the reopening phase of the Covid-19 pandemic underway, financial firms are grappling with whether they will return to the office or will continue to work remotely, as well as how those decisions will impact their staff. Compliance officers need to be strategic and agile in their approach to compliance management, now more than ever. The article explores a list of key compliance and risk considerations to keep in mind including: Policies, Procedures, and Controls; Operational Resilience; Testing and Monitoring; Employee Oversight; and Resources and Budget. (**Read full article here)**.

Privacy Considerations when returning to the workplace

With many jurisdictions easing stay-at-home restrictions, employees are being asked to return to their offices in phases. Employers will consequently have a significant role in preserving the physical well-being of their workforce and the broader public. This article looks into current and potential contact tracing methodology in light of privacy regulations. It examines what regulations have to say regarding virus tracking and similar situations and presents guidelines for privacy practices in implementing contact tracing and symptom tracking of employees. (**Read full report 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).**