CYBERSECURITY IN CREDIT REPORTING GUIDELINES

WORLD BANK GROUP

ICCR
INTERNATIONAL COMMITTEE ON CREDIT REPORTING

1818 H Street NW
Washington, DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

TABLE OF CONTENTS

LIST OF BOXES

LIST OF FIGURES

TABLE

ABBREVIATIONS AND ACRONYMS

APEC	Asia-Pacific Economic Cooperation
AI	Artificial Intelligence
BYOD	Bring Your Own Device
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CRSP	Credit Reporting Service Provider
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DoS	Denial of Service
DPO	Data Protection Officer
ENISA	European Union Agency for Cybersecurity
FIGI	Financial Inclusion Global Initiative
FINRA	Financial Industry Regulatory Authority
FSB	Financial Stability Board
G-7	Group of Seven
GPCR	General Principles for Credit Reporting
HW	Hardware
ICCR	International Committee on Credit Reporting
ICT	Information and Communications Technology
ID	Identification
IEC	International Electrotechnical Commission
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OECD	Organization for Economic Cooperation and Development

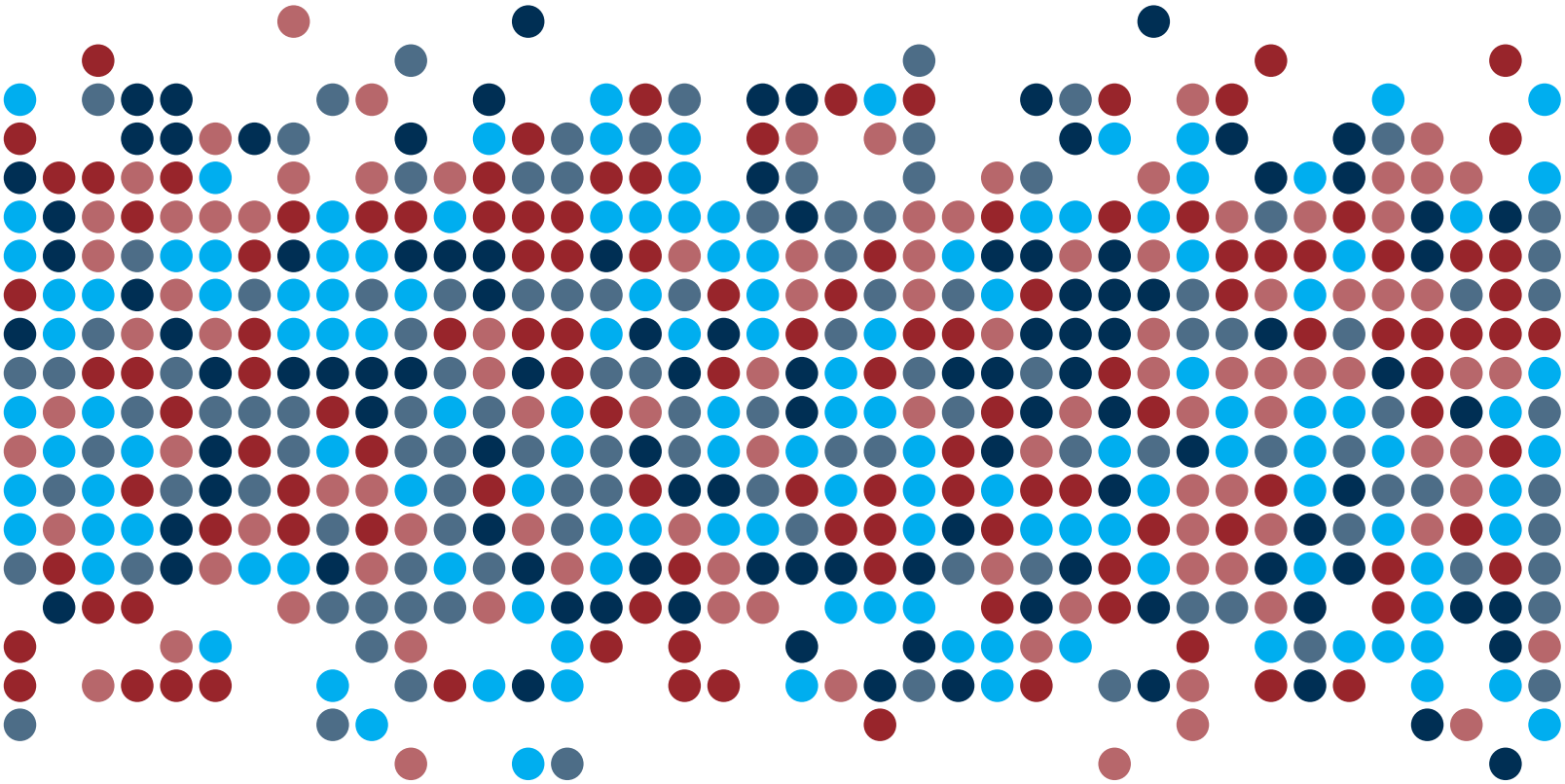
PCI DSS	Payment Card Industry Data Security Standard
SIEM	Security Information and Event Management
SOC	Security Operation Centers
SOC Report	Service Organization Controls Report
SSN	Social Security Number
WSP	Written Supervisory Procedures

ACKNOWLEDGMENTS

This guideline is a product of the International Committee on Credit Reporting (ICCR) and the World Bank Group (WBG) as an input to the Financial Inclusion Global Initiative guidance on cybersecurity for the financial infrastructure. This guideline builds on previous work conducted by the ICCR, namely "The General Principles for Credit Reporting" (2011) and existing work of the Financial Stability Board, the International Monetary Fund, European Union Agency for Cybersecurity, Committee on Payments and Market Infrastructure, International Organization of Securities Commissions, and Group of Seven on cybersecurity in financial sector.

The guideline was prepared by Marcelo Roldan (Senior Information Technology Officer, Security, Risk and Compliance), Aquiles Almansi (Lead Financial Sector Specialist), Collen Masunda (Financial Sector Consultant), and Luz Maria Salamina (Lead Financial Sector Specialist). The guideline benefited from a consultation process with not only the ICCR Cybersecurity Working Party, plenary members, and representative organizations, but also external peer reviewers.

The ICCR would also like to thank the Chairman of the ICCR, Sebastian Molineus; the ICCR Secretariat members Luz Maria Salamina and Collen Masunda; Neil Munroe, Chair of the ICCR Cybersecurity Working Party; and the other members of the Cybersecurity Working Party. Special thanks to colleagues from the World Bank Group who provided useful insights—Fredesvinda Montes and Dorothee Delort. The ICCR also acknowledges the managerial oversight by Mahesh Uttamchandani, the incoming ICCR Chair.



EXECUTIVE SUMMARY

The importance of credit reporting systems to the global financial system has been increasing over time. Robust credit reporting systems can promote not only access to affordable and sustainable credit for individuals and companies but also financial stability and economic growth. Credit reporting service providers (CRSPs) have been at the frontier of technology adoption to enhance their efficiencies as well as data acquisition, processing, and storage capabilities.

The credit reporting industry landscape has changed over the past decade with the adoption of new technologies and business models and the emergence of new players helping improve the speed of service provided and the quality and completeness of credit data. These positive changes in the credit reporting ecosystem, however, also present a source of risk for CRSPs. Several CRSPs have been subject to data breaches, denial-of-service attacks, and phishing attacks, among other cyber incidents in the past decade.

The incidents have resulted in severe financial, economic, operational, and reputational loss for the targeted organization and the industry at large. The implications can also be far reaching owing to increasing interconnectedness of the financial sector. Against this background, there is need for enhanced cybersecurity and data standards at the CRSP and jurisdiction levels.

This guideline provides findings of a landscaping survey conducted by the International Committee on Credit Reporting on CRSPs across the globe on current practices. The survey found that CRSPs worldwide generally were implementing cybersecurity practice. The survey also identified the following key issues and characteristics:

- CRSPs have been subjected to fewer attacks than have data providers and other prominent institutions.
- The most common incident among CRSPs has been denial of services.
- The majority of jurisdictions have enacted legislation or regulations to deal with cybersecurity and information security. Central Bank emerged as the regulatory authority for most of the respondents. All but one of the jurisdictions place an obligation on CRSPs to notify the affected parties.
- CRSPs have broadly embedded cyber and information security in their governance processes. They are also building capacity for both staff members and board members. A growing number of CRSPs have created a position of Chief Information Security Officer (CISO) or its equivalent that is responsible for cyber and information security.
- Cyber insurance is gaining prominence as one of the risk mitigation options.
- CRSPs are increasingly considering outsourcing of their critical services.

- The sharing of information on cyber incidents is gaining momentum; the majority of CRSPs participate in industry programs designed to promote information sharing. Third parties are also significantly contributing to information sharing.

- CRSPs are increasingly committing specific resources to improve their cybersecurity capabilities.

- The majority of CRSPs have a formal risk management framework that includes cyber risk as one of the risk areas. Institutions are also recognizing the importance of an internal audit as a central pillar in cybersecurity.

- Most CRSPs have documented incident response plans; however, notable gaps were observed with respect to partnerships with a computer emergency response team (CERT), external communications, and simulation exercises.

- CRSPs have implemented programs to monitor and prevent breaches and certain rules to control printing of sensitive information.

- CRSPs are successfully implementing controls against cyber risks.

Based on the survey results, this guideline provides detailed guidance to CRSPs on managing cybersecurity and data privacy risk. The guidance focuses on the areas of strategy, governance, risk management, compliance, functional operations, technology operations, data privacy, awareness and education, information sharing and communications, and incident response and business continuity. In addition, it emphasizes the need to ensure a risk-based approach and proportionality in the application of the guideline.

The guideline concludes by providing policy considerations that address some of the weaknesses identified in the survey. These recommendations are designed to enhance the security of national cyber space with respect to credit reporting. The policy considerations are as follows:

- Policy makers should consider implementing and/or enhancing cyber laws and regulations that provide incentives for better protection of data and systems.

- Regulatory authorities should consider developing national and/or sectorwide cybersecurity strategies and frameworks.

- To the extent possible, regulatory bodies should consider implementing practices or standards that promote the strengthening of cyber governance by CRSPs.

- Where applicable, regulatory bodies should ensure that CRSPs develop detailed programs for training their boards of directors.

- Regulatory authorities should issue guidance on the level and extent of disclosures of security and data breaches.

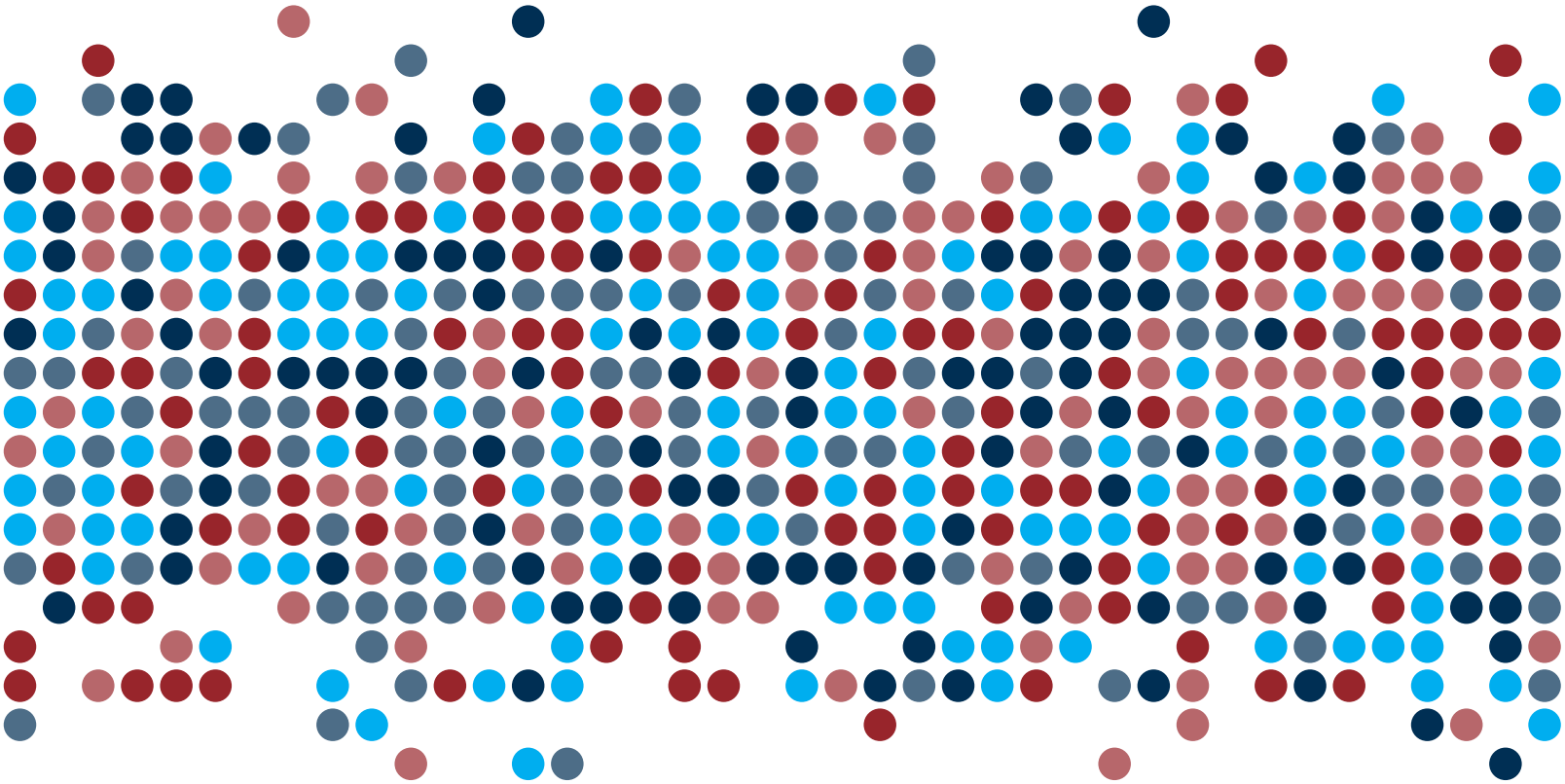
- Regulatory authorities should ensure that CRSPs implement sound outsourcing procedures that detail the controls and processes to be followed when evaluating and managing relationships with third parties.

- Regulatory authorities should also consider subjecting third parties that service CRSPs to the same level of risk management practices expected of the entities themselves.

- Supervisory authorities should consider conducting annual cybersecurity risk assessments of critical infrastructure players.

- In carrying out this responsibility, where possible, the supervisory authorities should consider using collaborative methods, such as including information sharing and joint assessments, to reduce regulatory burden on CRSPs.

- Authorities should consider encouraging CRSPs to conduct their own internal assessments on a periodic basis.
- Regulatory authorities should consider promoting regular cyber audits of cyber functions.
- Regulatory and/or industry bodies should consider developing mechanisms that foster and enforce cyber information sharing and collaboration among parties.
- Regulatory bodies should also publish or promote publication of redacted reports on cybersecurity issues on a semiannual basis.
- Regulatory authorities should ensure that CRSPs actively participate and collaborate with national cybersecurity actors such as CERTs.



GLOSSARY OF TERMS

Credit Reporting Service Provider
An entity that administers a mechanism enabling credit information collection, processing, and further disclosure to users of data as well as value added services based on such data. The main types of providers are credit registries, credit bureaus, and commercial credit reporting companies.

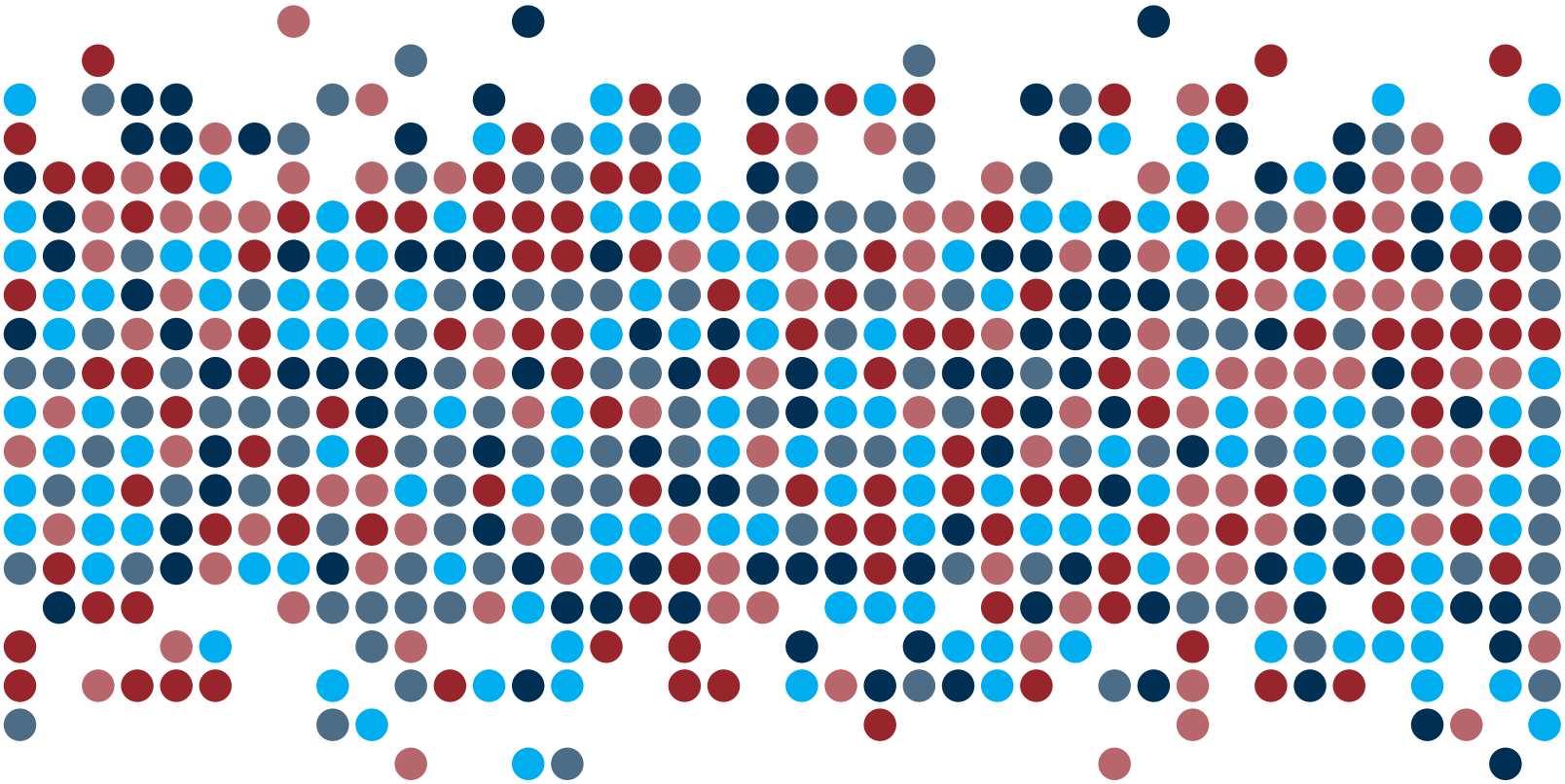
Cyber Attack
An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; destroying the integrity of the data; or stealing controlled information.

Cyber Incident
An occurrence that results in actual or potential violation of an explicit or implied security.

Cyber Risk
The risk of financial loss, operational disruption, or damage from the failure of the digital technologies employed for informational and/or operational functions via electronic means as a result of unauthorized access, use, disclosure, disruption, modification, or destruction.

Cyber Threat
An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss.

Cyber Vulnerability
A flaw or weakness in a system that can leave it open to attack.



1. INTRODUCTION AND BACKGROUND

Credit reporting systems are a crucial part of the financial infrastructure. Their function can have a significant impact on the stability of the global financial system.[1] Robust credit reporting systems can promote access to affordable and sustainable credit for individuals and companies and promote financial stability and economic growth.

Failure of the credit reporting infrastructure can impact the effective functioning of credit markets. Widespread cyber incidents can trigger lenders to curtail credit granting in response to fears of widespread frauds that could emanate from such data incidents. The resultant credit rationing can then impact on both aggregate demand by individuals and firms' profitability. Cyber incidents can also lead to an increase in the granting of fraudulent credit facilities which can translate into an increase in nonperforming loans.

The credit reporting industry has evolved over the past decade through the adoption of new technologies and new business models and the emergence of new players. The adoption of new technologies and the entrance of new players to the credit reporting ecosystem (EYGM 2014) has been seen as a way of improving the speed of service and the quality and completeness of credit data. New technologies are enhancing the ability of credit reporting service providers (CRSPs) to collect and share credit data in a faster, more efficient, and more cost-effective way, thus promoting financial inclusion. New players are tapping into new data sources to assist with a creditworthiness assessment, helping with the offer of credit to clients with thin or no credit files.

Notwithstanding the benefits, the evolution of credit reporting can become a threat and a source of vulnerability for the credit reporting system specifically and financial infrastructure in general. As cyber ecosystems grow, the potential sources of vulnerabilities increase. Vulnerabilities at individual entities are more likely to have an effect on the whole ecosystem.

The interconnectedness of the financial infrastructure exposes the global financial systems to systemic risk (Almansi 2018). A localized incident in one of the players can impact entities interfaced to it, thus triggering a widespread disruption across the entire system. This disruption might ultimately affect the whole financial ecosystem and, in turn, impact global financial stability.

IBM (2017) and IOSCO (2016) noted a surge in cyber attacks in the financial services sector in 2017. The financial services sector experienced 65 percent more attacks than the average client organization across all industries in 2016. This observation could be partly attributed to the fact that most of the new financial service providers and/or fintech start-ups may not have sufficient resources to invest in robust system security standards and

[1] The World Bank's (2011) General Principles for Credit Reporting acknowledges the importance of credit reporting systems as the foundation for robust and competitive credit markets. Credit reporting systems can also assist prudential regulation, hence minimizing risk.

data protection. As such, these institutions might find themselves at risk and eventually become a source of vulnerability for the whole ecosystem.

A cyber incident can have serious financial ramifications on credit providers. Cyber incidents can result in consumers experiencing financial harm, loss of privacy, and loss of trust in the financial system. Credit providers can also be affected by a cyber incident through decline in their enterprise value, loss of reputation, significant costs in breach remediation, regulatory and compliance costs, and higher insurance premiums (NNT 2017). A cyberattack on Equifax[2] in 2017 affected more than 143 million customers—revealing their personal information and identification numbers—and resulted in significant financial costs to the CRSP.

As a result of some cyber incidents experienced over the past years, CRSPs and their regulatory authorities are under increased scrutiny.[3] Some regulators have been challenged on how they have handled cyberattacks, particularly, the lack of timely disclosure of breaches to the public.

Against this background, members of the public and supervisory and regulatory authorities have a renewed focus on cybersecurity of the credit reporting ecosystem. Regulatory agencies, international financial institutions, and standard setting bodies have developed various types of guidance on cybersecurity for financial institutions. For example, the U.S. Financial Industry Regulatory Authority (FINRA) has developed basic checklists for alternative lenders, especially new financial players and third-party providers who support alternative lending approaches. The New York Department of Financial Services also implemented cyber regulations for credit reporting agencies in June 2018. The regulations require CRSPs to register with that department; comply with the state's strict cybersecurity standard, including a requirement to appoint a Chief Information Security Officer; and report known cyber breaches within 72 hours (Velasquez 2017).

The International Committee on Credit Reporting, through the General Principles for Credit Reporting (GPCR), provides high-level guidelines on security, data protection, and risk management (World Bank 2011). In terms of the GPCR, participants in a credit reporting ecosystem should undertake best efforts to implement commercially reasonable data security safeguards to protect data against cyber and other potential threats.

The objective of these guidelines is to provide detailed guidance on cybersecurity for CRSPs. These guidelines is produced as an input to the FIGI guidance on cybersecurity for the financial infrastructure and will build on existing work by the FSB, the IMF, ENISA, the CPMI, IOSCO, G-7, and others in the financial sector. In addition, the International Committee on Credit Reporting will leverage on earlier work of the GPCR on cybersecurity and the findings of the global credit reporting survey that was conducted on cyber and data security.

[2] Equifax experienced a data breach between May and July 2017, as a result of a website application vulnerability. The breach, which was disclosed in September 2017, exposed sensitive customer information for up to 143 million customers.

[3] Following the Equifax breach , there were a number of interventions by the U.S. Congress, the Consumer Financial Protection Bureau, and the Federal Trade Commission.

2. THE EVOLVING CREDIT REPORTING CYBER LANDSCAPE

Evolution of the Credit Reporting Cyber Ecosystem

The credit reporting cyber ecosystem[4] is undergoing a significant change as a result of the evolving credit reporting ecosystem, typified by the entrance of new players, emergence of new data providers, availability of new technologies, and proliferation of new data sets.

Emergence of New Data Providers and Sources

The credit reporting industry has witnessed the expansion of the types of data providers from the traditional financial institutions to now include other entities such as nonbank financial institutions, municipal authorities, telecommunication firms, payment firms, and governments. The sector has also seen the emergence of alternative lenders who are providing data and/or subscribing to credit reporting systems. The proliferation of big data has also resulted in the emergence of new data providers and sources including social media networks. The changes in the number and nature of data providers and subscribers bring new sources of cyber risks.

Emergence of New Data Subscribers

The emergence of new types of data subscribers is also increasing the complexity of information sharing. The Facebook–Cambridge Analytica incident is an example of how CRSPs must take extra precaution regarding what data users will do with the data they receive, even under contractual agreements. More important, the incident highlights the importance of trust within the ecosystem. In the Cambridge Analytica case, Facebook was punished for the commissions and omissions of its customer. Facebook suffered reputational risk, regulatory scrutiny, and an estimated loss of up to US$134 billion in its stock market valuation (Niemantsverdriet 2018).

Proliferation of New Data Sets

Credit reporting has traditionally been based on the use of credit data that focuses on specific subsets of available structured data, such as actual loan repayment behavior, linked to certain demographic and official data, such as address, date of birth, and government identity number. In some jurisdictions, the nature of credit data has expanded to include other nonconventional credit data such as postpaid utilities and court records. Some of these new data sets, particularly alternative data sets, are sourced in ways that may make credit reporting systems more susceptible to cyber risks.

Entrance of New Players

The industry has also experienced the emergence of new CRSPs in the form of alternative credit scoring providers, who are competing against or

[4] EYGM (2014, 1) defines a cyber ecosystem as "a complex community of interacting devices, networks, people and organizations, and the environment of processes and technologies supporting these interactions."

complementing the traditional players. The new players also bring new sets of innovative products and services, leveraging on advances in information technology that are providing increased computing, data mining, and analytic capabilities. These capabilities are also enabling CRSPs to leverage non-traditional data. Although these players are promoting access to credit for marginalized groups, some of these players are also a possible source of vulnerability to the industry.

Evolving Cyber Incidents in Credit Reporting Industry

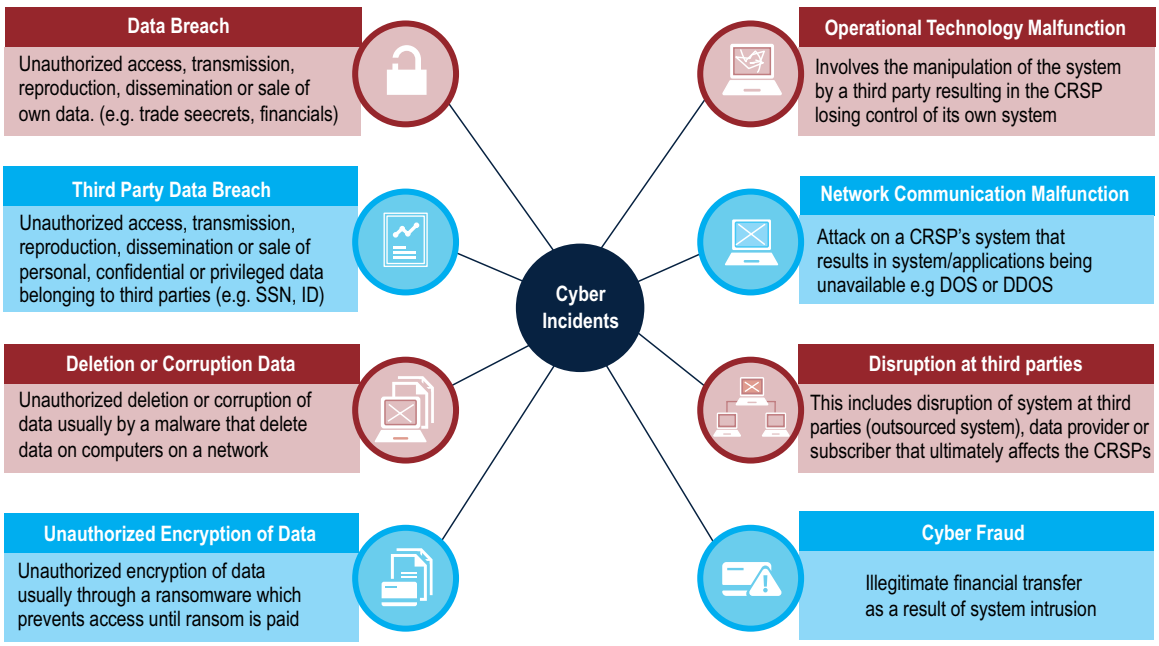
The cyber incidents that can affect CRSPs continue to evolve with the increasing sophistication of cyber actors. The CRO Forum as cited in OECD (2017) identified four main broad categories:

- Data breaches
- System malfunction
- Data integrity and availability
- Malicious activity

Figure 2.1: lists the different types of incidents.

Several CRSPs have been subject to some of the incidents shown in figure 2.1. Some examples of recent cyber incidents and attacks are given in box 2.1.

Figure 2.1: Common Type of Cyber Incidents That Affect Credit Reporting Service Providers



Box 2.1: Recent Cyber Incidents and/or Attacks of Credit Reporting Service Providers

Equifax Data Breach

Criminals exploited a U.S. website application development vulnerability to gain access to certain files. The company's investigation revealed that the unauthorized access occurred from mid-May through July 2017. The breach exposed records containing Social Security Numbers, birth dates, addresses, and, in some cases, driver's license numbers of more than 143 million consumers.

Experian Breaches

Experian US

In March 2012, Experian purchased the assets of Court Ventures, a company that focuses on collecting court records that contain limited personally identifiable information. As a side to its primary business, Court Ventures, at the time of acquisition, had a contract with USInfoSearch. That contract allowed customers of Court Ventures to access USInfoSearch's data to find the address of a person in order to determine which court records to review.

After Experian's acquisition of Court Ventures, the U.S. Secret Service notified Experian that Court Ventures had been selling and was continuing to resell data from a USInfoSearch database to a third party, possibly engaging in illegal activity. The suspect in this case posed as a legitimate business owner and had obtained access to USInfoSearch data through Court Ventures before Experian acquired the company.

Following notice by the U.S. Secret Service, Experian discontinued reselling USInfoSearch data and worked closely and in full cooperation with law enforcement authorities to bring Vietnamese national Hieu Minh Ngo, the perpetrator, to justice. Ngo pleaded guilty to his crimes and was sentenced. This breach did not compromise Experian's credit database.

Experian US

One of Experian's business units (not its consumer credit bureau) experienced an unauthorized acquisition of information from a server that contained data on behalf of one of its clients, T-Mobile, USA, Inc. The data included some personally identifiable information for approximately 15 million consumers in the United States, including those who had applied for T-Mobile USA postpaid services or device financing from September 1, 2013, through September 16, 2015, according to Experian's investigation. This incident did not affect Experian's consumer credit database.

Upon discovery of the incident, Experian took immediate action, including securing the server, initiating a comprehensive investigation, and notifying U.S. and international law enforcement organizations. The data acquired included names, dates of birth, addresses, and Social Security Numbers and/or an alternative form of identification such as a driver's license number, as well as additional information used in T-Mobile's own credit assessment. No payment card or banking information was acquired.

Experian notified consumers that may be affected and safeguarded their identity and personal information by offering two years of credit monitoring and identity resolution services.

Korea Credit Bureau

A consultant of Korea Credit Bureau stole credit card data over the course of several years to January 2014. The employee stole data by copying the data to an external hard drive. The data was then resold to credit traders and telemarketing companies.

Potential Sources of Risks

As the credit reporting industry grows, cyber crime actors are developing new infiltration techniques to target the credit reporting ecosystem. These techniques include targeting the CRSPs directly and/or the other participants of the credit reporting ecosystem. Some of the potential sources of vulnerabilities are discussed as follows.

Innovative Technologies

Several new technologies have emerged that enable better identification, transacting, networking, and sharing and hosting of data, all of which have implications for the credit reporting industry. Some of the key technologies include distributed ledger technologies, biometrics, advanced computing, artificial intelligence, and machine learning (World Bank 2019).

Notwithstanding their benefits, these technologies can possibly expose the credit reporting system to new sources of cyber risks (box 2.2). The adoption of technology and its widespread use within the credit reporting ecosystem increase the potential entry points and targets through which CRSPs can be attacked.

Interconnectedness

Credit reporting systems are a crucial part of the financial infrastructure and, in many cases, are highly interconnected to networks and institutions within the financial markets. The number of participants in the credit ecosystem is increasing owing to the emergence

Box 2.2: Innovative Technologies Are Also Susceptible to Cyber Attacks

Biometrics

Biometric technology has been hailed as a solution to enable the identification of data subjects. As a result, the adoption of biometric systems for user identification and authentication, particularly by financial institutions, has increased. Several major leaks of biometric data and instances of attempted use of leaked biometric data have already occurred (Kaspersky Lab 2019).

Distributed Ledger Technology

One of the major use cases of distributed ledger technology is blockchain. Although blockchain has been praised for its security, the recent experience of numerous cyber attacks on crypto exchanges has highlighted the vulnerability of the technology. More than 10 online exchanges have been subjected to cyber fraud, amounting to an aggregated figure of at least US$1.45 billion since 2013 (Bouveret 2018).

Cloud Computing

Most CRSPs have embraced various models of cloud computing services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software-as-a-Service (SaaS). As a result, data, services, and applications are being moved to the cloud. In instances of migration to a public cloud, CRSPs may outsource the security function of certain infrastructure to third parties, some of which are small and are not regulated. An attack on the service provider can affect CRSPs. The Equifax breach happened through a web application that the company outsourced (Newman 2017).

Mobile Applications

Some credit bureaus have developed consumer-driven data sharing platforms that are driven primarily by the need to provide portability of credit data. These innovations, although customer centric, can be another source of risk for the specific CRSPs and the whole ecosystem as they expand the surface of attack.

of new entities such as financial technology start-ups, some of which could be seen as relatively high risk because of their small cybersecurity budgets and limited visibility of their cybersecurity practices. Data transfer protocols, including web applications and application program interfaces, between entities in the infrastructure can also be a source of risks. The interconnectedness of the financial institutions and credit ecosystem infrastructure represent a single point of failure through which an attack can be propagated. The high degree of interconnectedness across firms can lead to rapid contagion effects. A disruption at one of the institutions might have implications on the whole financial market infrastructure or a significant number of large financial institutions (Bouveret 2018).

Outsourcing, Third Parties, and Fourth Parties

CRSPs are increasingly outsourcing some of their services to third parties. The outsourced services include infrastructure, software, and platforms. This practice is resulting in a growing reliance on third parties or even fourth parties for the management of outsourced services and, ultimately, the security of such services. The outsourced services can be nodes through which a credit reporting system can be attacked. The Equifax breach occurred through a bug on an unpatched outsourced enterprise system (Newman 2017).

Although CRSPs have increased their scrutiny and monitoring of third parties, less attention has been devoted to fourth parties. Fourth parties are companies that are connected to a CRSP through another party, usually a third party. These include such entities as subcontractors. An attack or incident at a fourth party can affect a third party that might have access to the CRSP's database or system.

Global Operations

Most CRSPs have global operations that are managed from a central point. Although centralization of similar functions improves efficiencies and reduces costs, this approach can also be a single point of entry for propagating an attack across the network. In addition, centralization might expose the network because system upgrades might not be implemented on time owing to the capital outlay required. CRSPs with global operations must also be wary of the cyber threats prevalent in the regions where they operate.

Internal Threats

Cyber criminals employ advanced social engineering techniques, targeting key staff members of CRSPs to get access into the company network and, in turn, access data. Staff members are being targeted through readily available data (for example, executives' e-mail addresses) and nonconfidential data. Rogue staff members are also a source of vulnerability because they can steal data belonging to data subjects or can hold CRSPs at ransom. This approach is especially typical with contractors or former staff members.

Business Operations

Connectivity to the internet dramatically improves operational tasks, but the increased connectivity can also lead to new security vulnerabilities. Poorly secured internet connections can heighten the risk of attacks.

Advanced Threat Actors

The credit reporting industry is not immune to attacks by threat actors. Both nation state and e-crime adversaries have increased their capabilities as they seek both geopolitical influence and financial gain. The average number of threats and their break-out time for 2018 were estimated at 240 billion per day and 4 hours and 37 minutes, respectively. E-crime adversaries tracked by CrowdStrike in 2018 were found to have conducted banking trojans, ransomware, and point-of-sale compromises, all of which increase cyber risk for CRSPs (CrowdStrike 2019).

Potential Impact of Cyber Incidents

Cyber incidents can have serious ramifications for CRSPs, consumers, and other parties including credit providers. The implications can be economic, financial, and reputational. These are discussed as follows.

Implications for Consumers

Cyber incidents can result in consumers experiencing financial harm, loss of privacy, and loss of trust in the financial system. Consumer data can be exposed to risk of theft, alteration or destruction, accidental disclosure, and loss of data, among others. The Equifax breach (see box 2.1) in 2017 affected more than 143 million customers by revealing their personal information and identification numbers, thus exposing them to the risk of identity fraud.

Economic Cost

Incidents also can have serious ramifications on the availability of credit and, ultimately, economic growth. Data breaches can result in fraudulent loans and credit cards being opened, which can cause organizations to incur increased losses. This possibility can lead to lenders adopting a more cautious approach to lending, and in instances where lenders proceed to lend in the face of breaches, they expose themselves to increased losses and reputational risk.

Financial Cost

The financial cost of a breach includes a decline in enterprise value, breach remediation costs, regulatory and compliance costs, fines and penalties, and higher insurance premiums. Following the disclosure of the data breach in September 2017, Equifax incurred damage-related costs of US$175 million (including professional and customer support) and was forecasted to have litigation costs of between US$56 million and US$110 million (NNT 2017). In other instances, entities such as shipping company Maersk had to reinstall 4,000 new servers, 45,000 new personal computers, and 2,500 applications as a result of the NotPetya infection at a cost of approximately US$300 million. Additionally, the United Kingdom's National Health Service experienced damages from the WannaCry infection estimated to total about 92 million pounds (US$115 million) (Niemantsverdriet 2018).

Several jurisdictions have laws and regulations that impose fines and penalties as a result of a data confidentiality breach involving personally identifiable information. The magnitude of these fines varies by jurisdiction and sector but are usually either a fixed amount or a percentage of turnover. The European Union's General Data Protection Regulation (GDPR), for example, imposes fines up to €20 million (US$22 million) or 4 percent of worldwide annual turnover (whichever is greater).

Another significant cost associated with a breach is that of public relations and communications. Following a breach, a CRSP can incur notification costs associated with advising the authorities and, in certain instances, the data subjects. In addition, massive budgets can be spent in media campaigns during and after the crisis. Significant public relations costs also can include the implementation of credit and identity theft monitoring mechanisms. Another heavy cost is the forensic investigation of the breach (OECD 2017).

Reputational Costs

Breaches also may cause a loss of reputation for CRSPs, in turn affecting their profitability and market value. In the five trading days following the breach disclosure, Equifax lost US$3.5 billion in market value and its third quarter profits decreased by 27 percent (Reuters 2017). The stock price remained 30 percent lower at the end of September (Pettersson 2017). In addition, reputational loss can result in loss of customers and business relations, though this effect has seldom been seen because most companies embark on a dedicated public relations drive to ensure it does not occur (OECD 2017).

3.
GLOBAL CREDIT REPORTING CYBERSECURITY LANDSCAPE

Introduction

This section presents the findings of the Cybersecurity Survey undertaken in February 2019. The survey was used to understand the cybersecurity practices of credit reporting institutions through a questionnaire with 74 questions covering 12 assessment factors. The assessment factors included the cybersecurity environment, legal and regulatory environment, governance and strategy, outsourcing, information sharing, training and awareness, resources, risk management and compliance, audit, incident response, data loss prevention, and preventive controls. A copy of the survey is included in appendix B of these guidelines.

A total of 43 respondents completed the survey. Eight responses were excluded on the basis of incomplete responses and duplications. As a result, 35 responses were analyzed.

Demographics of Respondents

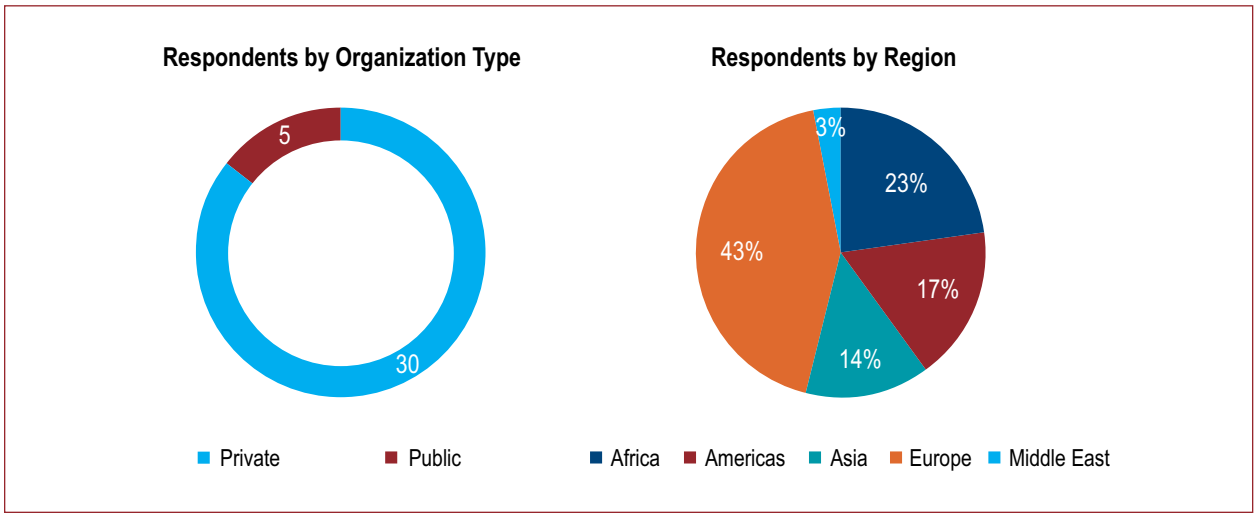
The survey respondents were drawn from credit reporting service providers in both the public and the private sectors. Figure 3.1 provides a breakdown of respondents by organization type and region.

Survey Findings

Local Cyber Environment

The increasing interconnectedness of the financial system requires that CRSPs pay particular attention to the broader cyber environment. The

Figure 3.1: Distribution of Respondents



Source: ICCR Cybersecurity Survey 2019.

survey revealed that data providers and prominent institutions in jurisdictions had been subjected to more attacks (43 percent and 26 percent, respectively) than have CRSPs (23 percent) during the past two years (figure 3.2). The survey findings reveal increasing susceptibility arising from parties other than the CRSPs themselves.

The survey revealed that the most common incident among the CRSPs was denial of services. Data breaches were most noticeable among data providers and other prominent institutions. All three types of organizations experienced ransomware and unauthorized network penetration.

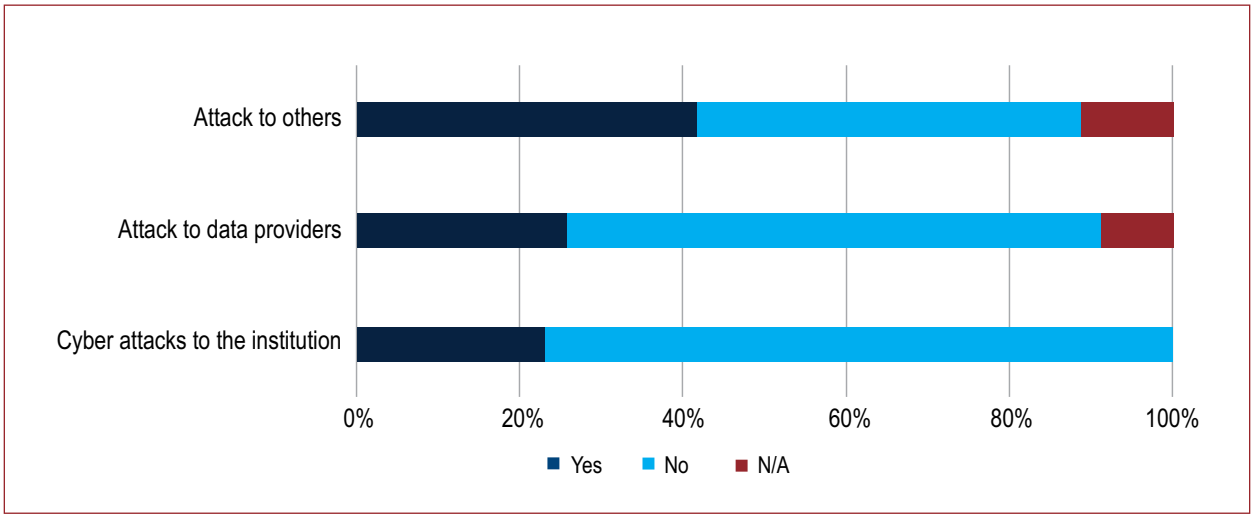
Indicative of the distribution of respondents, data breaches were more prevalent in Europe and Africa as shown in figure 3.3. Europe recorded the highest level of distributed denial of services and unauthorized network penetration incidents. Conversely, the Americas experienced other cyber incidents such as compromised banking systems. Asia had the least number of cyber incidents.

Legal and Regulatory Environment

The majority of the jurisdictions (83 percent) in which the respondents operate have enacted legislation or regulations to deal with cybersecurity and information security (figure 3.4). Most countries have enacted legislation on cybersecurity that sets acceptable standards, establishes financial and sociolegal sanctions, safeguards individual and national interests, mitigates against risk, and facilitates cooperation between countries. Not many African countries had enacted regulations compared to other regions. The Central Bank emerged as the regulatory authority for most of the respondents. The other major regulator was the equivalent of the supervisory authorities (such as GDPR supervisory authority). Figure 3.4 provides more detail on the legal and regulatory environment.

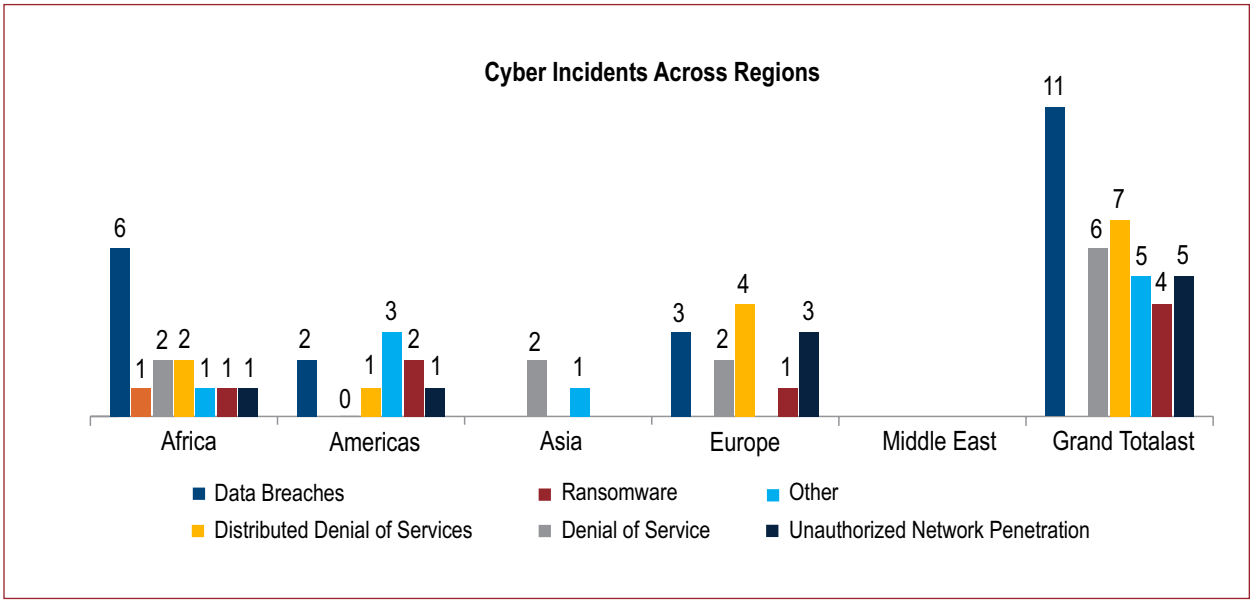
Cybersecurity regulations place responsibility on CRSPs by requiring them to notify affected parties of issues, report issues to regulators or supervisory authorities, and compensate affected parties. All existing legal and regulatory frameworks require the

Figure 3.2: Cyber Attacks and Incidents by Institution Category



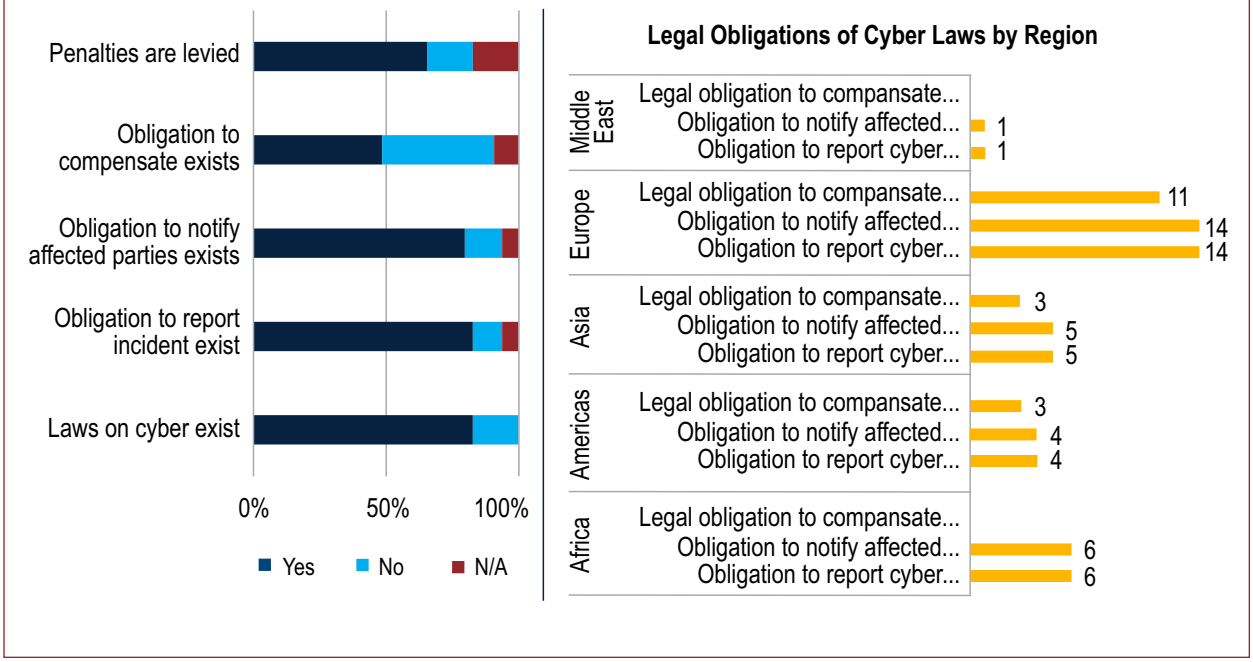
Source: ICCR Cybersecurity Survey 2019.

Figure 3.3: Cyber Incidents across Regions



Source: Cybersecurity Survey 2019.

Figure 3.4: Legal and Regulatory Frameworks



Source: Cybersecurity Survey 2019.

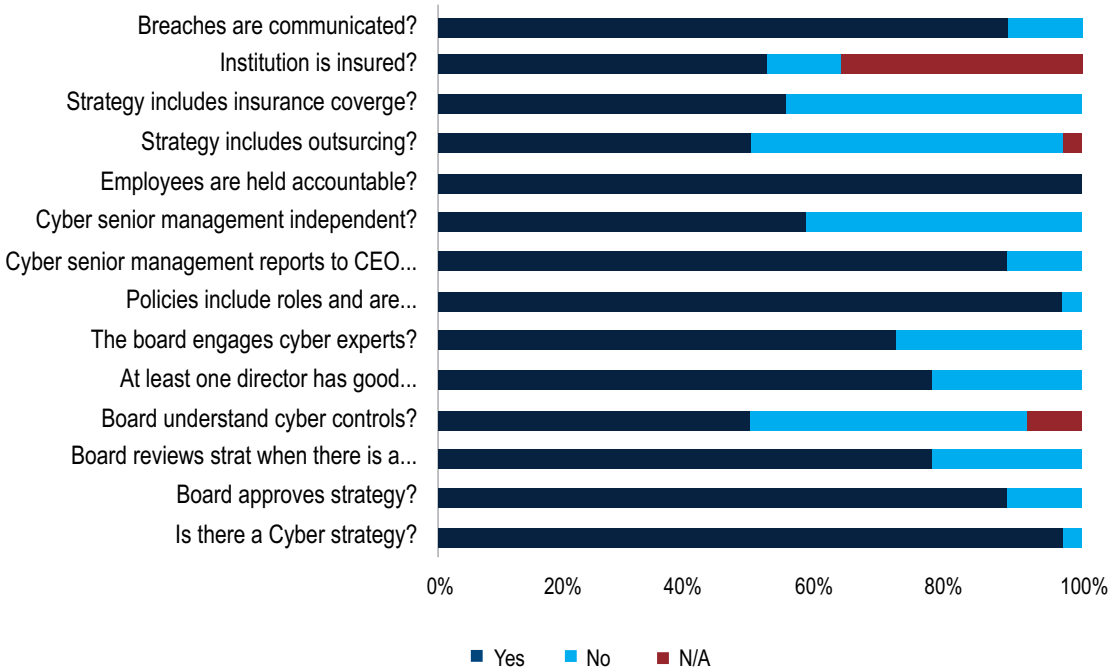
regulated entities to report cybersecurity incidents to regulatory authorities. Of these frameworks, only one does not place an obligation on CRSPs to notify the affected parties. Most of the laws (80 percent) provide for both financial and nonfinancial penalties. Nonfinancial penalties include civil and criminal penalties. Notwithstanding the penalty requirement, however, more than 21 percent of these laws do not provide for compensation of data subjects affected by cyber incidents.

Board, Management, and Cyber and Information Security Strategies

Credit reporting service providers have broadly embedded cyber and information security in their governance processes. All but one of the surveyed CRSPs have developed cybersecurity strategies, policies, and procedure manuals to enhance their security and resilience levels in view of evolving threats. Survey respondents indicated, however, that 11 percent of the strategies are not approved by their board of directors and 20 percent are not reviewed by the board on a regular basis. Failure by boards to ensure regular reviews of cybersecurity strategies can expose the institutions. Although most (54 percent) of the strategies contain a provision for cyber insurance, less than half (45 percent) include a provision on outsourcing.

Boards of directors are working on improving their cybersecurity knowledge. The majority (77 percent) of the respondents' boards have at least one director with cybersecurity knowledge and experience. Nearly half (48 percent) of the respondents stated that their board has an understanding of cybersecurity controls, which is reflected in the fact that 75 percent of the boards retain the services of cyber experts to enhance their members' understanding of cybersecurity (figure 3.5).

Figure 3.5: Board of Directors and Senior Management



Source: Cybersecurity Survey 2019.

A growing number of CRSPs have created a function of Chief Information Security Officer (CISO) or its equivalent who is responsible for cyber and information security. The emergence of a CISO position is founded on the need to separate information and communications technology (ICT) security from ICT risk taking functions. The survey revealed that the most senior officers responsible for cybersecurity were chief information officers (49 percent) and Chief Information Security Officers (40 percent). The remaining respondents had cybersecurity functions that reported to legal or risk departments or the chief executive officer or his or her equivalent. The survey revealed that 51 percent of senior cybersecurity officers were independent from areas using or administering the institution's information technology assets.

Cyber insurance is gaining prominence as one of the risk management options. Of the respondents, 51 percent are insured for cybersecurity events. This finding is consistent with the earlier finding that 54 percent of the respondents had embedded cybersecurity insurance as part of their strategy.

Outsourcing Critical ICT Services

In view of the evolving technological innovations and the need to enhance efficiency, some CRSPs (37 percent) are outsourcing critical ICT services such as security operations centers, data centers, and applications. Data centers are commonly outsourced in Africa and Europe, whereas in the Americas, CRSPs mostly outsource services including web and professional services. The prevalence of outsourcing data centers can be viewed as reflective of the benefits associated with this type of activity such as guaranteed uptime, higher scalability, better flexibility and speed, improved latency and connectivity, and improved business focus. Notwithstanding the benefits of outsourcing, it can be a source of risks for CRSPs in instances where contractors do not comply with cybersecurity, information security, and data privacy standards.

More organizations (54 percent) are increasingly considering outsourcing their critical services. Although only 37 percent of the respondents were outsourcing critical ICT services, the survey revealed that more than half of the respondents had implemented cybersecurity policies that provide guidance on relationships with third parties.

Sharing of Information on Cyber Incidents

Sharing of information on cyber incidents is gaining momentum. The survey revealed that although 66 percent of the boards of directors of CRSPs encourage their cyber teams to engage in information sharing arrangements with other institutions, the practice was less mature in Europe and Africa. The exchange of information can help CRSPs identify and adapt more quickly to evolving attacks.

Third parties are also significantly contributing to information sharing. Of the surveyed CRSPs, 77 percent receive timely notifications of cybersecurity incidents from service providers with whom they have material outsourcing arrangements. This approach is particularly important in the context of increasing levels of outsourcing and the potential for outsourced services to become a source of vulnerability.

A majority (63 percent) of respondents are participating in industry programs designed to promote information sharing. The survey revealed that most of the CRSPs also monitor the cybersecurity incidents within and outside of the financial services industry and participate in industry programs. This practice can help these CRSPs achieve an understanding of all the potential vulnerabilities given the increased levels of interconnectedness. Ultimately, such practices can improve the level of resilience of the financial industry and nations.

Training and Awareness

Training and awareness are important steps in creating a cybersecurity culture within a CRSP. As many as 85 percent of CRSPs have implemented ongoing training and awareness programs (figure 3.6). The training programs include target managers for incident responses and new trends, employees with privileged access permissions, and board members. The survey revealed, however, that training for board members is lagging the training of other staff members; only 25 respondents have trained their board members within the past 12 months. In terms of regional activity, Africa ranks lowest with regard to implementing cyber awareness programs.

Resources

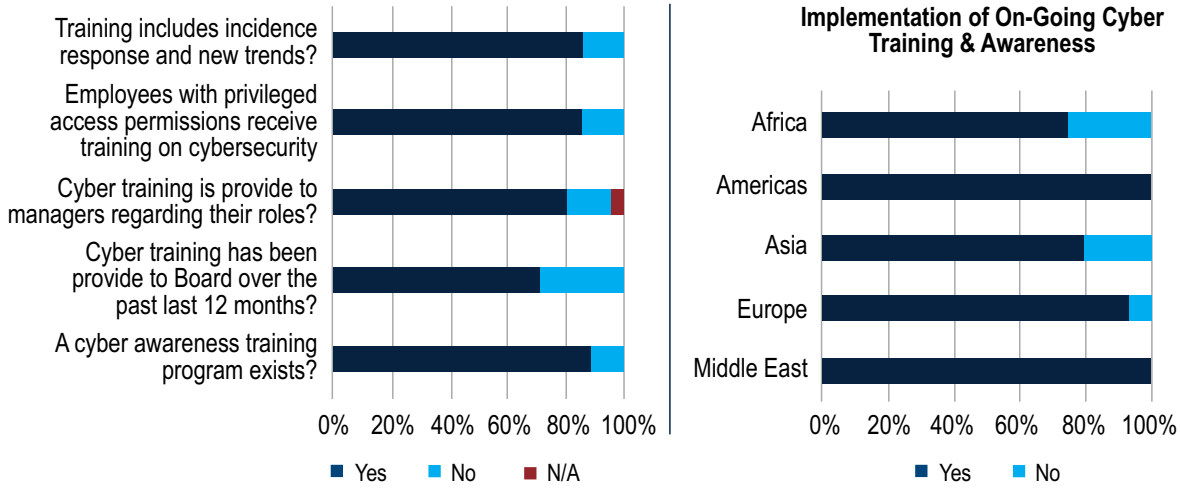
CRSPs are increasingly committing specific resources to improve their cybersecurity capabilities. Four-fifths of respondents recognize the importance of cybersecurity and have put in place specific cybersecurity budgets. Allocating resources for cybersecurity allows the institutions to invest in hardware, software, and human capital. A majority (88 percent) of respondents noted that their cyber budgets were commensurate with the risk levels.

Risk Management and Compliance

CRSPs have embedded risk management into cybersecurity. Most (94 percent) of the respondents have a formal risk management framework that includes cyber risk as one of the risk areas (figure 3.7). Embedding risk management in cybersecurity processes enables security to be an organization-wide responsibility. The risk management frameworks were considered commensurate to the level of cyber risk.

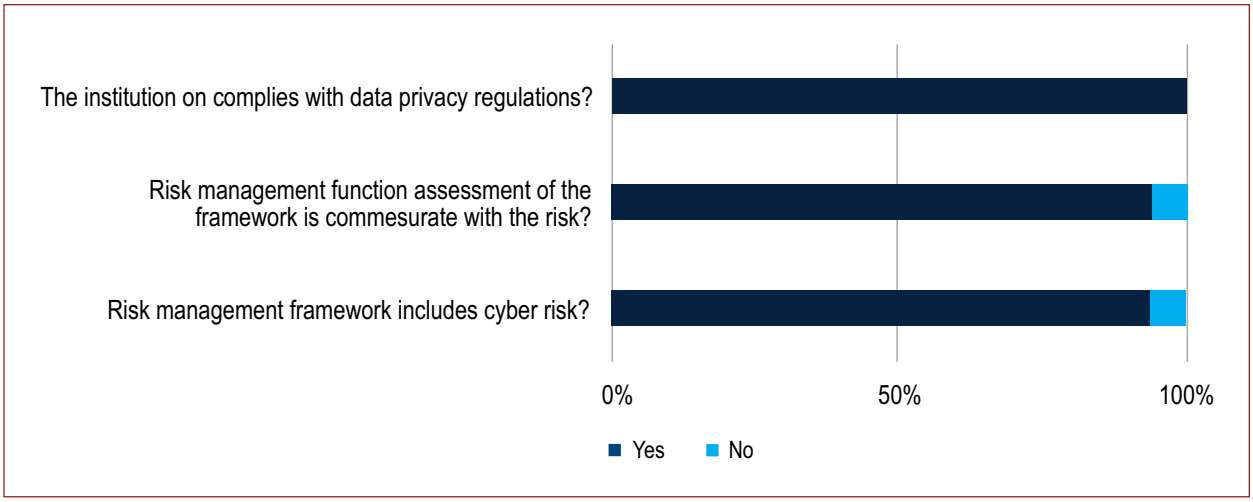
All respondents comply with data protection and privacy regulations. Consistent with the increasing regulatory environment on data protection and privacy across jurisdictions, CRSPs are putting in place mechanisms to ensure compliance.

Figure 3.6: Training and Awareness



Source: Cybersecurity Survey 2019.

Figure 3.7: Risk Management and Compliance



Audit

CRSPs are recognizing the importance of internal audit as a central pillar in cybersecurity. More than three-quarters (77 percent) of the respondents have enhanced their internal audit functions with resources and expertise to enable them to conduct cybersecurity assessments.

The audit (internal and external) functions are validating cybersecurity controls and processes. Most of the respondents have ensured that their audit function assesses the effectiveness of cybersecurity controls, incident response, and threat information. However, the survey revealed that 49 percent of the CRSPs' audit functions did not validate the effectiveness of third-party relationship management, reflecting an inherent risk area in view of the increased outsourcing of critical ICT services.

Incident Response

Awareness of the importance of a cybersecurity incident response plan is growing across CRSPs. More than 90 percent of the respondents have documented incident response plans. However, notable gaps were observed with respect to partnering with their national computer emergency response team, external communications, and performing simulation exercises (figure 3.8). Only 51 percent of the respondents have a partnership relationship with their national computer emergency response team, potentially depriving the CRSPs of access to advice and support that come with such platforms. Similarly, 35 percent of the CRSPs do not perform simulation exercises to assess the effectiveness of their incident response plans. Simulation exercises play an important role in helping CRSPs identify potential gaps and areas for enhancement.

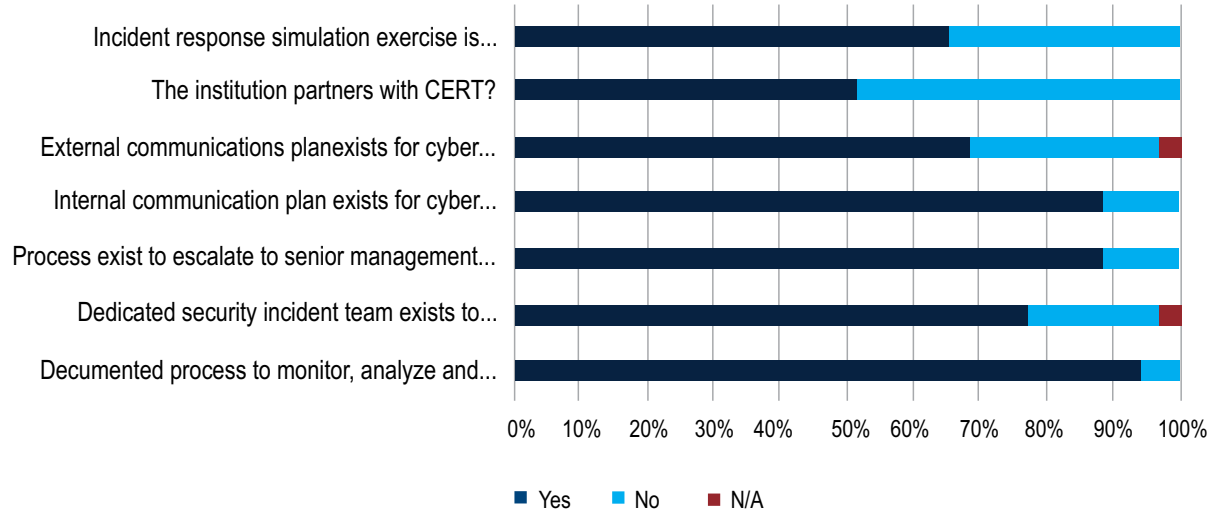
Data Loss Prevention

In view of the importance of data and the emerging laws on data protection and privacy, most respondents have stringent data protection or access components programs. Approximately 80 percent of them had implemented both programs to monitor and prevent breaches and some rules to control printing of sensitive information (figure 3.9). This finding is consistent with an earlier finding revealing that less than 5 percent of the CRSPs had been subject to a data breach. The survey revealed that 40 percent of the CRSPs have not implemented user verification mechanisms before sending e-mails.

Preventive Controls

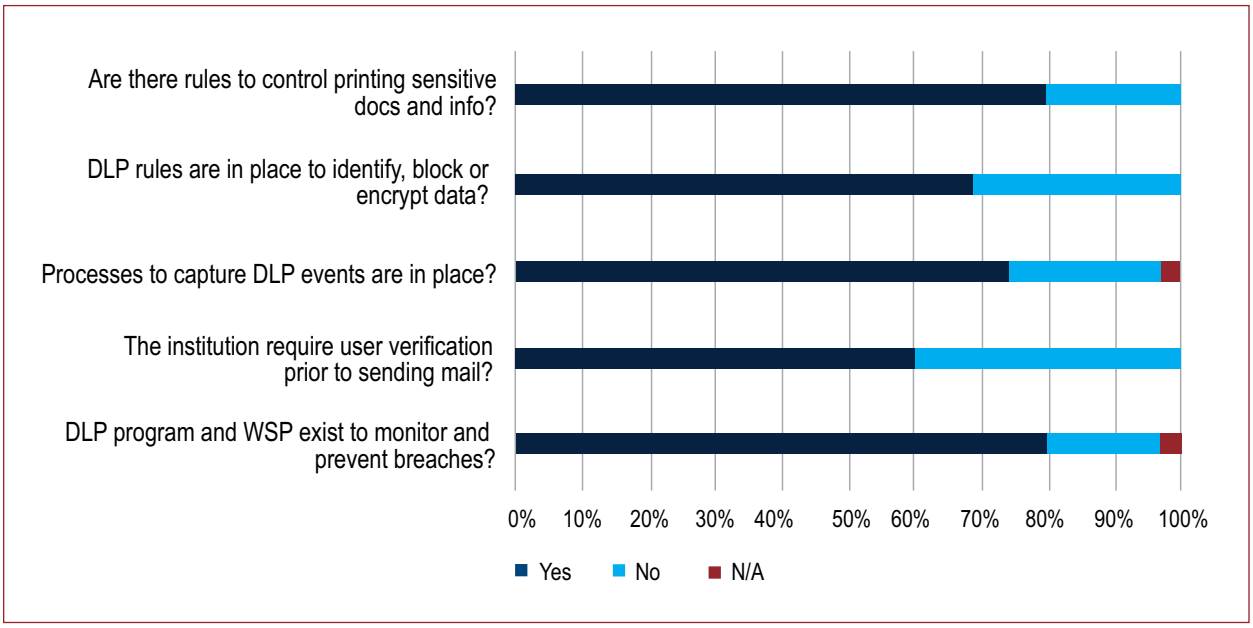
Respondents are successfully implementing controls against cybersecurity risks. All have implemented physical controls and created tight controls for administrative privileges. The CRSPs have not matured in terms of implementing detective controls, as reflected by 43 percent of entities lacking automated processes to detect and block unauthorized changes to software and hardware. As a result, these CRSPs are susceptible to system attacks because they have no mechanism to provide adequate warnings.

Figure 3.8: Incident Response



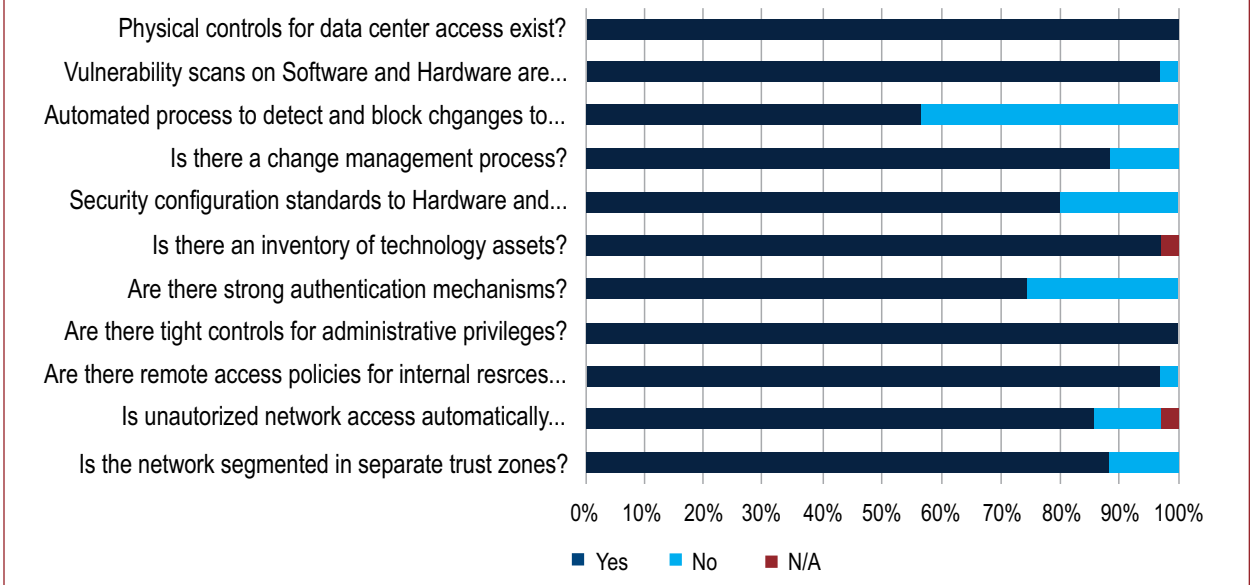
Source: Cybersecurity Survey 2019.

Figure 3.9: Data Loss Prevention

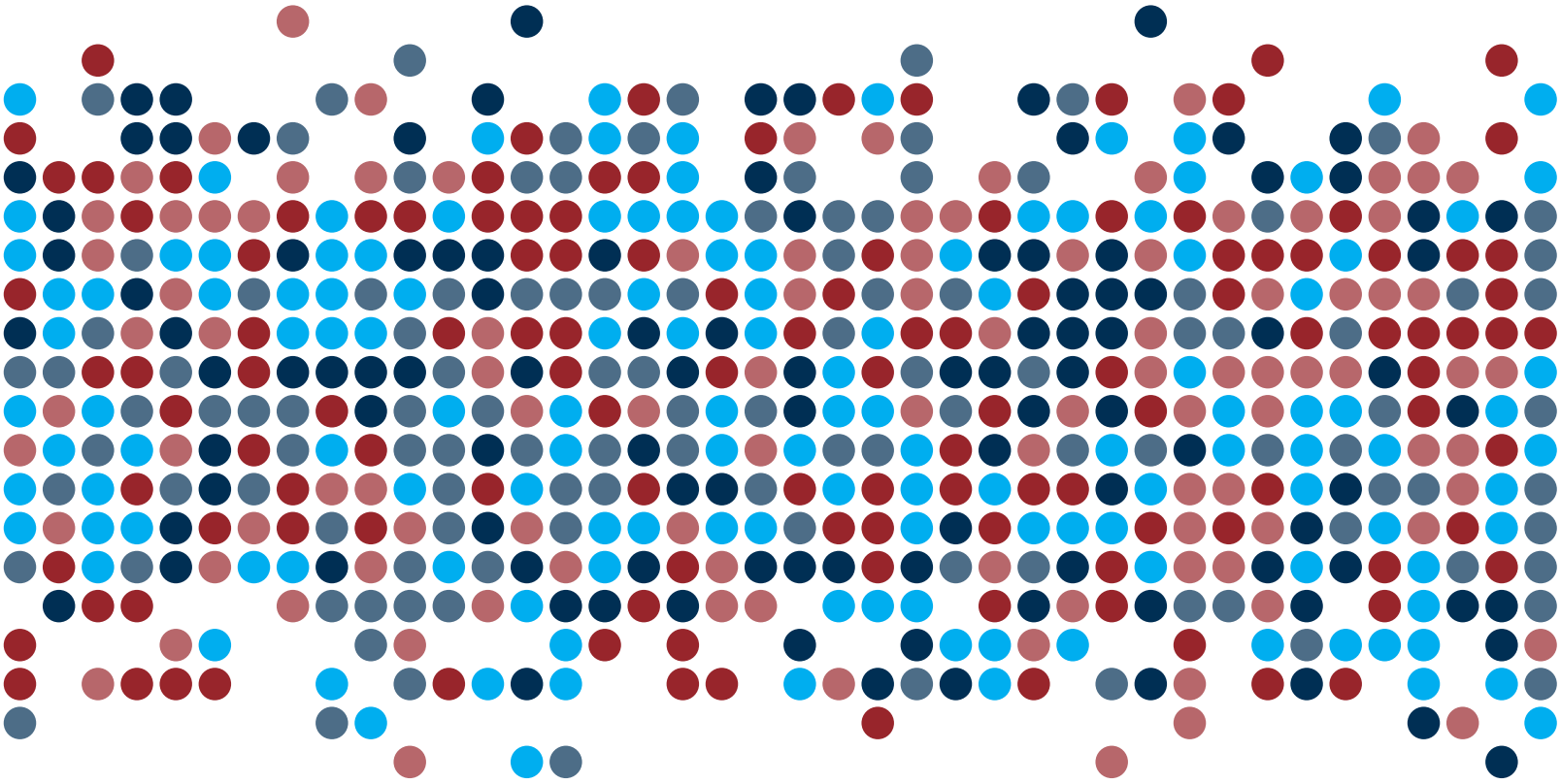


Source: Cybersecurity Survey 2019.

Figure 3.10: Preventive Controls



Source: Cybersecurity Survey 2019.



4. CYBERSECURITY GUIDELINES

Existing Credit Reporting Guidelines on Cybersecurity

The International Committee on Credit Reporting, in the General Principles for Credit Reporting (World Bank 2011) provides high-level guidance on cybersecurity. **General Principles 2 and 3 and Recommendation E outline the need for rigorous standards of security to ensure that data are protected (box 4.1).**

Against the background of growing importance of the credit reporting systems as a crucial part of the financial infrastructure and the changing credit ecosystem, providing more detailed guidance as outlined in this section is important. This guidance builds on the survey findings described in section 3.

Detailed Cybersecurity Guidance

Security controls are the safeguards and countermeasures prescribed for information systems or organizations and are designed to protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems and organizations. They must satisfy a set of defined security requirements

Box 4.1: Credit Reporting Guidance on Cybersecurity

General Principle 2: Data Processing—Security and Efficiency

"Credit reporting systems should have rigorous standards of security and reliability, and be efficient.... Credit reporting service participants should protect data against any loss, corruption, destruction, misuse or undue access.... All participants in a credit reporting ecosystem should undertake best efforts to implement commercially reasonable data security safeguards to protect data against these and other potential threats" (World Bank 2011, 30).

General Principle 3: Governance and Risk Management

"The governance arrangements of credit reporting service providers and data providers should ensure accountability, transparency and effectiveness in managing the risks associated with the business and fair access to the information by users" (World Bank 2011, 31).

Recommendation E

"Central banks, financial supervisors, and other relevant authorities, both domestic and international, should cooperate with each other, as appropriate, in promoting the safety and efficiency of credit reporting systems" (World Bank 2011, 4).

(NIST 2013). Figure 4.1 depicts the key areas of focus for cybersecurity.

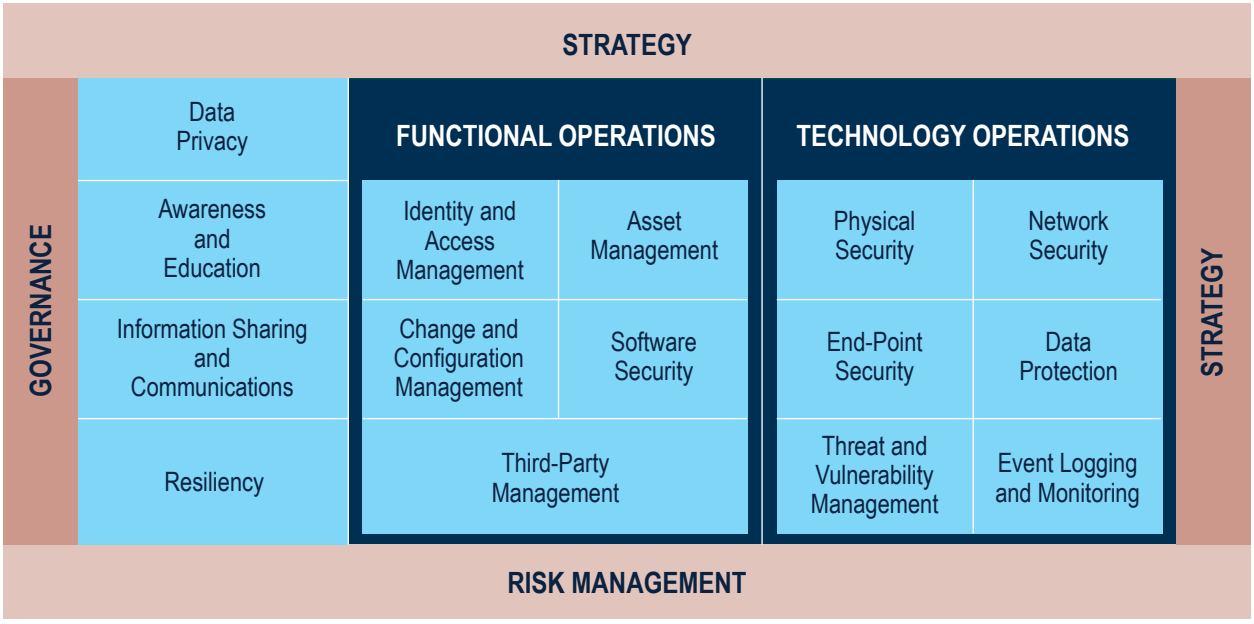
The principle of proportionality should be considered when an entity applies these guidelines. Proportionality responds to three main characteristics: adequacy, necessity, and nonexcessiveness. Hence, when applying these guidelines, organizations should consider security requirements according to their business nature, scale, and complexity and should adhere to regulatory standards applicable to their jurisdiction. A risk-based approach should be followed to ensure that security controls are commensurate with the risk to critical infrastructure and organizational objectives. The focus areas are discussed in the following sections.

Cybersecurity and Data Privacy Strategy

A cybersecurity and data privacy strategy is a key element for transforming the cybersecurity function into a business enabler, allowing the organization to take a proactive approach to managing cyber and data privacy risks. The strategy should aim to provide cohesion and strategic direction to the organization's cybersecurity and data privacy activities, organizing them with a purpose under a comprehensive program and facilitating its alignment with the organization's strategic goals. Thus, the strategy should be tailored to the culture and complexity of the organization's environment, taking into consideration the regulatory framework, the organization's risk appetite, and the relevant cybersecurity and data privacy exposures.

The cybersecurity and data privacy strategy must focus on delivering strategic value to the organization. Hence, it should be aligned with the business strategy to deliver strategic value by achieving increased stakeholder confidence, minimizing the effect on business in case of an incident, and improving market adoption. For example, if the organization intends to gain competitive advantage by leveraging technologies such as Cloud, Mobile, or Big Data, the strategy should be geared toward managing risks associated with those technologies.

Figure 4.1: Cybersecurity Focus Areas



Source: Authors.

Developing a cybersecurity and data privacy strategy requires a significant amount of effort, but a multipronged approach can be used to divide it into manageable phases as proposed in box 4.2.

Appropriate resources must be allocated for the successful implementation of the strategy. The cybersecurity and data privacy strategy should be explicitly approved by a board of directors or similar governing authority. Additionally, adequate senior management should be involved in the definition, implementation, and periodic review of the strategy and implementation plan.

Organizations also need to understand how they compare against peers and comparable organizations. To support continuous improvement and adjust the strategy as needed, organizations in the credit reporting industry should regularly conduct benchmark exercises to compare their cybersecurity and data privacy readiness against comparable industry organizations and peers. For this purpose, a leading cybersecurity assessment framework (for example, NIST Cybersecurity Framework) could be leveraged.

Innovation and cybersecurity have been seen traditionally at different ends of the business strategy, but there is an opportunity to change this perspective through the cybersecurity and data privacy strategy. Innovation is considered a driver for efficiency, growth, and revenue generation,

Box 4.2: Steps to Develop a Cybersecurity and Data Privacy Strategy

Steps to Develop a Strategy:

1. **Prioritize critical information assets.** Create an inventory of information assets (data, physical devices, information systems, and software) that support the organization's critical business processes. Identify the potential effect (financial, operational, and reputational) to the organization if the integrity, confidentiality, or availability of those assets is compromised, and assign a criticality rating to each asset. Prioritize the inventory of assets by criticality, and focus on the most critical information assets.
2. **Understand the threats.** Identify the threat actors (for example, state-sponsored entity, organized crime, hacktivist, or malicious insider) that are relevant to your organization. Rank them by capability and motivation to compromise the organization's critical assets.
3. **Assess current state.** Conduct a candid assessment of current cyber capabilities and performance using an industry-recognized cyber framework (for example, National Institute of Standards and Technology Cybersecurity Framework). Understand the weaknesses and shortcomings to meet the business and information technology strategic goals.
4. **Define the future state.** Set the vision and long-terms goals for the cybersecurity function, accounting for the organization's strategic goals. These goals should be aspirational shifts that set the direction for the future of the cybersecurity function in the organization.
5. **Create an implementation plan.** Conduct a gap analysis between the current cyber capabilities and the desired future state, and identify initiatives that would help bridge the gap. Estimate the cost and level of effort for each initiative, and determine the security benefit each would provide. Create an outline by arranging the list of initiatives in a multiyear time line, assigning high priority to those that provide significant benefit with low cost or level of effort to implement.
6. **Implement plan, and track progress.** Assign necessary resources to implement the outline. Track key performance indicators, and frequently report progress to senior management.

whereas cybersecurity can be seen as an obstacle for agility in service delivery. However, this viewpoint is changing, and boards of directors and business executive teams understand that cybersecurity is no longer a compliance exercise. The ability to deliver secure services leveraging disruptive technology such as robotic process automation, artificial intelligence, or Blockchain is a competitive differentiator that can help build long-lasting customer relationships. Having a mature cybersecurity and data privacy program can instill confidence among stakeholders and pave the way for seamless adoption of disruptive technologies. For specific security controls, refer to the "Strategy" section in appendix table A.1 in appendix A of these guidelines.

Governance

Implementation of the strategy must be monitored to ensure that the program delivers expected strategic value to the organization. Therefore, a cybersecurity and data privacy governance framework should be established to define roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of the strategy. Policies, standards, and guidelines should be documented, approved, published, regularly reviewed, and communicated to all relevant stakeholders. These documents should set the direction in line with business strategic goals and demonstrate support for cybersecurity and data privacy across the organization. Dependencies and critical functions for the delivery of critical services should be identified, along with the resiliency requirements to support the delivery of those services.

The roles and responsibilities of individuals supporting the cybersecurity and data privacy program must be formalized. Mature organizations usually have a qualified individual appointed as a Chief Information Security Officer (CISO), who is responsible for overseeing and implementing the cybersecurity program and enforcing the cybersecurity policies. Appropriate lines of reporting should be established for the CISO to communicate to the board of directors, or equivalent authority, the effectiveness of the cybersecurity program and any material cybersecurity risks and events. The same duties and communication lines should apply to the role of a Data Protection Officer (DPO), recognizing the importance of data privacy.

Sponsorship from a board of directors is crucial to sustain the execution of the cybersecurity and data privacy program outlined in the strategy. Accordingly, a board of directors or similar governing authority should ensure that adequate resources are allocated, appropriate authority is assigned, and access to the board or similar governing authority is established. A board of Directors also should take a proactive role and frequently ask questions of the CISO or DPO to understand the current state of cybersecurity and data privacy in the organization, the most significant risks that may be affecting the organization, and the way they are being addressed. Some examples of these questions are included in box 4.3. For specific security controls, refer to the "Governance" section in appendix table A.1 in appendix A of these guidelines.

Risk Management

Implementation of the cybersecurity strategy and execution of the program will inevitably uncover risks that need to be appropriately managed. Cybersecurity should be considered a dimension of the overall ICT risk management, which, in turn, should be integrated with the organization's enterprise risk management. Cybersecurity risks (including third-party and external dependencies risks) should be managed in a manner that is consistent with the organization's mission and business objectives outlined in the strategy to enable cybersecurity activities' prioritization and resource allocation.

A cybersecurity risk management framework provides guidance for the consistent identification, assessment, and response to cyber risks. The framework should include the risk taxonomy used to reduce risks identified from different sources and activities such as internal audits, incident reports, and new technology risk assessments. Similarly,

Box 4.3: Sample Questions that a Board of Directors Should Ask

Some sample questions are as follows:

1. What are the most significant cyber and data privacy risks that our organization faces?
2. What measures can we use to mitigate these risks?
3. What is the recommended method for the board to measure and monitor these risks?
4. Have we seen threats directed against our organization from capable adversaries, and how were those threats detected?
5. How will we respond to a cyber incident that could negatively affect our customers, our operations, or our reputation?
6. Has our program been audited, and, if so, what is our status in such audits?
7. What technical solutions and risk reduction measures should be implemented in the next 3 years?
8. How do we compare with our competitors in the industry?
9. Do we have the proper cybersecurity and data privacy teams with the required skills?
10. How do we keep our employees and customers prepared to play their role in cybersecurity?

the framework should provide guidance on how to assess risks in a consistent manner by defining likelihood and effect scales and thresholds. The framework should also provide guidance on risk treatments (avoid, mitigate, transfer, or accept), including a decision framework that outlines what level of authority can accept risks depending on different residual risk thresholds.

The cybersecurity risk management framework also describes the strategy to monitor and communicate risks. Because risks are dynamic, a reporting and monitoring mechanism should be established to allow cybersecurity risks to be timely communicated to a board of directors or similar governing authority. This approach, in turn, allows the board to monitor the effectiveness of the organization's mitigation plan and assess whether it is consistent with the approved risk appetite and tolerance thresholds. A risk register that includes the identified risks and associated attributes should be maintained to facilitate this process. The register may include attributes such as risk identification number, description, category (from the taxonomy), owner, residual likelihood and effect, risk triggers, mitigation, and contingency plan.

Leading organizations frequently conduct risk and control self-assessments to evaluate the effectiveness of the cybersecurity risk management and identify corrective actions. For these assessments to be successful, key process owners and stakeholders should participate in these exercises to identify risk and assess risks identified against key business objectives. Controls should then be discerned for each of those risks and the effectiveness of the controls assessed to determine whether the controls are working as intended. Control weaknesses or gaps should be documented along with proposed corrective actions. Finally, a high-level summary of the results of the risk and control self-assessment should be sent to a board of directors or similar governing authority. For specific security controls, refer to the "Risk Management" section in appendix table A.1 in appendix A of these guidelines.

Compliance

Compliance risk is still a top concern for a board of directors. On the one hand, noncompliance penalties can be very high as the scope of regulatory focus continues to increase. On the other hand, the traditional bottom-up compliance approach that focuses on the repetitive testing of controls contributes very little to reducing the residual operational risk of the organization. For this reason, organizations should review their security compliance program to find opportunities for better alignment with the overall risk management framework and to focus on residual risks that matter to the enterprise.

Compliance does not equal security, but some synergies should be maximized. The design, operation, use, and management of information systems in the credit reporting industry are subject to legal, regulatory, and contractual security requirements. Accordingly, organizations should have a compliance program in place to avoid breaches of any applicable law, regulations, contractual obligations, or requirements established in the security policies. To the extent possible, compliance and cybersecurity efforts should be aligned to minimize duplicative efforts (for example, control testing, risk assessments, and risk reporting) and facilitate a risk-based allocation of resources to address risks relevant to the organization.

Compliance with data privacy regulations is a key requirement for organizations in the credit reporting industry. CRSPs manage customers' personal data by nature of the business. Accordingly, they should ensure compliance with data privacy requirements in alignment with relevant legislation, regulations, and contractual agreements. To achieve compliance, organizations should obtain a comprehensive understanding of the data collected and the security controls implemented to meet those privacy requirements. The following "Data Privacy" section provides more guidance on privacy requirements and best practices.

For specific security controls, refer to the "Compliance" section in appendix table A.1 in appendix A of these guidelines.

Data Privacy

Recent high-profile data breaches and new privacy regulations around the world emphasize the importance of data privacy. Organizations in the credit reporting industry have recently observed high-profile data breaches that led to the compromise of the privacy of stored personal information about individuals. Even though the direct costs associated with these incidents are already high, usually they account for only the known costs (for example, technical investigation and cyber improvements, customer breach notification, and postbreach protection); however, they fail to account for other less visible costs (for example, reputational damage and loss of customer confidence, increased cost to raise capital, increased insurance premiums, and disruption of operations). Privacy regulations in Europe and Asia are further tightening the compliance requirements, and these will very likely be followed by similarly strict requirements in other geographical regions, further clarifying for organizations processing personal data that protecting the privacy of their personnel and customers' data is a business requirement.

A data privacy policy is the first step toward addressing the increased pressure on protecting the privacy of personal data. A data privacy policy should be documented, approved, published, regularly reviewed, and communicated to all relevant stakeholders, setting direction in line with business objectives and demonstrating support for data privacy across the organization. The policy should define personal data, provide guidance on security controls for protecting the privacy of personal data, and establish roles and responsibilities for protecting the privacy of personal data (for example, data owner and data custodian). The policy must consider legal, regulatory, and contractual data privacy requirements. Organizations should consider the appointment of a DPO to provide

guidance to internal and external users and service providers on their data protection responsibilities and the established procedures related to data privacy protection.

The effectiveness of data privacy protection efforts hinges on the organization's comprehensive understanding of the type of personal data collected or processed. In addition to completing a data inventory on a regular basis, organizations should consider conducting a data flow mapping exercise that enables them to trace the movement of personal data from the source to the point of use, providing visibility into all the ways data have changed throughout the data life cycle. This approach also would help organizations effectively identify and manage risks associated with personal data shared with third parties.

The risks arising from activities conducted by third parties require ongoing oversight. A board of directors is ultimately responsible for managing activities conducted through third-party relationships to the same extent as if the activity were handled within the organization. Before entrusting customer or staff member personal data to a third party, a CRSP should make appropriate contractual arrangements and obtain verified proof (for example, attestation from independent auditor) that the third party has implemented appropriate technical and organizational controls that meet applicable legal requirements to protect the personal data. Compliance with those requirements should be monitored on an ongoing basis.

Organizations should implement both technical and process controls to ensure confidentiality and integrity of personal data. Organizations must deploy technical controls such as data masking, encryption, strong authentication, data loss prevention, and logging to ensure access to personal data is restricted to business objectives. Similarly, process controls such as periodic impact assessments, incident response, and breach notification readiness can help reduce potential exposure to this risk.

An established breach notification process is not only a key requirement in most privacy regulations, but also a best practice for organizations taking data privacy seriously. The data breach notification process should describe the criteria, format, time line requirements, and procedures for notifying appropriate supervisory authorities and data subjects of a data breach in a timely manner. The data breach communication should describe the nature of the incident, the data that were involved, and recommendations to mitigate potential adverse effects.

Beyond compliance, consideration should be given to leading data privacy principles, standards, and frameworks. There are multiple relevant data privacy frameworks and jurisdiction-specific data privacy regulations (for example, the European Union's GDPR). There is some variation in the definitions, issues, and principles used in the frameworks.[5] However, some important concepts are similar across the frameworks and regulations and should be considered by all organizations trying to improve their data privacy efforts. Box 4.4 provides some examples of those key concepts. For specific security controls, refer to the "Data Privacy" section in appendix table A.1 in appendix A of these guidelines.

Awareness and Education

Employee awareness is as important as the technology or processes in place at the organization to manage cybersecurity risks. Cybersecurity attacks frequently target uninformed employees or contractors with a view to accessing an organization's systems. For example, phishing e-mail attacks are conducted by perpetrators pretending to be someone (for example, one of

[5] For example, see the APEC (Asia-Pacific Economic Cooperation) Privacy Framework and the OECD (Organisation for Economic Co-operation and Development) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Box 4.4: Some Key Data Privacy Considerations

Some considerations are as follows:

1. Choice and consent: Organizations should provide information to the data subjects of the available choices for accessing, updating, and restricting access to their personal data. Explicit consent should be obtained from the data subjects before using their data for specific purposes.
2. Purpose and collection limitation: Organizations should specify at the time of collection the purpose for which the personal data are collected. These personal data should be obtained by lawful and fair means.
3. Data minimization: Organizations should ensure that data collected on a subject are adequate, relevant, and limited to what are necessary in relation to the purposes for which they are processed.
4. Storage limitation: Organizations should not keep personal data for longer than necessary to support the purposes for which they were collected.
5. Openness, transparency, and notice: Organizations should communicate to data subjects their rights, details about the personal data that are being collected, and the purpose for collection. Organizations should answer questions in a manner that is clear and easy to understand.
6. Privacy by design and by default: Organizations should build appropriate safeguards into the full life cycle of personal data processing and implement appropriate technical and organizational controls for ensuring that, by default, only personal data that are necessary for each specific purpose of the processing are processed.
7. Accuracy and quality: Organizations should ensure that the collected personal data are relevant, necessary, accurate, complete, and current.
8. Individual participation: Organizations should provide easy-to-use processes to allow data subjects to access their personal data and have the data erased, rectified, completed, or amended and to withdraw consent to use their personal data.
9. Security safeguards: Organizations should establish technical and administrative security controls that address confidentiality, integrity, and availability of data and mitigate the risks of unauthorized or unlawful processing, loss, damage, or destruction of personal data.
10. Accountability: Organizations should be accountable for the governance and risk management of personal data and for the guarantee of compliance with all applicable legal requirements.

the organization's senior executives) or an internal operation (for example, the Help Desk) with the intention of tricking the user to provide sensitive information such as usernames and passwords. Phishing e-mails may also be used by the perpetrator to deliver malware (for example, ransomware) when the user opens an attachment or clicks on a link. Earlier on, phishing e-mails attacks were massively deployed through spams campaigns, but now the phishing attacks are more targeted (for example, "whaling," or phishing attacks targeting the organization's executives). To counter these types of attacks, organizations should implement cybersecurity awareness and education programs to equip the workforce with the appropriate knowledge to conduct their duties in a secure way and prevent becoming victims of cybersecurity attacks that could lead to the compromise of the organization's systems. Programs should periodically gauge the effectiveness of their awareness campaigns by conducting tests.

Employees in an organization can often be considered the weakest link, but with appropriate understanding of their role in protecting the organization against cyber attacks, they can also be the first line of defense. Cybersecurity awareness and education initiatives should be undertaken to keep personnel informed of common cybersecurity attack patterns and the way to protect the organization's assets from existing and evolving cybersecurity threats. These awareness efforts should ensure that all personnel understand their roles and responsibilities with regard to protecting the organization's information assets. For that purpose, the content of the awareness and education campaigns should be tailored to target different types of users, from ICT administrators and developers, all operation centers, and members of administration staff to members of senior management and the board of directors.

Furthermore, providing timely and relevant cybersecurity awareness and education training to customers is imperative. As financial institutions rely more and more on digital channels to communicate with the customers, educating these customers against common attack patterns has become crucial; training can help them distinguish between a legitimate request from the institution and a dangerous attempt through a phishing e-mail to compromise their user credentials or other sensitive information. Organizations are using all available channels, from the corporate website and mobile applications to social media postings, to educate their customers on how to prevent identity theft, fraud, and scams. For specific security controls, refer to the "Awareness and Education" section in appendix table A.1 in appendix A of these guidelines.

Information Sharing and Communications

Information sharing helps improve awareness among CRSPs. The interconnectedness of the financial infrastructure may expose the credit reporting industry to systemic risk. A localized breach in a CRSP could be propagated to others who are interfaced to it, triggering a widespread disruption across the entire credit ecosystem. Similarly, CRSPs may be unaware that a coordinated attack against several other CRSPs in the region is underway, hindering the ability to react timely and prevent the widespread disruption of services.

Sharing threat intelligence and recent attack patterns would help strengthen cybersecurity and enhance resilience in the credit reporting industry. Sharing tactical and technical information, such as threat intelligence and details on how vulnerabilities were exploited in recent cybersecurity attacks, allows organizations to learn about emerging attack patterns and improve their detecting and response capabilities. Collaboration among private and public entities and authorities allows for a deeper understanding of the vulnerabilities in the credit reporting ecosystem and the way they could be potentially exploited by an attacker, leading to the disruption of operations. To enhance the cybersecurity resiliency of the credit reporting industry, CRSPs and public authorities should identify and address impediments to information sharing. For specific security controls, refer to the "Information Sharing and Communications" section in appendix table A.1 in appendix A of these guidelines.

Resilience

When responding to a cybersecurity incident, having a formalized incident response plan is important. Reacting without a plan once the network has been infiltrated or data have been breached will result in confusion and slower overall response times. Plans, procedures, and technologies should be established and maintained by organizations to analyze and respond to cybersecurity events and to sustain operations throughout a cybersecurity incident. Such practices should be commensurate with the risk to critical infrastructure and organizational objectives. The incident response plan should define criteria for categorizing and prioritizing incidents and provide guidelines on the actions to be followed such as preparation, identification, containment, eradication, recovery, and lessons learned.

Establishing a dedicated computer security incident response team will boost the organization's capabilities to timely respond to cybersecurity incidents. Clear roles and responsibilities should be established for carrying out response activities that enable a rapid response in the case of cybersecurity events. Many leading organizations also rely on specialized security operation centers, internal or outsourced, as the first line of defense and focal point for coordination of efforts with local specialized teams such as a national computer emergency response team.

Business continuity and disaster recovery plans are key elements of cybersecurity preparedness, with the focus on the necessary activities to recover from a cyber incident. As modern organizations continue to rely on ICT to conduct their business activities, the ICT disaster recovery plan should be developed in conjunction with the business continuity plan. Whereas the business continuity plan focuses on the procedures to allow restoration of business operations, the ICT disaster recovery plan must detail the procedures to be executed to ensure timely restoration of systems and information assets. A business impact analysis should be frequently conducted to determine the information assets (including outsourced systems and services) that support critical business processes and to establish and adjust the required recovery objectives. Restoration activities should be coordinated with relevant internal and external parties (for example, internet service providers, vendors, local CERTs).

Incident response, business continuity, and disaster recovery plans may become obsolete if they are not frequently tested and updated. These plans should be continually tested against a variety of realistic scenarios involving relevant internal and external stakeholders. Scenarios such as extended power outages or distributed denial-of-service (DDoS) attacks should be tested through tabletop and functional exercises to evaluate the effectiveness of the plans and the readiness of the personnel to respond to an incident. Lessons learned from tests and forensic analysis conducted on real events should be incorporated into the plans to improve the organization's ability to effectively and timely respond to cyber events. For specific security controls, refer to the "Resiliency" section in appendix table A.1 in appendix A of these guidelines.

Technology Operations

The key components of the cybersecurity program described in this section are identity and access management, asset management, change and configuration management, software security, and third-party management.

Identity and access management

Access to critical information assets must be limited to only the necessary individuals at the necessary times based on business needs. Effective identity and access management is key to managing the risk of unauthorized access to an organization's information assets and to maintaining the confidentiality and integrity of information assets. Processes, procedures, and technologies should be established to appropriately manage the entire life cycle of digital identities and profiles for entities that may be granted logical or physical access to the organization's information assets.

Greater control of user access can help organizations reduce the risks of internal and external data breaches. Access to an organization's information assets should be managed, following the principles of least privilege and separation of duties. Access permissions should be duly authorized, assigned, monitored, periodically reconciled, and timely revoked. Remote access to the organization's network and information systems should be authorized and monitored and should be granted only after appropriate configuration requirements are met. Such requirements may include the use of encrypted communication channels or multifactor authentication, among others.

Special attention should be given to the allocation of privileged access rights. This practice may require conducting a more thorough and frequent review of a user's need to have those access rights and an evaluation of the measures in place to manage risks

associated with the concentration of privileged access on some individuals. Additionally, guidelines should be in place to determine when additional protection would be required for those privileged accounts, such as the use of strong authentication. For specific security controls, refer to the "Identity and Access Management" section in appendix table A.1 in appendix A of these guidelines.

Asset management

To manage cybersecurity risks effectively, organizations need to identify and prioritize the critical information assets that must be protected from the most relevant threat actors. Without a comprehensive understanding of the information assets (data, physical devices, information systems, and software) that enable the organization to achieve its business purposes, an organization would not be able to effectively prioritize activities and efficiently allocate resources to address cyber risks. Processes, procedures, and technologies should be established for managing the organization's information assets throughout all stages of their life cycle.

An inventory of all internal and external information assets should be maintained. The inventory should record important information such as a unique asset identifier, asset owner, data classification, software version, and physical location. Similarly, external assets such as information systems operated by third parties or data entrusted to third parties for processing should be catalogued. Internal and external assets should be prioritized on the basis of their classification, criticality, and business value. For specific security controls, refer to the "Asset Management" section in appendix table A.1 in appendix A of these guidelines.

Change and configuration management

Changes should be appropriately managed to avoid the introduction of vulnerabilities into information systems that enable the organization to achieve business purposes. The increase in complexity of information systems that support business operations also increases the likelihood of accidental errors when changes are made to the configuration of related information assets. This circumstance may expose them to cybersecurity attacks that could compromise the confidentiality, availability, and integrity of those assets. For example, cloud service providers offer powerful administration consoles to simplify the management of an organization's assets in the cloud. Recently, several cybersecurity events have been published where cloud repositories containing corporate sensitive information were accidentally made available to external users. Change and configuration management covers the continuous process of controlling and approving changes to information assets that enables the organization to achieve its business purposes.

Information asset configuration should be managed throughout the entire life cycle. Organizations following best practices usually establish and maintain processes, procedures, and technologies for managing the information asset configuration throughout the entire life cycle. This practice includes the definition of an approved configuration baseline and the verification that assets are configured according to the baseline. For specific security controls, refer to the "Change and Configuration Management" section of appendix table A.1 in appendix A of these guidelines.

Software security

Security vulnerabilities in enterprise applications could be exploited by attackers to access the organization's infrastructure and compromise critical information assets. A well-defined process for developing and acquiring software provides the foundation for the successful development, implementation, and operation of organizational information systems. Information security activities should be built in to the process to ensure that security requirements are identified in early phases of the project, and security controls added to ensure those requirements are included in the design of the solution.

Applications should be inspected for security vulnerabilities through the development phase.

Application security testing should be conducted throughout the different phases of the software development and acquisition life cycle to verify that the security controls are working as expected and the software is free from significant vulnerabilities. Any residual risks stemming from control gaps or vulnerabilities that cannot be fully mitigated should be assessed and accepted as per the organizational risk framework. Security activities such as risk assessment, architecture analysis, threat modeling, source code review, vulnerability and penetration testing, and security configuration review should be embedded in the different phases of the software development effort.

Software developed by third parties should be carefully tested to verify that it is free from significant security vulnerabilities. Appropriate processes, procedures, and technologies should be in place to evaluate, assess, and test the security of externally developed software before it is commissioned into production.

Developers' access to the production environment should be appropriately controlled to prevent potential unauthorized changes to enterprise applications. Segregation of duties for deployment of code into production should be enforced through technical controls to ensure that changes are appropriately tested before they are promoted to production. Access to code repositories and to development and testing environments should be restricted to only authorized individuals, keeping the development and testing environments separate from the production environment. For specific security controls, refer to the "Software Security" section in appendix tableA.1 in appendix A of these guidelines.

Third-party management

ICT services can be outsourced, but accountability for managing their associated cybersecurity risks should remain with the organization. Organizations across all industries are leveraging outsourcing capabilities such as cloud computing to more efficiently run their business and better serve their customers. Cost savings, increased scalability, flexibility, and resiliency are among the benefits that make this technology appealing to different enterprises. However, the accountability for managing the risks arising from the relationship with third parties remains with the organization. Hence, maintaining a comprehensive understanding of key relationships and managing their associated cybersecurity risks are essential for the secure, reliable, and resilient delivery of services. In this regard, organizations should establish an appropriate set of controls to manage these risks and ensure that third parties are aware of the expectations.

Contractual agreements should incorporate security and data privacy requirements for third parties. Contracts with third parties should contain appropriate terms and conditions that comply with applicable legal and regulatory requirements and should include appropriate service-level requirements. Also, contractual agreements should ensure that the organization retains the ability to frequently review the service provider's security posture and adherence to international standards and its compliance with industry-recognized security certifications. Finally, appropriate arrangements should be established to ensure business continuity in the event of an unforeseen interruption of the outsourced services. For specific security controls, refer to the "Third-Party Management" section in appendix table A.1 in appendix A of these guidelines.

Security Operations

The components of the cybersecurity program described in this section are physical and environmental security; network security; end-point security; data protection; threat and vulnerability management; and event detection, logging, and monitoring.

Physical and environmental Security

Physical security is one of the basic layers of an in-depth approach to defense. Unauthorized access, potential damage to critical assets, or interference

with the operations should be prevented by physical and environmental controls commensurate with the risk to critical infrastructure and organizational objectives. Among other factors, security perimeters should be considered in the protection of areas that contain information and information processing facilities. Access to those secure areas should be protected by entry controls in order to ensure that only authorized personnel are allowed. Similarly, environmental protection should be in place against potential damage from different forms of natural or human-made disaster.

Vendor security certifications should be frequently reviewed when data center services are outsourced. The data center service provider should produce evidence of compliance with security certifications and standards relevant to the organization's environment.[6] A CRSP should establish procedures to frequently review these certifications and identify and manage any residual risks associated with the outsourcing of data center operations. For specific security controls, refer to the "Physical and Environmental Security" section in appendix table A.1 in appendix A of these guidelines.

Network security

The network perimeter of organizations is extending with blurred boundaries between work and home networks, personal and business-issued devices, and on-premises and cloud infrastructure, but network security still needs to be managed. Appropriate procedures should be implemented to manage security at the network level, including access management; vulnerability management; incident identification and notification; device configuration and patch management; and network architecture, including wireless networks.

Among other factors, network segmentation should be considered for enhanced security. Organizations should consider segmenting networks in multiple but separate trust and security zones with defense-in-depth strategies (for example, logical network segmentation, hard backups, or air gapping) to mitigate the effect of potential cyber attacks, leveraging protective and detective technologies (that is, firewalls, intrusion detection systems, or intrusion prevention systems).

The corporate network should be protected against attacks from the internet that may affect service availability. Data breach investigation reports indicate that entities in the financial industry have increasingly been targeted in DDoS attacks. The purpose of these attacks is to disrupt the organization's processes by overwhelming their systems and telecommunications networks with massive amounts of data requests. Sometimes, the purpose of these attacks is to distract the attention of the incident response team while other more sophisticated attacks are conducted against the organization. In any case, organizations should ensure that appropriate DDoS mitigation measures are in place commensurate to the organization's tolerance to availability loss. For specific security controls, refer to the "Network Security" section in appendix table A.1 in appendix A of these guidelines.

End-point security

An increase in teleworking and bring-your-own-device (BYOD) practices are good examples of why organizations need to protect end points. Appropriate protection mechanisms and controls should be implemented and maintained at the end points (that is, workstations, servers, network components, and mobile devices). Mechanisms include but are not limited to antivirus protection, full disk encryption, malware protection, hardware access control, and patch management and should be commensurate with the risk to critical infrastructure and organizational objectives.

[6] See, for example, ISO (International Organization for Standardization) 27001, PCI DSS (Payment Card Industry Data Security Standard), and SOC (Service Organization Control) Reports.

Organizations need to develop, document, and maintain under configuration control a current baseline configuration of the end points. Baseline configurations should be documented, formally reviewed, and agreed upon for the end points. Automated mechanisms should be used to maintain an up-to-date, accurate, and readily available baseline configuration of the end points. For specific security controls, refer to the "End-Point Security" section in appendix tableA.1 in appendix A of these guidelines.

Data protection

A data breach can be a costly event. It can lead to direct financial losses, such as lost sales or fines, but loss or theft of essential financial information can also severely damage the organization's reputation and lead to loss of customers' trust and to a significant reduction in productivity. Data governance processes should be established together with appropriate mechanisms to prevent the compromise of sensitive data. These mechanisms include but are not limited to data loss prevention tools and cryptographic controls.

A data classification policy is a key aspect of data protection. The data classification policy and procedures should specify the criteria for classifying the data (for example, public, confidential, and strictly confidential) and provide guidance on required security controls for each type of data (for example, encryption at rest and in transit and data loss prevention). The data classification policy should also establish roles and responsibilities for protecting the data (for example, data owner and data custodian). Similarly, organizations should consider appointing a Data Protection Officer, who is responsible for providing guidance to internal and external users and service providers on their responsibilities and the established procedures related to data protection.

Encryption is a popular and effective data protection control, especially when sensitive data are stored outside the organization such as in a cloud service provider. Formal policies and procedures should be in place addressing the need to use cryptographic controls to protect sensitive data where they are stored and when they are in transit. Requirements for managing and protecting the encryption keys should also be addressed.

Critical data must be appropriately protected when they leave the production environment. Organizations should consider preventing the use of production data in development and testing environments unless appropriate controls (for example, data masking) are applied to protect data confidentiality. Policies and procedures should be established to restrict the use of removable media and to apply appropriate controls to prevent the loss or leakage of critical information. Finally, physical assets should be formally managed throughout removal, transfers, and disposition to prevent the loss or leakage of critical information stored in those assets, and data should be destroyed according to the established data disposition policy. For specific security controls, refer to the "Data Protection" section in appendix table A.1 in appendix A of these guidelines.

Threat and vulnerability management

The evolving cybersecurity threat landscape demands near-real-time knowledge of emerging threats and the way they could affect the operations of the organization. Threat and vulnerability management is a critical component of a cybersecurity program and addresses the activities related to learning and understanding new cyber threats and detecting and managing existing vulnerabilities to prevent cyber attacks. Following leading practices, organizations should establish and maintain processes, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities.

Up-to-date threat and vulnerability information should be obtained from reputable sources and necessary actions taken on the basis of criticality. Organizations should subscribe to and constantly monitor industry channels that provide updated information about threats and vulnerabilities,

recommended patches, and remediation actions to be taken. Threats should be analyzed and prioritized while considering the characteristics of the threat such as likely intent, capability, and applicability to the organization's technological environment. Vulnerabilities detected through automatic scans, penetration tests, cybersecurity exercises, and audits should be analyzed and prioritized on the basis of the potential effect of the vulnerability on the exposed asset and the criticality of the asset.

Many cybersecurity attacks could be prevented by following basic cybersecurity hygiene. Among other cybersecurity hygiene practices such as following documented security standards, securing administrative accounts, or implementing firewalls or antivirus solutions, organizations should deploy in a timely fashion relevant security patches to address known critical vulnerabilities. A process should be in place to obtain, test, and automatically deploy security patches and updates in a timely manner based on criticality. For example, a patch was available in March 2017 to address the vulnerability later exploited by the WannaCry ransomware attack in May 2017. This attack, which affected several hundred thousand machines worldwide, could have been prevented in most organizations by simply applying the patch in a timely fashion as part of a basic cybersecurity hygiene routine. In addition, organizations should also consider and mitigate any risks arising from the use of unsupported software for which security patches are no longer available.

For specific security controls, refer to the "Threat and Vulnerability Management" section in appendix table A.1 in appendix A of these guidelines.

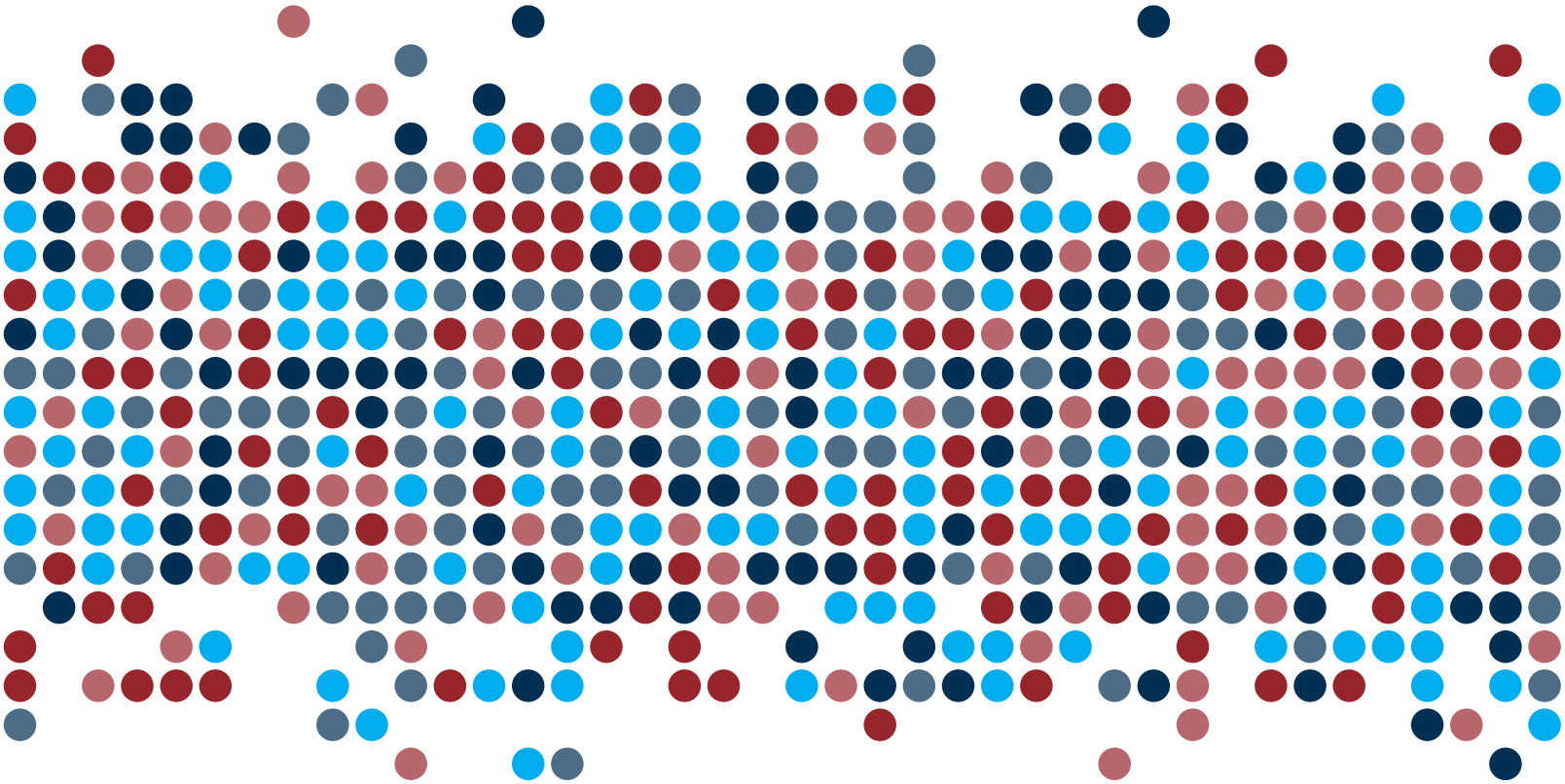
Event detection, logging, and monitoring

Anomalous activity should be detected promptly and its potential outcome understood for an effective response. To be able to effectively respond to potential cybersecurity events, organizations should develop and maintain a near-real-time knowledge of the dynamic environment in which they operate. Awareness of current relevant cybersecurity events external to the organization should be complemented by the appropriate detection, logging, and monitoring of events internal to the organization. For this purpose, processes, procedures, and technologies should be implemented and maintained to collect, protect, and analyze audit logs that record user and administrator activities, exceptions, information security events, and so on.

Event logs from different sources should be normalized, aggregated, and correlated to facilitate the analysis of suspicious activities. Ideally, logs from applications, infrastructure, and network components (for example, firewalls, IDS/IPS) should be sent to a centralized Security Information and Event Management (SIEM) system, where they can be aggregated and correlated for a better analysis of those suspicious activities. Access to the SIEM system should be appropriately restricted to ensure that logs are not tampered with or destroyed.

Automated analysis of security events should be conducted to identify potential cybersecurity attacks. Normal behavior and thresholds should be defined so that alerts can be triggered when suspicious activities are detected. For example, an attempt to connect to a server in headquarters by a user who works in a remote branch may be considered anomalous activity, and an alert will be triggered. The automated analysis of security events should be supplemented by expert analysis on such events to identify potential cyber attacks.

Roles and responsibilities for monitoring events should be clearly established. Organizations should establish clear roles and responsibilities for the personnel responsible for the monitoring of events, together with a framework for the timely analysis, categorization, and response to the alerts. Detection processes and technologies should be frequently tested and processes improved on the basis of testing results. For specific security controls, refer to the "Event Detection, Logging and Monitoring" section in appendix table A.1 in appendix A of these guidelines.



5. POLICY CONSIDERATIONS

In addition to the guidance to credit reporting service providers outlined in section 4 of this report, the survey indicated certain regulatory gaps that require policy intervention. This section outlines a set of policy considerations that policy makers and regulatory authorities should consider for enhancing cybersecurity within their jurisdictions.

The recommendations are designed to enhance regulatory oversight and ensure a systematic approach to cybersecurity across markets. The recommendations are also aimed at promoting industry-wide mechanisms that support specific practices of CRSPs, as a way of mitigating systemwide cybersecurity incidents.

Enhancement of the Cyber Legal and Regulatory Environment

Policy makers should consider implementing and/or enhancing cyber laws and regulations that provide incentives for better protection of data and systems. Specifically, they should consider implementing cyber laws and regulations, in instances where such legislation is nonexistent, or enhancing existing frameworks. The frameworks should provide the following:

- Mechanisms providing regulatory authorities with oversight to ensure that key public and private infrastructures, including financial infrastructure services providers, meet essential security standards
- Enforcement mechanisms, including penalties and breach compensation for data leaks
- Cybersecurity information sharing
- Notification and reporting practices

Development of Cybersecurity Strategy and Framework

Regulatory authorities should consider developing national and/or sectorwide cybersecurity strategies and frameworks (European Central Bank 2016). Although the focus of cybersecurity in some countries has been on CRSPs, countries should also consider developing national or sectoral cybersecurity strategies and frameworks that are informed by the cybersecurity threat and vulnerability landscape. The sectorwide cybersecurity strategies and frameworks should also outline interagency cooperation among their various state actors responsible for the credit reporting ecosystem.

Enhancement of Cyber Governance

To the extent possible, regulatory bodies should consider implementing practices or standards that promote the strengthening of cyber governance by CRSPs. In jurisdictions where CRSPs are subject to registration or licensing requirements, regulators should consider ensuring that CRSP cybersecurity reporting structures are commensurate with their size and complexities and promote independence of the ICT assets administration and ICT security. Authorities should consider evaluating the need for a Chief Information Security Officers or their variant as one of the key principal officers and functions within CRSPs, including providing this position with direct access to the board of directors.

Cyber Training for Members of a Board of Directors

Where applicable, regulatory bodies should ensure that CRSPs have in place detailed programs for training their boards of directors or other supervisory bodies. The survival and prosperity of companies are now more than ever tied to the robustness and resilience of the ICT assets, highlighting the importance of placing cybersecurity issues firmly within the remit of the board. As such, CRSPs should ensure that their annual training programs incorporate cyber training for staff members and, importantly, the board of directors (box 5.1). Regulatory authorities should work with CRSPs to ensure that boards of directors or other supervisory bodies are adequately trained.

Cyber Breach Disclosure Frameworks

Regulatory authorities should issue guidance on the level and extent of disclosures in times of breaches (see box 5.2). The framework should consider timeliness, details of breaches, and stakeholders that should be notified of the breach. Regulatory authorities should work with CRSPs to ensure that CRSPs develop and implement breach communication frameworks that clearly explain the communication strategy, sample statements for the media (print, electronic, and social media), and breach communication governance.

Outsourcing of Key ICT Services

Regulatory authorities should work with CRSPs to ensure they implement sound outsourcing procedures that detail the controls and processes to be followed when evaluating and managing relationships with third parties. The procedures should also outline the mechanisms for ensuring that the security of outsourced services remains visible to the CRSP and detail how to manage fourth parties. Entities should also ensure that their risk management frameworks incorporate risks inherent in outsourcing.

Regulatory authorities should also consider ensuring that third parties that provide services to CRSPs operate under risk management practices similar to those expected of the CRSPs themselves. In most cases, the third-party vendors are not under regulatory purview and do not need to comply with any regulatory requirements. This circumstance might affect their investments to upgrade their security. As a result, vendors dealing with critical infrastructure institutions should be subject to rigorous standards where applicable (for example, the European Union's GDPR), and the right to audit should be incorporated in the contracts with third parties.

Box 5.1: Training Members of Boards of Directors on Cybersecurity

UK National Cyber Security Centre (NCSC) Cyber Security Toolkit for Boards

The toolkit (National Cyber Security Centre 2019) is designed to make board members conversant in cyber-security and equips them with the knowledge to know and understand the proper questions to ask. The toolkit covers general cybersecurity, risk management measures, information security, cyber resilience, response to cyber incidents, collaborations, and partners. The toolkit assesses each of the sections on three levels: the specific actions, the oversight role, and the best practice that the board can consider as benchmarking the organization's performance.

Box 5.2: Case of a Breach Reporting Framework

Office of The Privacy Commissioner of Canada Guidance Framework

The Office of The Privacy Commissioner of Canada (OPC) issued a guidance framework on the obligations of institutions with respect to the mandatory reporting of breaches of security safeguards following the enactment of the Personal Information Protection and Electronic Documents Act (PIPEDA) in November 2018. The framework covers the following:

- Part 1: Your obligations for reporting breaches
- Part 2: Submitting a breach report to the OPC
- Part 3: You need to keep records of all breaches
- Part 4: When and how to notify individuals
- Part 5: Notification to organizations
- Part 6: Assessing real risk of significant harm
- PIPEDA breach report form

Periodic Cyber Risk Assessments

Supervisory authorities should consider conducting annual cybersecurity risk assessments of crucial infrastructure players. Authorities should consider conducting annual risk assessments to identify, estimate, and prioritize risk resulting from the operation and use of information systems. In cases of limitations, the assessments should target critical infrastructure such as credit reporting, payment, and settlement systems.

In carrying out this responsibility, where possible, the supervisory authorities should consider collaborative methods, such as including information sharing and joint assessments, to reduce regulatory burden on the CRSPs. This approach is relevant in cases where the supervisory functions are distributed across regulatory agencies.

Authorities should consider working with CRSPs to ensure the CRSPs conduct their own internal assessments on a periodic basis. CRSPs should conduct internal assessments or hire professionals to conduct assessments. The results of such assessments should be shared with regulatory bodies.

Periodic Cyber Audits

Regulatory authorities should consider working with CRSPs to ensure the CRSPs undertake regular audits of cybersecurity functions. The audit functions should develop audit plans that subject cyber assets and outsourced services to audits, in line with a risk-based approach to audits. Where possible, regulatory authorities should promote the use of external auditors to conduct reviews of cybersecurity functions of CRSPs.

Establishment of Cyber Information Sharing and Collaboration Mechanisms

Regulatory and/or industry bodies should consider developing mechanisms that foster and enforce cybersecurity information sharing and collaboration among parties. The mechanism should be public-private partnerships that encompass the critical

infrastructures and actors. Information sharing and collaboration frameworks should promote sharing of timely, actionable, and relevant unclassified information. The frameworks should consider the type of information to be shared, detail, frequency of meetings, and consequences of failure to share. CRSPs should share threats and vulnerability information, emerging risks, and ways of collectively dealing with cyber information. The framework should also include the penalties for failure or inadequate disclosures.

Regulatory bodies should also publish or promote publication of redacted reports on cybersecurity issues on a semiannual basis. The industry reports should promote disclosure of timely unclassified information and should be widely circulated within the CRSP countries.

Incident Response, Disaster Recovery, and Business Continuity

Regulatory authorities should work with CRSPs to ensure they actively participate and collaborate with national cybersecurity actors such as CERTs. CRSPs should actively participate with the teams in their country to contribute to research, enhancements of the system, and development of best practices and training in cybersecurity.

Regulatory authorities should work with CRSPs to ensure they develop comprehensive incident response plans that are subject to audit and simulation tests. The incident response plan should define the criteria for categorizing and prioritizing incidents and provide guidelines on the stages to be followed including the preparation, identification, containment, eradication, recovery, and lessons learned. The incident response plan should be formalized and reviewed, at least, annually.

Regulatory authorities should work with CRSPs to ensure the CRSPs conduct fully simulated cyber attack tests to assess the effectiveness of their incident response plan. The plan should be frequently tested against a variety of realistic scenarios involving relevant internal and external stakeholders. A typical test involves the following:

- Possible scenarios
- Simulation of the deployment of a known threat
- Execution of the associated incident response plan
- Documentation of the results

Scenarios such as malware infections, extended power outages, or distributed denial-of-service attacks should be tested through tabletop and functional exercises to evaluate the effectiveness of the plans and the readiness of the personnel to respond to an incident. Lessons learned from tests and forensic analysis conducted on real events should be incorporated into the plans to improve the organization's ability to effectively and timely respond to cyber events.

Regulatory authorities should work with CRSPs to ensure the CRSPs establish a dedicated Computer Security Incident Response Team (CSIRT). Establishing a dedicated CSIRT will boost the organization's capabilities to timely respond to cyber incidents. Clear roles and responsibilities should be established for carrying out response activities that enable a rapid response in case of cybersecurity events.

6. REFERENCES

Almansi, A. 2018. Financial Sector's Cybersecurity: Regulations and Supervision. Washington, DC: World Bank.

Bouveret, A. 2018. "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment." Working Paper WP/18/143, International Monetary Fund, Washington, DC.

CrowdStrike. 2019. "2019 Global Threat Report: Adversary Tradecraft and Importance of Speed." https://crowdstrike.lookbookhq.com/web-global-threat-report-2019/crowdstrike-2019-gtr.

European Central Bank. 2016. "G7 Fundamental Elements of Cybersecurity for the Financial Sector." October. https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf.

EYGM. 2014. "Achieving Resilience in the Cyber Ecosystem." EYGM. http://www.ey.com/Publication/vwLUAssets/cyber_ecosystem/$FILE/EY-Insights_on_GRC_Cyber_ecosystem.pdf.

IBM. 2017. "Security Trends in the Financial Services Sector." IBM X-Force Research. https://media.scmagazine.com/documents/296/2017_ibm_x-force-_security_tre_73846.pdf

IOSCO (International Organization of Securities Commissions). 2016. *Cyber Security in Securities Markets: An International Perspective. Madrid: IOSCO.*

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission). 2013. "ISO/IEC 27001:2013, Information Technology—Security Techniques—Information Security Management systems—Requirements." https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

Kaspersky Lab. 2019. "Cyberthreats to Financial Institutions 2019: Overview and Predictions." Kaspersky Lab, Moscow. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/11/27083106/Financial-cyber-threat-predictions-for-2019.pdf.

National Cyber Security Centre. 2019. Cyber Security Toolkit for Boards. National Cyber Security Centre, London.

Newman, L. H. 2017. "Equifax Officially Has No Excuse." Wired, September 14. https://www.wired.com/story/equifax-breach-no-excuse/.

Niemantsverdriet, J. 2018. "Cybersecurity in 2018 and 2019: Looking Back and Moving Forward." Deloitte, December 14. https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-in-2018-and-2019-looking-back-and-moving-forward.html.

NIST (National Institute of Standards and Technology). 2013. "Security and Privacy Controls for Federal Information Systems and Organizations." Special Publication 800-53, Revision 4, NIST, Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

———. 2018. Cybersecurity Framework. April, NIST, Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

NNT (New Net Technologies). 2017. "Equifax Profits Drop 27 Percent Following Data Breach." November 13. https://www.newnettechnologies.com/equifax-profits-drop-27-percent-following-data-breach.html.

OECD (Organisation for Economic Co-operation and Development). 2017. "Types of Cyber Incidents and Losses." In *Enhancing the Role of Insurance in Cyber Risk Management. Paris: OECD Publishing, 19–56.*

Pettersson, E. 2017. "Legal Experts See Room for Deal in Equifax Data Breach Lawsuits." Insurance Journal, September 25. http://www.insurancejournal.com/news/national/2017/09/25/465299.htm.

Reuters. 2017. "Lawsuits against Equifax Pile Up After Massive Data Breach," Reuters, September 11. http://www.reuters.com/article/us-equifax-cyber-lawsuits/lawsuits-againstequifax-pile-up-after-massive-data-breach-idUSKCN1BM2E3.

Velasquez, J. 2017. "NY Proposes Regulating Credit Reporting Agencies." Law.com, September 18. https://www.law.com/newyorklawjournal/sites/newyorklawjournal/2017/09/18/ny-proposes-regulating-credit-reporting-agencies/?slreturn=20180417120511.

World Bank. 2011. *General Principles for Credit Reporting. Washington, DC: World Bank.*

———. 2019. "Disruptive Technologies in the Credit Information Sharing Industry: Developments and Implications." Fintech Note 3, World Bank, Washington, DC.

7. APPENDICES

APPENDIX A: Focus Areas

Appendix table A.1 provides the mapping of the different focus areas discussed in these guidelines to industry-recognized security standards and frameworks that illustrate a method to achieve the outcomes associated with each focus area. These references are illustrative and not exhaustive.

Table A.1: Guideline Focus Areas

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
Strategy	ID.BE-1: The organization's role in the supply chain is identified and communicated.	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2	CP-2, SA-12
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated.	Clause 4.1	PM-8
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.		PM-11, SA-14
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.	A.11.2.2, A.11.2.3, A.12.1.3	CP-8, PE-9, PE-11, PM-8, SA-14
	ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)	A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1	CP-2, CP-11, SA-13, SA-14

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
Governance	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	A.6.1.1	CP-2, PS-7, PM-11
	ID.GV-1: Organizational information security policy is established and communicated.	A.5.1.1	Controls from all security control families
	ID.GV-2: Information security roles and responsibilities are coordinated and aligned with internal roles and external partners.	A.6.1.1, A.7.2.1, A.15.1.1	PM-1, PM-2, PS-7
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.		Controls from all security control families
	ID.GV-4: Governance and risk management processes address cybersecurity risks.		SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	PR.AT-4: Senior executives understand their roles and responsibilities.	A.6.1.1, A.7.2.2	AT-3, IR-2, PM-13
Risk Management	ID.GV-4: Governance and risk management processes address cybersecurity risks.	SA-2, PM-3, PM-7, PM-9, PM-10, PM-11	
	ID.RA-1: Asset vulnerabilities are identified and documented.	A.12.6.1, A.18.2.3	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.	A.6.1.4	SI-5, PM-15, PM-16
	ID.RA-3: Threats, both internal and external, are identified and documented.	Clause 6.1.2	RA-3, SI-5, PM-12, PM-16
	ID.RA-4: Potential business impacts and likelihoods are identified.	A.16.1.6, Clause 6.1.2	RA-2, RA-3, PM-9, PM-11, SA-14

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
Risk Management	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	A.12.6.1	RA-2, RA-3, PM-16
	ID.RA-6: Risk responses are identified and prioritized.	Clause 6.1.3	PM-4, PM-9
	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.	Clause 6.1.3, Clause 8.3, Clause 9.3	PM-9
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed.	Clause 6.1.3, Clause 8.3	PM-9
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.	Clause 6.1.3, Clause 8.3	PM-8, PM-9, PM-11, SA-14
Compliance	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5	Controls from all security control families
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	A.15.2.1, A.15.2.2	AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
	DE.DP-2: Detection activities comply with all applicable requirements,	A.18.1.4, A.18.2.2, A.18.2.3	AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
Data Privacy	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed,	A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5	Controls from all security control families
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4	AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
Awareness and Education	PR.AT-1: All users are informed and trained.	A.7.2.2, A.12.2.1	AT-2, PM-13
	PR.AT-2: Privileged users understand roles and responsibilities.	A.6.1.1, A.7.2.2	AT-3, PM-13
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities.	A.6.1.1, A.7.2.1, A.7.2.2	PS-7, SA-9, SA-16
	PR.AT-4: Senior executives understand roles and responsibilities.	A.6.1.1, A.7.2.2	AT-3, IR-2, PM-13
	PR.AT-5: Physical and information security personnel understand roles and responsibilities.	A.6.1.1, A.7.2.2	AT-3, PM-13
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4	PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
Information Sharing and Communications	PR.IP-8: Effectiveness of protection technologies is shared.	A.16.1.6	AC-21, CA-7, SI-4
	RS.CO-3: Information is shared consistent with response plans.	A.16.1.2, Clause 7.4, Clause 16.1.2	CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	Clause 7.4	CP-2, IR-4, IR-8
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	A.6.1.4	PM-15, SI-5
Resilience	PR.IP-4: Backups of information are conducted, maintained, and tested.	A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3	CP-4, CP-6, CP-9
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3	CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
	PR.IP-10: Response and recovery plans are tested.	A.17.1.3	CP-4, IR-3, PM-14
	RS.RP-1: Response plan is executed during or after an event.	A.16.1.1, A.16.1.4	AU-6, CA-7, IR-4, SI-4

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
Resilience	RS.CO-1: Personnel know their roles and order of operations when a response is needed.	A.6.1.1, A.7.2.2, A.16.1.1	CP-2, CP-10, IR-4, IR-8
	RS.CO-2: Events are reported consistent with established criteria.	A.6.1.3, A.16.1.2	AU-6, IR-6, IR-8
	RS.CO-3: Information is shared consistent with response plans.	A.16.1.2, Clause 7.4, Clause 16.1.2	CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	Clause 7.4	CP-2, IR-4, IR-8
	RS.AN-2: The impact of the incident is understood.	A.16.1.4, A.16.1.6	CP-2, IR-4
	RS.AN-3: Forensics are performed.	A.16.1.7	AU-7, IR-4
	RS.AN-4: Incidents are categorized consistent with response plans.	A.16.1.4	CP-2, IR-4, IR-5, IR-8
	RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).		SI-5, PM-15
	RS.MI-1: Incidents are contained.	A.16.1.5, A.12.2.1, A.16.1.5	IR-4
	RS.MI-2: Incidents are mitigated.	A.12.2.1, A.16.1.5	IR-4
	RS.IM-1: Response plans incorporate lessons learned.	A.16.1.6, Clause 10	CP-2, IR-4, IR-8
	RS.IM-2: Response strategies are updated.	A.16.1.6, Clause 10	CP-2, IR-4, IR-8
	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident.	A.16.1.6, Clause 10	CP-10, IR-4, IR-8
	RC.IM-1: Recovery plans incorporate lessons learned.	A.16.1.6, Clause 10	CP-2, IR-4, IR-8
	RC.IM-2: Recovery strategies are updated.	A.16.1.6, Clause 10	CP-2, IR-4, IR-8
	RC.CO-1: Public relations are managed.	A.6.1.4, Clause 7.4	

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
Resiliency	RC.CO-2: Reputation after an event is repaired.	Clause 7.4	
	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams.	Clause 7.4	CP-2, IR-4
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.	A.17.1.3	CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
Identity and Access Management	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
	PR.AC-2: Physical access to assets is managed and protected.	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8	PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
	PR.AC-3: Remote access is managed.	A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1	AC-1, AC-17, AC-19, AC-20, SC-15
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	A.7.1.1, A.9.2.1	AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4	AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	A.9.1.2	AC-3, CM-7

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried.	A.8.1.1, A.8.1.2	CM-8, PM-5
	ID.AM-2: Software platforms and applications within the organization are inventoried.	A.8.1.1, A.8.1.2, A.12.5.1	CM-8, PM-5
	ID.AM-3: Organizational communication and data flows are mapped.	A.13.2.1, A.13.2.2	AC-4, CA-3, CA-9, PL-8
	ID.AM-4: External information systems are catalogued.	A.11.2.6	AC-20, SA-9
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.	A.8.2.1	CP-2, RA-2, SA-14, SC-6
Change and Configuration Management	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).	A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
	PR.IP-2: A System Development Life Cycle to manage systems is implemented.	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5	PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
	PR.IP-3: Configuration change control processes are in place.	A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	CM-3, CM-4, SA-10
	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.	A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6	MA-2, MA-3, MA-5, MA-6
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	A.11.2.4, A.15.1.1, A.15.2.1	MA-4

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
Software Security	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	A.12.1.4	SC-16, SI-7
	PR.DS-7: The development and testing environment(s) are separate from the production environment.	A.12.1.4	CM-2
	PR.IP-2: A System Development Life Cycle to manage systems is implemented.	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5	PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
Third-Party Management	ID.AM-4: External information systems are catalogued.	A.11.2.6	AC-20, SA-9
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	A.6.1.1	CP-2, PS-7, PM-11
	ID.BE-1: The organization's role in the supply chain is identified and communicated.	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2	CP-2, SA-12
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established.	A.11.2.2, A.11.2.3, A.12.1.3	CP-8, PE-9, PE-11, PM-8, SA-14
	ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).	A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1	CP-2, CP-11, SA-13, SA-14
	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholder.	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2	SA-9, SA-12, PM-9
	ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	A.15.2.1, A.15.2.2	RA-2, RA-3, SA-12, SA-14, SA-15, PM-9

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
Third-Party Management	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	A.15.1.1, A.15.1.2, A.15.1.3	SA-9, SA-11, SA-12, PM-9
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	A.15.2.1, A.15.2.2	AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.	A.17.1.3	CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	A.14.2.7, A.15.2.1	CA-7, PS-7, SA-4, SA-9, SI-4
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	Clause 7.4	CP-2, IR-4, IR-8
	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams.	Clause 7.4	CP-2, IR-4
Physical and Environmental Security	ID.AM-1: Physical devices and systems within the organization are inventoried.	A.8.1.1, A.8.1.2	CM-8, PM-5
	PR.AC-2: Physical access to assets is managed and protected.	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8	PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
	PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities.	A.6.1.1, A.7.2.2	AT-3, IR-2, PM-13
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3	PE-10, PE-12, PE-13, PE-14, PE-15, PE-18

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
Physical and Environmental Security	PR.IP-7: Protection processes are improved.	A.16.1.6, Clause 9, Clause 10	CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	A.11.1.1, A.11.1.2	CA-7, PE-3, PE-6, PE-20
Network Security	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	AC-4, AC-10, SC-7
	PR.DS-4: Adequate capacity to ensure availability is maintained.	A.12.1.3, A.17.2.1	AU-4, CP-2, SC-5
	PR.PT-4: Communications and control networks are protected.	A.13.1.1, A.13.2.1, A.14.1.3	AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	A.17.1.2, A.17.2.1	CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2	AC-4, CA-3, CM-2, SI-4
	DE.CM-1: The network is monitored to detect potential cybersecurity events.		AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
	DE.CM-4: Malicious code is detected.	A.12.6.1	SI-3, SI-8
	DE.CM-8: Vulnerability scans are performed.	A.12.6.1	RA-5
	PR.IP-7: Protection processes are continuously improved.	A.16.1.6, Clause 9, Clause 10	CA-2, CA-7, CP-2, IR-8, PL-2, PM-6

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
End-Point Security	ID.AM-1: Physical devices and systems within the organization are inventoried.	A.8.1.1, A.8.1.2	CM-8, PM-5
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	A.8.2.1	CP-2, RA-2, SA-14, SC-6
	ID.RA-1: Asset vulnerabilities are identified and documented.	A.12.6.1, A.18.2.3	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7	CM-8, MP-6, PE-16
	PR.IP-3: Configuration change control processes are in place.	A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	CM-3, CM-4, SA-10
	DE.CM-4: Malicious code is detected.	A.12.2.1	SI-3, SI-8
	DE.CM-5: Unauthorized mobile code is detected.	A.12.5.1, A.12.6.2	SC-18, SI-4, SC-44
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	A.12.4.1, A.14.2.7, A.15.2.1	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
	DE.CM-8: Vulnerability scans are performed.		RA-5
Data Protection	PR.DS-1: Data-at-rest is protected.	A.8.2.3	MP-8, SC-12, SC-28
	PR.DS-2: Data-in-transit is protected.	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	SC-8, SC-11, SC-12
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7	CM-8, MP-6, PE-16

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
Data Protection	PR.DS-5: Protections against data leaks are implemented.	A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3	AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
	PR.IP-4: Backups of information are conducted, maintained, and tested.	A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3	CP-4, CP-6, CP-9
	PR.IP-6: Data [are] destroyed according to policy.	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7	MP-6
	PR.PT-2: Removable media is protected, and its use restricted according to policy.	A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9	MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
Threat and Vulnerability Management	ID.RA-1: Asset vulnerabilities are identified and documented.	A.12.6.1, A.18.2.3	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.	A.6.1.4	SI-5, PM-15, PM-16
	ID.RA-3: Threats, both internal and external, are identified and documented.	Clause 6.1.2	RA-3, SI-5, PM-12, PM-16
	ID.RA-4: Potential business impacts and likelihoods are identified.	A.16.1.6, Clause 6.1.2	RA-2, RA-3, SA-14, PM-9, PM-11
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	A.12.6.1	RA-2, RA-3, PM-16
	ID.RA-6: Risk responses are identified and prioritized.	Clause 6.1.3	PM-4, PM-9

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
Threat and Vulnerability Management	PR.IP-12: A vulnerability management plan is developed and implemented.	A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3	RA-3, RA-5, SI-2
	DE.CM-8: Vulnerability scans are performed.		RA-5
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	A.12.6.1	CA-7, RA-3, RA-5
Event Detection, Logging, and Monitoring	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	AU Family
	DE.AE-2: Detected events are analyzed to understand attack targets and methods.	A.12.4.1, A.16.1.1, A.16.1.4	AU-6, CA-7, IR-4, SI-4
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.	A.12.4.1, A.16.1.7	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
	DE.AE-4: Impact of events is determined.	A.16.1.4	CP-2, IR-4, RA-3, SI -4
	DE.AE-5: Incident alert thresholds are established.	A.16.1.4	IR-4, IR-5, IR-8
	DE.CM-1: The network is monitored to detect potential cybersecurity events.		AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	A.11.1.1, A.11.1.2	CA-7, PE-3, PE-6, PE-20
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	A.12.4.1, A.12.4.3	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
	DE.CM-4: Malicious code is detected.	A.12.2.1	SI-3, SI-8
	DE.CM-5: Unauthorized mobile code is detected.	A.12.5.1, A.12.6.2	SC-18, SI-4. SC-44
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	A.14.2.7, A.15.2.1	CA-7, PS-7, SA-4, SA-9, SI-4

Focus Area	NIST Cyber Security Framework	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
Event Detection, Logging, and Monitoring	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	A.12.4.1, A.14.2.7, A.15.2.1	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.	A.6.1.1, A.7.2.2	CA-2, CA-7, PM-14
	DE.DP-2: Detection activities comply with all applicable requirements.	A.18.1.4, A.18.2.2, A.18.2.3	AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
	DE.DP-3: Detection processes are tested.	A.14.2.8	CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
	DE.DP-4: Event detection information is communicated to appropriate parties.	A.16.1.2, A.16.1.3	AU-6, CA-2, CA-7, RA-5, SI-4
	DE.DP-5: Detection processes are continuously improved.	A.16.1.6	CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
	RS.AN-1: Notifications from detection systems are investigated.	A.12.4.1, A.12.4.3, A.16.1.5	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4

Sources: ISO/IEC 2013; NIST 2013, 2018.

APPENDIX B: Survey Questionnaire

International Committee on Credit Reporting

Cybersecurity Survey

Purpose of survey
This survey is being conducted by the ICCR to better understand the cybersecurity practices of credit reporting institutions and as an input to the guideline on cybersecurity in credit reporting that is being produced by the Committee. The purpose of this survey is to establish the status of oversight and strategy, resourcing, governance, information sharing, incident management, and training and awareness practices of credit reporting system providers. The survey also assesses the preventive controls, risk management and compliance, and audit practices.

Please note that all information supplied as part of the survey will be treated as strictly confidential and will only be made available for the purposes of the study to selected staff at the World Bank and to the independent consultant who has been engaged to analyze the results. Any information from the survey published in the study will be aggregated at a country level.

The survey should take less than 15 minutes to complete and we would ask that it is returned to (**lsalamina@ifc.org**) **by 02/21/19**. We would like to thank you in advance for taking the time to complete this survey. Your input is greatly appreciated.

Structure of the survey
This survey is divided in thirteen sections:

Thank you once again for your collaboration. If you have any questions, please contact lsalamina@ifc.org

i. Contact Information

Country:

Name of organization:

Your name:

Your e-mail:

ii. Local Cybersecurity Environment

1. Has your institution suffered a cybersecurity incident in the last two years?

☐ Yes | ☐ No If yes:

Please describe the incident (unauthorized network penetration, denial of service, ransomware, other).

_____

_____

_____

Has it been possible to identify the responsible, external or internal actors?

_____

_____

_____

2. Has any organization supplying data to, or getting data from, your institution suffered a cybersecurity incident in the last two years?

☐ Yes | ☐ No If yes:

please describe the incident (unauthorized network penetration, denial of service, ransomware, other).

_____

_____

_____

Has it been possible to identify the responsible, external or internal actors, and who carried out the attack?

_____

_____

_____

3. Has any prominent organization in your country, public or private, not in direct electronic contact with your institution suffered a cybersecurity incident in the last two years?

☐ Yes | ☐ No If yes:

Please describe the incident (unauthorized network penetration, denial of service, ransomware, other).

_____

_____

_____

Has it been possible to identify the responsible, external or internal actors, and who did it?

_____

_____

_____

iii. Local Legal and Regulatory Environment

4. Are there laws or regulations establishing minimum cybersecurity security or information security standards for credit reporting institutions in your country?

☐ Yes | ☐ No

5. If your answer to question 4 above is yes:

List the regulatory and supervisory agencies responsible:

_____

_____

_____

Is there a legal or regulatory obligation to report cyber-security or information security incidents to the supervisory agency?

☐ Yes | ☐ No

Is there a legal obligation to notify all parties affected by the loss of confidential data derived from a cyber-security incident?

☐ Yes | ☐ No

Is there a legal obligation to compensate the affected parties?

☐ Yes | ☐ No

Are there any penalties that are levied for the breach? If the answer is yes, please specify the levels (ranges) of penalty (financial and non-financial)?

☐ Yes | ☐ No Level of penalty_____

iv. Board, Management, and Cybersecurity and Information Security Strategies

6. Does your institution have a documented cybersecurity and/or information security strategy integrating technology, policies, procedures, and training?

☐ Yes | ☐ No

7. Does the board approve the cybersecurity and/or information security strategy?

☐ Yes | ☐ No

8. Does the board review the cybersecurity and or information security strategies whenever there is a change in the institution's information technology or when new threats appear?

☐ Yes | ☐ No

9. Do members of the board understand the key cybersecurity controls in place?

☐ Yes | ☐ No

10. Does the board include at least one director with a good understanding of information security in general and cybersecurity in particular?

☐ Yes | ☐ No

11. Does the board engage cybersecurity experts to assist in carrying out its oversight responsibilities?

☐ Yes | ☐ No

12. Do approved information security policies and procedures define key roles and responsibilities and have they been communicated to all relevant stakeholders?

☐ Yes | ☐ No

13. The most senior officer in charge of cybersecurity or information security is a:

☐ Chief Information Security Officer | ☐ Chief Information Officer | ☐ Other (please specify)

_____

14. Does the most senior officer in charge of cybersecurity or information security report to the chief executive officer, or to the board or to a board committee?

☐ Yes | ☐ No

15. Is the most senior officer in charge of cybersecurity or information security independent from areas using or administering the institution's information technology assets?

☐ Yes | ☐ No

16. Does management hold employees accountable for complying with information security policies?

☐ Yes | ☐ No

17. Does the institution's strategy include outsourcing critical information technology services (e.g., cloud services)?

☐ Yes | ☐ No

18. Does the institution's strategy include purchasing insurance against cyber incidents?

☐ Yes | ☐ No

19. If the answer to question 18 above is yes, is the institution insured?

☐ Yes | ☐ No

20. Does the institution's strategy include a process to notify authorities and other stakeholders of a breach of confidential data?

☐ Yes | ☐ No

v. Outsourcing Critical Information Technology Services

21. Does the institution currently outsource critical information technology services?

☐ Yes | ☐ No If the answer is yes,

Which services are currently outsourced by the institution?

_____

_____

_____

Do the cybersecurity policies of the institution detail the controls and processes to be followed when evaluating and maintaining relationships with these third parties?

☐ Yes | ☐ No

vi. Information Sharing

22. Does the board encourage the cybersecurity team to engage in information sharing arrangements with other institutions?

☐ Yes | ☐ No

23. Does the institution monitor cybersecurity incidents in the financial services industry and beyond by participating in industry programs (e.g., Financial Sector Information Sharing and Analysis Center [FS-ISAC])?

☐ Yes | ☐ No

24. Does the institution receive timely notifications of cyber incidents from service providers with whom the institution has material outsourcing arrangements?

☐ Yes | ☐ No

vii. Training and Awareness

25. Has the institution implemented an ongoing cyber awareness training program for all staff?

☐ Yes | ☐ No

26. Has the board undertaken any form of cybersecurity training in the last 12 months?

☐ Yes | ☐ No

27. Does management receive cybersecurity training relevant to their job responsibilities?

☐ Yes | ☐ No

28. Do employees with privileged account permissions receive additional cybersecurity training commensurate with their levels of responsibility?

☐ Yes | ☐ No

29. Does annual cyber-security or information security training include incident response, and current and emerging cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security)?

☐ Yes | ☐ No

viii. Resources

30. Has the institution a specific cybersecurity budget?

☐ Yes | ☐ No

31. Is there is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process?

☐ Yes | ☐ No

32. Given the risks that the institution faces, is the investment it makes on cyber defenses appropriate?

☐ Yes | ☐ No

ix. Risk Management and Compliance

33. Has the institution implemented a formal risk management framework that includes cyber risks?

☐ Yes | ☐ No

34. Does the risk management function assess that the risk management framework is commensurate with the organization's risk and complexity?

☐ Yes | ☐ No

35. Does the institution comply with data privacy and protection regulation?

☐ Yes | ☐ No

x. Audit

36. Does Internal Audit have sufficient resources and expertise to audit the cybersecurity or information security strategy implementation?

☐ Yes | ☐ No

37. Does an internal or external independent audit validate that the institution's threat information sharing is commensurate with the organization's risk and complexity?

☐ Yes | ☐ No

38. Does the internal or external independent audit validate that the institution's cybersecurity controls are commensurate with the organization's risk and complexity?

☐ Yes | ☐ No

39. Does an internal or external independent audit validate that the institution's third-party relationship management is commensurate with the organization's risk and complexity?

☐ Yes | ☐ No | ☐ N/A

40. Does an internal or external independent audit validate that the institution's incident response program and resilience are commensurate with the institution's risk and complexity?

☐ Yes | ☐ No

xi. Incident Response

41. Does the institution have documented procedures for monitoring, analyzing, and responding to cybersecurity incidents?

☐ Yes | ☐ No

42. Does the institution have a dedicated security incident team to respond to and mitigate suspected and/or known security incidents?

☐ Yes | ☐ No

43. Does the institution have a process to escalate breaches of limits and thresholds to Senior Management for significant or critical cybersecurity incidents?

☐ Yes | ☐ No

44. Does the institution have an internal communication plan to address cybersecurity incidents that includes communication protocols for key internal stakeholders (e.g., relevant business units, senior management, risk management, board of directors)?

☐ Yes | ☐ No

45. Does the institution have an external communication plan to address cybersecurity incidents that includes communication protocols and draft pre-scripted communications for key external stakeholders (i.e., customers, media, critical service providers, etc.)?

☐ Yes | ☐ No

46. Does the institution have a partnership relationship with a national Computer Emergency Response Team (CERT)?

☐ Yes | ☐ No | ☐ N/A

47. Does the institution conduct incident-response simulation exercises on a regular basis?

☐ Yes | ☐ No

xii. Data Loss Prevention (DLP)

48. Does the institution have a DLP program and Written Supervisory Procedures (WSP) to monitor and prevent data breaches that help to detect and mitigate insider (and other) threats?

☐ Yes | ☐ No

49. Does the institution require user verification prior to permitting the sending of outbound e-mails?

☐ Yes | ☐ No

50. Does the institution have established consistent structures and processes for capturing DLP events—such as outbound e-mails and attachments or file transfers containing sensitive information?

☐ Yes | ☐ No

51. Does the institution have established robust DLP rules to identify and block or encrypt the transfer of data, such as customer account numbers, Social Security numbers, etc.?

☐ Yes | ☐ No

52. Does the institution have established rules to control printing of sensitive data and documents?

☐ Yes | ☐ No

x.iii Preventive Controls

53. Is the institution's network segmented into multiple, separate trust zones?

☐ Yes | ☐ No

54. Is unauthorized network access (e.g., including wired, wireless, and remote access) automatically detected and blocked?

☐ Yes | ☐ No

55. Are there remote access policies and procedures (e.g., usage restrictions and configuration requirements) for accessing internal resources over a public network?

☐ Yes | ☐ No

56. Does the institution tightly control and manage the use of administrative privileges?

☐ Yes | ☐ No

57. Does the institution apply strong authentication mechanisms (e.g., two-factor authentication) to manage user identification and access?

☐ Yes | ☐ No

58. Does the institution maintain an inventory of information technology assets (e.g., hardware, software, data, and systems hosted externally)?

☐ Yes | ☐ No

59. Does the institution document, implement, and enforce security configuration standards to all hardware and software assets on the network?

☐ Yes | ☐ No

60. Is a change management process in place to request and approve changes to systems' configurations, hardware, software, applications, and security tools?

☐ Yes | ☐ No

61. Are there automated processes in place to detect and block unauthorized changes to software and hardware?

☐ Yes | ☐ No

62. Does the institution conduct regular hardware and software vulnerability scans and testing to identify security control gaps in client, server, and network infrastructure?

☐ Yes | ☐ No

63. Is the Data Center access restricted by physical controls?

☐ Yes | ☐ No

Thank you for completing the survey

WORLD BANK GROUP

ICCR
INTERNATIONAL COMMITTEE ON CREDIT REPORTING