Summary Report on the Virtual Conference on

"STRENGTHENING CYBERSECURITY PREPAREDNESS FOR BANKS"

Organized by the Asian Bankers Association (ABA) with the Support of Hatton National Bank on September 30, 2020, 02:30 PM – 04:30 PM, Taipei Time

INTRODUCTION

With the world of finance becoming increasingly digitized, banks can expect to come under a growing threat from cyber-attacks. In 2020, the trend seems to have been exacerbated by the rapid worldwide spread of the COVID-19 pandemic. Criminals are exploiting vulnerabilities opened up by the COVID-19 lockdown, increasing the risks of cyber-attacks.

Focusing on the topic **"Strengthening Cybersecurity Preparedness for Banks",** the webinar – the second one organized by the Asian Bankers Association with the support of Hatton National Bank (HNB) – aimed to help our members to explore how banks and financial institutions can find ways to protect their businesses from emerging cyber risks, as everyone – from large corporations to small businesses – is a potential target for hackers.

The two-hour webinar features six speakers who addressed the following issues:

- *Cyber risk regulation and supervision*
- *Cyber Resilience, COVID-19 Response and the "New Normal"*
- *CISO and its criticality in managing the bank's cyber related risks*
- *Training and capacity building for staff and customers on cyber risks*
- *Bringing Intelligence to Cybersecurity Management*
- *Cyber Risk Insurance: Pros and Cons*

SUMMARY OF THE DISCUSSIONS

A. Welcome Statement by the Chairman of the ABA Policy Advocacy Committee

Mr. Dilshan Rodrigo, Chief Operating Officer of Hatton National Bank and Chairman of the ABA Policy Advocacy Committee, welcomed all the participants and thanked the speakers for joining the webinar.

Mr. Rodrigo noted that over the past few months, the ABA has been undertaking activities as a way of maintaining contact with members and providing them the opportunity to learn from each other as everyone faces almost identical difficulties across the region. For instance, on July 29 this year, the ABA organized the webinar on **"Managing Business Continuity and Recovery During COVID-19 and Beyond."** Drawing the participation of some 400 bankers from around the region, the first-ever webinar conducted by the Association featured representatives from member banks who shared their views on what their respective organizations and government authorities in their country are doing to mitigate the impact on their economy and the financial industry.

For this second webinar, the topic of which is focused on the very timely and hot topic of cybersecurity, Mr. Rodrigo pointed out the turnout was even higher, with some 990 participants registering for the event.

Mr. Rodrigo proceeded to introduce the webinar Moderator – Mr. Eugene Acevedo, President and CEO of Rizal Commercial Banking Corporation (RCBC) from the Philippines. Mr. Rodrigo noted that prior to joining RCBC, Mr. Acevedo has held senior leadership positions in several banks, including the Philippine National Bank as President and CEO; Union Bank as Senior Executive Vice President; and Citibank where his last position was to lead the Hong Kong/Taiwan/Macau Global Markets Cluster and as Treasurer of Citicorp International Ltd. He completed the Advanced Management Program at the Harvard Business School. He is keenly interested in banking innovation and transformation and is a Digital Marketing Professional certified by The Wharton School.

B. Opening Remarks by the Moderator

In his Opening Remarks, Mr. Acevedo recalled the time when cybersecurity consisted mostly of limited access to the data center. This was before local area networks, before proliferation of servers, before mobile banking, before employees worked remotely using Virtual Private Networks (VPNs), he noted. All of these, he said, multiplied the points of vulnerability, increasing the risk of cyberattacks, from a bored university student or nation-state attacker unleashing a day zero malware.

Mr. Acevedo pointed out that with the acceleration of digital transformation, with the democratization and wide reach of financial services, cybersecurity has become

even more complex - and costly. The amount of money spent by each bank on cybersecurity, either through prevention or actual loss, has risen substantially, he further added.

Mr. Acevedo then proceeded to the webinar proper, which he said featured six gentlemen, experts all, who would help the participants understand the topic at hand.

C. Jermy Prenio, Senior Advisor, Financial Stability Institute (FSI), Bank for International Settlements

Jermy Prenio is involved in managing the FSI's outreach program for banking supervision. He contributes to the Institute's published work on policy implementation and other policy-related material. Previously, he was Deputy Director for regulatory affairs at the institute of international finance in Washington, DC. He also worked as a regulator in the Philippines where he headed the Task Force on Basel II Implementation. He has an MA from the University of the Philippines School of Economics.

Mr. Prenio addressed the topic "Cyber Risk Regulation and Supervision". Among the areas he touched on included the following:

(a) International regulatory initiatives - e.g., Group of 7, Financial Stability Board, Committee on Payments and Market Infrastructures, International Organization of Securities Commissions, and Basel Committee on Banking Supervisory
(b) Cybersecurity strategy, governance & risk management - regulatory expectations
(c) Cybersecurity strategy, governance & risk management – supervisory practices
(d) Cybersecurity incident response and recovery – regulatory expectations
(e) Cybersecurity incident response and recovery – supervisory practices
(f) Third party dependencies – regulatory expectations
(g) Third party dependencies - supervisory practices

D. Alon Cliff-Tavor, Partner, Digital, Oliver Wyman

Alon Cliff-Tavor is a member of the Digital and Corporate and Institutional Banking practices. He works with the region's leading financial institutions on a wide variety of topics and problems. He also advises CXOs across industries on topics like digitization, digital operating models, fintech collaboration, business transformation, technology risk, cyber risk and more.

His recent assignments include cybersecurity diagnostic to identify weaknesses and improvement opportunities for a southeast Asian bank, and the implementation of cyber and IT risk management for a southeast Asian financial institution.

Mr. Cliff-Tavor shared case studies of banks on how cyber risk vulnerabilities can be exposed. Highlights of his presentation included the following:

(a) COVID-19 has significantly amplified cyber risks
(b) New threats have emerged exploiting COVID-19
(c) Emerging trends in cyber threats
(d) Case Study One: Ransomware attack while moving employees to work from home
(e) Case Study two: Rise in MDM vulnerabilities as demand for email access on mobile devices increases
(f) Three cyber information security areas that require urgent attention, namely, enhancing security controls, assessing and addressing external threats, and assessing tech and security teams' resource and continuity planning (medium and long-term priorities)

E. Suresh Emmanuel, Chief Information Security officer, Hatton National Bank

Suresh Emmanuel has extensive background in security implementation, all stages of IT security audits, IT security reviews, vulnerability assessment and penetration testing, and other areas of network and vulnerability reviews. He has conducted various assignments for leading blue-chip companies and conglomerates in Sri Lanka, not just with banks but also telecoms, manufacturing and various other industrial sectors.

Mr. Emmanuel talked about critical issues surrounding the webinar topic of Strengthening Cybersecurity Preparedness for Banks. His presentation highlighted the following points:

(a) The current situation of cyber risk in banking
(b) Classification of cyber incidents in banking
(c) Identification of most likely risks and most severe risks in banking
(d) Key challenges in dealing with cybersecurity threats for banks
(e) The degree if impact from cyber attacks on key aspects of a bank's business
(f) Steps for strengthening cybersecurity preparedness (identifying business requirements, gap assessment, risk assessment, governance, planning and development, and implementation and review.
(g) Some key takeaways (big data and threat intelligence, patch and vulnerability

management, supply chain attack controls, cyber incident response and restoration capabilities, segmentation, next general malware protection, network and web security, email protection, security awareness training, and security testing and assurance

F. Keisuke Kamata, Regional Director to Japan and Asia, Financial Services Information Sharing and Analysis Center (FS-ISAC)

Keisuke Kamara started as an IT Engineer and administrator in both network and application area for three years, before shifting to cybersecurity functions. In 2011, he was with MUFG Bank's cybersecurity strategy and capability. Since 2014, he mainly worked on cybersecurity issues in the financial industry, focusing on technical operation, various types of executions and as government cybersecurity advisor. He has published a book entitled "Introduction to Cybersecurity Management"

Mr. Kamata expounded on Training and capacity building for staff and customers on cyber risks. He cited the following issues:

(a) Training and capacity-building for staff and customers on cyber risks is one of the biggest challenges on cybersecurity
(b) Importance of knowing who they are facing (What is their motivation? Who are they? What they will do and what is the impact?)
(c) What are the major threats (ransomware, phishing site, Business Email Compromise, APT/Spear phishing) and what are the impacts (business suspension/money loss, personal money loss, corporate money loss, and information loss)
(d) It is important to provide goof level security together with services, make it easy to understand and to do, and communicate the right message to the right people

G. Michael Araneta, Head of Research, IDC Financial Insights Asia Pacific

Mr. Michael Araneta regularly engages with key decision makers in top financial institutions and regulators. His role is to grow the financial services research and consulting practice among top banks and insurers in the Asia Pacific Region. He is recognized as a thought leader in the Asia Pacific financial services industry as the go-to analyst for a broad range of strategic and tactical issues such as M&A, product innovation, customer centricity and CRM initiatives, core systems, vendor product portfolio positioning and

customer channel effectiveness.

Mr. Araneta's presentation focused on the topic "Bringing Intelligence to Cybersecurity Management". Among the points he highlighted in his presentation were the following:

(a) Organizations have a long list of cybersecurity "needs", including a growing number of channels, devices, transactions, environments to protect; ability to deal with a rapidly growing sophistication of cyber threats; continued growth of compliance and regulations; identity integration; recognition of cyber crime as a business; proliferation of security tool sets; addressing the scarcity of qualified information security professions; new infrastructure security considerations and solutions; recognizing that speed of response matters; and acknowledging the primacy of analytics
(b) There is a need to recognize the promise of intelligence to resolve long-standing problems in cybersecurity (e.g., volume problem, dwell time problem, prioritization problem, and action problem)
(c) Important elements in cybersecurity include: analytics to drive insight into threat dynamics, using intelligence to index and collect sources of information, orchestration of multiple tool sets to mitigate a threat and harden the network, and triage and initiating the proper response.

H. Ross McNaughton, Chief Information Security Officer at Gulf Bank and Member, Risk Committee, Kuwait Banking Association

Ross McNaughton is a seasoned Chief Information Security Officer and cyber security professional. He currently serves are the CISO for Gulf Bank in Kuwait, where he provides the strategic framework and direction in information and cybersecurity risk, providing robust protection and management assurance. He has over 20 years of specialized experience, in over 12 countries, accelerating cybersecurity adoption and modernization programs for large financial institutions. He is consistently sought out for advice throughout his industry and in thought leadership circles, and he has worked with more than 30 companies and 16 banks.

Mr. McNaughton spoke on the pros and cons of cyber risk insurance, highlighting the following points:

(a) Advantages of cyber insurance (it mitigates residual risk and does not negate the need for a good control environment)

(b) Ensuring correct coverage (Identifying categories that are separated and will need coverage clarification)
(c) Determining the questions to ask the insurer based upon the risks the organization currently has and potential future scenarios that are identified
(d) Using cyber insurance to mitigate cyber threats from third parties
(e) Correctly valuing insurance coverage with risk management and cost of breach calculations
(f) Risk management, acceptance and insurance
(g) Key takeaways include: question the insurer based upon your known weaknesses; have your scenario threat assessments realistic and in line with your real technical environment risk; and ask questions to the insurer on potential contention points related to exclusions