IOPS Working Papers on Effective Pensions Supervision, No.37

Supervisory approaches to enhancing cyber resilience in the private pension sector: High-level summary of Members responses to the questionnaire

Nina Paklina
October 2021

IOPS WORKING PAPERS ON EFFECTIVE PENSIONS SUPERVISION

As the proportion of retirement income provided by private pensions becomes increasingly important, the quality and effectiveness of their supervision becomes more and more crucial. The IOPS Working Paper Series, launched in August 2007, highlights a range of challenges to be met in the development of national pension supervisory systems. The papers review the nature and effectiveness of new and established pensions supervisory systems, providing examples, experiences and lessons learnt for the benefit of IOPS members and the broader pensions community.

IOPS Working Papers are not formal publications. They present preliminary results and analysis and are circulated to encourage discussion and comment. Any usage or citation should take into account this provisional character. The findings and conclusions of the papers reflect the views of the authors and may not represent the opinions of the IOPS membership as a whole.

IOPS WORKING PAPERS
ON EFFECTIVE PENSIONS SUPERVISION
are published on www.iopsweb.org

SUPERVISORY APPROACHES TO ENHANCING CYBER RESILIENCE IN THE PRIVATE PENSION SECTOR

High-level summary of Members' responses to the questionnaire

Nina Paklina*

ABSTRACT

The reports looks at the main cyber threats and trends observed in regard to cyber incidents in the private pension field in recent years and during the Covid-19 period. It highlights supervisory practices that contribute to effective cyber security risk supervision in the private pension sector. Authorities from thirty six IOPS Members' jurisdictions participated in the survey.

The report reviews recent regulations on cyber security, especially covering private pensions entities. The report includes supervisory views and assessment of cyber risk management practices by pension entities and identifies a number of areas that require greater attention.

Supervisors are generally adopting a cross-sectoral approach to cyber threats. The report focuses on supervisory initiatives put in place to better monitor emerging cyber threats and measures directed to improve entities' operational resilience and cyber risk management by means of supervisory guidance, self-assessment frameworks, supervisory examinations, audits, reporting and use of cyber threat intelligence.

Finally, the report offers key findings and conclusions to strengthen cyber security under the current environment impacted by coronavirus pandemic.

Keywords: cyber threats, pension supervision, private pensions, risk management

JEL codes: J-32, G-38, G-28

* International Organisation of Pension Supervisors (IOPS).

Contents

Supervisory approaches to enhancing cyber resilience in the private pension sector 5

Background 5
Introduction 6
1. Cyber security strategy 9
2. Cyber threats in private pensions and related supervisory challenges 11
3. Regulations 14
4. Management of cyber risk by pension entities 18
5. Supervision of pension funds' cyber risk-management frameworks 22
5.1 Thematic surveys 23
5.2 Supervisory guidance with respect to cyber security 23
5.3. Supervisory cyber maturity self-assessment framework 25
5.4 Supervisory examinations – off-site and on-site inspections on cyber security 27
5.5 Post-inspection actions by supervisory authorities 31
5.6 Supervisory requirements for the conduct of external audits and assessments 31
5.7 Notification mechanisms for information security incidents 32
5.8 Supervisory sanctions 34
5.9 Supervisory knowledge on cyber security 35
6. Co-operation and information sharing 36
6.1 Co-operation at the national and international levels 36
6.2 Co-operation and information sharing with national or sectoral response teams 38
6.3 Increasing awareness with the industry 40
Key findings and conclusions 42
References 46
Annex 1 48

Boxes

Box 1. Regulations on cyber security for the financial sector, including private pensions 15
Box 2 The DNB assessment framework of information security maturity for financial institutions ... 26

Supervisory approaches to enhancing cyber resilience in the private pension sector

Background

The current project[1] on supervisory approaches to enhancing cyber resilience in the private pensions sector is part of the IOPS 2019-2020 Programme of Work, pursuant to the IOPS work stream on digitalisation[2]. In view of substantial risks posed by cyber attacks for financial institutions in general and, in this particular case, for pension entities, Members discussed over the course of several meetings supervisory measures and approaches to cyber security for private pensions. Work on the project was suspended temporarily after the outbreak of the Covid-19 pandemic at the end of 2019 and the urgent need for supervisors to focus on the challenges related thereto. Work on the project was subsequently resumed in July 2020.

This document contains a high-level summary of IOPS Members' responses to the survey[3]. Authorities[4] from thirty six (36) Members participated in the survey.

The report reviews supervisory experiences and approaches to assess the preparedness of financial institutions regarding cyber threats and to help institutions, including trustees and pension fund management companies, to mitigate, effectively respond to, and recover from cyber risk incidents. These initiatives may serve as guidance for other supervisory authorities.

[1] This project is Member-driven. The following IOPS Members Authorities from Austria; Chile; Hong Kong, China; Hungary; Kenya; Mexico and Turkey served as Project Team Members.

[2] In early 2019, IOPS published its first stocktaking report - IOPS WP 33 *Impact of the digitalisation of financial services on supervisory practices in the private pension sector*; as well as Case studies from: Hong Kong, China/Kenya/Mexico, 2019, www.iopsweb.org

[3] The questionnaire on cyber supervisory initiatives was prepared by the Project team members and sent to Members for completion in August 2020.

[4] www.iopsweb.org: Angola; Australia; Austria; Botswana; Brazil; Bulgaria; Canadian Association of Pension Supervisory Authorities (CAPSA); Chile; China; Colombia; Costa Rica; Croatia; Czech Republic; France; Germany; Honduras; Hong Kong, China; Hungary; Iceland; India; Ireland; Jamaica; Kenya; Republic of North Macedonia; Malawi; Mexico; Morocco; the Netherland; Poland; Portugal; Romania; Serbia; Slovak Republic; Turkey; Ukraine and Zimbabwe.

Introduction

Cyber security threats and attacks are evolving rapidly and are affecting all sectors of the economy. The frequency and potential impact of cyber attacks continues to increase as cyber attackers gain skills and technological sophistication[5]. The financial sector, together with the retail sector, are among the primary targets of cyber attacks. In view of the increasing use of various forms of outsourcing and partnerships in the financial sector, the associated opportunities and risks for information security and cybersecurity are also rising.

According to research conducted by the IMF in 2018, the damage to the global financial system caused by cyber attacks was estimated at around USD 100 billion annually[6]. The same research and supervisory sources[7] show that cyber risk has become one of the major concerns among emerging risks that financial firms have to manage.

In recent years, financial institutions, including private pension entities, have been relying increasingly on innovative technologies to develop new information technology (IT) solutions. These technologies have included customer-cycle digitalisation, data storage with external providers, and an increased use of cloud-based arrangements to enhance business processes and administrative efficiency. The growing interconnectedness of companies in the financial sector and the high dependence on their IT systems raises the vulnerability to and the potential scope of cyber attacks.

The Covid-19 pandemic has caused unprecedented disruption across all sectors and has also been a major challenge for the operational resilience of financial institutions, including pension funds. Restrictions on social mobility have forced financial institutions and pension companies to rapidly adjust to new ways of doing business. While critical services have been maintained, key processes have had to be changed to support customers and fund members in the wake of lockdown measures. In particular, the lengthy Covid-19 pandemic lockdown and post-lockdown periods have left financial service providers with few alternatives to expanding the pace and scope of digitalisation to provide information and services on-line, with staff working remotely from home and clients connecting via phone and digital channels. Digitalisation brings many benefits, but also brings a range of security concerns[8], including among others the capacity of virtual private networks to support remote working, the security of the information accessed remotely, and the security of the remote channels used by employees and customers/members. The evidence is clear that financial institutions of all types have become exposed to significant cyber threats.

While the pandemic certainly increased reliance on digital connectivity and the associated exposure to potential cyber threats, retirement schemes and pension services providers were considered to be susceptible to cyber risks, even before the pandemic, although perhaps to

[5] DNB annual report, 2019

[6] IMF WP/18/143, Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx

[7] http://www.iopsweb.org/membership/iops-members-observers.htm

[8] APRA Chair Wayne Byres – Remarks to the BCBS outreach meeting on operational resilience, https://www.apra.gov.au/news-and-publications/apra-chair-wayne-byres-remarks-to-bcbs-outreach-meeting-on-operational

a lesser extent than banks or other providers of payment services. Pension schemes hold a large volume of members' personal data[9] and assets[10], making them an attractive target for cyber criminals. Successful cyber attacks could have serious consequences for the pension companies, pension scheme members and beneficiaries. Individuals may suffer losses of their personal data and/or financial assets. For pension companies, cyberattacks may cause operational issues such as service disruption and business interruption, loss of member data, failure to deliver a financial promise, and non-compliance with fiduciary duties. These developments may, in turn, prompt regulatory action, as well as ombudsman complaints, litigation, loss of reputation or, in the worst-case scenario, failure of the business.

The answers to the IOPS survey point to differences across jurisdictions in the degree to which their private retirement systems might be exposed to cyber security incidents. Similarly, supervisory focus on this risk area may also vary by jurisdiction. The first reason for such differences may be linked to the maturity of private pension systems. Another important distinction relates to differences between occupational and employer-based arrangements versus personal (individual-based) arrangements. Occupational and employer-based arrangements may be less exposed to cyber risks because their major stages of distribution and communication take place directly between the employer and providers. By contrast, individual-based pension arrangements rely more heavily on on-line marketing, distribution, and communication channels with members.

The potential exposure of private retirement systems to cyber risks depends as well on factors in the operating environment, such as the degree of innovative technology development and its use in the private pension markets, which also tends to vary considerably across jurisdictions.

Cyber security is a major public concern and an area of increased supervisory attention at the national and international levels. The gravity and the scale of cyber security incidents and threats have urged leading international and regional organisations to develop important work on the subject, including standards and guidelines for the management of cyber risks in the financial sector. Examples include the G7 'Fundamental Elements of Cybersecurity for the Financial Sector' (2016); CPMI-IOSCO 'Guidance on cyber resilience for financial market infrastructure' (2016); OECD 'Recommendation of the Council on Digital Security of Critical Activities' (2019); the EU legislative proposal - 'Digital Operational Resilience Act' (DORA), as part of the 2020 EU Digital finance package[11], and work by European Supervisory Authorities (ESAs) and EIOPA[12].

[9] Pension schemes hold important personal information such as records of each member's name, address, national ID number, date of birth, salary information, etc. They may also hold private information on members' health issues and information about family members. For beneficiaries and members of DC pension funds, pension schemes may also hold financial information (bank details)

[10] OECD, Pension Markets in Focus, 2020 https://www.oecd.org/pensions/pensionmarketsinfocus.htm

[11] EUR-Lex - 52020PC0595 - EN - EUR-Lex (europa.eu)

[12] EIOPA 'Opinion on the supervision of the management of operational risks faced by IORPs', July 2019, https://www.eiopa.europa.eu/content/opinion-supervision-management-operational-risks-faced-iorps_en

At the national level, governments are adapting their cyber strategies and setting up dedicated national agencies to strengthen the cyber security of national critical infrastructure and ensure more comprehensive security in cyberspace. In a number of jurisdictions, supervisory authorities are developing their own cyber security strategies. They cite improvement of cyber resilience in the financial sector among their supervisory priorities and strategic objectives. In view of the evolving nature of cyber-attacks, as evidenced during the Covid-19 pandemic crisis, supervisors are likely to further strengthen and intensify their supervisory attention and interventions. In particular, cyber security and the information security of outsourced activities will be given more prominent attention.

The survey finds that **supervisors are generally adopting a cross-sectoral approach to cyber threats.** As cybersecurity threats and incidents are affecting the entire financial sector, supervisors most often take measures that cover several financial industries. That said, in some jurisdictions, authorities have developed **cyber security regulations and cyber supervisory initiatives specific for the pension sector,** drawing on and using the experiences and approaches developed in other financial sectors, especially in banking supervision. Close co-operation between banking and other financial sector regulators and supervisors is also being developed.

The survey results indicate that, similar to practices in other supervisory areas, when addressing cyber risk, **supervisors commonly apply the following four key principles: risk-based supervision[13] (RBS), technological neutrality, proportionality and integrity[14].** The RBS approach provides for supervisory assessment of the level of risk that entities face, which is then used to guide the nature and intensity of the supervisory response. The principle of technological neutrality assumes that entities and issues are treated according to the risk they pose and not according to the technology used *per se*. Supervisors are also deploying a proportionate approach, whereby the frequency and depth of interventions is in line with their supervisory priorities and prudential objectives. The spectrum of supervisory interventions ranges from "light", as in providing communication and guidance for all firms, to more "intensive" actions such as issuing supervisory binding guidance and circulars, imposing requirements for the appointment of external auditors and the conduct of self-assessments reviews, undertaking on-site and off-site inspections, etc. Effective risk management frameworks and good governance by supervised entities are key supervisory requirements and are the cornerstones of supervisory prudential provision.

Improving cyber security in the financial sector also requires close co-operation and information sharing, not only among financial sector supervisors but also involving public enforcement agencies and specialised authorities responsible for cyber security at the national and industry levels. Co-operation at the international level with international peers

EIOPA' IT and Cyber Security Project Group is in the process of finalising EIOPA Information and Communication Technology (ICT) guidelines, https://www.eiopa.europa.eu/content/eiopa-finalises-guidelines-information-and-communication-technology-security-and-governance_en;

EIOPA Guidelines on outsourcing to cloud service providers, 6 February 2020; https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers-now-available-national-supervisory_en

[13] IOPS Principles of Private Pension Supervision: http://www.iopsweb.org/principlesguidelines/IOPS-principles-private-pension-supervision.pdf

[14] BaFin Annual Report 2019, Annual report – BaFin, https://www.bafin.de

(supervisors) appears critical to addressing cross-border threats and sharing experience and best practices.

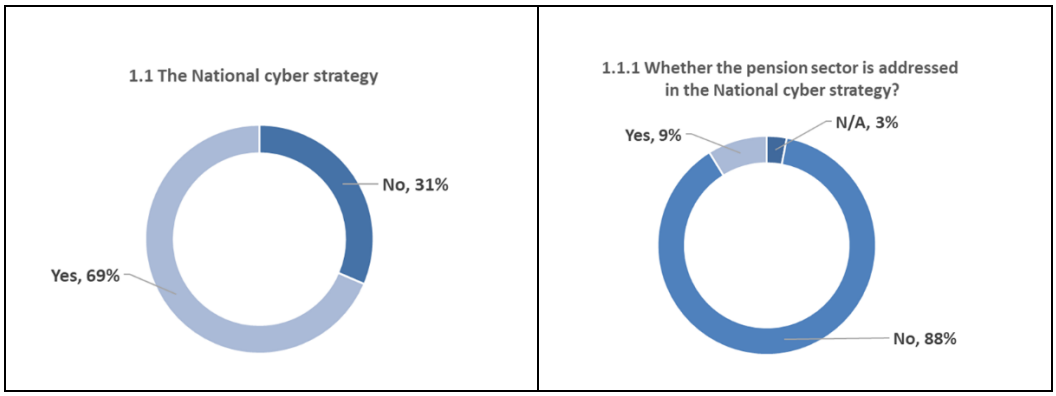
The report looks at supervisory approaches taken to help financial institutions, including pension entities, to mitigate, effectively respond to, and recover from cyber risks. Information on cyber risks related to private pensions is not always available but, where possible, the report aims to identify approaches and developments that are pertinent to private pensions.

1. Cyber security strategy

The survey follows a top-down approach to understand the development of supervisory strategies and approaches to strengthen cyber resilience in financial sectors, including private pensions.

Of the thirty-six respondents, twenty-four replied that the **national cyber security strategy was published** (Figure 1.1). Such strategies could be complemented by other legislation, including military laws that cover cyber defence provisions, as in France. In most respondent jurisdictions, **the pension sector was not specifically addressed in the national cyber security strategy**. In Turkey, for example, 'banking and finance' are listed in the strategy as a critical sector where security measures must be taken, but the private pension sector has not been specifically addressed. Only three authorities[15] indicated that their pension sectors, as part of the financial system being designated critical infrastructure, was included within the national strategies.

Figure 1.1



Source: Members responses to the IOPS 2020 survey

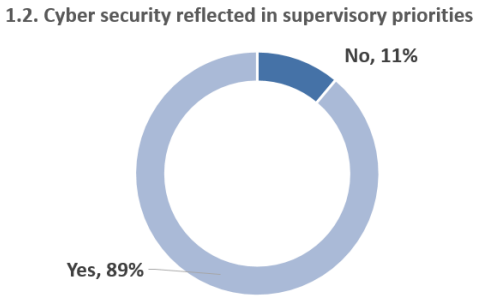
Twenty-six members **put in place IT or cyber supervisory initiatives to address cyber risk in the financial sector.** Such initiatives generally cover the entire financial sector (18 respondents) and many are specific to the private pension sector (12). Eleven Members noted their intention to develop such initiatives within the next 12 months.

A large majority of the respondent authorities (32) confirmed **that cyber security was included among their supervisory priorities** (Figure 1.2). Only four authorities stated that cyber issues were not listed among their priorities.

[15] Australia; India; Morocco.

Several supervisors have developed their own strategies on digitalisation or cyber security. They include, among others, APRA (Australia)[16], the FSC (Bulgaria), BaFin (Germany), the Central Bank of Hungary. In Australia, APRA's Corporate Plan[17] for the period 2019-2023 identified improving cyber-resilience in the financial sector among its four strategic focus areas. When reviewed in light of the Covid-19 pandemic, APRA's Corporate Plan for 2020-2024 reconfirmed and maintained its commitment to improving the cyber resilience of Australia's financial system. APRA's supervisory priorities for 2021 highlight the increased scrutiny placed on the cyber security capabilities of financial entities.

Figure 1.2.



Source: Members responses to the IOPS 2020 survey

In light of the on-going Covid-19 crisis and the new challenges it brought to private pension entities in relation to cyber security, **supervisory initiatives were put in place in 20 respondent jurisdictions specifically to mitigate the pandemic impact in the area of cyber/ICT risks**. These initiatives included the following recommendations for pension companies and actions[18] for supervisors:

Pension companies should:

- Re-evaluate contingency plans (Bulgaria; Iceland)
- Review new emerging risks, including cyber risks (Bulgaria)
- Strengthen information security and cyber security measures to operate under current exceptional circumstances (Colombia)
- Put in place mitigation plans to ensure security of electronic transfers to account holders (Costa Rica)

[16] https://www.apra.gov.au/news-and-publications/executive-board-member-geoff-summerhayes-speech-to-financial-services

[17] https://www.apra.gov.au/news-and-publications/apra-releases-2019-2023-corporate-plan

[18] For more information on pension supervisory measures to address Covid-19 pandemic crisis, see the IOPS Statement of 26 May 2020: http://www.iopsweb.org/iopsmembersmeasurestakentoaddressthecovid-19crisis.htm

- Establish an ad-hoc reporting on impacts of the Covid-19 pandemic on pension companies, including cyber risks to ITC system and related business continuity management (BCM) processes

Actions by Pension supervisors included:

- Issuing recommendations for extra security measures on official websites
- Developing new guidelines on remote working (Hungary[19]; Mexico)
- Conducting off-site inspections (supported by development of methodology for conducting supervisory inspections remotely)
- Organising meetings to inform and raise awareness on strengthening security protocols (Chile)
- Reminding the supervised entities of critical importance to manage cyber risks (Costa Rica; Hong Kong, China) and taking appropriate control measures
- Taking special measures with regard to potential pension scams that emerged during Covid-19 pandemic
- Educating supervisory staff

In contrast, one-third of the authorities responded that the Covid-19 pandemic crisis had no significant impact on their supervisory initiatives regarding cyber security.

2. Cyber threats in private pensions and related supervisory challenges

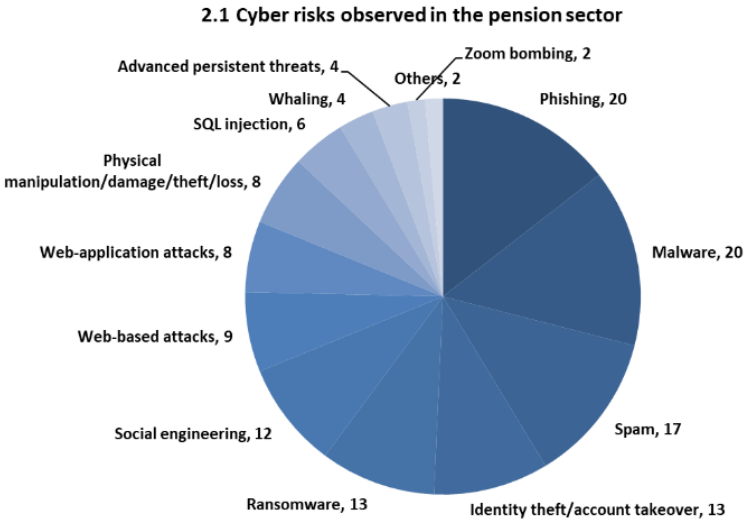
The IOPS survey attempted to gather information on cyber threats and types of cyber attacks to which pension entities have been exposed in the past and, more recently, during the Covid-19 pandemic crisis.

Although some authorities do not collect or do not have meaningful data or information on cyber security threats in the private pension sector, twenty-two authorities did provide feedback on the key cyber risks observed in their private pension sectors. It is assumed that such threats or attacks are also present in other parts of the financial sector, including, for example, the insurance sector. **The most common cyber security incidents outlined by Members are phishing, malware, spam, identity thief and account takeover, ransomware, and social engineering. (Figure 2.1)**. In relation to IT security and cyber incidents, supervisors highlighted the issue of internal weaknesses within financial institutions that allowed successful cyber attacks from external parties. In some cases, the vast majority of IT security incidents experienced by financial entities were, in fact, attributable to internal failings within the institutions themselves and only a small number of these incidents came from external attacks[20].

[19] https://www.mnb.hu/letoltes/12-2020-recommendation-of-teleworking.pdf

[20] BaFin, Supervisory priorities for 2020.

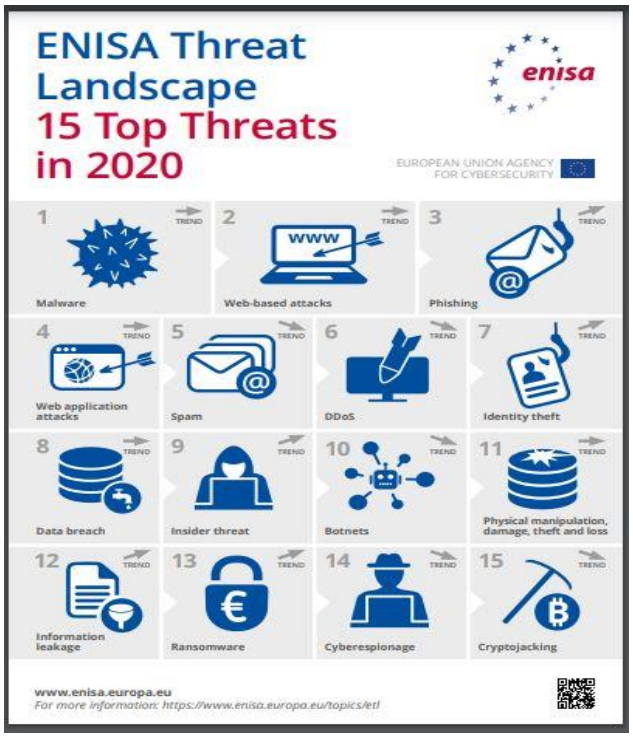
Figure 2.1



Source: Members responses to the IOPS 2020 survey

Similar key threats were highlighted by the European Union Agency for Network and Information Security (ENISA) Threat Landscape in its 15 Top Threats in 2020 (Figure 2.2)

Figure 2.2. ENISA Threat Landscape. 15 Top Threats in 2020



Source: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape-2020-top-15-threats

The most common cyber attacks in the financial sector listed in the previous ENISA report[21] published in 2019 were: malware (1st place); web-based attacks (2nd place); phishing (4th place); spam (6th place); data breaches owing to physical theft or loss of devices (8th place); physical manipulation/damage/theft/loss, all of which ranked in the top 10. The ENISA foresees that phishing attacks conducted by organised criminal groups will become increasingly targeted and persistent, threatening financial accounts or sensitive business data or even data stored by public authorities[22].

Another threat identified both by the ENISA and by a number of pension supervisory authorities participating in the IOPS survey relates to **increased outsourcing to external service providers.** This risk is linked, in particular, to increased deployment of cloud solutions.

Cloud-based solutions are becoming mainstream products in the financial sector[23]. In the private pensions area, an increasing number of pension funds are using cloud computing for administrative purposes (data/information storage and processing) as well as to transfer their IT infrastructure and IT services in the cloud through their network[24]. For example, the Austrian FMA Digitalisation report[25] (2019) shows that cloud services have been used by almost half of the supervised entities, with a further fifteen percent planning to use cloud infrastructure in the coming three years.

A key question concerning cloud computing is its security. As noted in the 2019 ENISA report, security policies of cloud providers need to be further strengthened: some seventy-three percent of providers had misconfigurations in their security policies that could lead to a data breach[26]. Also, the report underlines the high levels of interest cyber criminals appear to be showing to cloud infrastructure.

The potential threats notwithstanding, **about half (17) of respondents did not observe or report specific attacks** or **cyber threats to which pension entities were exposed during the Covid-19 pandemic.** Several reasons were proposed. Authorities were not collecting data (as no cyber incident reporting mechanisms for the pension sector had yet been established), or they were not aware of any specific attacks during this period, as data for 2020 was not yet available. Some authorities (as Prudential Supervisory and Resolution Authority (ACPR) of France) reported that pension entities were subject to the same vulnerabilities as other financial companies. A number of authorities (8) were able to bring

[21] The ENISA Threat Landscape Report 2018, published in January 2019 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[22] The European Union Agency for Network and Information Security (ENISA) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[23] Gartner survey of senior finance executives foresees that by 2020, 36 percent of enterprises will use the cloud to support more than half of their transactional systems of record; https://www.gartner.com/en/newsroom/press-releases/2017-09-13-gartner-says-finance-is-moving-to-the-cloudmuch-faster-than-expected.

[24] IOPS Working Paper No. 33, www.iopsweb.org

[25] FMA Austria, Digitalisation in the Austrian financial market

[26] ENISA Report, January 2019

some specific evidence and examples related to the pension sector[27]. **The most commonly reported types of cyber attacks in the pension sector during the Covid-19 pandemic were**:

- spam mails
- phishing attacks, as well as other social engineering attacks tailored to Covid-19
- identity theft attempts to register for and access a member's bank account
- fraudulent activities in relation to individual pension accounts through pension companies' websites
- malware programmes (some schemes and custodian data have been hacked and corrupted, Kenya)
- distributed denial-of-service attacks (DDoS) (Mexico, the Netherlands)
- zoom booming, especially during video conferences (Kenya)

Members were invited to offer their views on the **general trends** observed in regard to cyber incidents in the private pension field in recent years and during the Covid-19 period. **The findings were not entirely consistent**. Slightly less than half of the respondents reported that cyber attacks have increased in recent years on a continuing basis, both in frequency and complexity, but have not resulted in significant material losses, whereas the other half expressed the view that the pension sector either has not seen an increase in cyber attacks or has mostly stayed at the same level. Supervisors generally noted an **increased sophistication of cyber attacks in the financial sector**. In jurisdictions where supervisors flagged **increased cyber attacks** against pension entities, the attacks **have not generally resulted in significant material incidents affecting member balances or the integrity of pension funds**.

Similar answers were provided in relation to whether the Covid-19 crisis led to an increase in cyber incidents. Thirteen respondents reported an increase in cyber incidents attributed mainly to working from home. Conversely, fifteen respondents did not observe any increase in cyber incidents or did not receive reports indicating significant changes in the frequency of major incidents, including cyber incidents. The Czech Central Bank stated that cyber incidents were in line with the trend before the onset of the pandemic. The ACPR (France) noticed that, while the remote working mode had the potential to increase the vulnerability of financial sector, it did not actually lead to an increase in the number of incidents. The Dutch supervisor (DNB) reported that the attack frequency has increased, but this has not resulted in any significant change in the successfulness of attacks.

3. Regulations

Recognising a growing threat posed by cyber crime, supervisory authorities in a number of jurisdictions have undertaken work to review or introduce pension or financial market regulations and standards to address FinTech developments and account for cyber threats.

Thirteen jurisdictions have, in fact, adopted such regulations or regulatory standards on information security and IT. The measures adopted generally cover the entire financial sector, including private pensions. Regulatory measures have generally taken the form of

[27] Australia; Chile; Costa Rica; Kenya; Republic of North Macedonia; Mexico; Morocco; the Netherlands

principles-based or risk-based guidance, aligned with the risks in the industry and jurisdiction. This allows them to fit into the new, digital financial environment and leave space for innovation.

Box 1. Regulations on cyber security for the financial sector, including private pensions

Australia – On 1 July 2019, APRA adopted the new cross-industry Prudential Standard CPS 234: Information security focused on information security management. APRA also issued Prudential Practice Guide CPG 234 on the implementation of the Prudential Standard. This new standard sets out the following requirements: clearly define information-security related roles and responsibilities; maintain information security capabilities commensurate with the size and extent of threats to their information assets; implement controls to protect information assets and undertake regular testing and assurance of effectiveness of controls; and promptly notify APRA of material information security incidents and material information security control weakness which will not be able to be remediated in a timely manner.

Requirement in CPS 234 in relation to third party arrangements came into effect on 1 July 2020.

https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf; https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_1.pdf

Chile –In December 2020, the Superintendence of Pensions issued a new standard that aims to enhance security and cyber security management requirements for pension fund administrators (AFP) and the Administrator of Unemployment Funds (AFC). The new regulation requires that AFPs and AFC implement a security and cyber security management system. It also introduces an obligation on boards of directors to approve and review annually information security and cyber security policy. The general rule applies as of 1 July 2021 and the instructions referred to the management of information security and cybersecurity incidents, knowledge management and administration of the security and cybersecurity management system, will begin to take effect on 3 January 2022.

https://www.spensiones.cl/portal/institucional/594/w3-article-14279.html

Colombia – In November 2020, the circular 033 was issued to cover the entire financial sector, including pension entities. The circular includes three main elements: information security and cybersecurity management metrics and indicators; implementation of TLP protocol for incident reporting; Unique Cyber Incident Taxonomy (TUIC). This new circular is complementary to circular 007 of 2018 which defines the minimum requirements for information security management and cybersecurity.

Germany – Between 2017 and 2019, BaFin set out specific requirements for IT security aimed at supervised entities in the financial sector. **In July 2018, the Supervisory Requirements for IT in insurance undertakings** and the **occupational pension sector** in Germany (VAIT) were published. It clarifies BaFin's expectations and requirements with regard to IT strategy, IT governance, information risk management, information security management. As undertakings are increasingly obtaining IT services from third parties, including as part of outsourcing arrangements, the requirements also cover

outsourced services. BaFin has largely harmonised its requirements in the area of information security, including cyber security, reflecting the fact that IT security at banks, insurers, pension funds and asset management companies is broadly comparable.

https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Meldung/2018/meldung_181120_veroeffentlichung_vait_englisch_en.html

Hungary – The IT governance and IT security related sectoral requirements are defined for the entire financial sector in a principle- based and risk-proportional manner in the **Government Decree 42/2015 on the protection of the IT systems of financial institutions.** The Central Bank of Hungary (MNB) has a long-standing practice of issuing guidance of IT related topics, the first guidance on protection of information systems was issued in 2005. The following MNB recommendation and circulars were more recently adopted: **on the protection of information systems** (MNB 8/2020 (VI.22)); on the **IT security requirements of remote work and remote access** (MNB 12/2020 (XI.6.)); on **the use of community and public cloud services** (MNB 4/2019 (IV.1)); Executive circular on electronic contracts, etc.

https://www.mnb.hu/felugyelet/szabalyozas/informatikai-felugyelet

Kenya – [work in progress] The Retirement Benefits Authority (RBA) of Kenya is in the process of developing cyber security guidelines for pension sector in Kenya. The guidelines are expected to be finalised in 2021. They will cover four broad areas: governance, controls, incidence responses, and focus on future cyber risks.

The Netherlands – 2019/2020 DNB Good Practice Information Security aims to provide guidance and practical examples to the supervised entities on the implementation of control measures to manage their information security and cybersecurity risks in the areas of governance, organisation, people, processes, technology, facilities, outsourcing, testing and the risk management cycle. The document promotes setting up a sound information security and cyber security control framework, as well as procedures and processes that ensure the availability and integrity of all information within an institution. These control measures and information security procedures should be appropriate to the nature and objective of the institution.

https://www.toezicht.dnb.nl/en/binaries/51-237685.pdf

Mexico - On 16 November 2018, the Mexican pension regulator CONSAR introduced modifications in general regulations regarding operations of the Retirement Savings' System (SAR). The amendments, among others, introduced new regulatory obligations for the managers of pension funds (AFOREs) to strengthen cyber resilience of SAR operations and protection of workers' data. New **cybersecurity regulatory obligations** for AFOREs include: 1) conducting frequent tests to their Business Continuity and Contingency Plans, as well as comprehensive tests of their substantive processes against computer security attacks; 2) performing periodic (at least annually) assessments of technological risk and vulnerabilities; 3) conducting periodic (at least annually) audits with third-party specialists in cybersecurity; 4) ensuring necessary human resources to operate information technologies according to the standards of technological and cybernetic security; 5) integrating a specialised unit in charge of the Technological Risk administration; and 6) establishing cybersecurity groups.

Morocco – 2020 Law on cybersecurity establishes a legal framework that defines the protection measures for the IT systems of State administrations, public establishments and companies and any other legal person under public law, as well as those of critical

infrastructures and private operators. It also aims to develop digital confidence, to promote digitalisation of the economy and, more generally, ensure the continuity of economic and societal activities in Morocco to promote the development of a national cybersecurity ecosystem.

https://www.dgssi.gov.ma/sites/default/files/attached_files/loi_n-05.20_version_francaise.pdf

Romania – Secondary regulation and regulatory standards on IT security were issued in 2018 (revised in 2019). These rules lay down the requirements for entities authorised/licensed/registered by the ASF, for the identification, prevention and reduction of the potentially adverse impact of operational risks arising from the use of information and communications technology in terms of persons, processes, systems and external environments, including cybercrime acts.

https://asfromania.ro/files/engleza/legislation/Norma%204%202018_EN%20--converted.pdf

United States[28] **–** On 14 April 2021, the Department of Labor's Employee Benefits Security Administration (EBSA) adopted cybersecurity best practices for retirement plans, which are directed at plan sponsors, plan fiduciaries, record keepers and plan participants. The published guidance has a three-folds approach and includes **Cybersecurity Program Best Practices** aiming to assist plan fiduciaries and record-keepers in their responsibilities to properly manage cybersecurity risks; **Tips for Hiring a Service Provider** aiming to help plan sponsors and fiduciaries to prudently select a service provider with strong cybersecurity practices and monitor their activities in line with ERISA requirements, and **Online Security Tips**, directed to plan participants.

https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity

European Union – September 2020 EC proposal of regulation on digital operational resilience for the financial sector. The proposed legislation sets out requirements applicable to financial entities in respect of governance, ICT risk management, incident reporting, digital operational resilience testing, monitoring of ITC third-party risk, information sharing and raising awareness on cyber threats. The draft regulation also aims to establish an oversight framework for critical ITC third-party service providers and rules on cooperation between competent authorities.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

About half (15) of the respondent authorities plan to or are in the process of introducing cyber security regulations or supervisory guidance for the financial sector and/or private pension entities. Ten authorities with IT security or cyber regulations in place **developed them in collaboration with other financial sector regulators**, especially the banking sector. A number of authorities noted a close on-going collaboration with other relevant bodies and authorities and work in progress to harmonise cyber regulation and supervisory guidance across the financial sector.

In several respondent jurisdictions (such as France, Hungary, Jamaica), the information security and the requirements for data security are covered under pension or financial/insurance legislation. Such legislation applies to pension funds and/or includes

[28] Non IOPS Member.

other relevant legal provisions on outsourcing. This is also the case in Armenia. In Malawi and Morocco, the cyber security laws cover all economic sectors and activities, including private pension entities. In China, the cyber security requirements apply to all networks constructed, operated, maintained, and used in the country. The requirements are contained in the Network Security Law, which includes a series of basic, technical, and evaluation requirements for network security classified protection.

At the EU level, legislation such as the EU General Data Protection Regulation (GDPR) elaborated in April 2016, applies both to public and private sectors, whereas the EU Proposal for Regulation on Digital Operational Resilience in the Financial Sector[29] will cover "financial entities", defined to include institutions for occupational retirement pensions. The EIOPA guidelines that were issued or are under preparation for the insurance sector apply for the pension sector as well. These measures include recently adopted EIOPA Guidelines on outsourcing to cloud service providers (February 2020), and the current work towards developing a cyber-incident reporting framework and on guidelines on security and governance of information and communication technology.

4. Management of cyber risk by pension entities

The thematic reviews[30] conducted by supervisory authorities and the responses to the IOPS survey suggest that, **in the majority of respondent jurisdictions, pension entities have so far not experienced any serious cyber incidents** or **suffered a significant material loss**. Also, as already stated, no major cyber incidents have been reported during Covid-19 crisis.

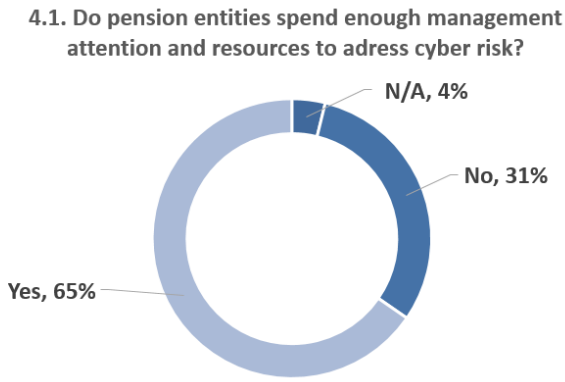
Members' responses generally indicate that **trustees and pension fund management companies are becoming increasingly aware of and have given priority to information and cyber security**.

Seventeen of the respondent authorities believe that pension entities in their jurisdictions devote sufficient management attention and resources to address cyber risk (Figure 4.1.). In several jurisdictions, the findings of on-site supervisory inspections indicate that pension entities were generally well-positioned against cyber risks (Austria; Chile; Hong Kong, China; Jamaica; Republic of North Macedonia; Serbia).

[29] EU legislative proposal - 'Digital Operational Resilience Act' (DORA) was elaborated as part of the 2020 EU Digital finance package, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595. The overall objective of the DORA is to streamline and upgrade existing rules on ICT governance, to manage ICT risks, the ICT related reporting requirements, to introduce rules where gaps were identified, in particular, digital testing. In addition, there are provisions in relation to information sharing and an oversight framework for critical ICT third-party providers, etc.

[30] Sources used: FMA Digitalisation Report, June 2019, APRA Insight issues 2016, 2017, 2018; APRA Information Paper 2015/2016 Cyber Security Survey Results; FCA, Cyber and Technology Resilience: Themes from cross-sector survey 2017/2018.

Figure 4.1.



Source: Members responses to the IOPS 2020 survey

Pension supervisors highlighted that supervised entities:

- take the issue of cyber risks seriously, e.g., by developing cyber strategies and incorporating cyber risk in their risk management processes
- put considerable effort and resources into protecting their IT assets
- manage any experienced incidents effectively, often supplemented by external expertise
- regularly test their ability to respond to and recover from cyber security incidents

It should be noted that the listed observations apply generally to all the supervised entities from different sectors and are not specific to private pension entities.

Although roughly **half of the respondents (17 Members) expressed the view that information security is generally well-handled by supervised entities, there are several areas that require greater attention.** These areas include: 1) assurance over the cyber capabilities of third-party service providers; 2) maintaining basic "cyber hygiene" (i.e. proper risk management practices), 3) greater visibility and better understanding at the board level of the risk of cyber attacks; 4) conducting regular and thorough security testing by independent internal or external parties; 5) developing training programs and increasing cyber security awareness of employees at all levels (e.g. executive management and employees); bringing cyber security into each organisations' corporate culture, etc.

Other supervisors also indicated that there is still considerable progress to be made. For instance, the Chilean supervisor noted that pension fund administrators have focused more on the implementation of vulnerability monitoring and detection tools than on the development of a robust information security and cybersecurity risk management system. Such systems should include IT governance, adequate controls, audits, developed cyber-resilience frameworks and security teams in order to manage risks at all levels, from senior management to the operational level. These areas have yet to be improved.

The task of identifying the types of risks that may affect a pension scheme, the likelihood of incidents occurring, and the potential impact of risks is usually included among the responsibilities of trustees or pension fund managers. However, **increasingly, supervisors have gone further to specifically require or recommend that trustees or scheme**

managers regard cyber risk as a significant risk. In accordance with these requirements, this ever-present key threat should be included in scheme managers' risk registers.

Cyber security risks are part of the risk management strategy of pension entities in most responding jurisdictions (28). Only seven Members replied that it is not yet the case.

A **written cyber security policy** is required in fifteen respondent jurisdictions, but such a requirement has not been established in twenty jurisdictions. In all but two jurisdictions (China and India), **the supervisory authorities do not certify or approve the written cyber security policies** established by trustees or pension fund management companies.

In most respondent jurisdictions (30), **there is no requirement to estimate the cost of cyber incidents** that have occurred in the private pension sector. Only three authorities, the FMA Austria, the Central Bank of Iceland, and the Insurance and Pension Commission of Zimbabwe, reported that pension entities must estimate direct or indirect costs of cyber incidents. For example, the FMA Austria requires pension sector undertakings to report the direct and an estimation of indirect costs of cyber incidents per year. Indirect costs are not tracked by most of these entities; the **direct costs** of cyber incidents have been **negligible**.

A uniform framework for measuring the effectiveness of cyber security resilience exists in about one-third of respondent jurisdictions. In general, these frameworks are developed by the supervisory authorities (see section 5.3). **In jurisdictions with no regulatory or supervisory requirement for self-assessment, pension entities usually adhere to recognised international and national technical standards or to industry best practices** (such as ISO/IEC 27001:2005) and deploy their own self-assessments and vulnerability tests.

The survey results suggest, in fact, that **pension entities in most jurisdictions (23 responses) perform periodic self-assessments or test their resilience to cyber threats.** In several jurisdictions (Bulgaria; Hungary; Mexico; Morocco; Romania), periodic assessments of cyber security are generally conducted on a yearly basis. Annual assessments are also conducted in other jurisdictions. In Hungary, pension entities have to perform penetration testing yearly and examine security arrangements of outsourced activities at least once a year. In Hong Kong, China, cyber security assessment is performed regularly.

By contrast, in some jurisdictions, assessments occur more frequently. In Colombia, for instance, such assessments are undertaken every six months, while in China, pension entities perform cyber risk assessments on a quarterly basis.

In a few jurisdictions, **self-assessment results, as well as their accuracy and completeness, are controlled by the supervisory authorities (**e.g., Chile; Iceland; the Netherlands)**.** In Iceland, the supervisory authority conducts its own assessment of all risks, at least every year for large pension funds and no less than every three years for small funds. An increasing focus is placed on Information and Communication Technology (ICT) risks and cyber risks. In a number of jurisdictions, data on the self-assessments or effectiveness of cyber security protections is not available or collected, owing to the low risk that cyber attacks are deemed to present for private pension funds (Brazil; Portugal).

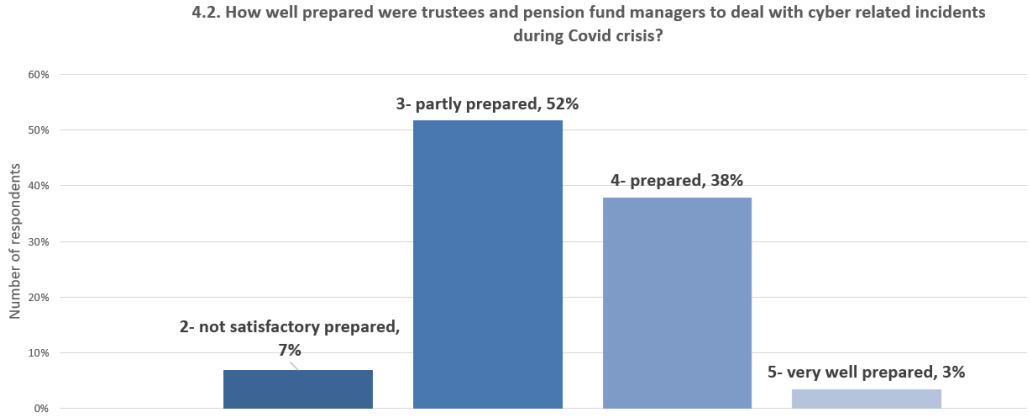
Member s' responses show that the **effectiveness of cyber security protection is often measured via both internal audits and external audits**. Internal audits evaluate the adequacy and efficiency of the internal control system and risk management systems, including with regard to outsourced activities. As an example, in Australia, each APRA-regulated entity's internal audit activities must include a review of the design and operating

effectiveness of information security controls, including those maintained by related parties and third parties (information security control assurance).

In a few other jurisdictions (France; Germany; India; Morocco), a function was established mandating the Information Security officer (ISO) to measure the effectiveness of cyber security protection. One of the tasks entailed is to ensure that information security objectives and measures defined in the undertaking's IT strategy, the information security policy, and information security guidelines, are transparent within the undertaking and that compliance with these requirements is reviewed and monitored.

More generally, it is a regular practice for pension entities **to engage third-party firms (audit, consultants) to conduct independent reviews of their cyber security,** in addition to the controls performed by internal audit, as internal staff may not possess the necessary expertise to conduct IT and cyber resilience audits. As an example, in Hong Kong, China, some trustees have engaged external consultants to conduct comprehensive reviews of their cybersecurity risk management frameworks, part of their efforts to enhance said frameworks. The reviews included a maturity assessment of the cybersecurity measures to identify gaps and areas for improvement. Newly adopted US cybersecurity best practices for retirement plans include a requirement to complete a reliable annual independent audit of the organisation's security controls to provide an unbiased report of existing risks, vulnerabilities, and weaknesses[31].

In addition to exploring general measures to cope with cyber security risks, the survey also addressed how well-prepared trustees, pension fund managers and administrators were to deal with the cyber related incidents experienced during the Covid-19 crisis (Figure 4.2). A few authorities did not provide a response, as this information is either not collected (Hong Kong, China; Germany) or not available (in Ireland, entities are not audited).



Source: Members responses to the IOPS 2020 survey

Note: Scores above are based on the results of the cyber maturity surveys carried out by supervisors.

Seventeen authorities provided information on **specific measures taken by trustees and pension fund managers during the Covid-19 pandemic**. These measures could be broadly categorised as:

- *Upgrades of existing technical measures* such as: firewalls, antivirus software, Intrusion Prevention/Detection systems (IPS/IDS); creation or re-dimensioning of

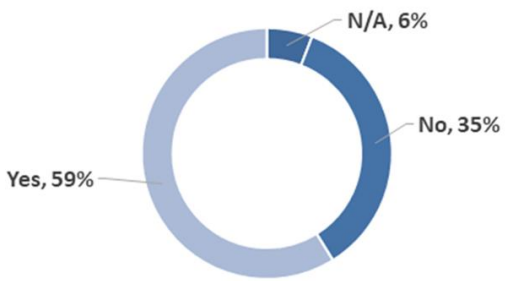
[31] https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity

Virtual private networks (VPNs); maintenance of hardware and software of IT systems; restricted remote access to company servers

- Measures to *secure user authentication process*: two-factor authentication, new processes for staff for logging in from home; reinforcement of members" identification processes
- Enhanced *monitoring of cyber events:* managers closely monitoring sensitivities or suspicious events in their ICT infrastructure
- *Budget resource allocation*: additional budget to acquire adequate and efficient security solutions
- *Increased exchange* between pension funds and services providers
- Launch of *information security awareness and training programmes* for staff: sensitising staff on security best practices, including during teleworking.

Cyber insurance is available, but not mandatory in 20 respondent jurisdictions (Figure 4.3.**)**.

4.3. Is cyber insurance available for the supervised entities?



Source: Members responses to the IOPS 2020 survey

5. Supervision of pension funds' cyber risk-management frameworks

Supervisors no longer perceive cyber threats as an emerging risk but, rather, **as a constant challenge for supervised entities regardless of their size and significance, one that** requires their utmost attention.

The FSB stocktaking report[32] also notes the systemic dimension of cyber risk and the importance of assessing cross-sector and cross-border cyber risks for the financial sector.

The FSB reviewed the key elements of the supervisory practices with respect to cybersecurity in the financial sector. Recent work in the area developed by other international organisations (G7, OECD, IOSCO, EU, EIOPA) complements and brings more detailed views of particular business activity in the financial sector.

Drawing on this work, this section reviews key supervisory measures put in place to reduce the impact of cyber incidents on financial institutions and to strengthen their cyber resilience. Most supervisory approaches are similar across the financial sector and are

[32] FSB, "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices", October 2017

generally applicable to different types of financial entities. Responses to the IOPS survey capture some new developments and supervisory practices regarding cyber resilience specific to the pension sector.

5.1 Thematic surveys

In a number of jurisdictions, supervisory authorities have conducted thematic surveys on digitalisation, including cyber risk, or have looked more specifically at cybersecurity incidents. Their purpose is to evaluate preparedness of the industry in regard to cyber risks and attacks and measures taken by supervised entities to protect technological assets and customer information and assets. Authorities also aim to collect information on cyber security incidents and their management. Generally, such surveys allow supervisory authorities to identify key risks and areas where additional supervisory guidance or supervisory actions are needed to improve cyber risk management. They also enable supervisors to share information on cyber experiences and industry best practices, which could help other entities to improve their cyber security risk management.

Results of the IOPS survey show that **eight respondent authorities have conducted thematic cyber security surveys in the recent past.**

5.2 Supervisory guidance with respect to cyber security

Issuing supervisory guidance or standards is regarded as another effective supervisory practice in addressing cybersecurity in the financial sector. Some of these guidelines[33] are cross-sector, but others are specific to the pension industry. Supervisory guidance fits into a broader framework of advice issued by other regulators or enforcement authorities/agencies. It supplements already existing high-level national and international cyber security guidance and industry practices and insights.

The survey finds that **supervisory guidance (binding, or non-binding) was issued in about half of the respondent (17) jurisdictions.** For the most part, the guidance is in the form of high-level principles. When applying them, supervised entities are expected to take measures proportionate to the cyber risks associated with their business activities and to take into account their company's individual circumstances, including, for example, the nature, scale, and complexity of their business and operation models.

Supervisors generally consider cyber risks to be part of operational risks, defined as the risk of incurring a loss owing to external events or internal processes and systems, including IT and people. The ability of institutions to ensure provision of secure and an uninterrupted service forms an important part of their operational risk considerations. Inasmuch as cyber and IT risks are usually analysed from a risk management or governance perspective, guidance on the management of cyber risk extends or complements existing risk management requirements and/or is established as part of good governance requirements. It is worth noting in this context the 2019/2020 examples of good practice on information security issued by the DNB, the Netherlands. The guidance communicates supervisory expectations with regard to control measures that supervised entities need to have in place to manage information security and cyber risk. The good practices[34] cover not only technological solutions, governance, and risk management, but also address

[33] Non-exhaustive examples include APRA, Australia; FMA, Austria; BaFin, Germany; RBA, Kenya (in the process); DNB, the Netherlands.

[34] https://www.toezicht.dnb.nl/en/binaries/51-237685.pdf

human actions, organisation, processes, facilities, etc. The good practices also include the **maturity model** that **the supervisors use to assess the information security and cybersecurity risk** management of financial entities under their supervision (for additional information, see section 5.3.).

In the pension sector, specific cyber supervisory guidance is issued for the attention of trustees or other fiduciaries, boards of directors, and senior management. It is also deemed relevant for risk and information security specialists responsible for the security of pension schemes or pension fund information and assets.

A number of similarities are observed across international or national cyber guidance, with many similar topics covered irrespective of different types of activities of financial entities[35]. These **common elements aimed at the executive management** (such as boards or trustees) of cyber and IT supervisory guidance are outlined below:

- *Governance* – ensures that the executive management of a supervised entity (boards, trustees and where appropriate sponsoring employer) is aware of and understands cyber risks and their potential implications (operational, reputational, financial) for the pension scheme. The executive management should also understand the cyber practices applied by third parties involved in the scheme (the entire chain) and the risks posed by these parties. Trustees and board members should be responsible for setting up a risk management framework and organising the company's preparedness as part of this framework to identify, prevent, and respond to potential cyber risks and incidents. Cyber risk and information-security roles and responsibilities should be clearly defined and assigned. Trustees and board members should be responsible for the development of a strong corporate risk culture that includes promotion of cyber and information security awareness
- *Cybersecurity strategy* – establish well-documented policies, procedures, protocols, and tools for effective management of cyber security risks
- *Capabilities and resources* – have, internally, the required skills and expertise suited to their size, business, and risk profile, to understand, assess, and manage cyber risks, and have access to external cyber security specialists
- *Scope* – include third-party service providers when developing and implementing cyber-security risk management strategies and activities
- *Identification of risks* – on a continuous basis identify all sources of ITC and cyber risks, particularly risk exposures from other financial entities and third-party providers
- *Controls* – establish strong control procedures and ensure that all third-party service providers have sufficient controls in place to protect members' data and to minimise the risks of cyber incidents
- *Monitoring* – undertake regular monitoring of systems, networks, and analytical logs to determine and address vulnerabilities
- *Assessment* – perform periodic assessments internally and/or arrange for these to be undertaken independently by an external auditor or specialised certified institution to evaluate the effectiveness of information security systems, controls,

[35] FSB "Stocktaking Report", October 2017.

and cyber-risk management measures; Assets and data stored in the cloud or managed by third-party service providers should be subject to appropriate security controls and independent security assessments

- *Incident response* – develop systems, processes, and capabilities to detect and respond to cyber security incidents in a timely manner and ensure the safe and swift resumption of operations; The process should include roles and responsibilities of the incident response team; critical functions and processes; crisis communication, process and timeline for notification of other parties, including the regulator, law enforcement, third parties, and, if necessary, members. Trustees and board members should ensure that they understand the incident response processes of third-party providers. Incidents should be documented, with major incidents followed up and reported to the competent authority(ies)
- *Reporting/disclosure* – have in place clear policies to report significant cyber threats, incidents, and response measures to the relevant public authorities, including pension supervisory authorities. Financial entities may also notify plan members/beneficiaries about such threats or incidents and the ways to prevent them
- *Cybersecurity awareness and training programmes* – organise on a regular basis cyber security awareness initiatives and training for all of the organisation's employees, focusing on how to recognise, prevent, respond to, and follow up on (potential) IT security incidents
- *Collaboration* – seek appropriate information and follow guidance on cyber security threats issued by relevant public authorities to improve prevention, detection, and response capabilities; Entities may also engage with other relevant forums, sources of intelligence, and cyber-response assistance in their jurisdiction.

The adoption of supervisory guidance is expected to stimulate further improvement of cyber-risk management standards within the financial industry, by supporting the development of robust identification of cyber incidents and related management and recovery practices. The guidance should enable financial entities to become better prepared to safeguard the confidentiality and integrity of their data and systems that allow for continued sound operation.

Once adopted, supervisory guidance serves as a benchmark for the conduct of supervisory on-site inspections to verify compliance with legal provisions and implementation of supervisory provisions.

5.3. Supervisory cyber maturity self-assessment framework

Ten Members participating in the survey (Austria; Chile; Colombia; Czech Republic; France; Iceland; India; the Netherlands; Poland; Romania; Turkey) reported that **self-assessment questionnaires/frameworks were developed by supervisory authorities** to evaluate maturity levels and effectiveness of controls aimed at managing information security and cybersecurity risks in the financial sector, including pension entities. A similar self-assessment questionnaire was also developed by the Central Bank of Armenia, based on the Federal Financial Institutions Examination Council (FFIEC) cybersecurity maturity assessment tool[36].

[36] https://www.ffiec.gov/cyberassessmenttool.htm

In Australia, the elaboration of a self-assessment framework is under consideration as part of APRA's 2020-2024 Cyber Strategy[37]. In Hong Kong, China, each trustee has deployed its own cybersecurity risk-assessment framework, by adhering to recognised cybersecurity standards.

The framework/questionnaires provide guidance and help financial entities to complete periodic self-assessments to evaluate their cyber competency and readiness relative to their counterparts.

Box 2 The DNB assessment framework of information security maturity for financial institutions

In the Netherlands, the DNB's good practice on information security offers an assessment framework that financial institutions could use to conduct self-assessment examinations of their information security. The self-assessment framework covers areas such as governance, organisation, human actions, processes, facilities, outsourcing, testing, technology, etc.

In addition, the good practice document includes the maturity models that supervisors use to assess information security and cybersecurity risk management. Dutch supervisors examine the quality of information security in the financial sector on a thematic basis. In this context, supervisors may ask supervised entities to complete periodic self-assessments to measure their operational maturity levels. The self-assessments verify whether entities' control of information security and cybersecurity is at the required level. For this purpose, supervisors use Maturity Models. Supervisors expect financial institutions to be in control and be able to demonstrate this. The supervisory model may include 58 control measures, which correspond to a maturity level score of at least 3, i.e., verifiable long-term operational effectiveness, or 55 control measures, and a maturity level score of at least 4 (e.g., managed and measurable) for the remaining 3 control measures – controls of IT risk-management framework, risk assessment and maintenance, and monitoring of an action plan for risk..

The requirement to complete a periodic self-assessment exercise may apply to the entire pension sector, as in Austria and the Netherlands, or it can relate only to the largest entities, as in France, where only the top 21 institutions have the obligation to respond. In Iceland, regulated entities that outsource to cloud service providers have an obligation to complete the questionnaire[38]. **Depending on the jurisdiction, the evaluation responses are reported and analysed by supervisors or verified and discussed with each entity during on-site inspections.** The outcome of the self-assessment exercise could provide a

[37] https://www.apra.gov.au/news-and-publications/executive-board-member-geoff-summerhayes-speech-to-financial-services

[38] Iceland: https://www.fme.is/media/gatlistar/Gatlisti-vegna-innleidingar-skyjalausna-hja-eftirlitsskyldum-adilum-2019.pdf

benchmark against which the results collected from other similar financial institutions[39] are assessed. Self-assessment exercises are repeated regularly, generally every two years.

In this respect, it is worth noting the EU initiative, TIBER-EU guide[40], developed in May 2018 by the European Central Bank (ECB) and the EU national central banks. **TIBER-EU offers a first EU – wide guide** on how authorities, entities, threat intelligence and "Red" team providers should work together to test and enhance the cyber resilience of entities, by **carrying out a controlled cyber attack**. The key objectives of the framework are to foster an adequate level of cyber resilience for the entities to ensure the proper functioning, stability, and integrity of the financial system. The exercise involves commissioning external "ethical hackers" to carry out simulated attacks on an entity. This simulation exercise tests how effectively the entity can prevent, detect, and respond to actual cyber attacks. TIBER tests are not focused solely on technical vulnerabilities, but also incorporate the "human" factor into the attack scenarios. The framework is applicable not only to the financial sector but can be also used in other critical sectors. It pursues the objective that threat-led penetration testing is conducted in a harmonised way across the EU, avoiding duplication of work for entities and authorities alike. It is foreseen that entities should procure only those providers that have achieved a formal TIBER-EU certification and accreditation.

The initial experience in the Netherlands shows that TIBER tests can be a promising concept for implementing threat-led penetration testing. The target group was first limited to financial institutions and their critical infrastructure. Subsequently, it has been expanded to include insurance companies and pension funds. Other countries have announced their implementation of the framework or are taking specific steps towards implementation.

A similar framework has been developed recently in Australia by the Council of Financial Regulators (CFR) Cyber Security Working Group. Cyber Operational Resilience Intelligence-led Exercises (CORIE) is a pilot programme that uses the targeted threat intelligence test to assess the overall effectiveness of a financial institution's cyber defence and response capability[41].

5.4 Supervisory examinations – off-site and on-site inspections on cyber security

Supervisors also increasingly incorporate cyber security in their supervisory examination priorities[42] and have started to conduct **dedicated inspections focused on IT and cyber security of pension entities and their service providers.** In this respect, it is critically important that supervisors have all the necessary powers to request relevant information,

[39] FSB "Stocktaking report", October 2017.

[40] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html; The European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU) - has been implemented in Belgium, Denmark, Ireland, and the Netherlands. It is being implemented in Germany, Romania and Sweden.

[41] 2020 Cyber Operational Resilience Intelligence-led Exercise in Australia: https://www.cfr.gov.au/publications/policy-statements-and-other-reports/2020/corie-pilot-program-guideline/pdf/corie-framework-guideline.pdf

[42] Cyber risk was identified by the FMA (Austria) as one of its supervisory priority topics in 2019. It was also the priority area for supervisory examinations in 2018 (as well as in recent past years) by the US SEC Office of Compliance Inspections and Examinations (OCIE).

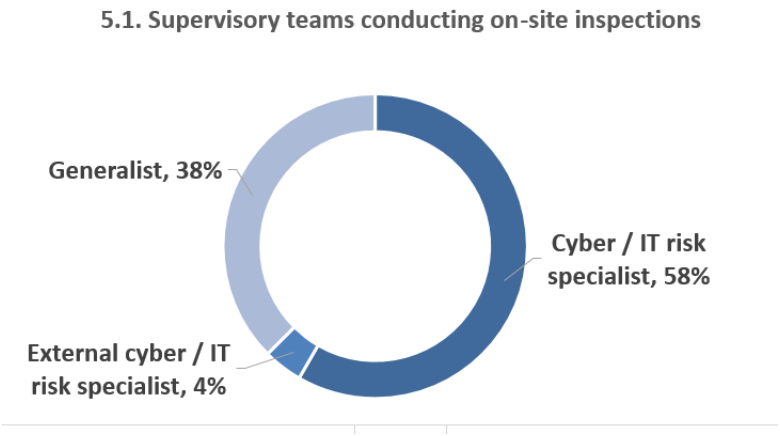
conduct investigations and inspections, as well as to follow up on how their recommendations are addressed.

Twenty-four (67%) authorities reported that they organise on-site inspections to form more qualitative judgements on measures taken to control information and cyber security. Supervisory examinations serve to monitor whether regulated institutions comply with regulatory requirements for information security or cyber security. The number of breach notices can be used as an indicator to measure the ability of institutions to deter, detect, and defend against cyber incidents, supported by other quantitative/qualitative information[43] .

These supervisor inspections could be complemented by targeted audits (Germany; Hungary; Mexico), including remote on-site audits conducted during the period of the Covid-19 pandemic. For example, the BaFin (Germany) aims to begin systematic supervisory IT audits. They will include not only the insurance undertakings and pension funds it supervises, but also their outsourced entities. The Supervisory Requirements for IT security in Insurance Undertakings published in 2018 provide the basis for these assessments.

In almost half of the respondent authorities (14), on-site examinations are conducted by specialised cyber/information security supervisory teams (Fig. 5.1). For example, in the ACPR (France), the cross-sectoral directorate for on-site inspections includes a specific unit for the supervision of information systems and data quality. In Hungary, the Central Bank (MNB) has an IT supervision department consisting of seventeen highly qualified IT experts. In one-third of the respondent authorities, inspections are conducted by generalist, non-specialised supervisory staff. In a few other jurisdictions (Austria; Chile; China; Costa Rica; Jamaica), supervisory teams may be supported, at least in the beginning of such activities, by external IT or cyber security specialists. In Jamaica, on-site examinations are conducted by pension supervisors, with the possibility to rely on external IT specialists if needed.

Figure: 5.1.



Source: Members responses to the IOPS 2020 survey

A number of authorities (Bulgaria; Colombia; Czech Republic; Hungary; Jamaica; the Netherlands) indicated that the frequency and intensity of inspections depends on a supervisory risk-based approach, such as on an entity's supervisory assessment and risk

[43] APRA Corporate Plan 2020/24.

classification. Some authorities undertake (or aim to do) a regular cycle of inspections in the area of cyber security, usually on an annual basis (Austria; Chile; Honduras; France; Germany; Mexico; the Netherlands; Romania) or every two (Republic of North Macedonia) or 3 years (Hungary). In Australia, more systemically important entities are reviewed more frequently than other entities.

As part of the supervisory examinations, cyber security risks are analysed from the strategic and governance perspectives down to the operational and technical levels.

Pension supervisors offered some examples of particular topics and prioritised areas for attention during on-site inspections:

- IT strategy: should be consistent with the business strategy of an undertaking
- IT governance: the structure used to manage and monitor the operation and further development of IT systems needs to be in line with the outlined IT strategy
- Information risk management: as part of this process, an entity needs to define and co-ordinate the tasks, competences, responsibilities, controls and reporting channels required for the management of information and cybersecurity risks
- Information security management: should make provisions for information security, define corresponding processes, and implement them
- IT system, including IT procurement and development:
    - Identification of critical SI assets
    - Access management
    - Data protection framework
- Third-party management. In the event IT services are outsourced, risk analysis should be performed in advance; this applies both for IT services provided by a service firm via a network and via technical interfaces and protocols (cloud services)
- IT contingency plans and their testing (penetration testing/ "Red" team exercises[44])
- Security awareness, staff training, personnel security
- Human resources (an entity's employees, external staff, and service providers) – are critical to the management of information security. Authorities should check if the entity recruits and retains personnel with adequate knowledge on information security and cybersecurity, whether it invests in education and offers training, and whether knowledge is shared across the entity.

In the Netherlands, the DNB selects approximately ten out of fifty-eight controls from their information security assessment framework[45]. The selection depends on the entity itself, its maturity, risks, the timing, and other factors. During on-site inspections, priority attention is given to five key topics. They are: data quality and its management, the internal controls

[44] A "Red" team imitates real-world attacks that can hit a company or an organization. Teams are focused on penetration testing of different systems and their levels of security programs. Their primary objective is to detect, prevent and eliminate vulnerabilities, https://securitytrails.com/blog/cybersecurity-red-blue-team

[45] DNB Good Practice Information Security 2019/2020, https://www.toezicht.dnb.nl/en/binaries/51-237685.pdf

framework, cyber-security (which can include any of 58 controls in the assessment framework), the IT strategy, with a focus on operational agility, and outsourcing to ensure that institutions are in control of information security and cybersecurity regarding outsourced activities.

A couple of authorities indicated that they have not yet carried out on-site inspections focusing on cyber security, owing to the fact that cyber risk is low in the pension sector (Brazil; Portugal).

The survey finds, based the supervisory on-site inspections results, that **the management of cyber risks from outsourced IT services and data management (the entire chain of subcontracting) by pension funds is regarded a key issue by supervisors** in several jurisdictions (Germany; Hungary; Iceland; Republic of North Macedonia; the Netherlands). Pension funds often delegate their IT and data management to **third-party providers, which may be outside the financial sector and, therefore, are themselves not under supervision.** Also, pension funds increasingly rely on the use of cloud technology, which is becoming a mainstream computing platform in the financial sector[46]. The FCA (UK) identifies data storage/outsourcing to the cloud as one of the three key emerging risk areas requiring special supervisory attention. In 2019, cloud computing was also a focal point of the supervisory examinations undertaken by the FMA (Austria), which included pension schemes and management companies.

In this vein, as part of on-site inspections, supervisors are increasingly devoting attention to management of ITC third-party risk by financial entities. From the supervisory prospective, it is essential that financial entities, including pension funds, have **sound management systems for ITC and cyber third-party risk**. The surveillance focuses on whether supervised entities have a strategy on ITC third-party risk as part of their ITC risk management framework and regularly review it. Supervisors also examine whether supervised entities have solid contractual arrangements on their use of ITC services, undertake assessments of ITC concentration risk and, in particular, for complex chains of sub-contracting (outsourcing) arrangements, conduct regular audits and inspections in line with supervisory expectations. Recently proposed EU legislation[47] includes provisions for an oversight framework for critical ITC third-party service providers and, among other objectives, seeks to achieve better co-ordination and efficiency of supervisory approaches at the EU level.

IOPS Members' responses to the survey identified **a number of areas of IT security to which pension entities need to pay special attention**:

- Continue to improve IT security, information risk management and information security management (Germany)
- Strengthen the role of information security and/or cyber security officers
- Manage third-party (outsourcing) risk and remote working (France, Hungary; Republic of North Macedonia; Mexico; Poland)

Respondents also cited the following technical issues:

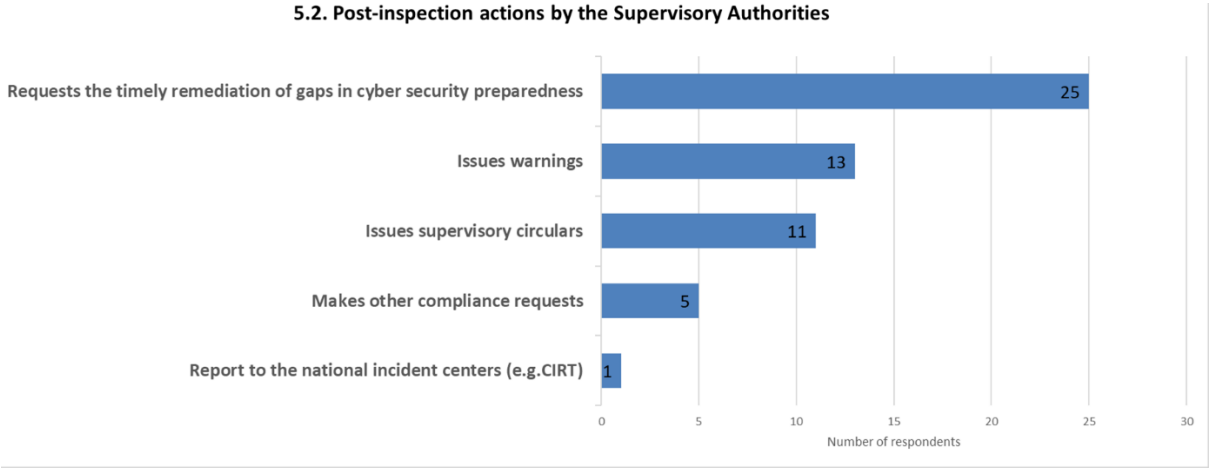
[46] See IOPS WP33 Impact of the digitalisation of financial services on supervisory practices in the private pension sector (2018) , www.iopsweb.org

[47] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

- Identification of vulnerabilities (Australia), active monitoring and detection of ongoing attacks, incident management, and patch management processes
- User identification/authentication (including privileged access) (Australia), management of access rights (France), and access controls, physical access controls, and controls over passwords (Zimbabwe)
- Identification of critical assets (France)
- Obsolete IT systems (Hungary)
- Business continuity management (BCM)/disaster recovery plans (Hungary, Malawi)
- Robustness of security testing (Australia; the Netherlands) and recovery plan testing (Jamaica)
- Continuously develop capacity building and capability actions to deal with massive cyber incidents, attacks, and crises (Bulgaria) and education of employees (Poland)

5.5 Post-inspection actions by supervisory authorities

Figure 5.2.



Source: Members responses to the IOPS 2020 survey

In reference to post-inspection actions by supervisory authorities, respondents most often mentioned requests for the timely remediation of gaps in cybersecurity preparedness or the issuance of warnings. Some authorities (Australia, Botswana, Chile, India and Kenya) can make additional compliance requests, such as issue supervisory requirements as part of on-site reviews (e.g. APRA, Australia); require provision of compliance plans by the supervised entities (Botswana); or monitor the commitments set forth by the pension fund administrators on improvement to action plans, followed by an audit (Chile).

5.6 Supervisory requirements for the conduct of external audits and assessments

In the majority of respondent jurisdictions (26)**, there are no regulatory requirements for pension entities to appoint an external auditor to perform assessments of IT systems.** Such requirements do exist, however, in about a quarter of respondent jurisdictions (Bulgaria; China; Costa Rica; Iceland; India; Mexico; Romania; Zimbabwe).

The absence of regulatory requirements notwithstanding, as Member responses show (see section 4), it is a regular practice for pension entities to engage third-party firms such as audit firms or consultants for independent reviews of their cyber security, in addition to the controls performed by internal audit and risk management functions.

In Mexico, recent regulatory changes introduced a requirement for pension management companies to conduct periodic audits with third-party cyber security specialists, at least annually.

In Australia, beginning next year (2022), boards must engage an external audit firm to review their CPS 234 compliance. This audit will be done in line with the new prudential standard, and compliance should be reported back to APRA. Furthermore, APRA's CPS 234 standard[48] requires the Internal Audit function to review information security. It should, however, be noted that the standard is silent on the use of third parties for this role; it neither mandates nor precludes their use. The standard does have a requirement for ongoing testing of information security, which can be performed by internal and external resources. APRA also has the power to require regulated entities to undertake special-purpose audits for the use of both the regulated entity and APRA.

In India, Central Recordkeeping Agencies (CRAs) and Pension fund regulations require mandatory appointment of chief information security officer (CISO) and external cyber security audit on annual basis as measures of cybersecurity and resilience. External (independent) audit assessment is conducted by a CERT-IN empanelled cybersecurity auditor. Apart from this, Central Recordkeeping Agencies (CRA's) also conduct internal cyber security audits and files the necessary regulatory compliance reports with the PFRDA (Regulator). The intermediaries are required to submit a compliance certificate as mandated in the PFRDA's Cyber Security Policy on quarterly basis.

In the United States, the recently adopted 2021 Cybersecurity best practices for retirement plans include a requirement for plan fiduciaries to have a reliable annual independent audit of security controls, which should include the entity's existing risks, weaknesses, and vulnerabilities[49].

5.7 Notification mechanisms for information security incidents

Collecting data and information on cyber risk events is critical to the supervisory process. The use of notification mechanisms for information security incidents alerts the authority when a material incident has occurred and provides information as to how the institution is responding to the incident. It also tells what actions were taken to prevent similar incidents from occurring in the future[50]. Consistent incident reporting mechanisms enable supervisors to properly assess and monitor risks and develop suitable supervisory requirements and measures to help financial entities to either prevent ICT-related and cyber incidents or limit their impact. The use of notification mechanisms should also allow for reduced administrative burdens and financial costs associated with reporting for financial entities.

[48] https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf; https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_1.pdf

[49] https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity

[50] APRA Annual Report 19/20.

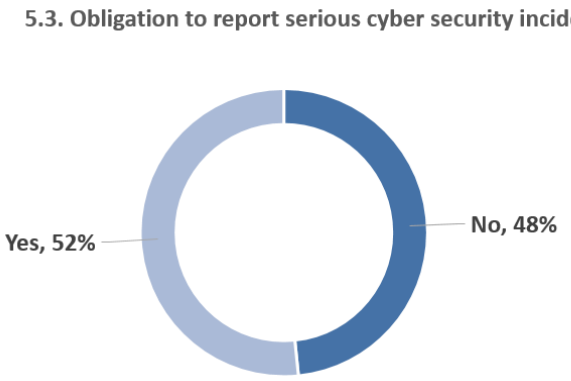
In about half of the respondent jurisdictions (Australia; Botswana; Bulgaria; Germany; Hong Kong, China; Iceland;; Mexico; the Netherlands; Romania; Serbia) **pension entities have an obligation to report serious cyber security incidents to the direct supervisor** (Fig. 5.3.).

In Germany, for example, in line with the requirement under the German Payment Services Supervision Act, supervised entities are required to report serious IT security incidents to BaFin. In the Republic of North Macedonia, pension funds must report serious incidents immediately. In Australia and Hong Kong, China, supervised entities must inform the supervisor within three (3) working days of any significant information security incident. In Kenya, such reporting should be made to the two peer supervisory authorities (the Central Bank and the Capital Market Authority). In Colombia, regulations require that supervised entities report serious cyber security incidents to three stakeholders: the supervisory authority (FSC), the entity in charge of the national cybersecurity and cyber defence strategy (COLCERT), as well to the affected financial consumers. In the Netherlands, there is a broader requirement to report any incident that may impede the governance system and/or operational management as defined in the Dutch financial supervisory law.

As part of the survey, Members also addressed any special reporting protocols (as in Colombia) or the adoption of a more systemised approach for reporting ITC and cyber incidents. In the EU, for example, the new EU draft proposal for regulation on digital operational resilience for the financial sector[51] establishes a requirement for financial entities, as part of the ITC-related management process, to monitor, log, categorise and classify ITC-related incidents, based on criteria that will be further elaborated by the European Supervisory Authorities (ESAs). Financial entities will have to report major ICT-related incidents to the relevant competent authority, within the timeframes prescribed and in accordance with harmonised reporting templates. Competent authorities will also be expected to provide information on incidents to other relevant institutions or authorities. The feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ITC-related incidents at financial entities is currently being explored. Draft regulation also introduces an obligation for the affected financial entities to inform users and clients about any major ICT-related incident that has or may have an impact on their financial interests and the measures being taken to mitigate it.

Figure 5.3.

[51] EC proposal for regulation on digital operational resilience for the financial sector; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595



Source: Members responses to the IOPS 2020 survey

In a number of authorities, pension entities are required to report to an authority other than the direct supervisor. For instance, in Jamaica it is the Ministry of Justice; in Morocco - the Directorate General of Information Systems Security; in Turkey - the Personal Data Protection Authority and the TR-CERT. In Austria, data protection notifications are to be addressed to the central Austrian Data Protection Authority, DSB. This is in line with the EU General Data Protection Regulation. In Croatia, if a cyber incident involved some sort of criminal activity, the police should also be informed.

In fifteen jurisdictions, pension entities do not have to report cyber incidents to the supervisory authorities. In France, Poland and the Slovak Republic, at present, only banks have such an obligation to report cyber events to the supervisory authority and the ECB, and in Ireland, to the National Cyber Security Centre. Nonetheless, the supervisory authorities have a legitimate expectation that the supervised entities will inform them of any major events that affect their activities, including cyber security incidents (France; Portugal).

5.8 Supervisory sanctions

In most respondent jurisdictions, **supervisory authorities have powers under their general frameworks to impose penalties, fines or corrective and remedial measures for noncompliance with IT or cyber security requirements for financial entities and third-party providers.** The measures range from warnings and compliance requests to suspension, disqualification, or withdrawal of the license to operate.

Decisions to impose penalties for non-compliance with regulatory requirements are usually determined according to a risk-based supervisory approach, whereby the severity of the sanction imposed depends on the type of risks identified or the nature of the infraction committed by the supervised entity, as well as according to the complexity, nature, and size of the operations of each entity.

A few jurisdictions shared information on the range or the maximum level of penalties imposed on physical and legal persons specifically for non-compliance with the supervisory requirements in the area of cyber security. Draft 2020 EU legislation[52] proposes to introduce a periodic penalty payment to compel critical ICT third-party providers to comply with supervisory requirements for digital operational resilience. The periodic

[52] EC proposal for regulation on digital operational resilience for the financial sector; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

penalty payments are foreseen to be imposed on a daily basis for a period up to, but not longer than, 6 months, until compliance is achieved and could amount to 1% of the average daily worldwide turnover of the provider in the preceding business year.

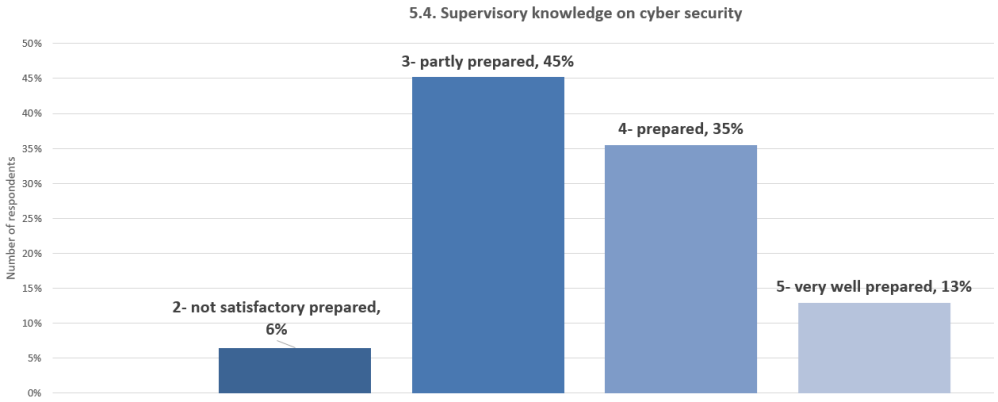
A few Members (Hong Kong, China; Kenya; Malawi; Turkey; Zimbabwe) indicated that there is no relevant regulation in the area of cyber security at present or changes in the pension law that would empower the pension supervisory authorities to impose fines or penalties and require corrective measures for identified breaches.

5.9 Supervisory knowledge on cyber security

Respondents noted that **one of the challenges for supervision of IT and cyber risks** relates to their **preparedness in terms of knowledge and skill sets** to conduct on-site supervision of pension entities' cyber security resilience.

Figure 5.4. presents an evaluation of respondents' supervisory capacity and adequacy to conduct on-site supervision of the cyber-risk resilience of pension entities.

Figure 5.4.



Source: Members responses to the IOPS 2020 survey

Nearly one-half of the respondents assessed their capacity to supervise cyber security issues as partly prepared. Thirty-five percent evaluated their capability as 'prepared' and 13 percent indicated they were very well prepared. Only six percent considered their preparedness to be unsatisfactory.

Among respondents, APRA (Australia) distinguished among levels of specialist expertise, with frontline supervisors identified as being "partly prepared" (level 3), while APRA's specialist team of technology experts, who assist frontline supervisors in conducting on-site and review activities, was rated at the highest level (5).

The **establishment of risk-based priorities for cyber risk supervision may help to address this capacity gap challenge**[53]. Respondent authorities also noted the possibility to mitigate the issue of preparedness and availability of appropriately qualified specialists in cyber risk space **through the use of external cyber threat intelligence analysts** (with a detailed understanding of the financial services sector), before conducting on-site inspections (Austria, Chile) or **engaging external professionals to perform examinations** (Costa Rica). Another solution put forward entails the **organisation** of technology risk and

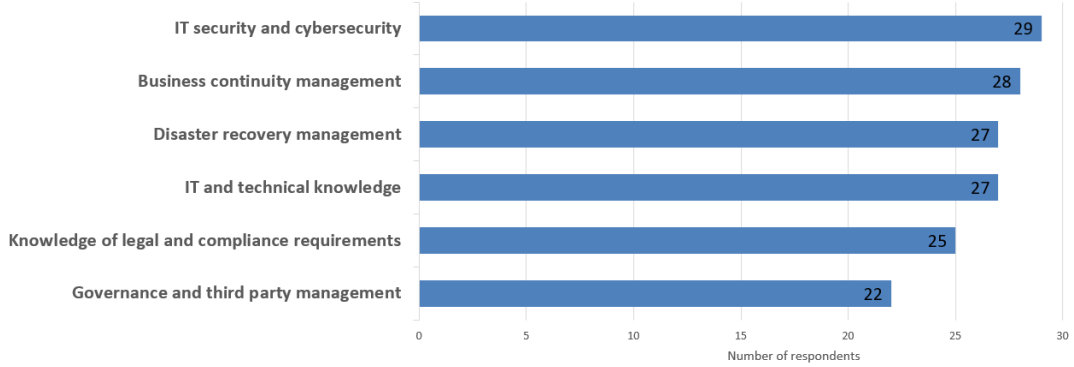
[53] Toronto Centre notes, Supervision of cyber risk, December 2018.

cyber-security **training programmes to increase supervisors' awareness of cyber risks**. The RBA of Kenya noted their experience in organising a series of training programmes for supervisory staff[54].

In addition to these approaches, **engaging and exchanging knowledge and expertise with other regulatory agencies** appears to be a useful tool to harness collective expertise. It also enhances authorities' ability to identify, assess, and respond to emerging risks with well-founded, risk-based decisions, including for risks arising in cyber space[55].

The survey also included a list of potential areas that would help supervisors obtain the necessary knowledge. Most respondents marked all of the options (Figure 5.5.). In addition, some supervisors are increasing their capacity with regard to supervision of emerging technological risks (Colombia; Kenya) and machine learning (Slovak Republic).

5.5. Areas where supervisors are increasing their capacity/capability to supervise cyber security resilience



Source: Members responses to the IOPS 2020 survey

6. Co-operation and information sharing

Effective supervision of cyber risk requires close co-operation and information exchange among the national financial sector regulators and other public authorities, as well as involving broader regional or international groupings. Efforts of supervisors to engage with the industry to raise awareness and share information in the area of cyber risk (e.g., via standards, guidance, other initiatives developed by national and international agencies that supervisory authorities support or recommend) are also crucial. These initiatives contribute to cyber capacity-building of supervisors and within the financial sector, including for private pensions.

6.1 Co-operation at the national and international levels

Pension supervisors develop close co-operation on cybersecurity with national governmental authorities to build a co-ordinated approach to address cyber risks.

[54] Training programmes organised for supervisory staff: on ICT technical knowledge; on cyber security and emerging issues; on BCP, business resilience and risk management; exposure on business resilience, disaster recovery systems and Business continuity planning; on ICT governance, risk management and third party risk to ensure that third party risk do not affect operations; on legal and compliance issues.

[55] APRA Corporate Plan 2020/2024, August 2020.

Generally, they share information on cyber security with other public authorities periodically and/or on a case-by-case basis. Information is shared according to relevant regulations, signed MoUs, mutual arrangements or bilateral agreements that explicitly describe the form of information transfer (e.g. Bulgaria; Croatia; France; Germany). **Different degrees of intensity of co-operation in the cyber area were reported**. In the view of certain supervisors, sharing information with peer regulators in the cyber security field is regarded as still insufficient and is a key focus in the development of a proper supervisory cyber strategy. In a few respondent jurisdictions (e.g. Portugal), information sharing mechanisms have not yet been put in implemented.

In Australia, in line with APRA's strategic focus on enhancing cyber resilience across the financial sector and work on a new 2020-2024 Cyber Security strategy, APRA will strive to influence the financial system more broadly and not just supervised entities. This effort will require developing and acting in greater concert with peer regulators and other public authorities, as well as aligning APRA's work with Australia's 2020 Cyber Security Strategy[56]. APRA participates with Australia's other key regulatory agencies within the Council of Financial Regulators (CFR) in working groups covering a range of topics, including cyber risk.

In the Netherlands, the Central Bank (DNB) has established bodies with participants from all relevant authorities, called CYBORG, to pose questions and exchange views on relevant topics and incidents, all performed in strict confidence.

In Botswana, the supervisory authority (NBFIRA) has mutual cooperation and information exchanges with the Financial Intelligence Agency and has a seat in the Financial Stability Council of the country, composed of the Central Bank, Ministry of Finance, and Financial Intelligence Agency.

In the Czech Republic, the Central Bank conducts consultations on benchmarks and shares general information with the National Cyber and Information Security Agency.

In Jamaica, cyber information is regularly shared (at least quarterly) with other regulators through a financial regulatory committee established by the agencies overseeing the Jamaican financial industry.

In Armenia, the Central Bank of Armenia is working on a broader initiative related to establishment of a Security Operation Centre (SOC) that will serve as an information sharing platform for the financial sector.

A number of (EU) supervisors noted the successful international co-operation and information exchange taking place at the ESAs and the EIOPA levels through the establishment of working groups and information hubs (Austria; Bulgaria; Slovak Republic). In China, the CBIRC cooperates with foreign supervisory authorities by signing MoUs and conducting bilateral supervisory meetings and participating in supervisory colleges. In Colombia, the FSC currently shares information with the authorities of the national cybersecurity and cyber defence strategy, supervisory authorities of the Central American region, entities attached to the Pacific Alliance, and other entities under surveillance. The main channel used is corporate email accounts, through which newsletters, alerts, IOCs and incident reports are sent.

[56] APRA Annual Report 19/20.

In the UK, the Authorities Response Framework (ARF) was established, involving co-operation among five authorities to allow for co-ordinated action on major cyber incidents.

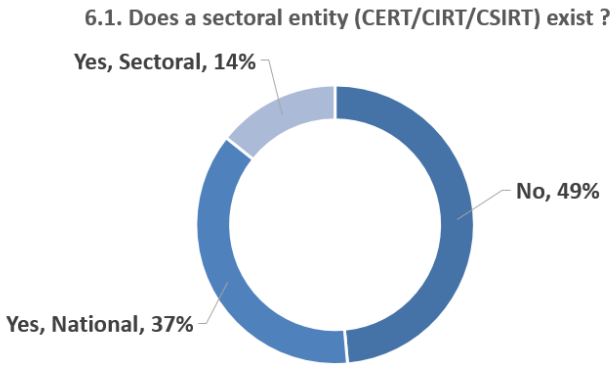
As part of interagency coordination efforts, many supervisors have put in place mechanisms to enable sharing of effective practices across the financial sector to enhance awareness and identify common cyber vulnerabilities. This arrangement, as in the case of proposed EU legislation, may include crisis-management activities and contingency exercises involving cyber-attack scenarios, with the aim of developing communication channels and gradually enabling an effective EU coordinated response in the event of a major cross-border ITC-related incident[57].

6.2 Co-operation and information sharing with national or sectoral response teams

The majority of respondent jurisdictions has response teams (CERT[58], CIRT[59], CSIRT[60]) at the national level (Figure 6.2). However, the survey found that **the information sharing between pension supervisory authorities and the National Computer Emergency Response Team (CERT) or similar bodies was either non-existent or immature** (Figure 6.2.1.).

In a few jurisdictions (Czech Republic; Germany; Ireland), computer emergency (or incident/security) response teams are part of the National Cyber Defence or Security Centres. For example, in Ireland, the CSIRT-IE is a body within the National Cyber Security Centre that provides assistance to constituents in responding to cyber security incidents at the national level. The body provides incident response services to government bodies and Critical National Infrastructure providers across Ireland, and acts as a national point of contact for international partners. Currently, there is no information sharing between CSIRT-IE and the Pensions Authority.

Figure 6.1.



Source: Members responses to the IOPS 2020 survey

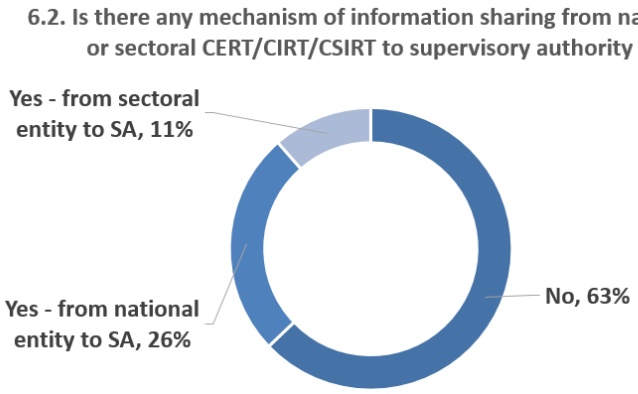
[57] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

[58] National Computer Emergency Response Team (CERT).

[59] National Computer Incident Response Teams (CIRT).

[60] National Computer Security Incident Response Team (CSIRT).

Figure 6.2.



Source: Members responses to the IOPS 2020 survey

Only a few pension supervisors reported tangible co-operation, focusing mainly on the exchange of information (on incoming threats and risks) or the sharing of reports on supervisory measures and the implementation of relevant legislation with the national incident centres.

In Germany, the National Cyber Defence Centre contributes to effective prevention of cyber risks through the permanent exchange of information among all federal authorities responsible for security. BaFin participates in the work of the centre and provides information regarding the financial sector.

In the Republic of North Macedonia, the national CIRT agency was established in 2020 and the MAPAS became a member.

The Colombian supervisor (FSC) is currently implementing the Malware Information Sharing Programme for the financial sector, for which the FSC is in charge. This platform will also be used for the exchange of cybersecurity information. The national CSIRT (COLCERT) exchanges newsletters, proofs of concept of the monitored entities, alerts, among others with the FSC.

In the Slovak Republic, the Ministry of Finance is the competent authority for cyber matters in the financial sector. Currently there are plans to change the law so that the National Bank of Slovakia becomes the competent authority in this area. Upon implementation of this change, the information from CIRT/CSIRT will become available for supervisory purposes.

Only a few jurisdictions have established financial or pension sector CERTs or similar entities (Colombia; Kenya; the Netherlands; Poland) with formal and informal channels to share information with supervisory authorities. In Kenya, the RBA set up a CERT computer emergency response (or readiness) team (SIRT). In the Netherlands, the Insurance-CERT and the Central Bank (DNB) exchange information and discuss relevant topics on cyber security via existing mechanisms (earlier mentioned CYBORG). In Poland, a CSIRT was established at the level of the supervisory authority (KNF). CSIRT KNF performs the tasks of the Sector Cybersecurity Team to coordinate activities and support the handling of security incidents affecting financial market entities. The KNF co-operates closely with CSIRT MON, CSIRT NASK and CSIRT GOV in the scope of coordinating the handling of serious cyber incidents.

6.3 Increasing awareness with the industry

Pension supervisors undertake the following **initiatives aimed at improving the awareness of supervised entities regarding cyber security matters**:

- Encourage firms to engage with and use guidance issued by national cyber security agencies and entities at the international level. The examples include Guidance published by the UK National Cyber Security Centre, on Cyber essentials, including the '10 Steps to Cyber Security'[61]; the recently released 'Board Toolkit: five questions for your Board's agenda'; in Belgium - Cyber Security Kit – materials prepared by the Cyber Security Coalition in Belgium[62]. In Australia, all regulated entities should consider engaging with the Australian Cyber Security Centre and further develop their cyber security capabilities through collaboration with other relevant forums and other sources of threat intelligence and response assistance[63]
- Developing **public/private testing for cybersecurity preparedness**: such testing is developed for the financial sector or its particular parts to periodically evaluate capabilities and functions included in the ICT and cyber risk-management framework of financial entities. Requirements for testing are usually based on the principle of proportionality, which takes into consideration the size, business activity and risk profiles of financial entities. Examples include the TIBER Test at the EU level; CBEST testing in the UK, which is work co-ordinated with the Bank of England and other partners, or cross-sectoral testing, involving multiple critical infrastructures
- Setting up dedicated platforms and web-pages with links to cybersecurity related resources at the authorities' websites (FCA, UK cyber resilience web-pages and FCA 'Good Cyber Security – foundations', UK Cyber information sharing partnership (CIPS platform))
- Publishing supervisory information such as circulars, reports, discussions papers, reviews, recommendations, periodic news messages/letters/flashes
- Contributing to national and international cybersecurity awareness campaigns. Examples include the national cyber security awareness campaign launched by the Centre for Cybersecurity Belgium and the Cyber Security Coalition in Belgium, supported by the FSMA, Belgium. In Hungary, the MNB participates in the European Cybersecurity Month[64], which is the European Union's annual campaign dedicated to promoting cybersecurity among EU citizens and organisations
- Organising joint cyber security events, including both cross-sectoral as well as pension-specific supervisory conferences (Austria)
- Organising training sessions (Colombia; Costa Rica; Kenya). In Kenya, the RBA incorporated cyber security topics in its Trustee Development Training Programme.

[61] https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

[62] www.cybersecuritycoalition.be

[63] APRA Information Paper, 2015/2016 Cyber Security Survey Results, September 2016.

[64] https://cybersecuritymonth.eu/

- Setting up supervisory education centres: The Polish Financial Supervision Authority has created the CEDUR (the Education Centre for Market Participants), which also focuses on cyber security matters.
- Maintaining formal and informal communication with individual entities (Austria, Bulgaria)

Key findings and conclusions

In most respondent jurisdictions, **the national cyber security strategies were published and dedicated national agencies were established** to strengthen cyber security of national critical infrastructure and ensure security in cyberspace. In a few jurisdictions, the pension sector, as part of the financial system designated critical infrastructure, was referenced within the national strategies. **Cyber risks in private pensions are similar to the risks prevalent in other parts of the financial sector.** They include phishing attacks, as well as other social engineering techniques, malware, spams, identity theft and account take-over, ransomware, web-based and web-application attacks, etc.

A number of jurisdictions witnessed **a distinct rise in the incidence of cyber attacks and their sophistication**. However, the attacks on pension entities have not resulted in serious material incidents affecting members' balances or the integrity of the pension funds. The **Covid-19 pandemic resulted in a spike in cyber threats,** like ransomware and phishing attacks. **Social engineering attacks** aimed at individuals have also become more frequent.

New IT and cyber regulations and revisions of existing requirements in the financial sector were adopted in about half of the respondent jurisdictions, with other jurisdictions also planning to do so. Regulations usually take the form of principles-based requirements, which enable them to fit into the increasingly digital financial environment and leave space for innovation. The Covid-19 pandemic, which presented important operational challenges, including for cyber security, accelerated adoption of these new regulations.

In parallel, **prudential requirements for operational resilience were reinforced**, with a focus on governance, risk management, testing of ICT systems, reporting on incidents, management of IT and cyber third-party risks, and reinforcement of surveillance in the area, alongside information and awareness sharing.

Harmonisation of regulatory and supervisory requirements in the areas of IT, cyber security, and cloud outsourcing was undertaken in a number of jurisdictions. In some jurisdictions, **cybersecurity regulations and standards relating to private pensions were developed,** taking into account the specificities of private pension entities.

Priorities to improve IT and cyber security of supervised undertakings is becoming an **area of strategic supervisory focus**, underpinned in some jurisdictions by **supervisory cyber security strategies**. Many of the respondents either have developed specific measures for the private pension sector (1/3 of the respondents) or plan to do so (another 1/3).

Pension supervisors usually act in concert and **draw on the accumulated expertise of peer regulators and other government agencies,** to design measures in support of the national cyber security strategy. They are generally **adopting a cross-sectoral approach** to address cyber risk, which is deemed a cross-financial-industry risk. In response to increased reliance on virtual working arrangements and remote technologies during the pandemic, dedicated **supervisory initiatives and recommendations were issued** requiring adoption of extra IT and cyber security measures, developing new guidelines including on IT security requirements for teleworking and remote access, conducting off-site inspections, introducing ad-hoc reporting requirements, including on cyber risks to ITC systems and related business continuity management, adopting special measures on potential pension scams, educating supervisory staff, etc.

Management of cyber risk by pension entities: About half of surveyed supervisors believe pension entities devote sufficient management attention and resources to cyber risk. However, a number of areas require greater attention by supervised entities:

1) governance and risk management practices
2) response and recovery, including business continuity plans
3) management of third-party risks
4) adequate training of staff regarding cyber security
5) comprehensive procedures related to cyber security by supervised entities; regular supervisory compliance assessment including cyber security disclosure control procedures
6) cyber security embedded into the organization's culture

In most respondent jurisdictions, there is no requirement for pension entities to estimate the cost of cyber incidents. In about half of the respondent jurisdictions, the entities are required to **adopt a written cyber security policy**.

In most jurisdictions, pension entities **perform periodic self-assessments of cyber security arrangements,** measured on the basis of both internal audits and external audits. Two-thirds of respondent jurisdictions have no regulatory requirements for pension entities to appoint an external auditor to assess their IT systems and cyber resilience. In contrast, a few jurisdictions mandate supervised entities to engage independent auditors to assess their information security controls and, if applicable, compliance with prudential regulations on cyber practices. In certain jurisdictions, self-assessment results and their accuracy and completeness are controlled by the supervisory authorities.

Supervisory measures: A **uniform framework** developed by supervisory authorities can provide useful guidance to financial entities, including pensions, **regarding performance of their own self-assessments and tests of their cyber security arrangements**. Such frameworks generally cover the information security strategy, policy and governance, training, awareness and resources; risk management and business continuity; management of configuration and access rights; risk management of outsourced services and IT tools; and reporting on security incidents. Guiding frameworks are also used by supervisors and enable them to evaluate levels of controls of information security and cybersecurity practices of the supervised entities.

Other supervisory tools and measures include **regular surveys of information systems** and **data quality** and publication of aggregated results. The surveys may steer the scope of more in-depth supervisory examinations and enable supervisors to share information on cyber experiences and identify industry best practices.

Half of the respondent **supervisors issued guidance on IT and cyber security,** mostly in the form of high-level principles. Such principles can be cross-sectoral or specific to the pension industry. The guidance focuses on governance, capability and resources, controls, monitoring, assessment, incident responses, reporting and disclosure, cyber awareness, and training.

Supervisory inspections: Two-thirds of respondent authorities organise **dedicated on-site inspections of control information and cyber security**. The examinations serve to monitor compliance with regulatory cyber-security requirements and supervisory guidance. They increasingly focus not only on financial institutions, but also on their

capacity to identify, handle and follow up on IT security incidents at third-party service providers.

Special **supervisory attention** is placed on **cyber security arrangements implemented by external third-party service providers** of pension entities and **the entire chain of sub-contracting arrangements.**

The **frequency and intensity** of such inspections is usually determined under a supervisory risk-based approach and in accordance with the principle of proportionality. A regular cycle of inspections in the area of cyber security is performed, usually on an annual basis or every two to three years. More systemically important entities could be reviewed more regularly than others.

Examinations can be conducted in partnership with other public authorities and supervisors (e.g., regarding vulnerability testing and threat intelligence, and "Red" team exercises to test a financial entity's cyber defences and response capability).

One of the reported **challenges** relates to the **preparedness and knowledge of supervisors**. Roughly half of the respondents evaluated their supervisory capacity as partially prepared. In the opinion of supervisors, regular training would appear to be a more cost-effective investment for supervisors in the long run than engaging external cyber threat intelligence analysts.

Conclusions:

The survey identified, amongst other things, **the need to improve data collection regarding major cyber incidents, along with analysis, classification and reporting to supervisory authorities** using the established protocols and templates. Consistent incident reporting mechanisms should enable supervisors to properly assess and monitor risks and develop suitable supervisory requirements. It should also help to reduce the associated costs to financial entities and generate cross-industry insights on best practice examples.

Effective supervision of cyber risk requires **close co-operation and information exchange between national financial sector regulators and other public authorities**. Survey results showed different levels of intensity of co-operation in the cyber risk area. Based on the insights from the survey, there may be a need to foster greater co-operation and enable supervisory exchanges on cyber security among the competent authorities. Supervisors also highlighted the importance of broadening open dialogue with the financial sector.

Supervisors recognised **the need to continue increasing cyber knowledge and cyber awareness across regulated entities and in relation to third-party service providers.** There is a need to increase such awareness at all staff levels of the supervised entities. Entities bear ultimate responsibility for the sharing of cyber knowledge throughout the entire sub-contracting chain. Supervisors also encourage information sharing initiatives that enable financial entities to exchange cyber threat information and intelligence on tactics, techniques, procedures, alerts and testing amongst themselves.

In view of the evolving landscape of cyber threats, their cross-border nature, and the interdependence of the global financial system, **it is important to promote continued international debate on cyber security and close international co-operation[65] among**

[65] BaFin Annual report 2019

supervisors[66], regulators, law enforcement agencies and financial institutions to develop a common understanding of the problem, and work together at the international level on a co-ordinated approach to issues to achieve more effective protection of financial entities and users against cyber threats.

[66] DNB Annual report 2019

References

APRA, Information paper, 2015/2016 Cyber Security Survey Results, www.apra.gov.au

APRA, Information papers, 2021, www.apra.gov.au

APRA Prudential Standard CPS 234: Information security, July 2019

APRA, Prudential Practice Guide, CPG 234 Information security, July 2019, www.apra.gov.au

APRA Insight Issue Three 2016, Insight Issue Four 2017, Insight Issue One 2018

APRA Annual Report 2019/2020

APRA Corporate Plan 2020/24

APRA Self-assessment – 2019/2020 financial year

BaFin Annual Report 2019, Annual report – BaFin, https://www.bafin.de

BaFin, Supervisory priorities, 2020

BaFin Perspectives Issue 1/2020, Cyber security

Centre for Cyber Security Belgium, Cyber security Incident Management Guide

CPMI - IOSCO, Guidance on cyber resilience for financial market infrastructures, June 2016

EIOPA, Outsourcing to the Cloud: EIOPA's contribution to the European Commission FinTech Plan, EIOPA 2019

EIOPA, Consultation paper on the proposal for Guidelines on outsourcing to cloud service providers, July 2019

EIOPA, Opinion on the supervision of the management of operational risks faced by IORPs, July 2019

ENISA Threat Landscape Report 2018, 15 Top Cyber threats and Trends, January 2019

FCA, TPR, Regulating the pensions and retirement income sector: our joint regulatory strategy, October 2018

FCA, Cyber security – industry insights, March 2019

FCA, Cyber and Technology Resilience: Themes from cross-sector survey 2017/2018, November 2018

FMA, Austria, Guide on IT Security for pension funds, December 2018, www.fma.gv.at/fma/fma-leitfaeden/

FMA, Austria, Digitalisation in the Austrian Financial Market, Status Quo, Outlook and Call for Input, June 2019

FMA, Facts and Figures, Trends and Strategy 2019, https://www.fma.gv.at/download.php?d=4025

FSB, Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practice, October 2017

G7 Fundamental Elements of Cybersecurity for the Financial Sector, October 2016

G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector

IAIS, Application Paper on Supervision of Insurer Cybersecurity, November 2018

IMF, Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, Antoine Bouveret, WP/18/143

IOPS, IOPS Statement on pension supervisory actions to mitigate consequences of Covid-19 crisis, May 2020

KPMG, Regulation and supervision of FinTech, Ever-expending expectations, March 2019, www.kpmg.com

Mandatory Provident Fund Schemes Authority (MPFA) of Hong Kong, China, Annual Report 2017-2018; Annual Report 2016-2017

The Pension Regulator, Cyber security principles for pension schemes, April 2018

Toronto Centre, Supervision of Cyber Risk, December 2018

U.S. Securities and Exchange Commission (SEC), 2019 and 2018 National Exam Program Examination Priorities, Office of Compliance Inspections and Examinations

U.S. SEC Office of Compliance Inspections and Examinations (OCIE), National Exam Program, Risk Alert, OCIE's 2015 Cybersecurity Examination Initiative, Volume IV, Issue 8, 2015

U.S. SEC Office of Compliance Inspections and Examinations (OCIE), National Exam Program, Risk Alert, Cybersecurity: Ransomware Alert, Volume VI, Issue 4

World Bank, Financial Sector's Cybersecurity: A regulatory Digest, May 2019

Annex 1

National Cyber security strategies

Australia	2020	Australia's cyber security strategy 2020 https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf
Austria		Austrian cyber security strategy https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf
Botswana	Draft	(Draft) National cyber security strategy https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00042_02_botswana-national-cybersecurity-strategy.pdf
Bulgaria	2020	National Cyber Security Strategy "Cyber Resilient Bulgaria 2020" http://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1120 (in Bulgarian only).
Colombia	2020	National Trust and Digital Security Policy Year 2020: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf Year 2016: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf Year 2011: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf
Costa Rica	2017	National Cyber Security Strategy https://www.micit.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf
Croatia	2015	The National Cyber Security Strategy and the Action Plan for the implementation of the National Cyber Security Strategy https://narodne-novine.nn.hr/clanci/sluzbeni/2015_10_108_2106.html
Czech Republic	2015	The National Cyber Security Strategy for the Czech Republic for the period from 2015 to 2020) https://nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/
France	2011	Information systems' defence and security – France's strategy https://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite-2/
Hungary	2013	The National Cyber Security Strategy of Hungary https://2010-2014.kormany.hu/download/a/b6/21000/National_Cyber_Security_Strategy_of_Hungary.pdf
Iceland	2019	Recommendations on risks management in the operation of information systems of the regulated entities (tbc) https://www.fme.is/media/leidbeinandi_tilmaeli/Leidbeinandi-tilmaeli-numer-1-2019.pdf
Ireland	2019	Ireland's National Cyber Security Strategy

		https://www.dccae.gov.ie/en-ie/communications/topics/Internet-Policy/cyber-security/national-cyber-security-strategy/Pages/NCSC-Strategy.aspx
Kenya	2014	National Cyber Security Strategy http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf
Malawi	Draft	National Cyber Security Strategy (Final Draft) https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00019_07_Malawi%20national-cybersecurity-strategy.pdf
Morocco	2012	National Cyber Security Strategy https://www.dgssi.gov.ma/sites/default/files/attached_files/strategie_nationale.pdf
The Netherlands	2018	Dutch cyber security agenda: The Netherlands digitally safe https://www.rijksoverheid.nl/onderwerpen/cybercrime-en-cybersecurity/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig
Poland	2019	Cyber security strategy of the Republic of Poland https://www.dziennikustaw.gov.pl/MP/rok/2019/pozycja/1037
Portugal	2015	The Portuguese National Strategy for the Security of Cyberspace https://www.cncs.gov.pt/content/files/rcm_36-2015.pdf
Slovak Republic	2015-2020	National Cyber Security Strategy https://www.nbu.gov.sk/en/cyber-security/national-cyber-security-strategy/index.html
Turkey	2013	National Cyber Security Strategy (reviewed periodically) https://www.uab.gov.tr/siber-guvenlik

Supervisory Authorities' Strategies on IT security, Digitalisation or Cyber risk

Australia	2020	APRA's Cyber Security Strategy 2020-24 as referenced in the 2020-24 Corporate Plan APRA 2020-2024 Corporate Plan | APRA
Bulgaria	2018-2020	FSC Financial Technology Monitoring Strategy for non-banking financial sector https://www.fsc.bg/bg/finansovi-inovacii/strategiya-za-nablyudenie-na-finansovite-inovatsii-fintech/ (in Bulgarian only).
Germany		BaFin's Digitalisation Strategy https://www.bafin.de/EN/DieBaFin/ZieleStrategie/Digitalisierungsstrategie/digitalisierungsstrategie_artikel_en.html
Hungary		The MNB FinTech Strategy 'Financial innovation and stability' https://www.mnb.hu/en/innovation-hub/news/the-mnb-published-its-fintech-strategy
Slovak Republic	2020	Strategy for the supervision of cyber security at supervised entities