Box 8.1: Cyber Security – Emerging Trends, Challenges and Policy Response

Technology is changing the landscape of various business sectors around the world including the financial services sector. It is helping the financial institutions (FIs) to grow faster than ever by minimizing their costs, improving their operational efficiency, and expanding their reach. COVID-19 also brought about a paradigm shift in consumers' preferences who are now increasingly realizing the advantages of digital finance products and services. However, as FIs are increasingly adopting technology for their operations, it also exposes them to various risks and challenges including unintended incidents and intentional attacks. This also raises concerns for the regulators as they have to continuously enhance their regulatory and supervisory frameworks to counter the emerging and evolving risks from these arrangements in a proactive manner. While these frameworks provide a minimum mandatory level of security standards and controls, FIs need to put strong internal controls in place to effectively identify, assess, and manage such risks and remain vigilant to the evolving nature of cyber-attacks and threats.

With the fast-paced innovation and adoption of digital finance products by customers, cybersecurity has emerged as a leading challenge for the security and stability of financial sector …

The financial sector has been witnessing remarkable innovation in terms of adoption of technology in business processes and products; accordingly, the complexities and interconnectedness in the sector are on the increase. However, the widespread use of technology and innovation in products and services are accompanied by rising cyber threats across the world. Cyber-attacks can lead to different types of losses for the financial industry including business disruptions, financial and reputational losses, damage to integrity, and non-availability of assets and services, amongst others. From the perspective of systemic risk, any large enough cyber-incident in one major institution could potentially affect the financial system as a whole. Further, repeated cyber-attacks disrupting the business operations will also undermine the trust of public in the financial industry and could potentially lead to a panic in the market.

*Use of **Digital Financial Services (DFS)** are on the rise with an added impetus provided by COVID-19…*

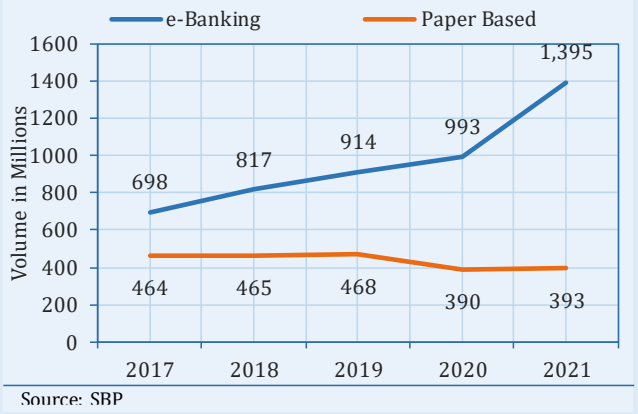
The COVID-19 pandemic has caused a paradigm shift in customers' preferences by exposing them to the benefits of digital finance products and services. Both financial institutions and policy makers are now increasingly realizing the potential of technology and digital finance, and they are endeavoring to explore their potential to achieve cost and operational efficiencies, enhance customer convenience, promote financial inclusion and facilitate documentation of the economy.

Pakistan has also seen a significant increase in use of digital modes of transactions since the start of the COVID-19 pandemic (**Chart 8.1.1**). In this regard, the SBP's special support measures and precautions against the cyber frauds also played an important role in promoting the use of digital modes and payments.[197] Of late, SBP has also taken a

[197] SBP waived all charges on funds transfers through online banking channels such as IBFT and SBP's Real Time Gross Settlement Systems in March 2020. SBP also advised banks to increase vigilance and monitoring on digital channels in the wake of rising digital transactions. For further details, read SBP Press Release dated March 18, 2020.

landmark step to introduce the first Instant Payment System (**IPS**) of Pakistan in the form of Raast, which is expected to exponentially increase the use of digital financial services. Raast facilitates bank account to bank account transactions (across the industry) at a relatively low cost and at near to real-time.[198]

Chart 8.1.1: Financial Transactions



Source: SBP

Digital transformation is accompanied by rise in cyber security risks and challenges…

However, digital transformation also exposes the financial sector to several new risks and challenges. As the financial sector is more digitized, it is exposed to different kinds of challenges including unintended incidents and intentional attacks. These cyber threats can be of varying nature including ransomware, phishing, data leakage, denial of service, malware propagation, or cyber extortion, etc. FIs are seeing a rapid rise in the cyber-attacks over the years as they have increasingly employed technology to improve their business operations. According to *The Global Risks Report, 2021* by World Economic Forum, cybersecurity failure ranks among the highest risks of the next ten years in terms of both likelihood and impact (**Chart 8.1.2 and 8.1.3**).[199] The *Global Risks Report, 2022*, published earlier, also notes that, among others, cybersecurity failure risk has also worsened since the start of the pandemic.[200] The *PwC 24th Annual Global CEO Survey* notes that cyber threats are fast becoming a major source of anxiety for the institutions and their top management around the world. Nearly 50% of the CEOs are concerned about cyber threats in 2021 as compared to only 33% in 2020. Cyber threat ranked second after pandemic and health crises in the list of threats that CEOs were extremely concerned about in 2021.[201] However, according to the PwC 25th Annual Global CEO Survey, cyber risks have surpassed health risks to become the top ranked threat to growth as per the CEOs.[202]

[198] Under Raast P2P fund transfers and settlement services, bank customers can send and receive funds in their accounts using their bank's mobile application, internet banking or over the counter services. Banks allow their customers to create a Raast ID by linking their preferred International Bank Account Number (IBAN) with their registered mobile phone number. The customers can then share Raast ID with others to receive funds in their account. Bank customers can use Raast service for sending or receiving funds using their IBANs even if they do not have a Raast ID. For further details, visit SBP's Raast homepage.

[199] The Global Risks Report 2021, World Economic Forum. Accessed on May 15, 2022

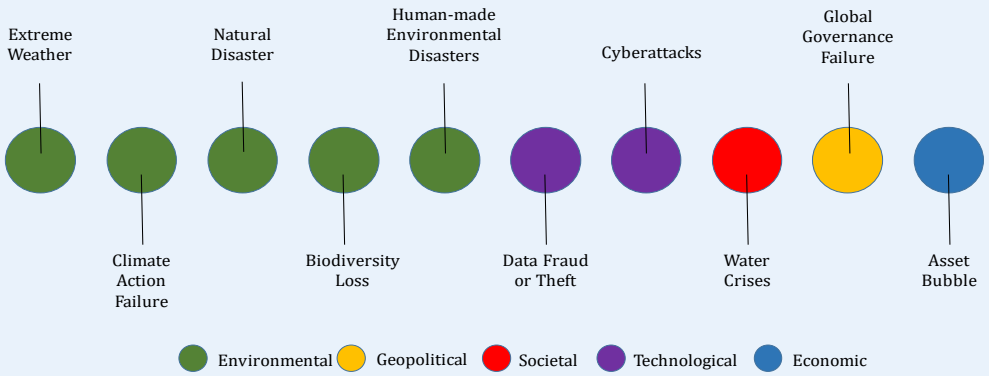
[200] The Global Risks Report 2022, World Economic Forum. Accessed on May 15, 2022

[201] PwC 24th Annual Global CEO Survey. Accessed on May 15, 2022

[202] PwC 25th Annual Global CEO Survey. Accessed on May 15, 2022

Chart 8.1.2: Top 10 Risks Over the Next 10 Years

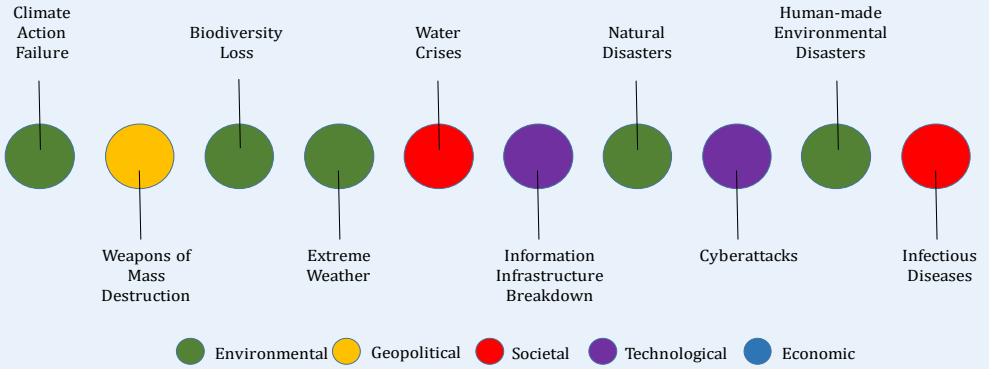
Long-Term Risk Outlook: Likelihood



Source: The Global Risks Report 2021, World Economic Forum

Chart 8.1.3: Top 10 Risks Over the Next 10 Years

Long-Term Risk Outlook: Impact



Source: The Global Risks Report 2021, World Economic Forum

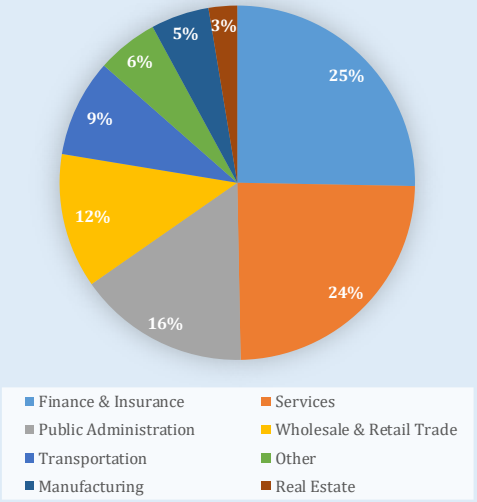
Financial sector is a preferred target for cyber-attacks across the world…

The financial industry has huge monetary and non-monetary resources including large databases of sensitive and valuable personal information of the public. As such, it offers multiple avenues of profit for hackers and fraudsters. Therefore, the industry is proving to be a special target for the unscrupulous elements across the world. The ensuing lockdowns following the pandemic necessitated remote working across the world, and the institutions had to employ remote access technologies to enable the employees to work from their homes. This phenomenon left the institutions more vulnerable to the risks of cyber threats and attacks. Furthermore, FIs use products and services from a wide range of third party service providers for delivering their services, which further increases their cyber risk exposure. In this regard, in the last couple of years, there has been an increase in number of cyber supply chain attacks, where the cyber criminals are able to compromise the supply chain of these products. Moreover, some of the IT products and services have systemic impact due to their concentration; hence, any issues with these products or their suppliers can have systemic impact on the larger financial system.

According to the Global Islamic Bankers' Survey, 2021 by General Council for Islamic

Banks and Financial Institutions, cybersecurity features in the top three risks faced by the Global Islamic Banking Industry.[203] Bank for International Settlements (**BIS**) has noted that the financial sector has been attacked by hackers relatively more often than other sectors during the COVID-19 pandemic (**Chart 8.1.4**).[204]

Chart 8.1.4: COVID-19 Related Cyber Events by Sector



Source: BIS

Pakistan has also witnessed increasing instances of cyberattacks especially after the onset of the pandemic…

Cybersecurity has emerged as one of the leading concerns also in Pakistan. Besides increase in the instances of cyber frauds, there have also been large scale cyber-attacks on the some of the state institutions and banks. Moreover, the latest SBP's SRS shows a significant rise in the participants' perception regarding the cybersecurity risks.

As such, **SBP has instituted a comprehensive regulatory and supervisory framework** to mitigate the cybersecurity risks (**Chart 8.1.5**).

Different aspects of framework have been discussed in the following paragraphs.

Chart 8.1.5: SBP Measures to Mitigate Cybersecurity Risks

Source: SBP

Cybersecurity measures by SBP – regulatory framework provides guidance and minimum standards of safety for managing cyber risks …

SBP's regulatory regime on cybersecurity of banks is based on National Institute of Standards and Technology's (**NIST**) Cybersecurity Framework and BIS's *Guidance on cyber resilience for financial market infrastructure*.[205, 206] SBP has taken several policy and regulatory measures to protect itself, the financial market infrastructure, FIs, and their customers from cyber threats. These measures aim to improve overall governance arrangements in FIs and at service providers' end that provide IT services to FIs, strengthen the operational resilience in SBP itself and the FIs it regulates, and promote a culture of collaboration and coordination in the industry to respond to cyber threats in real time. As technology becomes an integral part of the operations of FIs, such technology usage and dependence, if not properly managed, could heighten technology risks. Anticipating these risks, SBP developed a framework on *Enterprise*

[203] Global Islamic Bankers' Survey, 2021. Accessed on May 15, 2022

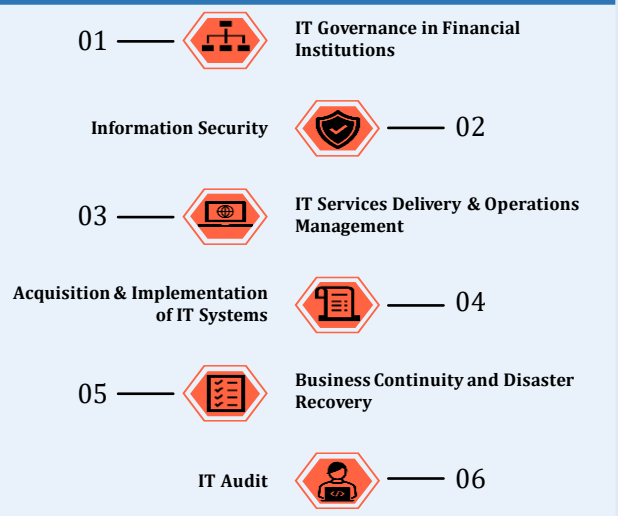
[204] BIS Bulletin No. 37 - Covid-19 and cyber risk in the financial sector. Accessed on May 15, 2022;
The sample in the graph excludes the health sector (57 COVID-related cases) and affecting health-related items of the manufacturing sector (163 cases)

[205] NIST's Cybersecurity Framework Accessed on May 15, 2022

[206] BIS's Guidance on Cyber Resilience for Financial Market Infrastructure. Accessed on May 15, 2022

Technology Governance & Risk Management Framework in Financial Institutions in 2017, with a vision to provide baseline technology governance and risk management principles to the FIs (**Chart 8.1.6**).[207] This framework is to be integrated with the FIs' overall enterprise risk management program to identify, measure, monitor and control technology risks. There are mandatory requirements for FIs to carryout full-scale vulnerability assessment and penetration testing of the digital infrastructure with the objective to identify potential weaknesses in their technology platforms. SBP has further advised FIs to adequately cover the cybersecurity threat intelligence and advisory services including update of the indicators of compromise (**IOCs**) and ensure immediate compliance with preventive actions. Since the technology landscape and the associated risks are evolving at a fast pace, SBP has enhanced its focus for continuous review and strengthening of its regulatory frameworks.

Chart 8.1.6: Overview of the SBP Enterprise Technology Governance and Risk Management Framework for Financial Institutions



Source: SBP

SBP has setup dedicated structure and mechanism to deal with its own information security risks …

For the purpose of ensuring cyber resilience of its information assets, SBP has a dedicated office of information security, which takes strategic actions to ensure protection of network, infrastructure, and related IT systems of the bank. This office strategically manages organization-wide information security and provides cost-effective security services in support of SBP IT systems and infrastructure. It performs regular operational security activities in all three facets of cybersecurity covering people, process and technology. Recently, SBP invested in establishment of resilience capabilities of its key security systems and re-enforced its internal cyber resilience capacity by engaging relevant stakeholders in mock drills of cyber incident management. This capacity building along with round the clock cybersecurity monitoring of IT infrastructure has resulted in early detection of threats and improved overall effectiveness and response time of teams.

Keeping in view the future growth and direction of IT advancements and related emerging cyber threats, SBP has rolled out a new set of control requirements in its internal IT Security Policies and Risk Management Framework, and performs major risk assessments of IT business and support systems.

Further, in the wake of pandemic, SBP continued its efforts to bring cultural shift by arranging virtual sessions of cyber security awareness. The user capabilities are also measured through quizzes, and targeted trainings are imparted wherever required. All these efforts have augmented cyber security posture, maturity, and resilience of SBP and its hosted services for financial sector.

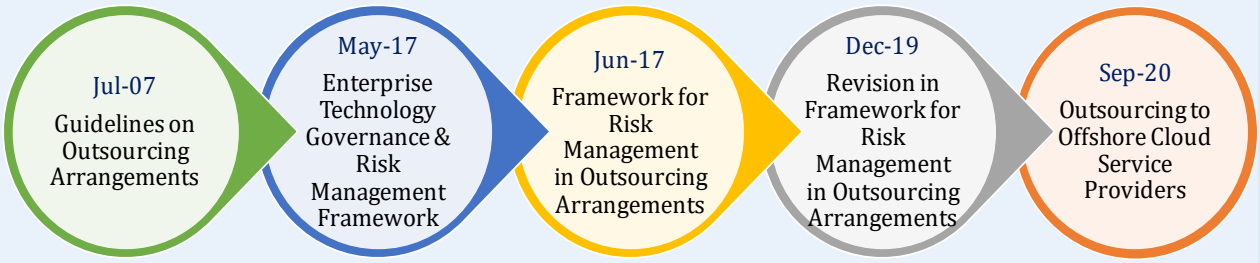
SBP's overall regulatory guidelines for cyber security risks are complemented by detailed guidelines on crucial areas…

FIs operating in Pakistan, over the years, have been cautiously increasing their usage of

[207] BPRD Circular No. 05 of 2017

outsourcing arrangements for some of their functions. This approach has increased their dependence on third party service providers and consequently their risk profile. SBP requires the banks to ensure that outsourcing neither should reduce the protection available to depositors and investors nor be used as a way of avoiding compliance with regulatory requirements. In view of an increasing use of outsourcing of a number of services by banks and the potential impact of associated risks on the banks, SBP first issued *Guidelines on Outsourcing Arrangements* in 2007.[208] Under these instructions, banks are only allowed to outsource their non-core functions and business support functions while the core functions are not allowed to be outsourced.[209, 210] SBP regularly reviews and updates these instructions in the light of emerging best practices and lesson learnt to facilitate the FIs in effectively managing the risks associated with the outsourcing arrangements (**Chart 8.1.7**). These instructions were broadly revised and updated in 2017 as *Framework for Risk Management in Outsourcing Arrangements by Financial Institutions*.[211]

Chart 8.1.7: SBP – Outsourcing Guidelines and Instructions



Source: SBP

Sustainable innovation is the crux of SBP's policy as SBP adopts measured approach to effectively balance the risks and benefits of technology and innovation …

Mindful of the associated risks, SBP strives to encourage the innovation and use of technology for improvement in the service delivery of the FIs to their customers without compromising their safety and security. SBP is deploying its technology adoption policies in a phased manner. The purpose is to give sufficient time to FIs to develop and strengthen their cybersecurity systems before employing advanced technological systems in their business operations. For example, SBP first formulated and issued regulations for **EMIs** in 2019.[212] SBP then issued live licenses to two

[208] BPRD Circular No. 09 of 2007
[209] Non-Core operations and business support functions include HR Modules, Procurement Functions, Non-Production Environment, Sandboxing, Inventory Management, Supply Chain Management, Office Productivity, Customer Relationship Management Tools (WhatsApp, Facebook etc.), Communication Tools, Security Tools, Computation and Processing Services, Data Analytics and Risk Modeling, Middleware and Payments Processing Services/ Platforms etc.
[210] Core operations and business functions include all banking applications and allied infrastructure, which are used to store and process customers' information relating to deposits, loans and credits and details of balances & transactions in ledger accounts of customers/ borrowers.
[211] BPRD Circular No. 06 of 2017
[212] EMIs are entities that offer innovative, user-friendly and cost effective low value digital payment instruments like wallets, prepaid cards, and contactless payment instruments. E-money has played a crucial role in

EMIs in 2021 to launch their commercial operations while four EMIs were granted pilot approvals during 2020 and 2021.[213] Furthermore, SBP recently launched licensing and regulatory framework for setting up digital banks in Pakistan as a separate and distinct category in the banking business while ensuring safety and soundness of the banking sector.[214] SBP also introduced the CDO Framework for opening accounts digitally by resident Pakistanis in 2021. This initiative will help bring efficiency and effectiveness in the account opening process using technology. SBP, earlier in 2020, had also enhanced the scope of its guidelines on outsourcing to Cloud Service Providers (**CSPs**) by FIs (**Chart 8.1.8**).[215] Previously, for all types of cloud services including Software as a Service (**SaaS**), Platform as a Service (**PaaS**) and Infrastructure as a Service (**IaaS**), the CSPs had to be located in Pakistan and all physical servers and services (data centers and allied infrastructure) had to reside and operate from Pakistan. Under the revised guidelines, FIs can now avail all types of cloud service models from domestic as well as off-shore CSPs for non-core operations based on certain conditions and ensuring satisfactory internal controls in these outsourcing arrangements. Going forward, SBP plans to review the proposal of allowing outsourcing of core services first to domestic CSPs and later to international CSPs after ensuring that FIs have satisfactory security systems and controls in place to ensure compliance with legal requirements and have the required capacity to manage such arrangements.

Chart 8.1.8: SBP Cloud Adoption Approach

Source: SBP

Supervisory framework complements the regulatory framework by addressing any gaps in FI's operational and risk management practices …

SBP has established a dedicated division in its Banking Supervision Group for continuous oversight and supervision of the cybersecurity risks. The prime objective of SBP's supervisory processes is to delineate supervisory activities for supervising the FIs according to their size, complexity, and riskiness. This risk focused approach, results in more rigorous oversight of FIs that pose enhanced risk to the financial system. The supervisory process for this purpose include both onsite and offsite assessments.

A Cybersecurity Supervision Framework based on **RBS** methodology was developed and implemented for effective supervision of the cyber risks emanating from the FIs. The framework was developed after considering related cybersecurity standards and best practices. This framework provides mechanism for assessing the emerging cyber risks and related controls. The major assessment domains include cybersecurity governance, information asset management, risk management, access controls, data security, cybersecurity awareness, incident detection

digitizing different types of payments in various countries. The EMIs in Pakistan are expected to offer interoperable and secure digital payment products and services to end users.

[213] SBP List of EMIs;
[214] BPRD Circular No. 1 of 2022
[215] BPRD Circular No. 04 of 2020

and response, etc. Cybersecurity inspection of the FIs are conducted using this framework.

Cyber Hygiene (**CH**) plays a prominent role in providing baseline fortification against the cyber incidents. In this regard, an exercise is being conducted to strengthen the CH of the FIs through self-assessment and ownership of their senior management.

Digital banking frauds is another important area of concern for SBP. In this regard, several measures ranging from awareness campaigns, and oversight to granular engagement with the FIs were taken. Further, SBP has been coordinating with Pakistan Telecommunication Authority **(PTA)** and FIA on the subject to curtail the digital banking frauds.

Way forward…

The world of technological advancement is evolving fast and so are the concomitant challenges arising as a result of these advancements. FIs are facing rising cyber-attacks with an increasing sophistication level. As such, FIs need to have robust cybersecurity measures and controls in place and constantly monitor and upgrade these protocols in order to cope with various types of cyber incidents. Besides the technological controls in place, human resources also constitute a major part of any defense protocol against cyberattacks. Social engineering attacks effectively use the people to breach the systems. Therefore, it is of utmost importance that resources be spent on building capacity within the organization. Moreover, all such efforts need to be supplemented by effective coordination between the industry members and the regulators. The flow of information between the stakeholders needs be robust and real-time so that cyberattacks can be responded in effective manner. On this point, SBP is working to establish a Computer Emergency Response Team in the financial sector (FinCert) under the mandate of National Cyber Security Policy 2021 by the Ministry of Information Technology and Telecommunication. Moreover, SBP has already issued instructions along with standardized formats to FIs to collect information on digital banking frauds or attempted frauds through call centers.[216] Considering that cyberattack on any one FI has the implication for the rest of the system, it is imperative that the industry as a whole put their resources for combating such attacks. Lastly, international collaboration is of immense importance in countering the risks arising from cyber-attacks. These attacks are mostly of global in nature and collaboration among states, regulatory and supervisory authorities, law enforcement agencies, and FIs is vital for effectively managing and mitigating the risks arising from the attacks.

[216] BC&CPD Circular No. 02 of 2021