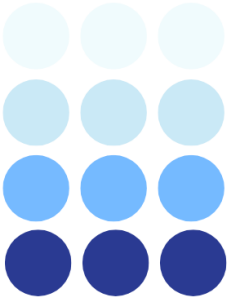
*IADI Fintech Briefs provide high-level overviews and key takeaways on Fintech topics of relevance to deposit insurers.*



# FINTECH BRIEF

## CYBERSECURITY AND DEPOSIT INSURANCE
AN INTRODUCTION

**NO. 18**

JAY S. MUNNELLY & COLIN P. LEACH

**November 2024**

IADI Fintech Briefs are written by Members of the IADI Fintech Technical Committee (Fintech TC), and from time to time by other authors, and are published by IADI. They provide high-level overviews and key takeaways on fintech topics of relevance to deposit insurers. The views expressed are those of the author(s) and do not necessarily represent the views of IADI or the institution to which the authors are affiliated. The authors are grateful to the Fintech TC, Edward Garnett, Rachel Youssef, Mario Diaz, Rob Drozdowski, Lloyd McIntyre, William Henley, Jr., Mathew Reed, Todd Eves, Nancy Lim, Shannon Dahn, Jan Nolte, Kazuaki Hara, Nan Zhou, Bert Van Roosebeke, and Ryan Defina for helpful comments.

The editor of the IADI Fintech Brief series is Bert Van Roosebeke (IADI).

This publication is available on the IADI website (www.iadi.org).



International Association of Deposit Insurers (IADI), C/O Bank for International Settlements,
Centralbahnplatz 2, CH-4002 Basel, Switzerland. Tel: +41 61 280 9933 Fax: + 41 61 280 95

Jay S. Munnelly
FDIC
jmunnelly@fdic.gov

Colin P. Leach
FDIC
cleach@fdic.gov

# CYBERSECURITY AND DEPOSIT INSURANCE: AN INTRODUCTION

**Executive Summary**

This introductory brief provides foundational background on cybersecurity for IADI members and aims to:

1 Create awareness of cybersecurity risks and threats to deposit insurance system operations and member institutions;
2 Introduce the existing standards, frameworks, and best practices to describe, respond, and recover from cyber incidents;[1]
3 Provide brief case studies of deposit insurers (DIs) responding to cyber incidents; and
4 Introduce resources for capacity building of cybersecurity strategy for DIs.

The financial services industry faces increasing cyberattacks from domestic and international hackers, state actors, and criminal groups. According to one estimate, the global average cost of a data breach is USD 4.88 million.[2] Several notable cybersecurity breaches have affected the financial sector and caused major disruptions including financial, legal, and reputational impacts.

Deposit insurers and other financial safety net participants also should consider the possibility of an institution's failure due to a cybersecurity event. Most preparations for an institution's failure focus on insolvency or liquidity problems. However, deposit insurers and other safety net players must consider operational failure scenarios and contingencies should they be called upon to intervene.

The brief also provides useful cybersecurity global standards, frameworks, and best practices that DIs and deposit-taking institutions can use to avert or mitigate cyberattacks. Importantly, these resources provide a structured methodology for identifying, assessing, and managing cyber-related risks to businesses of all types and sizes to improve their cybersecurity preparedness and risk management functions.

Lastly, the lessons learned from the DI case studies highlight several common themes in deposit insurers' approaches to cybersecurity. First, all have incorporated cybersecurity as a critical element of their information technology modernisation programs. By doing so, cybersecurity is implemented "by design and default" across the entirety of a deposit insurers' technological infrastructure. DIs are also using private sector expertise to supplement their own in-house knowledge and expand the scope of preparation. Finally, deposit insurers also partner with other financial safety net players to exchange knowledge and conduct joint exercises, allowing them to position their cybersecurity practices in the context of the broader financial safety net.

[1] Financial Stability Board, "Cyber Lexicon" (April 13, 2023), https://www.fsb.org/wp-content/uploads/P130423-3.pdf , p. 10. The FSB cyber lexicon defines a cyber incident as "a cyber event that: i. jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or ii. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not."
[2] IBM Security, "Cost of a Data Breach Report 2024," https://www.ibm.com/reports/data-breach, p. 5.

# 1 Cybersecurity in Financial Services

Cybersecurity is defined differently depending on the industry and individual jurisdiction concerned. For financial services, the Financial Stability Board's (FSB) Cyber Lexicon provides a clear definition. The Cyber Lexicon supports standard-setting bodies such as the Basel Committee on Banking Supervision (BCBS), the Committee on Payment and Markets Infrastructure (CPMI), and the International Organization of Securities Commissioners (IOSCO) in their efforts to address cybersecurity risks to the financial sector.[3]

The lexicon defines cybersecurity as "the preservation of confidentiality, integrity, and availability of information and/or information systems through the cyber medium. In addition, other properties such as authenticity, accountability, nonrepudiation, and reliability can [and should] also be involved." Table 1 below provides definitions for each of the properties.

**Table 1. FSB Lexicon Definitions of Cybersecurity Properties[4]**

| Property | Definition |
|---|---|
| **Accountability** | The actions of an entity may be traced uniquely to that entity. |
| **Authenticity** | An entity is what it is supposed to be. |
| **Availability** | Information is accessible and usable on demand by an authorised entity. |
| **Confidentiality** | Information is neither made available nor disclosed to unauthorised individuals, entities, processes, or systems. |
| **Integrity** | Information is accurate and complete. |
| **Non-Repudiation** | An event or action's occurrence can be proved and traced back to the originating entity. |
| **Reliability** | A system demonstrates consistent intended behaviour and results. |

These properties have significance for deposit insurance systems. Financial supervisors and other safety net players have the power to access information alongside DIs and must rely on the confidentiality, integrity, and availability of depositor information needed to perform their duties. Similarly, DIs and deposit-taking institutions (DTIs) must have safeguards in place to ensure that only authorised persons can access their information systems holding depositor information, and they function as designed. These properties are also symbiotic; for example, confidentiality protects the integrity of the information and makes it available only to authorised users.

# 2 Background

The evolution of digital financial services and, by extension, the evolution of cyberattacks, has made cybersecurity a critical concern for both DIs and DTIs. This concern is partially motivated by the potential cost of cyberattacks for DIs and DTIs. A 2024 IBM report found that the top five countries with the highest average cost of a data breach for all 17 industries were the United States at USD 9.36 million, Germany at USD 5.31 million, Italy at USD 4.73 million, Canada at USD 4.66 million, and the United Kingdom at USD 4.53 million.[5] The global average total cost of a data breach increased 10% in one year to USD 4.88 million from USD 4.45 million in 2023.[6] These costs can increase dramatically depending on the size of the enterprise and the scope of the breach.

The 2017 Equifax breach, which exposed the personal information of more than 147 million individuals, cost the firm at least $1.7 billion, including $800 million in settlements to affected individuals and $337 million on other related

[3] Financial Stability Board, "Cyber Lexicon" (April 13, 2023), https://www.fsb.org/wp-content/uploads/P130423-3.pdf, p. 3. This definition is adopted from work by the Committee on Payments and Market Infrastructures (CPMI)-International Organization of Securities Commissioners (IOSCO), which cites the National Initiative for Cybersecurity Careers and Studies.
cyber medium relates to, within, or through the interconnected information infrastructure of interactions among persons, processes, data, and information systems.
[4] Ibid., pp. 7-12.
[5] This report calculates costs for four categories- lost business, detection and escalation, notification, and post-breach response. IBM Security, "Cost of a Data Breach Report 2024," https://www.ibm.com/reports/data-breach, p. 9.
[6] Ibid., p. 8. Financial services firms accounted for 14% of the 17 industries sampled.

issues, including additional technological and data security.[7] Attacks of this magnitude could be particularly problematic for DIs, given that 87% of DIs have an operating budget below USD 20 million.[8] These limited resources could mean that many DIs are limited in their ability to respond to a data breach or other cybersecurity event.

Cybersecurity is also critical to the financial services industry.[9] U.S. financial institutions reported the highest number of cyberattacks, followed by those based in Argentina, Brazil, and China. A 2022 report from cloud computing firm VMware highlights the global financial sector's particular cybersecurity challenges:[10]

- 63% of DTIs experienced an increase in destructive attacks, a 17% increase from the previous year.
- 74% of DTI security executives reported that their institutions experienced one or more ransomware attacks in 2021, and 63% of those victims paid the ransom.
- 66% of DTI security executives acknowledge that their institutions experienced attacks targeting market strategies, and 25% stated that market data is the primary target for cyberattacks.
- Most DTIs planned to increase their IT budget by 20-30 percent.

DTIs are also prioritising cybersecurity because of the sheer scope and scale of some cyberattacks, such as the 2007 cyberattack on Estonia's banks,[11] the 2016 theft from the Bangladesh Bank's account at the Federal Reserve Bank of New York,[12] the 2017 Equifax breach,[13] and the May 27, 2023 zero-day attack[14] by the Cl0p (Clop) cybercrime group on MOVEit file transfer web application, a managed file for securely sending large volumes of sensitive data. Clop exploited vulnerability on all MOVEit file transfer versions affecting over 2,000 organisations globally and surpassing 60 million individuals.[15] Clop immediately started extorting victims in early June 2023 to post stolen data for unpaid ransom and may earn up to USD 100 million from the MOVEit campaign.[16]

One of the most notable cybersecurity incidents to affect a DTI was the attack on U.S.-based CapitalOne in 2019, which compromised data belonging to approximately 106 million credit card holders and applicants in the United States and Canada between 2005 and 2019.[17] Insecure firewall configurations enabled an insider's theft of information such as names, addresses, social security numbers, and bank account numbers. CapitalOne ultimately settled in a USD 190 million class action lawsuit, one of the costliest in industry history.[18] The CapitalOne example is also notable because a company insider conducted the attack, reinforcing that cybersecurity is not just a policy issue, but also an aspect of company culture.

---

[7] Ben Lane, "Equifax expects to pay out another $100 million for data breach" *Housing Wire*, (February 14, 2020), https://www.housingwire.com/articles/equifax-expects-to-pay-out-another-100-million-for-data-breach/
[8] IADI Annual Survey Data, 2023. Based on 82 members which provided operating budget figures.
[9] Sebastian Doerr, Leonardo Gambacorta, Thomas Leach, Bertrand Legros, and David Whyte, "Cyber risk in central banking," *BIS Working Papers* No. 1039 (September 2022), https://www.bis.org/publ/work1039.pdf
[10] Tom Kellerman, "Modern Bank Heists 5.0: The Escalation from Dwell to Destruction," *VMWare,* (April 20, 2022), https://news.vmware.com/security/modern-bank-heists-5-0-the-escalation-from-dwell-to-destruction
[11] Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," "Cooperative Cyber Defence Centre of Excellence," (October 2018), https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
[12] Joshua Hammer, "The Billion Dollar Bank Job," *New York Times* (May 3, 2018), https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html
[13] Federal Trade Commission, "Equifax Data Breach Settlement," (December 2022), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement
[14] NIST defines this as "an attack that exploits a previously unknown hardware, firmware, or software vulnerability." NIST Cybersecurity Resource Center, "Glossary: Zero Day Attack", https://csrc.nist.gov/glossary/term/zero_day_attack
[15] Help Net Security (September 26, 2023), Cl0p's MOVEit attack tally surpasses 2,000 victim organizations - Help Net Security
[16] Bank Info Security (July 24, 2023), As Ransomware Monetization Hits Record Low, Groups Innovate
[17] Edward Krost, "10 Biggest Data Breaches in Finance," *UpGuard* (May 3, 2023), https://www.upguard.com/blog/biggest-databreaches-financial-services
[18] Jennifer Surane, "CapitalOne Settles Class Action Lawsuit for $190 Million," *Bloomberg* (December 23, 2021), https://www.bloomberg.com/news/articles/2021-12-23/capital-one-agrees-to-190-million-settlement-in-cyber-lawsuit#xj4y7vzkg

Internationally, there are some regional distinctions in motivations underlying attacks.[19] Financial motivations are the primary incentive across all regions, ranging from 96% in Northern America (NA) to 54% in the Asia-Pacific (APAC). Other motivations such as espionage vary across regions, accounting for 46% of attacks in APAC and 21% in Europe, and the Middle East and North Africa (EMEA), but just 3% in NA and 2% in Latin America and the Caribbean (LAC). Attack types also differ within these four regions. For example, social engineering[20] attacks predominate in NA and EMEA, whereas ransomware,[21] malware,[22] and hacking[23] are more prevalent in APAC and LAC.

These various motivations and attack vectors further illustrate the challenges DIs and DTIs face in cybersecurity. As will be covered in later sections, reporting requirements and supervisory regimes can differ depending on the country. Differences in data protection and sharing requirements may address challenges in some regions, but potentially create them in others, and supervisory regimes add to these challenges.

## 2.1 Cybersecurity Impact on DIs and DTIs

A 2022 U.S. Financial Stability Oversight Council (FSOC) report notes that the U.S. financial sector's reliance on global computer networks make it potentially vulnerable to threats from nation-state actors. The report highlights several cyberattacks by a number of state-affiliated actors against the U.S. Treasury and both U.S. and non-U.S. DTIs.[24] A November 2021 ransomware attack on the Industrial and Commercial Bank of China (ICBC), disrupted ICBC's operations, preventing it from settling some pending U.S. Treasury trades and causing a spike in yields. Moreover, it also left ICBC's U.S. broker dealer owing BNY Mellon approximately USD 9 billion.[25] Ultimately, ICBC opted to pay the ransom, a decision that highlights a dilemma facing DTIs: should priority be given to restoration of operations at any cost, or should the priority be defeating a cyberattack?

What are the real implications of cyberattacks for institutions and regulators, including deposit insurers? In table 2, the FSOC identifies three channels through which a cyberattack could harm the financial system.

[19] Verizon Communications, "2022 Data Breach Investigations Report (DBIR)," https://www.verizon.com/business/engb/resources/2022-data-breach-investigations-report-dbir.pdf , pp. 80-85

[20] As defined by NIST, "An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks." NIST Computer Security Resource Center, "Glossary: Social Engineering," https://csrc.nist.rip/glossary/term/social_engineering

[21] As defined in the FSB Cyber Lexicon, "Malware (malicious software) that is used to commit extortion by impairing the use of an information system or its information until a ransom demand is satisfied." *FSB Cyber Lexicon,* p. 13.

[22] As defined in the FSB Cyber Lexicon, "Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems." Ibid., p. 12.

[23] As defined by NIST, "An unauthorized user (i.e., a hacker) who attempts to or gains access to an information system." NIST Computer Security Resource Center, "Glossary: Hacker" https://csrc.nist.gov/glossary/term/hacker

[24] Financial Stability Oversight Council, "2022 Annual Report," https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf, pp. 66-67.

[25] The Fallout from the ICBC Ransomware Attack Continues. https://www.paymentsjournal.com/the-fallout-from-the-icbchttps://www.paymentsjournal.com/the-fallout-from-the-icbc-ransomware-attack-continues/ransomware-attack-continues/

**Table 2. FSOC Threats to Financial Stability from Cyber Incidents[26]**

| Channel | Incident Effects |
|---|---|
| I | First, the incident could **disrupt key institutions with few or no substitutes**, such as central banks, exchanges, sovereign and sub-sovereign creditors, including U.S. state and local governments (such as e.g. the deposit insurer), custodian banks, and payment clearing and settlement systems. It could also disrupt other providers of critical services such as fund administrators, pricing or other data providers, specialty software providers, or cloud service providers. |
| II | Second, the incident could **compromise the integrity of critical data** and disrupt the stable functioning of the financial institutions and the financial system. If data is corrupted on a sufficiently large scale, it could lead firms not to trust their internal information and information they are receiving from counterparties and thus disrupt system functionality. A significant data corruption event would pose further problems if a systemically important failing firm had to be resolved. Determining the accuracy of records or ascertaining the financial standing of various counterparties, depositors, and obligors may not be possible, which would impede the deposit insurer's resolution actions. |
| III | Third, a cybersecurity incident that causes a loss of confidence at a key financial institution could **cause customers or market participants to question the safety or liquidity of their assets or transactions**, leading to the significant withdrawal of assets (e.g. deposits) or activity from the markets. Additionally, a cybersecurity incident involving the theft of sensitive data has privacy implications for consumers, which could lead to identity theft and fraud, resulting in a loss of confidence. |

## 2.2 What are the risks and the threats to financial stability?

Cyberattacks have evolved and are becoming more frequent, complex, and severe, affecting DTIs and government agencies globally. As IADI noted in a September 2021 policy brief, "cybersecurity is increasingly becoming a factor of risk to the provision and availability of digital financial products, and thus to financial stability as a whole … Moreover, DIs themselves may be exposed to cybersecurity risks in their operations."[27]

The global financial regulatory community has already identified cybersecurity as a key priority for several years. In March 2017, the G20 Ministers and Governors Meeting made the G20's first statement on financial services and cybersecurity: "The malicious use of Information and Communication Technologies (ICT)[28] could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability."[29] The G20 ministers committed to promoting "the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20."[30]

A subsequent October 2017 assessment conducted by the FSB at the G20's request found that all FSB member jurisdictions had released regulations or guidance related to cybersecurity in the financial sector, and that 72% of them were planning to issue new regulations by 2018.[31] The FSB continues to have an active role in shaping regulatory Format

[26] Ibid., p. 66.
[27] Bert Van Roosebeke and Ryan Defina, "Policy Brief No. 4: Five Emerging Issues in Deposit Insurance," International Association of Deposit Insurers (September 2021), p. 5.
[28] NIST defines ICT to include "all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks)."
https://csrc.nist.gov/glossary/term/information_and_communications_technology
[29] Communique of the G20 Finance Ministers and Central Bank Governors Meeting, Baden-Baden, Germany, (March 17-18, 2017), https://carnegieendowment.org/files/g20-communique.pdf
[30] Ibid.
[31] Financial Stability Board, "Stocktake of Publicly Released Cybersecurity Regulations, Guidance, and Security Practices," (October 13, 2017), https://www.fsb.org/wp-content/uploads/P131017-2.pdf, p. 3.

for Incident Reporting Exchange (FIRE) proposal, which focuses on harmonising cyber incident reporting by financial institutions across jurisdictions.[32]

Cybercriminals routinely search for vulnerabilities to exploit in order to gain access to or compromise systems. These vulnerabilities can be caused by lax security configurations or misconfigurations within their information systems, weak logical and physical control environments, lack of training, or poor cyber hygiene practices. Attackers can also use various attack vectors such as ransomware attacks, stolen credentials,[33] phishing attacks,[34] supply chain attacks,[35] DDoS attacks, fraudulent money transfer, and others. IBM's 2022 report on data breaches noted that stolen credentials[36] may expose DTIs to a range of risks that include loss of confidentiality and integrity of sensitive data, such as customer information and confidential business information. They also enable cybercriminals to disrupt and degrade systems or process fraudulent financial transactions that may not be recovered by the institutions.

Cyberattacks present clear costs for DTIs in terms of business loss due to service unavailability and funds spent on recovery and restoration from attacks. A cyberattack could also have an important impact on public confidence in the individual DTI and potentially the broader financial system. Although there is no documented case of a DTI's failure due to a cyberattack, the SolarWinds attack in December 2020[37] and the Colonial Pipeline cyberattack in May 2021 provide examples of where public reaction to an attack had a greater impact than the attack itself.[38]

A similar scenario could occur if a DTI was unable to conduct business or failed due to a cyberattack, leading to a loss of public confidence in both the affected and unaffected institutions. Such contagion could occur if a cyberattack disrupted significant service providers, which could in turn affect the customers of hundreds of DTIs offering core banking applications. The International Monetary Fund (IMF) stated similar concerns in a March 2023 blog, noting that "tight financial and technological interconnections" are not just a conduit for cyberattacks themselves, but could also cause loss of confidence.[39]

## 3 Cybersecurity Resolution Risk from Operational Failure

As the pace and intensity of cyberattacks increase, a cyberattack on a DTI of sufficient severity and duration may require DIs or resolution authorities to resolve a failing DTI. As authorities typically resolve DTIs that are failing for financial reasons, an operational failure stemming from a cybersecurity event presents a different challenge entirely. In an operational impairment situation, DTIs will implement their incident response plans with the focus on their cybersecurity resiliency and recovery capabilities until they are made whole. If these efforts fail, resolving the institution may be the only available option left to the authorities.

Therefore, DIs may want to contemplate their legal authority to intervene in a DTI failing for operational reasons. This scenario is plausible given the growing dependencies of DTIs on IT core banking products and services from third-party vendors that are further exacerbated by the increasing frequency of cyberattacks. DIs may therefore wish to prepare for contingencies and scenarios in case they are called upon to intervene. Also, DIs would likely have to account for sudden

---

[32] Financial Stability Board, "Format for Incident Reporting Exchange (FIRE): A possible way forward," (April 13, 2023), https://www.fsb.org/2023/04/format-for-incident-reporting-exchange-fire-a-possible-way-forward/

[33] As defined by NIST, evidence attesting to one's right to credit or authority.

[34] FSB Cyber Lexicon: A digital form of social engineering that attempts to acquire private or confidential information by pretending to be a trustworthy entity in an electronic communication.

[35] NIST definition: Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.

[36] Cybercriminals perform attacks to steal users' credentials such as passwords, usernames, e-mail addresses, and other forms of identification used by customers, employees, and third parties to authenticate themselves to systems as well as theft of system credentials, such as certificates.

[37] U.S. Department of the Treasury, Office of Financial Research, "Annual Report to Congress 2022," (January 12, 2023), https://www.financialresearch.gov/annual-reports/files/OFR-Annual-Report-2022.pdf, p. 87.

[38] Danny Brando, Antonis Kotidis, Ann Kovner, Michael Lee, and Stacy L. Schreft, "Implications of Cyber Risk for Financial Stability," *FEDS Notes* (May 12, 2022), https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-forfinancial-stability-20220512.html

[39] Tobias Adrian and Caio Ferreira, "Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards," *IMF Blog* (March 2, 2023), https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-needbetter-safeguards

and abrupt operational impairments brought on by a cyber incident with little to no advance warning. This shorter timeframe may negatively impact insured depositors and exacerbate risks to the deposit insurance fund.

To date, there are no known resolution efforts undertaken by any authorities resulting from an operational impairment of a failing DTI caused by a cybersecurity event. In 2022, the otherwise solvent Amsterdam Trade Bank (ATB) went bankrupt due to sanctions imposed by U.S. and U.K. on the lender and its Russian parent company, Alfa Bank. In addition to the direct implications for its links to the financial system, the sanctions caused Microsoft to pull ATB's email accounts, and Amazon and other technology providers to pull cloud and other services.[40] In this sense, ATB failed not because of any financial factor but rather because it was unable to access its third-party technology service providers.

In the United States, DIs would allow a DTI undergoing a severe cyber incident to focus on remedial action and notify the appropriate authorities when required by regulation. The lingering question is when the DIs should get involved without interfering with the DTI's operation. Typically, in this scenario, DIs render advice as necessary and communicate regularly with DTIs to ensure incident resolution.

# 4 Cybersecurity Laws, Regulations, Standards, Frameworks and Best Practices

Cybersecurity standards and frameworks provide a structured methodology for identifying, assessing, and managing cyber-related risks to businesses of all types and sizes to improve their cybersecurity preparedness and risk management functions. Although *standards* may be unique and specific to their size, industry, or sectors, cybersecurity *frameworks* are generally applicable to all organisations.

Cybersecurity standards are a set of guidelines or *best practices* that organisations such as the DTIs can use to improve their cybersecurity posture. Cybersecurity frameworks should be designed to include *best practices* used to protect information systems and networks, and to manage cybersecurity risk within an enterprise's critical infrastructure.

On an enterprise level, the development of a cybersecurity program should include a clear plan and an understanding of the institution's preparedness for cyber risk and consider management's risk appetite, risk management practices, and overall strategic direction. As such, the cybersecurity strategy should include the three critical areas of governance, technology, and operations. Once adopted, the strategy should help reduce exposure to cyberattacks, and assist in the identification of potential security gaps or weaknesses.

While a full review of standards and frameworks is out of this brief's scope, it will cover widely-used or required standards and frameworks along with the associated regulations in this section as they apply primarily to DTIs.[41] This section first covers U.S. laws and regulation and also introduces examples from other jurisdictions before dealing with standards and frameworks both from the U.S. and other jurisdictions and closes with a number of best practices.

## 4.1 U.S. Cybersecurity Law and Regulation

In the U.S., banks leverage their respective cybersecurity standards, frameworks, and self-assessment tools to manage the risks of evolving cybersecurity threats, ensure operational resilience, and satisfy the Federal Banking Agencies' (FBA) expectations set forth through regulation and guidance.[42] The principal cybersecurity and information security requirements derive from the Interagency Guidelines Establishing Information Security Standards for Safety and Soundness (Appendix B to Part 364)[43] that are issued as specified by the Gramm-Leach-Bliley Act (GLBA) of 1999. GLBA requires the FBAs to establish appropriate standards that:

- Ensure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of such records;

[40] Jacob Atkins, "Solvent but Bankrupt: How Sanctions Felled Amsterdam Trade Bank," *Global Trade Review* (May 31, 2022), https://www.gtreview.com/news/europe/solvent-but-bankrupt-how-sanctions-felled-amsterdam-trade-bank/

[41] Ibid., ISO/IEC 27001. For instance, the frameworks such as the MITRE ATT&CK®, Committee of Sponsoring Organizations (COSO), and Information Technology Infrastructure Library (ITIL) that are in limited use by DTIs are not covered here.

[42] In the United States, the Federal Banking Agencies include the Office of the Comptroller of the Currency, the Federal Reserve Board, and the Federal Deposit Insurance Corporation. 12 USC 1462, "Definitions," https://www.govinfo.gov/content/pkg/USCODE-2015-title12/html/USCODE-2015-title12-chap12-sec1462.htm

[43] Gramm-Leach-Bliley Bill, Section 501b https://www.ffiec.gov/exam/infobase/documents/02-con-501b_gramm_leach_bliley_act-991112.pdf.

- Protect against unauthorised access to or use of such records or information which could result in substantial harm or inconvenience to any customer; and
- Ensure the proper disposal of customer information and consumer information.

The GLBA Information Security Standards address administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information that DTIs are expected to follow when operating in the U.S. marketplace. These foundational standards underpin DTI cybersecurity programs.

DTIs operating in the U.S. marketplace are also subject to information reporting expectations that provide the FBAs with awareness of potential systemic cybersecurity risks and criminal activity. For example, the Bank Secrecy Act (BSA) of 1970 requires DTIs to submit Suspicious Activity Reports (SARs) for suspicious transactions that involve cybersecurity events.[44]

The U.S. FBAs issued a joint final rule in November 2021 on *"Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers"* that requires DTIs to notify their primary federal regulator as soon as possible and no later than 36 hours after it determines that a "notification incident" (as identified in the regulation) has occurred.[45] The Computer-Security Incident Notification rule also requires a bank service provider to notify a DTI's central point of contact *"as soon as possible"* when an incident has lasted four or more hours.

In addition to the FBA regulations, the Sarbanes-Oxley Act (SOX) of 2002 requires that all publicly-traded companies, including publicly-traded DTIs, address common cybersecurity risks that could impact financial activity.[46] SOX shares common cybersecurity controls with the National Institute of Standards and Technology (NIST) Cybersecurity Framework that will be discussed later.

## 4.2 Cybersecurity Law and Regulation in Other Jurisdictions

The European Union (EU) has introduced many key cybersecurity regulations affecting financial services firms, including DTIs. The 2015 Revised Payment Systems Directive (PSD2) requires all payment service providers to implement strong customer authentication (e.g., two-factor authentication) for users and also requires payment services providers to implement cybersecurity policies such as regular testing, risk assessment procedures, and requiring strong customer authentication for payment initiation and processing.[47]

The 2018 General Data Protection Regulation (GDPR) extends existing rights to privacy into the digital sphere by giving users greater control over how their personal data is used. Compliance is mandatory for all businesses processing data as part of its activities in the EU, regardless of where the firm is based. The GDPR enshrines integrity and confidentiality as key principles of the regulation and requires firms to not only implement "appropriate technical and organisational measures" for cybersecurity, but also to include data protection considerations "by design and default" in new systems.[48] The U.K. also incorporated the GDPR in its domestic law following its departure from the EU.

The EU will also implement the Digital Operational Resilience Act (DORA) in 2024. DORA requires financial services firms to, among other things, set clear risk tolerances, identify critical functions that could be targets for cyberattack, and record all significant cyber threats.[49] DORA also requires financial service firms to notify clients and counterparties to take protective measures to defend against exposure to significant cyber threats.[50]A similar focus can be found in the

[44] FinCEN FAQs on Cyber-Events: https://www.fincen.gov/frequently-asked-questions-faqs-regarding-reporting-cyber-eventscyber-enabled-crime-and-cyber
[45] Briefly defined, a "notification incident" refers to an incident that has or is likely to materially disrupt or degrade a DTI's ability to carry out operations, business lines whose failure could result in a material loss of profit, or operations whose failure would threaten U.S. financial stability. The full definition can be found in "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers", *Federal Register* 86, no. 223 (November 23, 2021), https://www.govinfo.gov/content/pkg/FR-2021-11-23/pdf/2021-25510.pdf, pp. 66424-66444.
[46] Top 8 Cybersecurity Regulations for Financial Services, SOX: https://www.fincen.gov/frequently-asked-questions-faqsregarding-reporting-cyber-events-cyber-enabled-crime-and-cyber
[47] European Central Bank, "The revised Payment Services Directive (PSD2) and the transition to stronger payments security," *MIP Online* (March 2018), https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html
[48] Ben Wolford, "What is GDPR, the EU's new data protection law?," *GDPR.EU, https://gdpr.eu/what-is-gdpr/*
[49] Deloitte Ireland, "Digital Operational Resilience Act," https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/ierisk-advisory-digital-operational-resilience-act-dora-05102022.pdf
[50] Ibid., p. 2

forthcoming revision of Network Information Security Directive, which broadens coverage of non-financial service firms that require optional reporting of significant cyber threats.

Other jurisdictions have also implemented comprehensive data protection laws with cybersecurity implications. The following examples, while by no means comprehensive, demonstrate the importance that financial regulators assign to cybersecurity.

- Brazil's 2020 General Data Protection Law (LGPD) requires firms to adopt "security, technical, and administrative" measures able to protect personal data.[51]
- Similarly, Canada's draft Consumer Protection Privacy Act expands the scope of security safeguards to protect personal information breaches and imposes an obligation on firms collecting data to maintain adequate safeguards for personal information.[52]
- South Korea's Personal Information Protection Act imposes similar requirements to maintain adequate standards for storing and transmitting personal data but also specifies that encryption is likely required.[53]

These and other regulations can be found in the World Bank Group's Cybersecurity Digest,[54] which was most recently updated in August 2021 and covers recent laws, regulations, guidelines, and other cybersecurity that are relevant for the financial sector. In addition to national regulations, the digest also includes work from standards setting bodies and international organisations such as the ISO/IEC, NIST, BCBS, IADI, European Telecommunications Standards Institute, G7, and the FSB. The digest is intended for financial regulators, supervisors, and DTI executives, and as such may be a useful resource for DIs looking to build knowledge of cybersecurity.

## 4.3 U.S. Cybersecurity Standards and Frameworks

The FBAs and U.S. DTIs use the following standards and frameworks or in combination, including the Federal Financial Institutions Examination Council (FFIEC) developed self-assessment program to meet or exceed regulatory compliance:

- The NIST Cybersecurity Framework (CSF) 1.1 addresses a set of cybersecurity activities, desired outcomes, and applicable references common to all critical infrastructure sectors, including financial services.[55] It includes five concurrent and continuous functions (i.e., identify, protect, detect, respond, and recover) that provide a high-level lifecycle view of the organisation's management of cybersecurity risk.[56] NIST states that a revision to the framework in early 2024[57] will include additional elements such as linkages to other NIST standards, implementation guidance, and discussion of cybersecurity supply chain risk management.[58]

- The Information Systems Audit and Control Association (ISACA) developed the Control Objectives for Information and Related Technologies (COBIT) 2019, an IT governance framework used by many U.S. and international firms and organisations, including several large DTIs in the Middle East.[59] COBIT aligns with several relevant standards, frameworks and/or regulations, including Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense, Committee of Sponsoring Organizations (COSO) Enterprise

[51] International Association of Privacy Professionals, "Brazilian General Data Protection Law (LGPD, English translation), October 2020, https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/
[52] Lisa R. Lifshit, Roland Hung, and Cameron McMaster, "Proposed Canadian Privacy Bill Introduces Fines and New Requirements for Private Organization," *American Bar Association* (July 6, 2022) https://www.americanbar.org/groups/business_law/publications/blt/2022/07/canadian-privacy-bill/
[53] Thales Group, "South Korea's PIPA Compliance," https://cpl.thalesgroup.com/compliance/apac/south-koreas-pipa
[54] World Bank's Cybersecurity Digest (April 2021). https://thedocs.worldbank.org/en/doc/3c28bd048d78efd27744987253e2c44a-0430012021/related/CybersecDigest-v6-FINAL-vs.pdf
[55] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," (April 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, 3.
[56] Ibid.
[57] NIST, *Updating the NIST Cybersecurity Framework – Journey To CSF 2.0*, https://www.nist.gov/cyberframework/updatingnist-cybersecurity-framework-journey-csf-20
[58] NIST, "NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework" (January 19, 2023), https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf
[59] ISACA, "COBIT Case Studies," https://www.isaca.org/resources/cobit/cobit-case-studies

Risk Management Framework, European Committee for Standardization (CEN) e-Competency Framework (eCF), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 and 38500 series standards, ITIL, NIST standards, to name a few.

- The Payment Card Industry Data Security Standard (PCI DSS), developed by the Payment Card Industry Security Standards Council, is an internationally recognised information security standard that applies worldwide to any entity processing credit card data, including most DTIs. There are twelve requirements that must be met, including protection of all systems against malware,[60] which is one of the primary causes of cybersecurity incidents. Other requirements include firewall configuration, changing vendor-supplied defaults, protecting data, testing security systems/processes, and maintaining an information security policy.
- The Center for Internet Security Critical Security Controls (CIS Controls), include prioritised safeguards to mitigate the most prevalent cyberattacks against systems and networks. CIS Controls are mapped to and referenced by multiple legal, regulatory, and policy frameworks. They align with existing independent standards and security recommendations such as NIST, Cloud Security Alliance (CSA), Software Assurance Forum for Excellence in Code (SAFECode), MITRE ATT&CK, and Open Web Application Security Project® (OWASP®). The CIS Controls version 8[61] has been enhanced to cover developments such as cloud-based computing, virtualisation, mobility, outsourcing, and remote work. It also addresses the ever-changing attacker tactics and supports an enterprise security management approach to integrating guidelines, policies, and proactive measures for various threats.
- The FFIEC also developed the optional Cybersecurity Assessment Tool (CAT) that is used by many DTIs[62] to identify risk and assess cybersecurity preparedness. The CAT provides the DTIs a repeatable and measurable self-assessment process to evaluate preparedness over time. It also gives DTI management and directors insight into regulatory expectations and raises their awareness of cybersecurity risks.
- The Cyber Risk Institute (CRI) is a coalition of financial institutions and trade associations focused on protecting the global economy by enhancing and standardising cybersecurity and resilience. The CRI is the developer and custodian of the CRI Profile (Profile),[63] which is the benchmark self-assessment toolset for the financial services industry that is used by U.S. DTIs and bank service providers with global footprint in four continents.[64] The Profile draws on widely used frameworks, standards, and supervisory guidance and assessment tools, such as the NIST CSF, NIST Ransomware and CPMI-IOSCO. It also maps directly to the FFIEC CAT, FFIEC IT Business Continuity Management Booklet, the New York Department of Financial Services regulation, the European Central Bank's framework, the European Banking Authority's guidelines, ISO/IEC 27001/2 controls (discussed in the next section), and international regulations from G7 member nations, APAC, and EMEA. In the future, the Profile will likely expand to cover more issues of significance for DIs and DTIs, including emerging technologies (e.g., AI, cloud technology, quantum computing), privacy issues, financial digitalisation, and resilience planning and adoption.

## 4.4 Cybersecurity Standards and Frameworks in Other Jurisdictions

In addition to the standards and frameworks mentioned above, there are others also available to the international DIs and DTIs listed below appropriate for use in their jurisdictions.

- The Basel Committee on Banking Supervision (BCBS) Principles for Operational Resilience (POR)[65] include cybersecurity. The operational resilience principles hinge on seven categories: 1) governance; 2) operational risk management; 3) business continuity planning and testing; 4) mapping of interconnections and interdependencies of critical operations; 5) third-party dependency management; 6) incident management; and

[60] Abi Tyas Tunggal, "Best Practices for Cybersecurity Compliance Monitoring in 2023," *UpGuard* (April 6, 2023), https://www.upguard.com/blog/compliance-monitoring
[61] Center for Internet Security, "CIS Controls," https://learn.cisecurity.org/control-download
[62] FFIEC, "Cybersecurity Assessment Tool", (May 2017), https://www.ffiec.gov/cyberassessmenttool.htm
[63] Cyber Risk Institute, New CRI Updates Reflect Profile's Ability to Adapt, January 25, 2023, https://cyberriskinstitute.org/newcri-updates-reflect-profiles-ability-to-adapt/
[64] Cyber Risk Institute, Our Strategic Plan, https://cyberriskinstitute.org/three-year-plan/
[65] Basel Committee on Banking Supervision, "Principles for Operation Resilience," *Bank for International Settlements* (March 2021), https://www.bis.org/bcbs/publ/d516.htm

7) resilient ICT including cyber security. Although these principles are currently undergoing revision, their basic points remain relevant for DIs and DTIs alike.[66] With respect to ICT, the POR notes that DTIs should incorporate cybersecurity measures such as robust protection from and detection of threats, adopt appropriate situational awareness, and convey timely information to support risk management purposes and ensure continuity of service.[67] The principles form part of the larger Basel Framework on prudential regulation of DTIs.

- The ISO/IEC 27000 series standards are designed to help organisations protect against cyberattacks and manage the cyber-related risks associated with technology use.[68] It is based on a risk management approach that includes guidance on incident response and recovery. Baseline coverage entails security practices for stakeholders in the cyberspace[69] that covers:
    - An overview of cybersecurity,
    - An explanation of the relationship between cybersecurity and other types of security,
    - A definition of stakeholders and a description of their roles in cybersecurity,
    - Guidance for addressing common cybersecurity issues, and
    - A framework to enable stakeholders to collaborate on resolving cybersecurity issues.

## 4.5 Best Practices

The following areas cover best practices recently introduced that may be useful to both DIs and DTIs in the course of averting and mitigating cybersecurity exposures. They are the FSB Cyber Incident Reporting (CIR) and NIST's National Online Informative References (OLIR) Program. There are other best practices such as the table top exercises and Zero Trust Architecture (ZTA) that are likely to produce optimal results for DIs and DTIs if they are widely adopted.

### 4.5.1 FSB Cyber Incident Reporting

The FSB's April 2023 report "Recommendations to Achieve Greater Convergence in Cyber Incident Reporting (CIR)"[70] identifies 16 recommendations to promote CIR best practices. Broadly speaking, the FSB recommendations focus on key areas of improvement for financial regulators and financial institutions, including creating an organisational culture that encourages CIR, defining clear and appropriate CIR thresholds, smoothing cooperation with local and international safety net providers, and establishing common definitions for key CIR-related terms.

The FSB cautions that its CIR recommendations should not be treated as prescriptive mandates, and should be tailored to individual institution needs. Further, cyber incidents that could be reported under CIR go beyond cybersecurity to include things such as insider misuse, card skimming, and web application attacks.

In line with the FSB's suggestions on CIR reporting, the IMF offered several suggested actions in a March 2023 blog to help improve cybersecurity posture, including developing explicit cybersecurity strategies, focusing on addressing routine lapses that can lead to larger breaches, and devising operational plans that emphasise continuous delivery of services in a disruption instead of disaster recovery.[71]

### 4.5.2 NIST's National Online Informative References (OLIR) Program

As noted in this brief, information and communications technologies are governed by many different technical standards and guidelines and, depending on the jurisdiction, frameworks and regulations Consequently, DIs and DTIs may find it

---

[66] Basel Committee on Banking Supervision, "Core Principles for Effective Banking Supervision," *Bank for International Settlements* (July 2023), https://www.bis.org/bcbs/publ/d551.pdf , p. 3.
[67] Ibid., p. 7.
[68] Standards of particular interest for this brief include 27001: Information security management systems, 27002: Information security controls, and 27032: Security techniques.
[69] NIST defines cyberspace as "A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." https://csrc.nist.gov/glossary/term/cyberspace
[70] Financial Stability Board, "Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report," (April 13, 2023), https://www.fsb.org/wp-content/uploads/P130423-1.pdf
[71] Tobias Adrian and Caio Ferreira, "Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards"

difficult to navigate these various references and identify connections between them. To mitigate this difficulty, NIST OLIR program[72] facilitates cooperation between subject matter experts in better mapping internal references between standards and frameworks. Such projects will help facilitate adoption of standards and frameworks for cybersecurity and offer clearer guideposts for compliance. Work has already begun with specific examples of standards/frameworks (e.g., ISO/IEC, COBIT 2019, etc.) that have been compared to the NIST Cybersecurity Framework version 1.1.

### 4.5.3 Table Top Exercises

Cybersecurity training can take many forms. One of the most common is table top exercises,[73] where team members in an informal setting discuss the business continuity plan and their roles and responsibilities. The exercise is hosted by a facilitator, who poses different scenarios to the team and asks questions to reinforce and validate participants' understanding of practices.

Ongoing training exercise programs can reinforce staff knowledge of monitoring and detection of cybersecurity activities and cyberattacks. This type of training is in line with the BCBS POR, which include business continuity planning and testing.[74] POR 3 notes that DTIs (and, by implication, their supervisors) should integrate business continuity concerns into their corporate culture, including offering regular training and awareness programs to employees and conducting exercises to assess employees' performance during an operational disruption.[75] For example, the European Central Bank (ECB) is planning a stress test for the 109 DTIs under its supervision, focusing on response recovery from a successful cyberattack. The ECB is expected to discuss their findings and share lessons learned with each DTI who in turn will assess their own risk profile.[76]

### 4.5.4 Zero Trust Architecture (ZTA) Approach to Cybersecurity Implementation

DIs and DTIs may also need to reassess their cybersecurity implementation approach. They may want to move away from building a perimeter around computing resources to an approach that protects each individual enterprise resource better known as Zero Trust (ZT) or ZTA. Traditionally, most cybersecurity approaches have been based on the perimeter principle, which focuses on protecting the entirety of the network against attack. Such an approach is now insufficient given the spread of cloud-based services, use of virtual private networks, and mobile devices. Therefore, a ZTA approach should include implementation of multifactor authentication (MFA) and the principle of least privilege strategy, particularly for private clouds that may be interconnected with other applications.

ZTA, in contrast, focuses on securing each individual asset on the system and ensures continuous authentication of users looking to access those assets. DIs and DTIs may find ZTA to be a useful approach given its emphasis on reduced attack surfaces, faster detection time, and overall improved data layer protection. ZTA may also be appealing from a business perspective as it can streamline cybersecurity reviews and provide greater visibility into asset utilisation.[77]

## 5 Case Studies from Deposit Insurers

Considering the increased pace and intensity of cyberattacks on the financial sector, several DIs have adopted stronger cybersecurity postures and implemented measures to enhance their preparedness for a future cyberattack. Some examples are provided below for consideration.

---

[72] NIST Computer Security Resource Center, "National Online Informative References Program," https://csrc.nist.gov/projects/olir

[73] NIST defines tabletop exercise as "a discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario." NIST Computer Security Resource Center, "Glossary: Tabletop Exercise," https://csrc.nist.gov/glossary/term/tabletop_exercise

[74] BCBS, "Principles for Operational Resilience," pp. 3-4.

[75] Ibid., p. 5.

[76] ECB to stress test banks' ability to recover from cyberattack (January 3, 2024). https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240103~a26e1930b0.en.html

[77] Andrew Kennedy, "Adaptive Trust: Zero Trust Architecture in a Financial Services Environment," *Bank Policy Institute* (March 21, 2022), https://bpi.com/adaptive-trust-zero-trust-architecture-in-a-financial-services-environment/

## 5.1 Canada Deposit Insurance Corporation (CDIC)

In its 2022 annual report, CDIC (Canada) identified cyberattacks as a risk to DTIs' resilience and, ultimately, depositors' access to funds.[78] CDIC has thus prioritised cybersecurity in its multi-year Enterprise Technology Strategy, which is intended to modernise its overall approach to information technology management.[79] As part of the strategy, CDIC is continuing migration to a cloud-based secure data environment and improving data governance regimes. CDIC also conducted simulations throughout 2021-2022 to assess their resilience in a crisis environment, including cyberattacks.[80]

## 5.2 Chinese Taipei's Central Deposit Insurance Corporation (CDIC)

In recent years, CDIC (Chinese Taipei) has taken measures to enhance their cyber resilience program. This program includes 1) enhanced defence in depth strategies to further augment CDICs cybersecurity protection capabilities; 2) continued maintenance of its ISO 27001 international certification; and 3) engagement with the private sector to manage its advanced Security Operations Center, which continuously monitors threats and issues real-time alerts. CDIC has also actively participated in the "Taiwan Financial Information Security Alliance" and its associated Financial Information Sharing and Analysis Center,[81] which facilitates the exchange of cybersecurity intelligence, collaborative defence strategies, and personnel training.

## 5.3 France's Deposit Insurance and Resolution Fund (FGDR)

The FGDR[82] adopted a multi-year, three-part security plan covering the deployment of technical and functional security systems, migration to a new outsourced IT providers, and simulated attacks against core FGDR applications.[83] FGDR notes that it has conducted simulated attacks against its systems regularly since 2014, and that it uses a variety of vendors with different methods to do so.[84]

## 5.4 Korea Deposit Insurance Corporation (KDIC)

As part of its 2020 Information System Master Plan, KDIC identified three cybersecurity-related tasks: building next generation information protection, establishing an integrated security control centre, and building backup/disaster recovery systems.[85] In support of these tasks, KDIC established a "cyber shelter" to protect its systems against DDoS tasks, and partnered with public and private sector partners to conduct cyberattack response training.[86] KDIC's work in this area has thus far safeguarded the organisation from any cyberattack and earned recognition from the National Intelligence Service as a leader in cybersecurity preparedness.

## 5.5 Türkiye's Savings Deposit Insurance Fund (SDIF)

The SDIF prioritised cybersecurity as part of its 2018-2022 strategic plan.[87] SDIF considers cybersecurity a priority as it is the trustee for failed financial institutions and thus takes control of the failed institutions' data. Moreover, SDIF must comply with Law 6698 on personal data protection, which sets forth requirements that must be met for security of sensitive personal data.[88] To that end, SDIF has conducted internal audits of its information security management system, which has been set up in accordance with the ISO/IEC 27000 series. The Turkish Standards Institute supplemented SDIF's internal audits with its own, and deemed the system to be compliant with the ISO/IEC 27000 series.

---

[78] Canadian Deposit Insurance Corporation, "2022 Annual Report," https://www.cdic.ca/wp-content/uploads/cdic-2022-annualreport.pdf, p. 15.
[79] Ibid., p. 30.
[80] Ibid., p. 12.
[81] Financial Supervisory Commission established the Financial Information Sharing and Analysis Center (F-ISAC), referring to the practices of FS-ISAC in the US. https://service.tabf.org.tw/TTB/Article/DetailEn?aID=707
[82] From the French Fonds de Garantie des Dépôts et de Résolution
[83] FGDR, "Annual Report 2021," https://www.garantiedesdepots.fr/sites/default/files/2022-05/FGDRRapport_Annuel_2021%20EN.pdf, p. 24.
[84] Ibid.
[85] KDIC, "2021 Annual Report," https://www.kdic.or.kr/english/annual_reports.do, p. 48.
[86] Ibid.
[87] SDIF, "2021- Annual Report," https://www.tmsf.org.tr/File/Download?fileId=DBF710C5-1EFE-47B7-B6BA6F8C14087B30&typeId=1, p. 18.
[88] Ibid.

# 6 Key Takeaways

The IADI Core Principles (CPs) are the international standard for establishing or safeguarding effective deposit insurance systems. They also have implications for DIs' approaches to cybersecurity. DIs need to be granted the resources to address cybersecurity concerns, and, if relevant to their mandate, the proper powers and guidance for assessing DTIs' compliance with cybersecurity roles and responsibilities (CP 2 – Mandate and Powers). DIs may consider including strategies to mitigate cybersecurity concerns in their internal control framework (CP 3 – Governance).[89] DIs are generally not responsible for guarding against cyber threats to the financial system, and where relevant should collaborate with other financial safety net players in cyber preparedness (CP 4 - Relationships with other Safety-Net Participants), such as through assessing risk, contingency planning, testing the plans, and incorporating lessons learned from exercises and actual responses (CP 6 - Deposit Insurer's Role in Contingency Planning and Crisis Management), including strengthening their operational resilience, continuity, and response capabilities during crisis management. As noted earlier, DIs with expanded mandates should have strategies in place to monitor for cyber events that can affect a DTI's viability (CP 13 - Early Detection and Timely Intervention), and if necessary and appropriate, should have powers to resolve institutions that are failing due to a severe cyber incident that include safety and soundness indicators (CP 14 - Failure Resolution) through effective use of available resolution tools and methods.

As presented in this brief, global standards setting bodies such as the FSB and the BCBS have developed principles and guidance to help national authorities place cybersecurity within supervisory frameworks. National authorities have developed cybersecurity regulations of their own, to guide the DTIs they regulate as well as monitor their own activities. DIs and DTIs can call on a host of standards and frameworks, outlined in this brief as examples to stay informed and to implement the cybersecurity regimes of choice suitable to their organisation.

Finally, DIs can also evaluate the feasibility and application of the U.S. FFIEC cybersecurity awareness and related self-assessment tools, and examination work program guidance documents available in the IT Booklets that may serve as helpful examples to implement their own guidance.[90]

# 7 Next Steps

Future analysis by IADI could focus on the five following areas to facilitate cybersecurity understanding and efforts: emerging technology, supervisory examination, training, insurance, and third-party risk management (TPRM).

## 7.1 Artificial Intelligence (AI) and Quantum Computing

Cybersecurity's importance will only increase in the coming years with the emergence of new technologies and, by extension, new methods of attack. For example, the popularisation of AI through services such as ChatGPT, Bard, HuggingChat, Bing AI, Sparrow, YouChat, and others may present both benefits and drawbacks. AI could potentially help in identifying cyber threats and also improve response time. But the adversaries may use AI to design cyberattacks against systems, including phishing attacks through social engineering. Similarly, quantum computing could vastly improve cybersecurity capability and allow for greater protection of data; however, it may render many existing forms of encryption obsolete once it has matured.[91]

## 7.2 Cybersecurity Supervision Examination Regime

Although some jurisdictions have integrated cybersecurity into their DTI examination regime, as the U.S. has done through the FFIEC, many others have been slow to adopt or implement such cybersecurity strategies. As the IMF noted in a 2022 survey, slow implementation is a particular problem for emerging markets.[92] Therefore, work needs to continue at standards-setting bodies on helping supervisors define and implement the Basel Framework's Core Principles for Effective Banking Supervision, which most authorities integrate in their supervisory framework.[93]

---

[89] CP-3, EC-4 The deposit insurer is well-governed and subject to sound governance practices, including appropriate accountability, internal controls, transparency and disclosure regimes. The institutional structure of the deposit insurer minimises the potential for real or perceived conflicts of interest.
[90] FFIEC, "IT Booklets," https://ithandbook.ffiec.gov/it-booklets.aspx
[91] NIST Computer Security Resource Center, "Post-Quantum Cryptography", https://csrc.nist.gov/Projects/post-quantum-cryptography
[92] Tobias Adrian and Caio Ferreira, "Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards"
[93] BCBS, "Core Principles for Effective Banking Supervision", (September 2012), https://www.bis.org/bcbs/publ/d551.pdf

Generally, in the U.S., the FBAs do not impose disclosure requirements for cybersecurity risk posture from examined DTIs and service providers. FBAs evaluate cybersecurity controls as part of their IT examination routine via the InTREx (Information Technology Risk Examination) program or the FFIEC CAT discussed earlier for DTIs and the FFIEC work programs for service providers. Cybersecurity is rated under the URSIT (Uniform Rating System for Information Technology), that is incorporated into the management component of the UFIRS (Uniform Financial Institutions Ratings System) commonly referred to as the CAMELS rating system.[94]

## 7.3 Cybersecurity Training

Awareness and training are integral part of an organisation's personnel and partners to educate and stay abreast of the changing cybersecurity landscape. Cybersecurity-related duties and responsibilities become much clearer and more consistent when they align with existing policies and procedures. DIs should consider having a formal cybersecurity training program.

## 7.4 Cyber Insurance

Cyber insurance is an important component of individual risk management programs, as well as broader risk management strategies that includes identification, measurement, mitigation, and monitoring of cyber risk exposure.[95] Cyber insurance is a type of liability insurance that helps cover costs associated with data breaches and cyberattacks, including recovery measures, forensic investigation, and potential liability claims.[96] Although U.S. DTIs are not required to subscribe to cyber insurance, it may assist DTIs in recovery efforts following a cyberattack. DIs may wish to assess the present and potential future role of cyber insurance in their regulatory frameworks.

## 7.5 Third-party Risk Management

As mentioned in Section 4.1, the Computer-Security Incident Notification rule includes provisions for bank service providers to notify a DTI's central point of contact "as soon as possible" when an incident has lasted four or more hours. One of the primary reasons behind this requirement is the vulnerability of third-party providers and products used by bank service providers, particularly those that serve smaller institutions. DTIs should therefore assess their risks arising from their third-party relationships, develop a comprehensive approach to operational resilience and supply chain risk, and integrate this approach into their overall cybersecurity posture. To that end, in the U.S., the FBAs issued final guidance on third-party risk management on June 6, 2023. The guidance promotes consistency in the FBAs' supervisory approaches, and covers risk management process across the third-party relationship lifecycle from planning through contract negotiation and monitoring and termination.[97] On December 4, 2023, the FSB released the final version of its Toolkit for "Enhancing Third-Party Risk Management (TPRM) and Oversight".[98] The toolkit does not itself contain specific requirements or guidance for DTIs, but rather offers examples of best practices for DTIs, and, by extension, supervisory considerations for DIs and other financial safety net players.

---

[94] Financial Institution Letter – Adoption of Revised "CAMELS" Rating System (December 26, 1996). https://www.fdic.gov/news/financial-institution-letters/1996/fil96105.html

[95] FFIEC Issues Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs: https://www.ffiec.gov/press/pr041018.htm

[96] Federal Trade Commission, "Cyber Insurance," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyberinsurance

[97] Federal Deposit Insurance Corporation, "Agencies Issue Final Guidance on Third-Party Risk Management" (June 6, 2023), https://www.fdic.gov/news/press-releases/2023/pr23047.html. The FBAs have also published a guide to assist community banks (e.g. those with less than $10 billion in assets) in implementing third-party risk management processes. Federal Deposit Insurance Corporation, "Third-Party Risk Management: A Guide for Community Banks" (May 2024), https://www.fdic.gov/system/files/2024-06/third-party-risk-management-guide.pdf

[98] Financial Stability Board, "Enhancing Third Party Risk Management and Oversight: A toolkit for financial institutions" (December 4, 2023). https://www.fsb.org/wp-content/uploads/P041223-1.pdf

## References


Bankers Resource Center Technical Assistance Video Program. https://www.fdic.gov/resources/bankers/technicalhttps://www.fdic.gov/resources/bankers/technical-assistance-videos/index.html?source=govdelivery&utm_medium=email&utm_source=govdeliveryassistance-videos/index.html?source=govdelivery&utm_medium=email&utm_source=govdelivery

Information Security Magazine (October 18, 2023) "Are Tabletop Exercises Still Relevant for Modern Cybersecurity?" https://www.infosecurity-magazine.com/opinions/tabletop-exercises-relevant/

Information Security Magazine (October 18, 2023) "Global Economy Could Lose $3.5trn in Systemic Cyber-Attack." https://www.infosecurity-magazine.com/news/economy-could-lose-35tr-systemic/

Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis (FRBNY). https://www.newyorkfed.org/research/staff_reports/sr909

FDIC 2023 Report on Cybersecurity and Resilience. https://www.fdic.gov/regulations/resources/cybersecurity/2023https://www.fdic.gov/regulations/resources/cybersecurity/2023-cybersecurity-financial-system-resilience-report.pdfcybersecurity-financial-system-resilience-report.pdf

FRB 2023 Report on Cybersecurity and Resilience. https://www.federalreserve.gov/publications/files/cybersecurityreport-202308.pdf

European Union Agency for Cybersecurity (ENISA) (March 29, 2023) "ENISA Foresight Cybersecurity

Threats for 2030." https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

European Union Agency for Cybersecurity (ENISA) (March 27, 2023) "ENISA Cybersecurity Market Analysis Framework (ECSMAF) -V2.0." https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysishttps://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf-v2.0framework-ecsmaf-v2.0

European Union Agency for Cybersecurity (ENISA) (2005-2023) "Cybersecurity Policy." Available at https://www.enisa.europa.eu/topics/cybersecurity-policy

International Organization for Standardization (2009) ISO Guide 73:2009 – Risk management – Vocabulary (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/44651.html

European Union Agency for Cybersecurity (ENISA) (2005-2023) "ENISA pioneers the development of proper mechanisms and consistency for cyber incident and crisis management." https://www.enisa.europa.eu/topics/cyberhttps://www.enisa.europa.eu/topics/cyber-crisis-managementcrisis-management

Carnegie Endowment for International Peace, "Timeline of Cyber Incidents Involving Financial Institutions" (accessed 31 March 2023), https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

Hari Ravichandran (March 15, 2023): "How AI Is Disrupting And Transforming The Cybersecurity Landscape,"

Forbes. Thomas Scanlon (April 10, 2023): "Cybersecurity of Quantum Computing: A New Frontier," Carnegie Mellon

University Software Engineering Institute.

NIST Cybersecurity Publication Search Engine: https://www.nist.gov/publications/search?ta%5B0%5D=248731

U.S. Department of Treasury, Illicit Finance Risk Assessment of Decentralized Finance

IBM Security Intelligence (April 10, 2023): How LockBit Changed Cybersecurity Forever

Hack Read (April 12, 2023): US, India and China Most Targeted in DDoS Attacks, StormWall Q12023 Report

Fintech News (April 10, 2023): Cybercriminals are targeting digital bill payment: 4 ways to fight back

## Previous issues in this series

| | | |
|---|---|---|
| No. 1<br>September 2021 | Introductory Brief<br>Challenges for deposit insurers | Rachel Youssef, Rose Kushmeider, and Diane Ellis (FDIC) |
| No. 2<br>September 2021 | Data Standardisation | Daniel Hoople (FDIC) |
| No. 3<br>September 2021 | Machine Learning Methods<br>Potential for Deposit Insurance | Ryan Defina (IADI) |
| No. 4<br>September 2021 | E-Money in the United Kingdom A<br>Case Study | Paola Crosetta (FSCS) |
| No. 5<br>November 2021 | Central Bank Digital Currencies The<br>Motivation | Bert Van Roosebeke and Ryan Defina (IADI) |
| No. 6<br>December 2021 | E-Money and Deposit Insurance in Kenya | Ryan Defina, Bert Van Roosebeke (IADI) and Paul Manga (KDIC) |
| No. 7<br>April 2022 | Beneficiary Accounts:<br>Challenges for Deposit Insurance Schemes | Carlos Colao (FGD) and Roman Kahanek (GSFT) |
| No. 8<br>June 2022 | Introductory Brief (Part II): Opportunities for Deposit Insurers (DepTech) | Edward Garnett, Rachel Youssef, and Daniel Hoople (FDIC) |
| No. 9<br>August 2022 | E-Money in Ghana: A Case Study | Samuel Senyo Okae (BoG) and Eugene Yarboi Mensah (GDPC) |
| No. 10<br>September 2022 | Prepaid Cards: A Case Study of Japan, the United States and the European Union | Hiroaki Kuwahara and Kazuaki Hara (DICJ) |
| No. 11<br>September 2022 | Islamic Fintech: Nascent and on the Rise | Mohamad Hud Saleh Huddin, Mark Lee and Mohd Sobri Mansor (PIDM) |
| No. 12<br>November 2022 | Misdirected Money Transfers: The Role of the Korea Deposit Insurance Corporation | Sanjae Lee & Jeongeun Park (KDIC) |
| No. 13<br>December 2022 | Central Bank Digital Currencies: A Review of Operating Models and Design Issues | Bert Van Roosebeke and Ryan Defina (IADI) |
| No. 14<br>January 2023 | The Use of Fintech in Enhancing the Supervision of Internet-only Banks in Chinese Taipei | Wenwen Yeh (CDIC) |
| No. 15<br>May 2023 | Public Awareness Considerations in the Fintech Era: A Canadian Case Study | Canada Deposit Insurance Corporation (CDIC) |
| No. 16<br>September 2023 | E-Money in Uruguay: A Case Study | Gabriel Lemus (COPAB) |
| No. 17<br>April 2024 | E-Money Regulation in Brazil | Daniel Lima and Luis Vicente (FGC) |