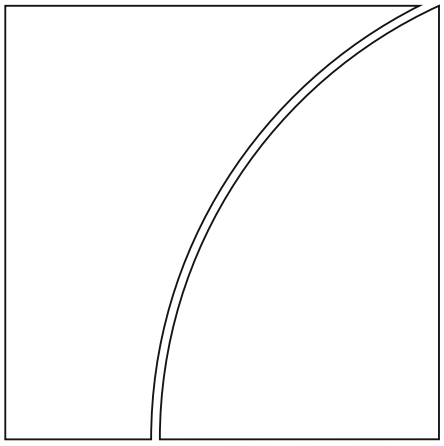


BIS Working Papers

No 1039

Cyber risk in central banking

by Sebastian Doerr, Leonardo Gambacorta, Thomas Leach, Bertrand Legros and David Whyte

Monetary and Economic Department

September 2022

JEL classification: E5, E58, G20, G28.

Keywords: cyber risk, central banks, financial institutions, cloud services, cyber regulation.

BIS Working Papers are written by members of the Monetary and Economic Department of the Bank for International Settlements, and from time to time by other economists, and are published by the Bank. The papers are on subjects of topical interest and are technical in character. The views expressed in them are those of their authors and not necessarily the views of the BIS.

This publication is available on the BIS website (www.bis.org).

ISSN 1020-0959 (print)
ISSN 1682-7678 (online)

Cyber risk in central banking

Sebastian Doerr, Leonardo Gambacorta, Thomas Leach, Bertrand Legros and David Whyte*

Abstract

The rising number of cyber attacks in the financial sector poses a threat to financial stability and makes cyber risk a key concern for policy makers. This paper presents the results of a survey among members of the Global Cyber Resilience Group on cyber risk and its challenges for central banks. The survey reveals that central banks have notably increased their cyber security-related investments since 2020, giving technical security control and resiliency priority. Central banks see phishing and social engineering as the most common methods of attack, and the potential losses from a systemically relevant cyber attack are deemed to be large, especially if the target is a big tech providing critical cloud infrastructures. Generally, respondents judge the preparedness of the financial sector for cyber attacks to be inadequate. While central banks in most emerging market economies provide a framework for the collection of information on cyber attacks on financial institutions, less than half of those in advanced economies do. Cooperation among public authorities, especially in the international context, could improve central banks' ability to respond to cyber attacks.

JEL classification: E5, E58, G20, G28.

Keywords: cyber risk, central banks, financial institutions, cloud services, cyber regulation.

* Sebastian Doerr, Leonardo Gambacorta, Bertrand Legros and David Whyte are at the Bank for International Settlements (BIS). Thomas Leach is at the University of Pavia. We would like to thank Codruta Boar and Sameh Mekhail for very valuable input on the content of BIS Innovation Hub projects. Giulio Cornelli provided excellent statistical assistance. Box A on: "Cyber resilience benchmarking – an example for central banks" has been written by Raymond Kleijmeer (De Nederlandsche Bank). The views expressed in this paper are those of the authors and not necessarily those of the BIS and the De Nederlandsche Bank.

1. Introduction

Cyber attacks are becoming more frequent and sophisticated every year, and firms and policy makers alike list cyber risk as a major concern.[1] Financial institutions and financial market infrastructures (FMIs) are particularly at risk, and the financial industry consistently ranks as one of the most-attacked industries. The rise of the crypto universe has further increased the likelihood of hacks in the wider financial sector (Boissay et al (2022)).

While there exist several studies and surveys on cyber threats for the private sector – and firms in the financial sector in particular – little is known about central banks' assessment of cyber attacks. What are their main concerns and how do they see the threat landscape? What measures do they enact to pre-empt or counter cyber attacks? And how do central banks assess the risks to and the readiness of the financial sector at large? Answers to these questions are pressing as cyber attacks, either directly on central banks or on critical FMIs, could seriously impair central banks' ability to fulfil their mandates and threaten financial stability.

This paper sheds new light on assessments of the cyber risk landscape in the central banking community, leveraging on a survey conducted in 2021 among the members of the Global Cyber Resilience Group (GCRG). The group was set up in 2020 as a forum where central bank Chief Information Security Officers can discuss both tactical and strategic cyber resilience topics.

The survey contains responses from 21 participants and asks detailed questions on the salient cyber risks that central banks see, how they prepare themselves, and how they assess the readiness of the financial sector in their jurisdictions. The survey includes answers by central banks from advanced economies (AEs, 9 respondents) and emerging market economies (EMEs, 12 respondents).

The survey reveals four main insights.

First, central banks from AEs and EMEs differ in their assessment of the frequency and cost of different cyber attacks. All central banks deem phishing and other forms of social engineering as the most likely type of attack vectors. AE central banks are significantly more worried about supply chain attacks[2] than their EME counterparts. When it comes to the costs resulting from an attack, advanced persistent malware and ransomware attacks rank highest. Turning to the who of these attacks, AE central banks deem organised crime and state-sponsored entities to be the main perpetrators. Among EME central banks, it is organised crime and individuals or activists.

Second, central banks actively discuss and develop policy responses to cyber attacks and have increased their cyber security-related investments notably since 2020. Technical security control and resiliency feature high on the priority list in terms of areas for investment in cyber security. Training existing staff on cyber security or hiring new staff with the relevant skills are also considered important, especially among EME central banks. Beyond investments, central banks focus on developing concrete policy responses. All central banks put a high focus on developing an

---

[1] See AXA (2021).

[2] A supply chain attack is a cyber attack that seeks to damage an organisation by targeting less-secure elements in its supply chain. For more details, see Section 2.

incident response plan in case their own institution is attacked, and several central banks are also developing a formal strategy for responding to an attack on the financial system at large. All central banks run internal exercises to simulate cyber attacks, and the most frequently modelled scenarios are an attack on the system of the central bank itself, as well as an outage of the payments system or other critical FMI.

While supervisory authorities in most EMEs provide a framework for the collection of information on cyber attacks on financial institutions, less than half of those in AEs do. Similarly, while supervised firms are mandated to report losses related to cyber attacks to the central bank in almost all EMEs, only two-thirds of AE respondents report that such disclosure is required. No jurisdiction requires firms to disclose such losses publicly, however.

Third, central banks deem the potential losses from a systemically relevant cyber attack to be large, and think that losses from cyber attacks in the financial sector have increased over the past year. Only a few central banks fully agree that the financial sector is adequately prepared for cyber attacks, and over half of the respondents think that investment in cyber security has been inadequate over the past year. Beyond traditional financial institutions, respondents reported that they see fintechs to be more at risk from a cyber attack than big techs, even though most respondents agree that a successful attack on a big tech would lead to materially higher aggregate costs than an attack on a fintech.[3]

And fourth, central banks in AEs and EMEs already cooperate widely on a range of topics. Bilateral cooperation among central banks, as well as cooperation in bodies at the regional and global levels, is the norm. When it comes to specific topics related to cooperation, information sharing, simulations and policy formulations to improve cyber resilience stand out in AEs. Among EMEs, central banks frequently cooperate in the realms of information sharing and policy formations. In addition, over two-thirds of respondents develop common standards and protocols for the financial sector. The BIS supports central banks' cyber security work, as well as global cooperation in this domain, in several ways – for example, through its Cyber Resilience Coordination Centre or projects of the BIS Innovation Hub.

This paper's main contribution is to highlight the cyber threat landscape as seen by central banks. Recent studies investigate cyber risk for non-financial corporates or financial institutions. Chande and Yanchus (2019) use the Advisen dataset to study losses from cyber events across sectors and provide an initial estimate of firm risk by sector. With the same dataset, Aldasoro et al (2022) find that relative to other sectors "finance and insurance" appears more resilient to cyber risks. Moreover, sectors with higher investment in IT are associated with lower losses. Duffie and Younger (2019) find that some of the most systemically important US financial institutions have sufficient stocks of high-quality liquid assets to cover wholesale funding runoffs during an extreme cyber event. Eisenbach et al (2022) show that the impairment of

[3] "Fintech" refers to technology-enabled innovation in financial services with associated new business models, applications, processes or products, all of which have a material effect on the provision of financial services. "Big tech" refers to large existing companies whose primary activity is in the provision of digital services, rather than mainly in financial services. Therefore, while fintech companies operate primarily in financial services, big tech companies offer financial products only as one part of a much broader set of business lines. For more details, see Frost et al (2019).

any of the five most interconnected banks in the US due to a cyber incident can result in significant spillovers to other banks.

Kashyap and Wetherilt (2019) outline some principles for regulators to consider when regulating cyber risk in the financial sector. The Basel Committee has also published guidelines for banks regarding best practice regarding cyber risk (Basel Committee on Banking Supervision (2018)). In addition, the high degree of uncertainty and variability surrounding cost estimates for cyber security incidents has consequences for policy makers. For example, it is difficult to foster robust insurance markets, as well as to make decisions about the appropriate level of investment in security controls and defensive interventions (Biener et al (2015); Wolff and Lehr (2017)).

This paper complements the existing literature by providing the first systematic assessment of how central banks assess cyber risk and associated macroeconomic costs, and how they judge the preparedness of the financial sector in their jurisdiction.

The rest of the paper is organised as follows. Section 2 provides a general overview on cyber risk and highlights key implications for cyber risk stemming from increasing cloud adoption and remote work for central banks. Section 3 leverages the survey to show which cyber attacks central banks deem as the most likely and how they assess their impact and costs. It then highlights the actions central banks undertake to guard themselves against cyber attacks. Section 4 provides an overview of central banks' assessment of cyber risk in the financial sector, and Section 5 illustrates cooperative efforts by central banks in the realm of cyber risk. Section 6 concludes.

2. Defining cyber risk and assessing the threat landscape

This section first provides a general introduction to cyber risk. It then highlights key implications for cyber risk stemming from increasing cloud adoption and remote work, with a focus on their relevance to central banks.

A general taxonomy

"Cyber risk" is an umbrella term encompassing a wide range of risks resulting from the failure or breach of IT systems. According to the Cyber Lexicon of the Financial Stability Board (2018), cyber risk refers to "the combination of the probability of cyber incidents occurring and their impact". A "cyber incident", in turn, is "any observable occurrence in an information system that: (i) jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not".

Cyber risks include both unintended incidents and intentional attacks. Examples of the former are accidental data disclosure, and implementation, configuration and processing errors. Estimates suggest around 40% of cyber incidents are intentional and malicious, rather than accidental, ie they are cyber attacks (Aldasoro et al (2020)).

Three types of attack stand out.

Phishing remains by far the most common initial attack vector. Traditionally, phishing emails have been used to trick a user to run a malicious attachment so that malware could be installed to take over the user's actual device. Credential phishing

has a different goal. It is the practice of stealing a user's login and password combination by masquerading as a reputable or known entity in an email, instant message, or another communication channel. Attackers then use the victim's credentials to carry out attacks on additional targets to gain further access. The frequency of phishing attacks is increasing: for example, between January and June 2021, the monthly average of phishing emails targeting cloud services almost doubled.[4] Attackers rely on ever more targeted and tailored malicious emails, through which they can either compromise end-user devices or gain an entry point for privileged access to local infrastructure or cloud-based services. Such unauthorised access can result in large damages.

Supply chain attacks occur when a threat actor infiltrates a legitimate software vendor's network and uses malicious code to compromise the software before the vendor sends it to their customers. Such attacks take advantage of established relationships of trust and the machine-to-machine communications used to provide essential software updates. They are thus difficult to mitigate and target both service providers (eg the 2020 SolarWinds Attack) and key technologies (eg Microsoft Exchange servers in 2021). Supply chain attacks are less frequent, but they can have great and potentially systemic consequences.

Ransomware is a type of malware deployed by attackers on a victim's computer network to encrypt their files and hold them for ransom. It typically propagates from a compromised end-user device through the entire organisation's IT environment. It can compromise not only the availability of information and IT assets, but also their confidentiality and integrity. The use of ransomware has grown massively over the past few years and incidences have tripled over the past year alone. Ransomware is mostly used by organised crime.

The type of attacker can vary. Beyond outright criminal and terrorist organisations, there can be industrial spies, "hacktivists", or state and state-sponsored players. In consequence, the motive of a cyber attack can be to simply earn a profit (eg ransomware, industrial spying), but can also be geopolitical concerns (state-sponsored attacks on critical infrastructures) or general discontent (hacktivism).

Cyber incidents can have monetary and/or reputational consequences. Business disruptions and IT system failures can damage integrity and availability. Data breaches compromise confidentiality, with financial and reputational losses. Fraud and theft include the loss of funds or any information (eg intellectual property) that may or may not be personally identifiable.[5]

Implications of cloud adoption and remote work

Cloud adoption, fostered by new digital ways of working, presents many opportunities for cyber attacks. Even though central banks themselves do not rely on cloud services to run their critical operations, cloud adoption by financial institutions also brings additional challenges. Specifically, traditional security perimeters that rely on a bounded and well-defined corporate network may no longer be fit for purpose in the era of cloud technologies. Now sensitive data also reside outside the network.

---

[4] See Verizon (2021) and Microsoft (2021).

[5] For an analysis of the costs of cyber incidents see, amongst others, Aldasoro et al (2022).

Consequently, targets move from the network to end users and their devices and identities, typically relying on social engineering techniques. The new digital perimeter that must be protected has shifted to identity – the cornerstone of modern security controls in the cloud – and the primary control enforcement on users, devices and data. All this leads to three main challenges.

The first challenge of cloud adoption is that, in the absence of a well-defined perimeter, information security is threatened by a lack of consistently applied security controls. Examples include vulnerable application programming interfaces (APIs), incorrect configurations and weak identity and access management (IAM).

The second challenge relates to the choice of cloud provider, not least when considering data sovereignty issues. The legal and regulatory framework in place in the country in which the data are hosted and/or processed becomes a key criterion when choosing which critical services to move to the cloud.[6]

The third challenge is the skills gap. It is difficult for most central banks to hire, retain and continuously retrain its workforce, but particularly so in this area given the limited labour supply, high costs and a fast-changing technological environment. For example, a 2020 report from Enterprise Strategy Group (ESG) and Information Systems Security Association (ISSA) revealed that 70% of cyber security professionals say that their organisations have suffered from a cyber security skills shortage and more than 60% that security positions remained vacant for at least three months.

These cloud-related challenges are being reinforced by increased remote working. Remote working, propelled by the outbreak of Covid-19, brings with it challenges of eg targeted phishing emails, unsecured home Wi-Fi networks and the use of personal devices for work.

The growing adoption of cloud-based services as well as the shift to remote work by both central banks and the industry has key implications for cyber security strategies.

First, the blurring of an organisation's digital and physical boundaries requires new strategies. One common approach is the so-called zero-trust concept. It assumes that it is impossible to trust the perimeter's defences or even the internal network. In zero-trust strategies, adaptive security policies grant access to resources as a function of multiple factors (such as user identity, endpoint attributes, location and indicators of behaviour).

Second, increased discipline in information classification and strong configuration-related automated controls are essential. Information classification is particularly important for collaboration technologies as information assets are transferred to the cloud to allow for collaboration. Misconfigurations cause nearly two out of three cloud environment breaches (De Beck (2021)).

And third, Cyber security strategies need to cope with the risk of a weakening of the governance process. A common misconception is that the cloud provider has sole responsibility for maintaining infrastructure security. In fact, data security, secure configurations and vulnerability management are a shared responsibility. This can test an organisation's capabilities – even more so as the organisation lacks full visibility

[6] For example, see the US Clarifying Lawful Overseas Use of Data (CLOUD) Act, enacted in 2018.

and control over its infrastructure because it relies on the cloud provider's security controls.

3. The cyber risk landscape for central banks

This section documents which cyber attacks central banks deem as the most likely and how they assess their impact and costs. It then highlights the actions central banks undertake to guard themselves against such attacks.

Attack types and associated costs

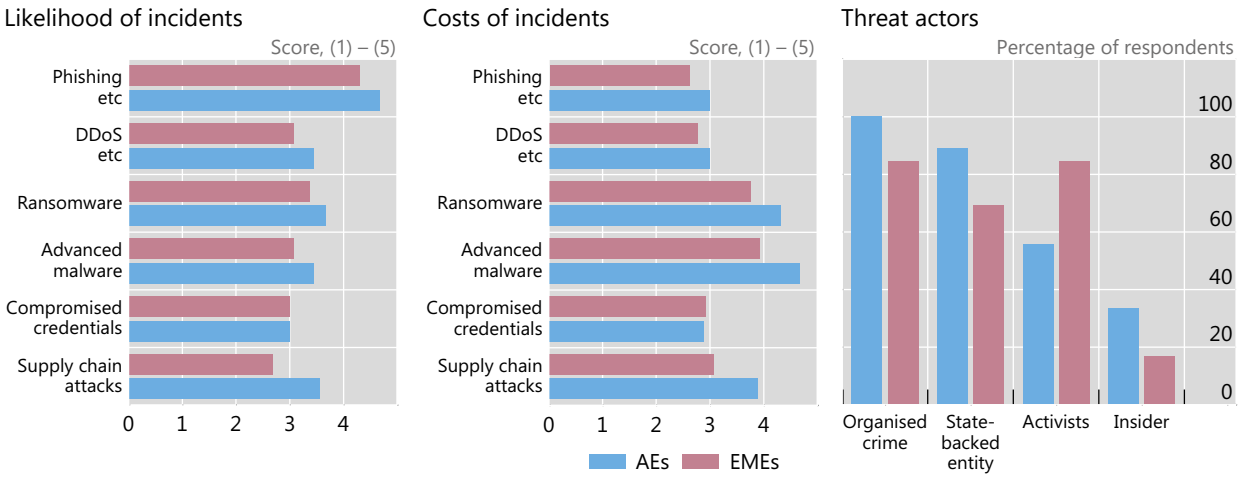
Central banks are typically responsible for the management and oversight of critical infrastructure (eg payment systems) in the financial sector. Consequently, a successful cyber attack on a central bank or critical infrastructure could not only entail significant monetary and reputational damage to the institution itself, but also lead to widespread disruption in the financial system and ultimately significant societal costs (Eisenbach et al (2020)). Furthermore, central banks safeguard highly sensitive information often sought after by criminals. For example, confidential material regarding future policy may be a target for criminals and nation state entities involved in cyber espionage.

Against this backdrop establishing an understanding of what type of cyber attacks are most frequent and damaging can help institutions to identify trends in cyber threats and to prepare.

Central banks in AEs and EMEs alike deem phishing and other forms of social engineering as the most likely type of attack (Graph 1, left panel). This could reflect that this type of attack usually entails sending many emails to increase the probability that an individual will fall victim to such an attack. Moreover, such attacks require little investment on the attackers' behalf. While there are no material differences when it comes to perceived likelihood of eg ransomware or denial of service attacks, AE central banks are significantly more worried about supply chain attacks than their EME counterparts.

When it comes to the costs resulting from an attack, advanced persistent malware and ransomware attacks rank highest (Graph 1, centre panel). In light of the rise in popularity of ransomware, the associated high costs are of particular concern. Again, central banks in AEs rate the cost of supply chain attacks relatively higher than those in EMEs. The costs arising from denial-of-service attacks and phishing are generally perceived to be lower. Costs from cyber incidents are multifaceted: central banks in AEs and EMEs alike assessed the financial loss from a cyber attack as significant, but the possible operational impact and associated reputational considerations (eg trust in the central bank or payment system) score as even higher concerns.

Frequency, costs and actors behind cyber incidents — Graph 1



The left panel reports the mean score of respondents' answers to the question "On a scale of 1 (very low) to 5 (very high), how would you rate the likelihood of the following attack vectors on your institution?". The attack vectors considered are on the y-axis and are the following: phishing/social engineering; distributed denial-of-service (DDoS); ransomware; advanced malware; compromised credentials; and supply chain attacks. The centre panel reports the mean score of respondents' answers to the question "On a scale of 1 (very low) to 5 (very high), how would you rate the result cost of the following attack vectors on your institution?". The attack vectors considered are analogous to those in the left panel. The right panel reports the share of respondents that selected each answer to the question "Which actors do you perceive to be the main perpetrators of cyber attacks on your institution?". Respondents could choose multiple options.

Source: Authors' calculations.

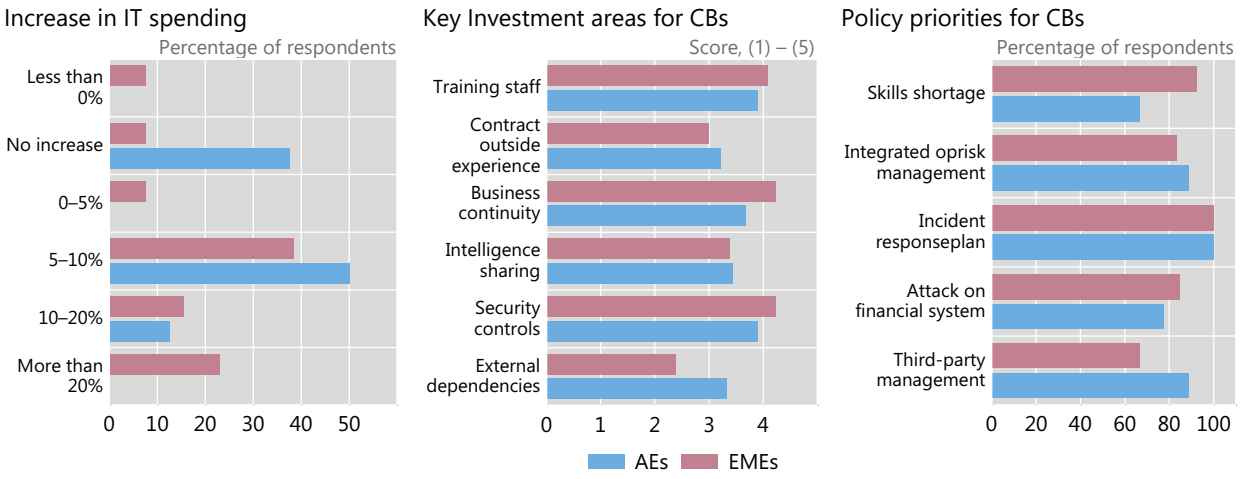
Turning to the "who" of these attacks, AE central banks deem organised crime and state-sponsored entities to be the main perpetrators of cyber attacks (Graph 1, right panel). Among EME central banks, organised crime and individuals/activists are listed as the most common perpetrators. Interestingly, only one EME central bank thinks that inside actors are an important threat, while one third of AE central banks thinks so. Insider threats could be perceived to be low, but their importance should not be underestimated as insiders may act as abettors to criminal entities (Upton and Creese (2014)).

Improving resilience to cyber attacks

Information technology has long been at the core of the financial system, consequently cyber security and associated threats have long been on the radar for maintaining continuity in central banks' day to day operations. However, a rising trend in cybercrime has elevated cyber security to be a key policy issue for regulatory and supervisory authorities. Against this backdrop, the survey investigates what are the key aspects for central banks' own cyber risk management and the wider policy issues that should be brought to attention of the financial system.

Investment in cyber security and policy issues

Graph 2



The left panel reports the share of respondents that selected each answer to the question "By how much has your institution increased its budget for investment in cyber security since the beginning of 2020?". The centre panel reports the mean score of respondents' answers to the question "On a scale of 1 [low priority] to 5 [high priority], which are priority areas for investment in cyber security?". The right panel reports the share of respondents that selected each answer to the question "What is the focus of the analysis and policy development on cyber risk within your institution?". Respondents could choose multiple options.

Source: Authors' calculations.

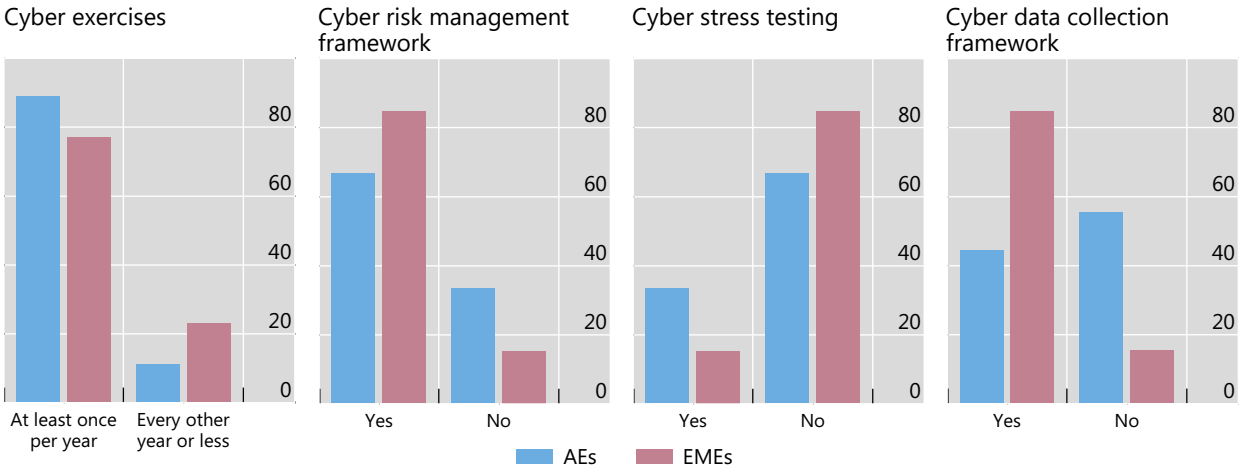
Most central banks in AEs and EMEs have increased their budget for investment in cyber security by at least 5% since 2020. Almost a quarter of EME based central banks even indicated increases upwards of 20% (Graph 2, left panel). Around one-third of AE central banks, however, have not seen any changes in their budget. Making sure that IT investments are funnelled into the right areas is also key. Technical security control and resiliency feature high on the priority list in terms of areas for investment in cyber security (Graph 2, centre panel). Training existing staff in cyber security aspects or hiring new staff with the relevant skills are also considered as very important – as is the case when it comes to developing IT capabilities in central banks more generally (Doerr et al (2021)). External dependency management, for instance the dependence on cloud providers, is relatively more important for AE than EME central banks.

Beyond investments, central banks focus on developing concrete policy responses. All central banks put a high focus on developing an incident response plan in case their own institution is attacked (Graph 2, right panel). Several central banks also report that they are developing a formal strategy on how to respond to an attack on the financial system at large. Among AE central banks, integrated operational risk management and third-party vendor management score highly, while addressing the cyber security skills shortage is especially important among central banks in EMEs.

Several policy initiatives are already being put into action. All central banks run internal exercises to simulate cyber attacks, and the majority does so at least once a year (Graph 3, left panel). In such exercises, the most-frequently modelled scenarios are an attack on the system of the central bank itself, as well as an outage of the payments system or other critical financial market infrastructure.

Scenarios and exercises, supervisory frameworks

As a percentage of respondents — Graph 3



The first panel reports the share of respondents that selected each answer to the question "How often do you run internal exercises to simulate cyber attacks (e.g. "fire drills")?". The second panel reports the share of respondents that selected each answer to the question "Does the relevant supervisory authority in your jurisdiction provide a risk management framework to financial firms on cyber security?". The third panel reports the share of respondents that selected each answer to the question "Does the relevant supervisory authority in your jurisdiction conduct cyber-stress testing of financial firms?". The fourth panel reports the share of respondents that selected each answer to the question "Does the relevant supervisory authority in your jurisdiction provide a framework for the collection of information on cyber attacks at financial institutions and associated losses?".

Source: Authors' calculations.

In most jurisdictions, but especially in EMEs, the relevant supervisory authority already provides a risk management framework for cyber security, or is planning to introduce such a framework (Graph 3, centre-left panel). At present, regular cyber stress testing of financial firms is not common. Yet one third of AE central banks and around 15% of EME central banks indicated they conduct cyber stress tests (Graph 3, centre-right panel). Of the respondents which do not currently undertake these exercises, two thirds of EMEs indicated they had plans to introduce them, while less than 30% of AEs plan to do so. The G7's fundamental elements for ethical red teaming[7] or threat-led penetration testing have encouraged central banks to conduct such exercises (Prenio et al (2019)).[8]

Supervisory authorities in most EMEs provide a framework for the collection of information on cyber attacks on financial institutions (Graph 3, right panel). Among respondents from AEs, less than half report that such a framework is in place. A similar picture emerges when it comes to whether supervised firms are mandated to report

[7] Red team testing can be defined as "a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations. Red teams comprise security professionals who are experts in simulating real-world attacks on systems and breaking into defences.

[8] For details on the G7's fundamental elements of cybersecurity for the Financial Sector, see: https://www.gov.uk/government/publications/g7-fundamental-elements-for-cyber-security.

losses related to cyber attacks to the supervisor. While this is the case in almost all EMEs, only two-thirds of AEs require reporting of incidents to the supervisor. No jurisdiction requires firms to disclose such losses publicly. That said, such a policy may not be optimal as it can lead to large reputational costs to firms (Kamiya et al (2021)).

These answers are in line with a general shift in central banks' cyber security practice. The latter is moving away from a compliance-based focus to a risk management and resilience focus. Cyber resilience, in this context, can be defined as the ability of a central bank/monetary authority to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents that do not exceed the organisation's operational limit.[9]

As part of this shift, three trends are emerging.

First, there is a greater adoption of a risk-based and priority-focused approach. Previous approaches focused on an audit-inspired comprehensive compliance to standards or on constantly adding new technology tools. A risk-based approach anchors key controls to actual attack scenarios.[10] Robustness is typically tested using full-scope, multi-layered simulated attacks.

Second, cyber security management is increasingly integrated into enterprise risk management frameworks. Benefits include better expression of risk appetite, prioritisation across risk types and, importantly, better recognition of accountabilities on the front lines in managing the cyber security risk exposures of business processes.

Third, cyber security shifts to cyber resilience. The concept of risk appetite accepts that zero risk does not exist. Accordingly, the focus is shifting to an organisation's ability to anticipate and withstand attacks and to continue its critical operations during the response and recovery phases. Hence the priority given to response and recovery processes such as incident management.

4. Central banks' assessment of cyber risk in the financial sector

Prior to the pandemic, several studies have indicated that the financial sector has remained robust in the face of cyber incidents (see for example, Aldasoro et al (2020)). Nonetheless, financial institutions are an increasingly attractive target for cyber attackers. In response, the financial sector is a large investor in IT and devotes significant resources to IT departments (ENISA (2021)). It has also developed a considerable amount of human capital and knowledge in cyber security and defence of IT systems. Recent trends have seen the financial sector outsourcing IT and also adopting more cloud based technologies, which present new risks to institutions.

In terms of the maximum loss in percent of annual GDP that could result from a systemically relevant cyber attack on a financial institution, most central banks

---

[9] This definition has been adopted from the Financial Stability Board (2018a) Cyber Lexicon.

[10] An increasing number of central banks rely on a modelling framework such as MITRE ATT&CK. As described in Prenio et al (2019), the MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

estimate a loss of 5% or less, although some EME central banks estimate costs to exceed 10%. These high costs reflect that the financial sector provides critical infrastructure. In light of these material costs and frequent attacks, how do central banks assess the readiness of the financial sector to cope with cyber attacks in their jurisdiction?

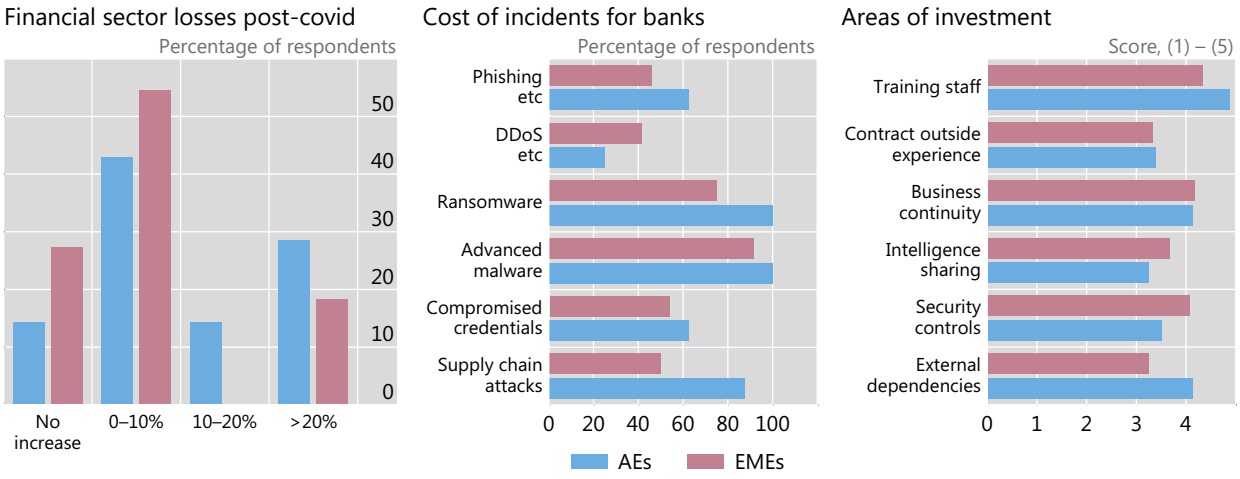
The majority of central banks in AEs and EMEs think that losses from cyber attacks in the financial sector have increased in 2020-21, relative to the pre-pandemic era (Graph 4, left panel). Most AEs noted an uptick in losses and, in particular, larger increases in losses among financial institutions. Almost 30% of AE respondents indicated losses having increased by more than 20%. Meanwhile most EME respondents report either no increase or a more modest increase of 0-10% in losses. Central banks noted that this increase in losses is driven not only by a higher frequency but also by a larger severity of cyber attacks.

What type of cyber incidents does result in the largest monetary losses for financial institutions? Similar to central banks' assessment of their own risks, among both AE and EME respondents, advanced persistent malware and ransomware attacks rank highest (Graph 4, centre panel). Supply chain attacks also feature prominently among AE respondents, but less so in EMEs. In general, denial of service attacks are deemed to be the least costly type of attack.

In response to the rising frequency and severity of cyber incidents, respondents state that financial institutions should prioritize their investments in cyber security towards training staff on cyber security, ensuring that business continuity is maintained, and managing their external dependencies (Graph 4, right panel).

Cyber attacks and costs in the financial sector

Graph 4



The left panel reports the share of respondents that selected each answer to the question "By how much do you think have annual losses from cyber attacks increased in 2020-21 in your financial sector, relative to the pre-pandemic period?". The centre panel reports the share of respondents that selected each answer to the question "Which type of incidents result in the largest monetary losses for financial institutions?". Respondents could choose multiple options. The right panel reports the mean score of respondents' answers to the question "On a scale of 1 [low priority] to 5 [high priority], which should be the priority areas for investment in cyber security by financial institutions in your jurisdiction?".

Source: Authors' calculations.

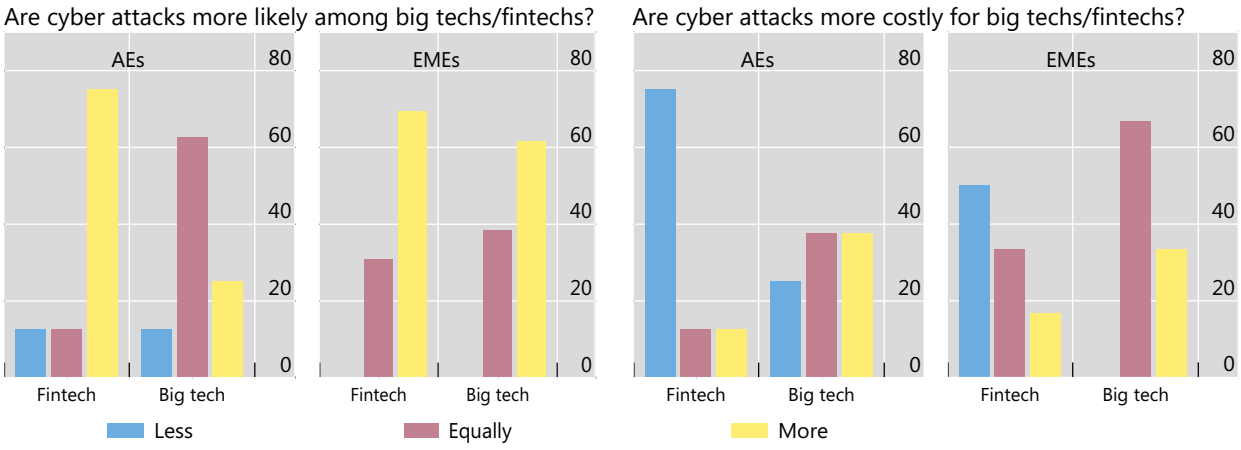
Beyond traditional financial institutions, cyber security is also an important issue for the fintech industry – a vibrant area for innovation, with many new providers offering cyber security-related services. While fintech providers generally fall under industry-wide or national cyber security frameworks, they do face some specific risks, for instance from the potential for theft of funds in crowdfunding or hacks on crypto exchanges that fall out of the traditional remit of financial supervision. Further, big techs are also providers of critical cloud infrastructure, which creates a dependency between the financial sector and big techs as a service provider.

Central banks reported that they see fintechs to be especially at risk from a cyber attack. Relative to a financial institution, three-quarter of respondents from AEs and two-thirds of EME respondents think that fintechs are more at risk of becoming the target of a successful cyber attack (Graph 5, left panels). Among EMEs, almost two-thirds of respondents also think that big techs are more at risk of a successful attack, while approximately two-thirds of AEs found a big tech to be equally likely to suffer a cyber attack, but only one-quarter of AE respondents believed it to be more likely.

When it comes to aggregate losses in terms of GDP, however, these patterns are strikingly different. Among EME and AE respondents, the majority thinks that a successful attack on a fintech will lead to a similar or lower loss in terms of GDP than a successful attack on a traditional financial institution (Graph 5, right panels). Among big techs, however, only one-quarter of AE respondents and no respondent from an EME assess the cost to be lower than that of an attack on a traditional financial institution.

Cyber attacks and associated costs: Financial institutions vs big techs and fintechs

As a percentage of respondents — Graph 5



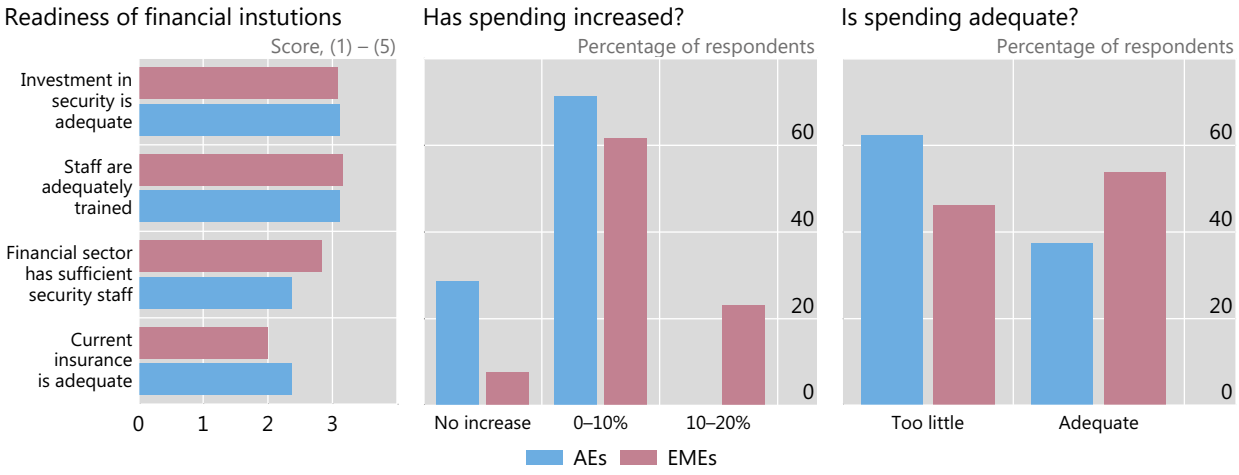
The first graph in the left panel reports the share of respondents from advanced economies that selected each respective answer to the two questions "Relative to traditional financial institutions, do you think that a) fintechs are less/equally/more at risk of becoming the target of a successful cyber attack? b) big techs are less/equally/more at risk of becoming the target of a successful cyber attack?". The second graph in the left panel reports the share of respondents from emerging market economies that selected each respective answer to the same two questions. The first graph in the right panel reports the share of respondents from advanced economies that selected each respective answer to the two questions "Relative to cyber attacks on traditional financial institutions, do you think that an attack on a) fintechs is less/equally/more costly (in terms of the maximum loss in % of annual GDP)? b) big techs is less/equally/more costly (in terms of the maximum loss in % of annual GDP)?". The second graph in the right panel reports the share of respondents from emerging market economies that selected each respective answer to the same two questions.

Source: Authors' calculations.

With an eye of the fintech industry, the public sector (governments, central banks, and regulatory agencies) can contribute to greater cyber resilience in two ways. First, it can establish sandboxes or other types of similar arrangements in which fintech firms and firms involved in cyber security can collaborate on projects and build in cyber security from the outset. Second, it can regulate and incentivise the fintech industry to further improve its cyber security capabilities. While national authorities in many countries have established sandboxes (Cornelli et al (2020), relatively few known initiatives have aimed specifically at fintech companies with the scope of strengthening their cyber security capabilities.

How do central banks assess the readiness of the financial sector in their jurisdiction when it comes to cyber risks? Only a few central banks agree that the financial sector is adequately prepared (Graph 6, left panel). On a scale of one to five, where five means full agreement, respondents gave on average a score of three when asked about whether spending on cyber security is adequate or financial institutions' staff is sufficiently trained. When asked about whether the financial sector employs enough staff to work on cyber threats, agreement was even lower. Both EME and AE respondents agreed the least with the statement that current insurance policies are adequate to cover losses from severe attacks.

IT spending and cyber insurance in the financial sector — Graph 6



The left panel reports the mean score of respondents' respective answers to the following questions "On a scale of 1 [do not agree at all] to 5 [fully agree], do you think that in your jurisdiction: a) spending on cyber security in the financial sector is adequate? b) the staff in the financial sector is sufficiently trained in cyber security? c) the financial sector employs enough cyber security professionals to defend itself from cyber threats? d) current insurance policies against cyber attacks are adequate for financial institutions to compensate for the consequences of severe attacks?". The centre panel reports the share of respondents that selected each respective answer to the question "By how much do you think the financial sector has increased its investment in cyber security in 2020-2021 relative to the pre-pandemic period?". The right panel reports the share of respondents that selected each respective answer to the question "Do you think that investment on cyber security has been too little/adequate/too much over the past year?".

Source: Authors' calculations.

These patterns are also echoed in answers to the question of whether investment on cyber security has been adequate over the past year. Most central banks stated that the financial sector has materially increased its investment in cyber security (Graph 6, centre panel). And yet, while around half of EME respondents (and almost 40% of AE respondents) think investment has been adequate, the remaining respondents think it has been too little (Graph 6, right panel). Similarly, most respondents state that less

than half of the financial institutions in their jurisdiction hold cyber insurance policies. The vast majority of respondents agree that insurance markets are not yet sufficiently mature to effectively price and cover losses in the event of a cyber attack.

5. Policy cooperation

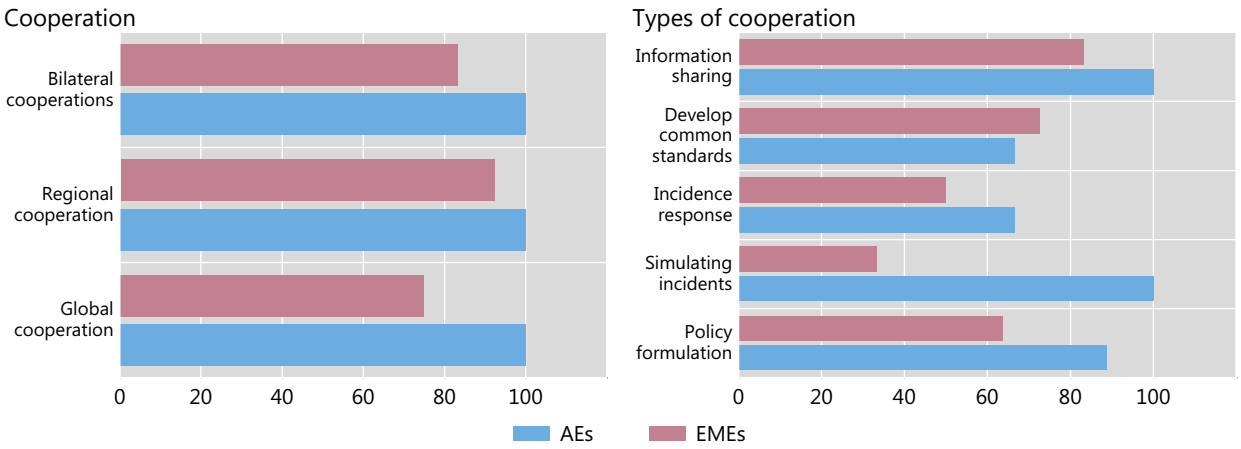
International cooperation in the realm of cyber security could help to develop best practices and learn from common experiences. It could also overcome the issue that cyber security efforts by individual institutions might fall short, as they do not take into account the systemic implications of a cyber attack (Kopp et al (2017)).

Indeed, central banks in AEs and EMEs already cooperate widely on a range of topics. As the left panel of Graph 7 shows, there is bilateral cooperation among central banks, as well cooperation in bodies at the regional and global level. Among AEs, all respondents indicate that they already cooperate in the respective areas, and so do most respondents from EMEs.

When it comes to specific topics of cooperation, information sharing, simulations (eg joint table top or cyber range exercises) and policy formulations to improve cyber resilience stand out in AEs (Graph 7, right panel). Among EMEs, central banks frequently cooperate in the realms of information sharing and policy formations, albeit at lower levels. In addition, over two-thirds of respondents from both AEs and EMEs develop common standards and protocols for the financial sector.

Cooperation across institutions

As a percentage of respondents — Graph 7



The left panel reports the share of respondents that selected each respective answer to the question "How does your institution cooperate internationally on cybersecurity aspects?". Respondents could choose multiple options. The right panel reports the share of respondents that selected each respective answer to the question "On what specific topic does your institution cooperate internationally on cybersecurity aspects?". Respondents could choose multiple options.

Source: Authors' calculations.

The BIS supports central banks' cyber security work, as well as global cooperation in the domain, in several ways.

The cyber resilience coordination centre (CRCC), established in 2019, has the overall mandate to provide a structured approach to knowledge-sharing, collaboration, and operational readiness among central banks in the areas of cyber resilience. Among its security services, the CRCC has formed a group of senior IT security experts, the GCRG. The CRCC is a key instrument for the active promotion of technical exchanges, cyber range simulations and cyber resilience assessment methodologies.

One key project supported by the GCRG is the development of Cyber Resilience Assessments (CRAs, see Box A). Its purpose is to provide central banks with a common framework to assess their cyber resilience posture and to improve their cyber resilience practices in the delivery of critical business services. Such a central bank-tailored methodology could help with quantitative-based common benchmarking and self-assessments.

Box A: Cyber resilience benchmarking – an example for central banks (by Raymond Kleijmeer)

Benefits of benchmarking

There are direct benefits for organisations and industries to use benchmarking as part of the assessment of their cyber resilience capabilities to compare their performance to peer organisations. For instance, it provides a focused means to help target security investment decisions. Accordingly, through these peer comparisons, an organisation can gain specific insights on how and where to work on improvement efforts. One of the methodologies that can be used to perform these types of benchmarks is the Cyber Resilience Assessment (CRA).

Critical business service

The CRA methodology is based on the Resilience Management Model developed by the Software Engineering Institute at Carnegie Mellon University (SEI-CMU). It focuses on assessing the resilience of critical business services and the strategies that are in place to protect and sustain them. It looks in detail at the underlying assets that directly support the delivery of the service thus allowing the organisation to accomplish its mission. The underlying assets are categorised into four types: people, information, technology and facilities. Disruptions can affect one or more of the assets which in turn can negatively impact the business process and eventually lead to mission failure of the organisation(s) involved in delivering the critical business service.

Cyber resilience capabilities

The CRA looks at practices that are performed in ten domains (see Graph A1). One of the key characteristics of the CRA is that it looks at a baseline first in each of these domains and subsequently at the maturity of the organisational capabilities in place. For this purpose, the following maturity indicator levels (MIL) are used in the CRA:

- MIL-1 Performed: the level of practices performed complete;
- MIL-2 Planned: the level of programmatic planning;
- MIL-3 Managed: the level of performance of management processes;
- MIL-4 Measured: the level of measuring performance and periodic review;
- MIL-5 Defined: Sharing improvements and lessons learnt.

The MIL rating assigned to each domain informs the organization at what maturity indicator level the organization performs and whether it meets its target levels for that domain. In the CRA there are 299 questions across ten domains; 110 questions are marked as basic hygiene based on common industry practices in these domains.

BIS Central bank pilot

In 2021, the BIS organised with its BIS member central banks a first round of resilience assessments and based on these aggregate findings a first cyber resilience benchmark has been developed for central banks. The experiences have shown that the methodology helps organisations focus and prioritise their improvement efforts based on the outcomes of their cyber resilience assessments.

Example – a foundational level of cyber resilience

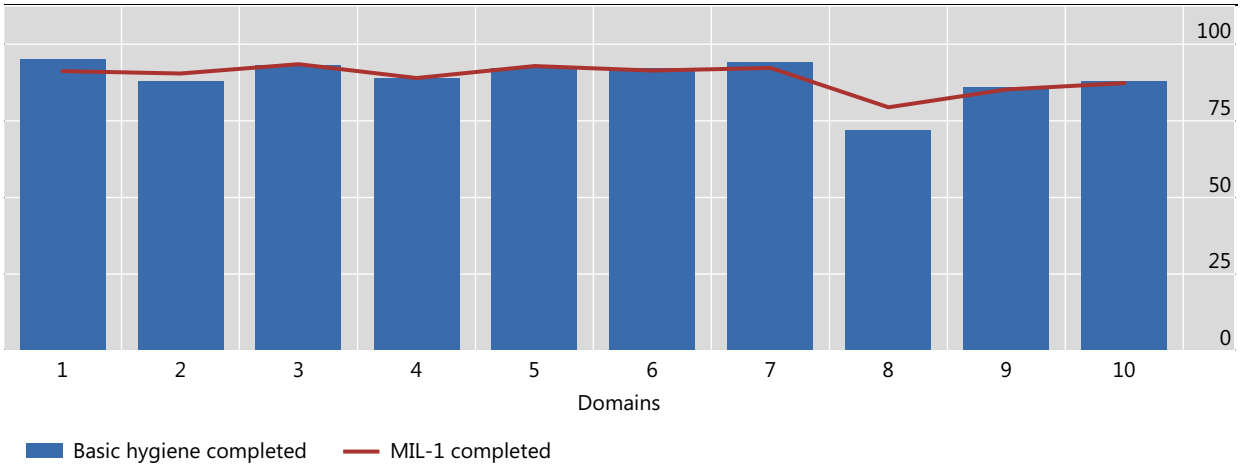
To illustrate with a practical example how the aggregate findings in a benchmarking group can be used, Graph A1 below gives an indication of the foundational levels of cyber resilience from our central bank pilot group across ten domains. The scores reflect the basic hygiene questions in the CRA as well as the completed practices in every domain. When looking specifically at the basic hygiene questions and the completed practices in ten domains represented by maturity indicator level 1 (MIL-1), we can observe that there is a close relationship between the performance of basic hygiene and completeness of practices. When organisations use the CRA outcomes to make improvements, the foundational level of practices provides a good starting point for the first improvement efforts. The CRA has four additional levels of cyber resilience capabilities to help assess the maturity of performance of organisations in the ten domains.

Risk-based decisions on improvements

The CRA methodology provides a structured and consistent way to work on cyber resilience improvements of an organisation's critical business services. The outcomes can be used by an organisation to inform how it performs against its objectives in the different domains and how to address potential gaps thus helping an organisation to understand and decide the appropriate levels of investment in the different domains. It is important to note that the outcomes themselves do not prescribe to invest more – or less – in a domain, this will require risk-based decision making by the organisation. Benefits in wider adoption of benchmarking practices include allowing a comparison with not only general industry practices but also their relevant peer organisations. The more comparable the benchmarking is for an organisation, the more meaningfully it can inform the risk-based decision-making processes in organisations. As the CRA methodology is publicly available, the materials are accessible for any organisation that is interested in performing a similar assessment on a critical business service.

Basic hygiene completed practices and MIL-1 completed practices

In per cent — Graph A1



Domains 1 = asset management; 2 = controls management; 3 = configuration and change management; 4 = vulnerability management; 5 = incident management; 6 = service continuity management; 7 = risk management; 8 = external dependencies management; 9 = training and awareness, 10 = situational awareness. MIL-1 = maturity indicator level 1.

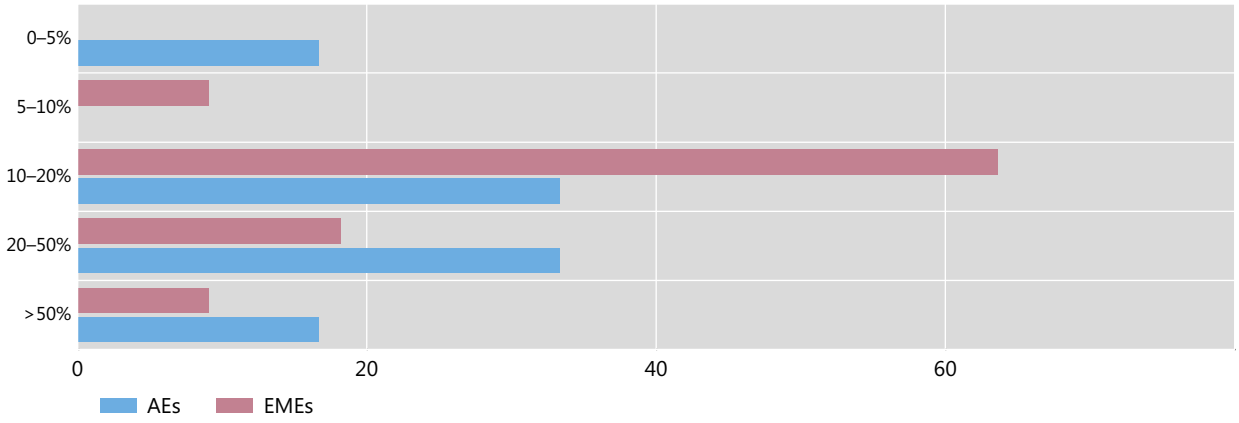
Source: Authors' calculations.

The BIS Innovation Hub (BISIH) can also play an important role in developing technologies that address cyber threats relevant for central banks and the broader financial sector. A Secure Coding Competition was hosted by the Swiss Centre and the BIS Cyber Resilience Coordination Centre in the last quarter of 2020 as an informal and friendly coding training for central banks. It attracted around 60 developers from more than 20 central banks who competed to develop their skills across multiple programming languages.

Several other projects are underway. The BISIH Eurosystem centre is currently investigating the implications of post-quantum cryptography for payment systems. This project aims to investigate and test potential cryptographic solutions that can withstand the vastly improved processing power of quantum computers. The goal is to test use cases in various payment systems and examine how the introduction of quantum-resistant cryptography will affect their performance. Project Sela in Hong Kong centre explores the technical implementation of a cyber secure two-tier retail Central Bank Digital Currency (CBDC) architecture together with Bank of Israel and Hong Kong Monetary Authority. Project Polaris in the Nordic centre explores resilience and security issues related to using CBDCs offline. By providing a platform for collaboration these BISIH initiatives aim also to reduce costs. The introduction of central bank digital currency (CBDCs) could in fact add to the complexity of the IT environment and necessitate greater resources devoted to cyber security (Graph 8).

Estimated increase in cyber budgets due to CBDC

As a percentage of respondents — Graph 8



The graph reports the share of respondents that selected each respective answer to the question "Would the introduction of a CBDC require a substantial increase in your cyber security budget?".

Source: Authors' calculations.

The resilience of Financial Market Infrastructures (FMIs), to cyber risks among others, is a decisive factor in the overall resilience of the financial system and the broader economy. This is recognised in the 2016 CPMI-IOSCO guidance to the Principles for Financial Market Infrastructures (PFMI) on cyber resilience – the first internationally agreed guidance on cyber security for the financial industry. Given the high degree of interconnectedness in the FMI ecosystem, the CPMI together with IOSCO will continue to engage with a wide range of relevant industry stakeholders in

promoting the effective use of the CPMI-IOSCO cyber guidance and fostering cross-border and cross-sectoral approaches.

More generally, cooperation and effective information-sharing are key to reducing cyber risk collectively, preventing major cyber incidents and containing them quickly should they occur. Much international work has been conducted or is ongoing, including by standard-setting bodies, the FSB and G7.[11]

6. Conclusion

Cyber attacks are becoming more frequent, and they continue to evolve in terms of their complexity and sophistication. At the same time, there are significant shifts in technology in the financial sector and within central banks, notably cloud adoption and increased remote working.

This paper discusses cyber risk priorities and challenges from the perspective of experts and practitioners in central banks for their own operations, including the critical financial market infrastructures they operate.

Using the results of a survey of the Global Cyber Resilience Group, we show that central banks have notably increased their cyber security-related investments since pandemic, with a priority on technical security control and resiliency. Central banks see phishing and social engineering as the most common methods of attack, and the potential losses from a systemically relevant cyber attack are deemed to be large, especially if the target is a big tech providing critical cloud infrastructure.

Combined, these factors have important implications for cyber security strategies in central banks. These strategies are shifting away from a compliance focus and are embracing risk management and resiliency concepts. They are also taking into account the more pervasive nature of attacks by adopting zero-trust models, a concept that acknowledges the blurring of organisational physical and digital boundaries.

Generally, respondents judge the preparedness of the financial sector for cyber attacks to be inadequate. While central banks in most EMEs provide a framework for the collection of information on cyber attacks on financial institutions, less than half of those in AEs do.

Cooperation among public authorities, especially in the international context, could improve central banks' ability to respond to cyber attacks. The CPMI-IOSCO guidance on cyber resilience for FMIs represents an important benchmark for governance, business continuity management and identification of the sources of operational risk. Much international work has been conducted by standard-setting bodies, the FSB and the G7. The BIS's Cyber Resilience Coordination Centre provides a structured approach to knowledge-sharing, collaboration and operational readiness among central banks in the areas of cyber resilience. Finally, by providing a platform for collaboration between central banks, regulatory authorities, financial institutions, technology firms and cyber security experts, the BIS Innovation Hub aims to facilitate

[11] Besides CPMI-IOSCO (2016), see Basel Committee on Banking Supervision (2018); Basel Committee on Banking Supervision (2021); Financial Stability Board (2020); and G7 (2016).

the development of specific projects to limit cyber threats for central banks and the broader financial sector.

References

Aldasoro, I., Frost, J., Gambacorta, L., Leach, T. and Whyte, D. (2020): "Cyber risk in the financial sector", *SUERF Policy Note*, Issue No. 206.

Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T. (2022): "The drivers of cyber risk", *Journal of Financial Stability*, vol 60, p. 100989.

AXA (2021): "AXA Future Risks Report 2021", September.

Basel Committee on Banking Supervision (2018): "Cyber-resilience: Range of practices", December.

Basel Committee on Banking Supervision (2021): "Newsletter on cyber security", September.

Biener, C., Eling, M. and Wirfs, J.H. (2015): "Insurability of cyber risk: An empirical analysis", *The Geneva Papers on Risk and Insurance-Issues and Practice*, vol 40(1), pp.131-158.

Boissay, F., G. Cornelli, S. Doerr and J. Frost (2022): "Blockchain scalability and the fragmentation of crypto", BIS Bulletin, no 56.

Chande, N. and Yanchus, D. (2019): "The cyber incident landscape", *Staff Analytical Note,* No. 2019-32*,* Bank of Canada.

Cornelli, G, J Frost, L Gambacorta, R Rau, R Wardrop and T Ziegler (2020a): "Fintech and big tech credit: a new database" BIS Working Papers, 887

Cornelli, G., S. Doerr, L. Gambacorta and O. Merrouche (2020): "Inside the regulatory sandbox: effects on fintech funding", BIS Working Paper, no 931.

CPMI-IOSCO (2016): "Guidance on cyber resilience for financial market infrastructures", June.

De Beck, C. (2021), "IBM X-Force Report: No shortage of resources aimed at hacking cloud environments", *Security Intelligence,* 15 September.

Doerr, S., Gambacorta, L., and J.-M. Serena Garralda (2021): "Big data and machine learning in central banking", BIS Working Paper, no 930.

Duffie, D. and Younger, J. (2019): "Cyber runs", *Hutchins Center Working Paper No. 51.* Brookings.

Eisenbach, T.M., Kovner, A. and Lee, M.J. (2021): "Cyber risk and the US financial system: A pre-mortem analysis", *Journal of Financial Economics.*

ENISA (2021): "NIS Investments", November.

Financial Stability Board (2018a): "Cyber Lexicon", November.

Financial Stability Board (2020): "Effective Practices for Cyber Incident Response and Recovery: Final Report", October.

Frost, J, L Gambacorta, Y Huang, HS Shin, and P Zbinden (2019): "BigTech and the changing structure of financial intermediation", Economic Policy, 34(100): 761–99.

G7 (2016): "Fundamental elements of cybersecurity for the financial sector", October.

Kamiya, S., Kang, J.K., Kim, J., Milidonis, A. and Stulz, R.M. (2021): "Risk management, firm reputation, and the impact of successful cyberattacks on target firms", *Journal of Financial Economics,* vol 139, pp. 719-749.

Kashyap, A.K. and Wetherilt, A. (2019): "Some principles for regulating cyber risk", *AEA Papers and Proceedings*, vol 109, pp. 482-87.

Kopp, E, L Kaffenberger, and C Wilson (2017): "Cyber risk, market failures, and financial stability", International Monetary Fund.

Microsoft (2021): "Microsoft Digital Defence Report", October.

Prenio, J., Yong, J and Kleijmeer, R. (2019): "Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions", *FSI Insights,* No. 21.

Upton, D.M. and Creese, S. (2014): "The danger from within", *Harvard business review*, vol 92, pp.94-101.

Verizon (2021): "DBIR 2021 Data Breach Investigations Report", May.

Wolff, J. and Lehr, W. (2017): "Degrees of Ignorance about the Costs of Data Breaches: What Policymakers Can and Can't Do about the Lack of Good Empirical Data", SSRN.

Previous volumes in this series

1038 September 2022	Building portfolios of sovereign securities with decreasing carbon footprints	Gong Cheng, Eric Jondeau and Benôit Mojon
1037 August 2022	Big Techs vs Banks	Leonardo Gambacorta, Fahad Khalil and Bruno M Parigi
1036 August 2022	The scarring effects of deep contractions	David Aikman, Mathias Drehmann, Mikael Juselius and Xiaochuan Xing
1035 July 2022	Cross-border financial centres	Pamela Pogliani and Philip Wooldridge
1034 July 2022	Debt sustainability and monetary policy: the case of ECB asset purchases	Enrique Alberola, Gong Cheng, Andrea Consiglio and Stavros A Zenios
1033 July 2022	The Holt-Winters filter and the one-sided HP filter: A close correspondence	Rodrigo Alfaro and Mathias Drehmann
1032 July 2022	Capital flows and monetary policy trade-offs in emerging market economies	Paolo Cavallino and Boris Hofmann
1031 July 2022	Risk capacity, portfolio choice and exchange rates	Boris Hofmann, Ilhyock Shim and Hyun Song Shin
1030 July 2022	Mis-allocation within firms: internal finance and international trade	Sebastian Doerr, Dalia Marin, Davide Suverato and Thierry Verdier
1029 July 2022	Bank of Japan's ETF purchase program and equity risk premium: a CAPM interpretation	Mitsuru Katagiri, Junnosuke Shino and Koji Takahashi
1028 July 2022	Fiscal deficits and inflation risks: the role of fiscal and monetary regimes	Ryan Banerjee, Valerie Boctor, Aaron Mehrotra and Fabrizio Zampolli
1027 July 2022	What drives repo haircuts? Evidence from the UK market	Christian Julliard, Gabor Pinter, Karamfil Todorov and Kathy Yuan
1026 June 2022	Monetary policy announcements and expectations: the case of Mexico	Ana Aguilar, Carlo Alcaraz Pribaz, Victoria Nuguer and Jessica Roldán-Peña
1025 June 2022	Communication, monetary policy and financial markets in Mexico	Ana Aguilar and Fernando Pérez-Cervantes
1024 June 2022	Forward guidance and expectation formation: A narrative approach	Christopher S Sutherland

All volumes are available on our website www.bis.org.