Financial Sector Cybersecurity Webinar Series
Summary Note

The World Bank Group Seoul Center for Finance and Innovation (SCFI) hosted a *Financial Sector Cybersecurity Webinar Series,* from December 2021 to May 2022, to raise awareness of the growing cybersecurity challenges in the financial sector. Regulators, experts, and peer practitioners were invited to discuss key issues that the East Asia and Pacific (EAP) region should consider and pathways to strengthen financial sector cyber resilience in individual jurisdictions and the region at large. This summary note offers a recap of the key takeaways.

INTRODUCTION

The digital transformation of the financial sector has been rapidly accelerated as firms and governments sought to respond to the challenges of the COVID-19 pandemic, creating the conditions for both great benefit and harm. The explosion of digital financial services has provided increased access and usage to individuals and firms that were previously neglected; however, the sophistication and scale-up of cyber threats are posing a major risk to this accelerated digital development and to the post-pandemic economic recovery. The evolving attacks over the years on financial services and infrastructure providers have resulted in severe financial, economic, operational, and reputational loss on both the targeted organization and the industry. Fortifying cybersecurity in the financial sector is therefore critical to build better, resilient, and inclusive recovery from the pandemic.

The three-part webinar series, hosted by SCFI, addressed the issues of financial sector cybersecurity challenges and the preparedness of jurisdictions in the EAP region. The first webinar in December 2021 provided a general overview of cybersecurity threats in the financial sector; the second webinar in February 2022 took a deep dive into developing and implementing strategies to mitigate the cybersecurity risks; and the third webinar in May 2022 focused on the pressing issue of third-party risks. Distinguished speakers from the Bank of Albania, Bank of Thailand, Financial Security Institute of Korea, Financial Services Commission of Korea, Financial Services Information Sharing and Analysis Center (FS-ISAC), FNS Value of Korea, International Monetary Fund, Monetary Authority of Singapore, National Bank of Georgia, World Bank Finance, Competitiveness and Innovation (FCI), and World Bank Information and Technology Solutions (ITS), as well as participants from the EAP region and beyond, convened to share their experiences, lessons learned, and future steps.

The webinar series was met with great enthusiasm and drew the interest of a total of 618 registrants from 23 countries, 437 of whom attended the virtual events. Most of the participant

feedback revealed that the webinars were very useful and relevant, with requests for an extension of the series.[1]

KEY TAKEAWAYS

Financial Sector Cybersecurity Risks and Preparedness

From a cybersecurity perspective, it is important to understand the threat actors (organized crimes, nation state actors, etc.), their motivations (financial, espionage, disruption of financial/social/political order, or retaliation), and the typical techniques used in these attacks. Given that cyber activities frequently cross borders, international collaboration is essential, along with nurturing a strong cyber defense workforce and paying due attention to emerging areas of digital technology for both prevention and defense. It is also worth noting that the geopolitical drivers behind cyber-attacks are real, often following kinetic operations or physical military clashes on the border. Often, it is not the case of attacks directed by state agencies but hacktivists picking up their own nations' flag and conducting hacktivist-type operations against predominantly government websites.

Intelligence sharing is vital to protecting the financial sector against cyber threats. By aggregating and sharing intelligence from different financial industry actors, it is possible to analyze trends and patterns of behavior across the larger threat landscape. This information can then be disseminated across the community to update the existing lines of defense. Smaller financial institutions, including third-party vendors, are susceptible to greater harm than bigger financial entities as the former usually lack sufficient depth in terms of cyber threat intelligence as well as patching resources to sufficiently respond to and recover from cyber incidents.

The community of regulatory/supervisory agencies recognizes the need for coordination, especially on the international level. There is a conscious effort to reference established practices and avoid overcrowding the space, as well as recognition of the need to collaborate via public and private channels to leverage expertise across specialties. From the regulator's perspective, cooperation across sectors is also crucial as attacks can come from other interconnected sectors.

The existing financial sector cybersecurity frameworks are not one-size-fits-all models. While regulators and supervisors have taken the positive step of adopting the widely referenced National Institute of Standards and Technology's (NIST) cybersecurity framework and its five components—identify, protect, detect, respond, and recover—each entity must diligently

[1] The organizers would like to convey their gratitude to all participants for their contributions to knowledge building on this critical topic, and extend a special thanks to the following people: Jeong Yeon Kim for her flawless interpretation, Jinhee Park (World Bank ITS) and Sung Kyun Son (Fintech Center Korea) for their help in recruiting excellent speakers, and Kevin Yunil Kim (World Bank Korea Office) and FCI EAP colleagues for their support in widely promoting this event.

conduct its own risk assessment and determine its level of compliance with cybersecurity regulations.

As risks evolve, so must responses. Special attention must be paid to three main types of risks that are currently threatening financial stability: (1) third-party risks, stemming from financial institutions' increasing reliance on third parties to provide products and services that cannot be performed in-house; (2) cybersecurity risks, wherein attackers leverage the high degree of cyber interconnectivity within the financial sector; and (3) digital transformation risks, where a poor understanding of digital technology and preparedness for vulnerabilities can lead to service disruption and damage to a firm's reputation. The concerns over growing third-party risks demand serious attention.

Financial Sector Cybersecurity Strategy and Preparedness Analysis

For effective cyber resilience, financial sector authorities must have a high-level map of the system and the threat landscape in a particular jurisdiction. Who are the threat actors? Why are they attacking? How are they attacking? Understanding how these actors can have an adverse impact on the financial institutions of interest can help prepare a potential counterresponse to these threats. In addition, understanding the operational interconnectedness of the financial system will help identify the critical nodes in the system that, if attacked, would have reverberating impacts across the entire system, and thus help prepare an appropriate crisis response.

Financial sector authorities must also regularly assess their cybersecurity preparedness, with senior management or the board engaged in the process. There is a need to educate not only peer practitioners but also decision makers about the importance of cybersecurity awareness and building cyber resilience. The field demands renewed attention and approaches that befit the complexity and gravity of cyber threats. The authorities need to redress the lack of information on cyber-attacks, both within and outside of the financial system, given the interconnectedness of the cyberspace across sectors and borders. In addition, tracking incidents, identifying, and inventorying critical information assets—for example, being aware of key applications and the key technology components that support them—will help provide a holistic view of the system and a clearer understanding of the implications of changes implemented in the system.

Coordination, cooperation, and information sharing is key to maximize the potential of limited capacities and to defend against limitless/borderless threats. Cyber risks can only be addressed by the collective efforts of the relevant institutions. Joint action is needed to create a coherent regulatory framework and a supervisory framework, ensure that objectives are aligned among different areas within the regulatory authority as well as among national and international actors, and consistently feed information and tighten integration among the established lines of defense

for cybersecurity risk management, such as internal/external audit committees, operational risk management groups, and the Information Technology (IT) department.

Central banks are more susceptible than any other institution in the financial ecosystem to serving as systemic cyber risk transmission channels for financial instability. There is no substitute; confidence in the financial system is essentially underpinned by the central bank; and it is an institution that is fundamentally interconnected within the financial system. This, in turn, means that central banks must play a leading role in building cyber resilience within the financial sector and managing relevant risks.

Certification does not equal security: policies and procedures should not simply exist on paper but should be put into practice. Sufficiently skilled resources must be made available to implement and monitor the organization's compliance with established cybersecurity measures.

Cybersecurity and the Financial Sector: The Third-Party Risk Challenge

Financial institutions carry the ultimate responsibility for monitoring third-party service providers, manage third-party IT risks, and protect their digital users from cyber threats. Technology and cyber risks arising from financial institutions' third-party engagements (especially non-outsourcing engagements), whilst not a new phenomenon, have risen sharply, and the reliance on third parties is only expected to grow. The high level of concentration in a single vendor and low substitutability greatly amplifies the risks. Identifying material third-party engagements and establishing appropriate due diligence standards are important first steps in the risk mitigating process. Cloud risks need to be managed and supervised differently.

The lack of an enterprise's complete visibility across its extended supply chain renders the enterprise vulnerable to cyber-attacks. In cybersecurity, a supply chain involves resources (hardware and software), storage (cloud or local), distribution mechanisms (web applications, online stores), and management software. Enterprises should identify and document types of suppliers and service providers, define risk criteria accordingly, and routinely assess and monitor supply chain risks.

The tone at the top is important for effective third-party risk management (TPRM). Undervaluing TPRM outcomes in budgets leads to the prioritization of tactical initiatives over strategic improvements. A risk-based approach, allocating resources to highest-risk arrangements, is advised as teams contend with a growing body of work that expands across all risks, domains, and types of third parties.

Zero trust ("never trust, always verify") is the new normal in cybersecurity. Any password is proven to be vulnerable and hackable, and 8 of 10 security breaches involve compromised passwords. It must be recognized that suppliers are working to develop advanced solutions that can provide a convenient, secure, trusted, and sustainable digital user experience for all

stakeholders of digital financial services, such as distributed and decentralized multi-factor authentication (MFA) and the latest password-less blockchain secure authentication (BSA) schemes.

CONCLUSION

Cybersecurity is never a case of *whether* an attack will happen, but *when* it will happen. The challenge, therefore, is to determine how the financial sector can effectively prepare against the threats of cyber-attacks and manage the consequences in a way that allows users to continue to have confidence in the system. In the face of ever-evolving cyber-attacks and the increasing interconnectivity between systems, cybersecurity risk preparedness and strategies require continuous improvement and coordination across sectors and borders.

Falling behind in innovation will mean more than foregone growth and benefits to society. In the context of the digital transformation of the financial sector, it can lead not only to disrupted recovery from the pandemic, but also to risks associated with financial instability. Financial authorities, regulators, and supervisors must take the lead in building the proper strategies and safety nets to protect the system and its users' interests. Effort must also be made to empower not only experts but everyone who depends on technology to deliver and receive financial services and to engage with technology in an informed way to harness the benefits, manage the risks, and have trust in the process. This will be a precondition for reaping the rewards of digital innovation in the financial sector.

ANNEX

No.	Agenda
1	**Financial Sector Cybersecurity Risks and Preparedness -** December 14, 2021 • Session 1 | The Challenge of Cybersecurity and the Financial Sector: A Global Perspective • Session 2 | Cyber Resilience in the Financial Sector: A Korean Perspective • Session 3 | A Framework for Cybersecurity and Resilience in the Financial Sector: Lessons from a Regulator *A broad overview of cybersecurity threats from a global security perspective, followed by an observation of regional cybersecurity trends in threats, risks and challenges, specifically for the financial sector, as well as efforts made toward building cybersecurity resilience, including experiences shared from Korea and Thailand*[2] Link to full video recording
2	**Financial Sector Cybersecurity Strategy and Preparedness Analysis -** February 17, 2022 • Session 1 | Financial Sector and Cybersecurity Preparedness Analysis: Lessons from Europe • Session 2 | Financial Sector and Cybersecurity Preparedness in EAP and the World: What Do We Know and Issues for Consideration *Sharing of survey findings from the World Bank and experiences of regulators in Europe—namely, the Bank of Albania on the cybersecurity implications of its financial systems expansion and the National Bank of Georgia on the development of its cyber resilience process in response to state-sponsored systemic incidents—followed by an examination of the role of the financial sector authorities for cybersecurity and suggestions based on issues observed in East Asia*[3] Link to full video recording

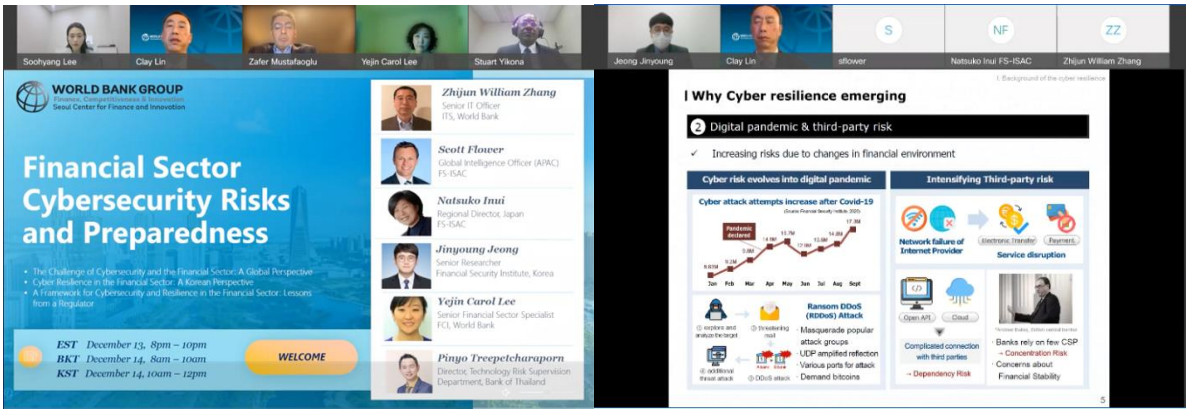
[2] **Moderator:** Clay Lin (World Bank ITS); **opening remarks**: Zafer Mustafaoglu (World Bank FCI); **speakers:** William Zhang (World Bank ITS), Natsuko Inui (FS-ISAC Japan), Scott Flower (FS-ISAC Asia Pacific), Jinyoung Jeong (Financial Security Institute, Korea), Yejin Carol Lee (World Bank FCI), Pinyo Treepetcharaporn (Bank of Thailand); **closing remarks:** Jason Michael Allford (World Bank Korea Office).

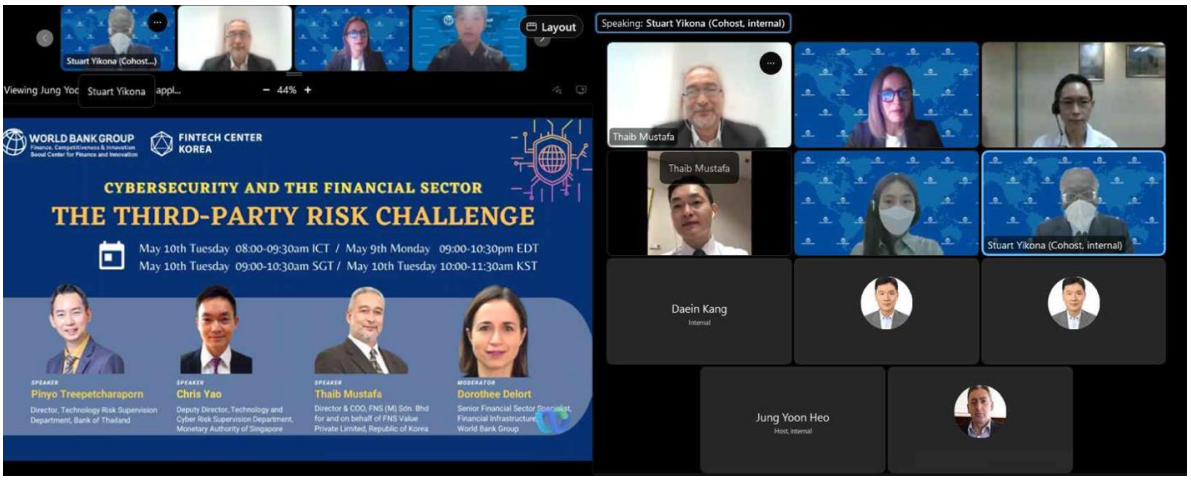
[3] **Moderator:** Stuart Yikona (World Bank FCI); **opening remarks:** Sooho Kim (Financial Services Commission, Korea); **speakers:** Aquiles A. Almansi (International Consultant), Ledia Bregu (Bank of Albania), David Papuashvili (National Bank of Georgia); Emran Islam (IMF Monetary and Capital Markets Department), David Ray (World Bank ITS); **closing remarks:** Zafer Mustafaoglu (World Bank FCI)

3 **Cybersecurity and the Financial Sector: The Third-Party Risk Challenge -** May 10, 2022

- Panel Discussion

Perspectives from regulators in Singapore and Thailand on securing an effective third-party risk management process, and from a Korean financial technology (Fintech) service provider on mitigating third-party risks[4]





[4] **Moderator:** Dorothee Delort (World Bank FCI); **opening remarks:** Zafer Mustafaoglu (World Bank FCI); **panelists:** Chris Yao (Monetary Authority of Singapore), Pinyo Treepetcharaporn (Bank of Thailand), Thaib Mustafa (FNS Value, Korea)