FSB FINANCIAL STABILITY BOARD

Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence

19 October 2021

The Financial Stability Board (FSB) coordinates at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations.

Contact the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Copyright © 2021 Financial Stability Board. Please refer to the terms and conditions

Table of Contents

Executive summary

Cyber incidents remain a threat to the financial system and are rapidly growing in frequency and sophistication. In light of increasing financial stability concerns, especially given the digitalisation of financial services and increased use of third-party service providers, the Financial Stability Board (FSB) explored whether harmonisation in cyber incident reporting could be achieved.

The FSB found that fragmentation exists across sectors and jurisdictions in the scope of what should be reported for a cyber incident; methodologies to measure severity and impact of an incident; timeframes for reporting cyber incidents; and how cyber incident information is used. This subjects financial institutions that operate across borders or sectors to multiple reporting requirements for one cyber incident. At the same time, financial authorities receive heterogeneous information for a given incident, which could undermine a financial institution's response and recovery actions. This underscores a need to address constraints in information-sharing among financial authorities and financial institutions.

Recognising that information on cyber incidents is crucial for effective actions and promoting financial stability, the FSB identified three ways that it will take work forward to achieve greater convergence in cyber incident reporting:

- **Develop best practices**. Identify a minimum set of types of information authorities may require related to cyber incidents to fulfil a common objective (e.g. financial stability, risk assessment, risk monitoring) that authorities could consider when developing their cyber incident reporting regime. This set of information would also help authorities in determining reporting thresholds, timeframes for reporting and notification, while recognising that a one-size-fits-all approach may neither be appropriate nor possible.

- **Identify common types of information to be shared**. Identify key information items that should be shared across sectors and jurisdictions, and to understand any legal and operational impediments to sharing such information. This would facilitate more information-sharing and help authorities obtain a better understanding of impacts of a cyber incident across sectors and jurisdictions. As a multilateral solution to information-sharing problems would be challenging, it would be essential for FSB member jurisdictions to continue bilateral and regional efforts to reduce legal and operational barriers to information sharing.

- **Create common terminologies for cyber incident reporting**. Harmonised cyber incident reporting schemes necessitate a 'common language'. In particular, a common definition for 'cyber incident' is needed that avoids the reporting of incidents that are not significant for a financial institution or financial stability.

Greater harmonisation of regulatory reporting of cyber incidents would promote financial stability by: (i) building a common understanding, and the monitoring, of cyber incidents affecting financial institutions and the financial system, (ii) supporting effective supervision of cyber risks at financial institutions; and (iii) facilitating the coordination and sharing of information amongst authorities across sectors and jurisdictions.

The FSB will develop detailed timelines and modalities for taking this work forward by the end of 2021.

1. Introduction

Enhancing cyber resilience is a key element of the FSB work programme to promote financial stability. This work includes the identification of fragmentation in supervisory and regulatory approaches to cybersecurity and/or information technology risk,[1] creation of a Cyber Lexicon[2] and development of effective practices for cyber incident response and recovery, which highlighted fragmentation in cyber incident reporting.[3]

The objective of this report is to explore whether greater convergence in the reporting of cyber incidents[4] could be achieved, including how authorities define a cyber incident. To inform this work, the FSB took stock of regulatory reporting of cyber incidents by financial institutions to their financial authorities, had follow-up discussions with financial authorities and engaged with external stakeholders on their experiences with reporting cyber incidents to authorities. The work explored financial authorities' cyber incident reporting regimes with a view to identify areas where greater harmonisation could enhance the effectiveness of cyber incident information to support authorities' understanding of risks to the financial institution and system. Areas explored include: the types of information collected; criteria for reporting cyber incidents; how cyber incident information is used; and the mechanisms for sharing information related to cyber incidents with other financial authorities and institutions. More details on the stocktake can be found in the Annexes.

The following sections discuss areas where fragmentation exists in cyber incident reporting and how information-sharing related to cyber incidents could be improved (within the constraints of data confidentiality and national security restrictions), and hence, support greater convergence. The conclusion identifies three ways to achieve greater convergence.

2. Fragmentation in cyber incident reporting

There are many common elements in cyber incident reporting across jurisdictions and sectors. This includes the date and time of the incident; impact of the incident on customers, reputation and financials; date and how the incident was identified (e.g. by a customer, employee, third-party service provider) and cause of the incident. Notwithstanding these commonalities, there are significant differences in: how a cyber incident is defined; thresholds for reporting cyber incidents, definitions of materiality; how incident information is used; and the timeframe for reporting an incident. These differences are elaborated below, and result in fragmentation in the reporting of cyber incidents. In particular, financial institutions that operate across jurisdictions and sectors are subjected to multiple reporting requirements for one incident. At the same time,

---

1 The FSB stocktake of existing supervisory and regulatory practices identified 56 schemes of regulations and guidance targeted to cybersecurity and/or information technology (IT) risk, covering a variety of content elements. See FSB (2017), *Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices*, 17 October.

2 FSB (2018) *Cyber Lexicon*, 12 November.

3 FSB (2020), *Effective Practices for Cyber Incident Response and Recovery*, 20 October.

4 A cyber incident is a cyber event that:
(i) jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or
(ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.
See FSB (2018), *Cyber Lexicon*, page 9.

financial authorities receive heterogeneous information for a given cyber incident which impacts their assessment of the risk to the financial institution and financial system.

- **Scope of cyber incident reporting'**. The scope of 'cyber incidents' required to be reported by financial institutions to financial authorities varies across jurisdictions and sectors. For example, some authorities do not distinguish between broader operational incidents and cyber incidents or define a 'cyber incident' more broadly than others, often using it interchangeably with a 'cyber event', which is generally associated with 'any observable occurrence in an information system'. This may lead to excessive notification and reporting of incidents that can usually be managed by financial institutions.

- **Thresholds for reporting cyber incidents.** The thresholds for reporting cyber incidents vary across jurisdictions and sectors often due to a lack of established methodology to measure impact and severity, and can be very low. In some cases, for example, reporting thresholds are linked to the number or percentage of customers impacted, to market share or financial loss, or to qualitative indicators such as reputational risk. Recognising that cyber incidents impact financial institutions of different size and complexity differently, some authorities expect supervised institutions to define their own materiality thresholds, furthering differences in the materiality threshold across institutions.

- **Reporting timeframe**. The required timeframes for reporting cyber incidents vary across jurisdictions and sometimes within jurisdictions, ranging from 'as soon as identified' to 48 hours or longer, in addition to regular updates. While providing early notifications to authorities would facilitate timely supervisory response, it is similarly recognised that requiring financial institutions to provide a full report within a short timeframe diverts precious resources from containing and addressing the cyber incident in a timely manner. It could also result in providing incomplete information because of the time needed to collect and assess the scope of a cyber incident. Early reporting becomes more challenging if the incident involves third-party service providers.

- **Use of information reported**. Financial authorities use information from cyber incidents for different purposes depending on, for instance, the relevant mandates, and this may affect how they set their respective reporting requirements. For instance, more authorities use the reported information to monitor and assess vulnerabilities for a financial institution, rather than to assess how cyber incidents could pose risks to the financial system.

3. Information-sharing related to cyber incidents

Fragmentation in cyber incident reporting is often the result of differences in the relevant authorities' mandates, for example between prudential and other types of authorities. Moreover, many financial institutions are subject to supervision by multiple regulators. Enhanced information-sharing arrangements would help to reduce fragmentation in cyber incident reporting and promote a common understanding of the risk to the financial institution and financial system.

While many financial authorities have formal or informal information-sharing arrangements with one or more authority outside their jurisdiction,[5] there are substantial differences in the scope, depth and the form of such information-sharing across jurisdictions and sectors. This is often due to legal and confidentiality constraints as well as lack of clarity on the information that could be shared. Improvements in cooperation can be made through written cooperation arrangements between regulators, which cover timely notification and communication among authorities as well as cooperation in response and mitigation activities. Developing a better understanding of the possible systemic impacts of cyber incidents on financial institutions that operate in different jurisdictions would help authorities better understand what types of information is needed and more easily identify other authorities with whom the information should be shared.

Enhancing the consistency of the structure, content and timeliness of reports would also improve information-sharing and authorities' ability to respond to an incident, particularly when multiple authorities need to be engaged. This could include developing a standardised exchange format and methodology for cyber incident reporting or a shared protocol which facilitates cooperation (i.e. by specifying what kind of information should be shared, when information should be shared, who should share with whom, and how information should be shared). For instance, extending the use of common reporting platforms, such as by encouraging the financial industry to establish or join domestic (or regional) cyber information-sharing platforms, could help. These platforms could be cross-sectoral, with the participation from both the industry and authorities from respective sectors. Automation may also facilitate sharing of information.

4. Conclusions

Achieving greater convergence in cyber incident reporting is not straightforward. Jurisdictional differences will remain, such as reporting to national security and data protection agencies. Recognising that there are a number of impediments, including cross-sectoral considerations, that make convergence in cyber incident reporting regimes particularly challenging, due consideration should be taken in any approach that tries to address fragmentation in cyber incident reporting and avoid creating new fragmentation.

Further, confidentiality, privacy and other legal constraints, as well as other practices may constrain the ability for authorities to share information, even within the same jurisdiction. There also may be a lack of clarity on what and how information could be shared over a secure platform. Moreover, there is often not a strong incentive at an individual level to share information, even if it is in the collective interest of the relevant stakeholders.

Against this backdrop, the FSB has identified three ways to achieve greater convergence in cyber incident reporting, which would facilitate information-sharing across jurisdictions and sectors:

- **Develop best practices**. Identify a minimum set of types of information authorities may require related to cyber incidents to fulfil a common objective (e.g. financial stability, risk

[5] Authorities may also have information-sharing arrangements with cyber security or data privacy agencies within the same jurisdiction.

assessment, risk monitoring) that authorities could consider when developing their cyber incident reporting regime. This set of information would also help authorities in determining reporting thresholds, timeframes for reporting and notification, while recognising that a one-size-fits-all approach may neither be appropriate nor possible.

- **Identify common types of information to be shared**. Identify key information items that should be shared across sectors and jurisdictions, and to understand any legal and operational impediments to sharing such information. This would facilitate more information-sharing and help authorities obtain a better understanding of impacts of a cyber incident across sectors and jurisdictions. As a multilateral solution to information-sharing problems would be challenging, it would be essential for FSB member jurisdictions to continue bilateral and regional efforts to reduce legal and operational barriers to information sharing.

- **Create common terminologies for cyber incident reporting**. Harmonised cyber incident reporting schemes necessitate a 'common language'. In particular, a common definition for 'cyber incident' is needed that avoids the reporting of incidents that are not significant for a financial institution or financial stability.

The FSB will develop detailed timelines and modalities for taking this work forward by the end of 2021.

Annex 1: Stocktake of authorities' cyber incident reporting regimes

The FSB took stock of authorities' regulatory reporting of cyber incidents by financial institutions (e.g. banks, insurers, asset managers, FMIs). The FSB also had follow-up discussions with financial authorities and engaged with external stakeholders.

Over 80 responses were received from 23 out of 24 FSB member jurisdictions plus the European Union (EU), and 29 members of the six FSB Regional Consultative Groups (RCGs).[6] The stocktake focused on: (1) institutional scope of cyber incident reporting from financial institutions; (2) criteria for reporting and characteristics of reportable cyber incidents; (3) usage of reported information by financial authorities; (4) cooperation and coordination among authorities within and across jurisdictions; (5) challenges to implementing cyber incident reporting regimes; and (6) how authorities use the FSB Cyber Lexicon in their policy development and interactions with financial institutions.

1. Institutional scope of cyber incident reporting

Most authorities that responded to the stocktake require financial institutions under their oversight to report cyber incidents but make no distinction between cyber incidents and broader operational incidents for regulatory reporting purposes. As a result, cyber incidents are reported to the relevant financial authorities under the broader operational risk reporting framework as a subset of operational (or information technology/cybersecurity) incidents. Many authorities also issue guidelines or frequently asked questions (FAQs) to clarify the details of their cyber incident reporting requirements.

Many 'home' authorities require financial institutions in their jurisdiction to report cyber incidents at their subsidiaries, branches or other operations in foreign jurisdictions, but only a small number of authorities require such information to be reported to 'host' authorities.[7] Additionally, many 'home' authorities require cyber incidents at third-party service providers (including cloud-service providers) to financial institutions in their jurisdiction to be reported to them as 'home' authorities. Although only a few require such information to be reported to 'host' authorities, a number of authorities encourage financial institutions to share such information with 'host' authorities.

1.1 Types of cyber incident information to be reported

There are many common types of information reported about cyber incidents across jurisdictions and sectors (see Graph 1). This includes the date and time of the incident; impact of the incident on customers, reputation and financials; date and how the incident was identified (e.g. by a customer, employee, third-party service provider) and cause of the incident.

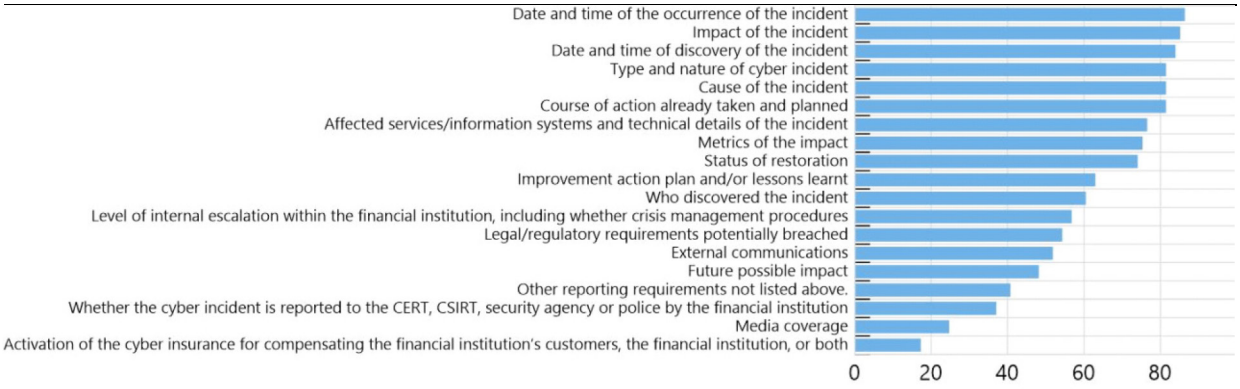
---

6 See Annex 2 for a list of the authorities that responded to the survey.

7 A few 'home' authorities set criteria for reporting significant cyber incidents at financial institutions' subsidiaries, branches or other legal entities in foreign jurisdictions. However, it is unclear whether the criteria apply to a 'significant' impact on the financial institution as a whole, on the 'home' authority's financial system, or the 'host' authority's financial system.

Types of required information to be reported about cyber incidents

Percent of survey respondents **Graph 1**



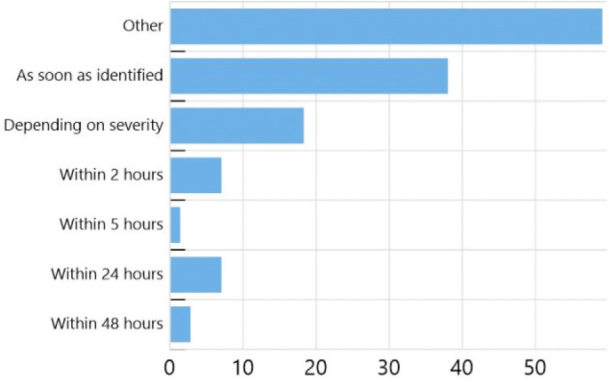
Source: FSB.

Notwithstanding these commonalities, there are significant differences in: how a cyber incident is defined; thresholds for reporting cyber incidents, definitions of materiality; how incident information is used; and the timeframe for reporting an incident. For instance, the timeframe for reporting a cyber incident and how incidents are communicated vary across sectors and jurisdictions (see Graph 2). Authorities often require specific timeframes for reporting an incident once identified which can vary widely, and may be in addition to periodic updates depending on the severity of the incident. The channels for communicating cyber incidents also vary across jurisdictions, with most financial institutions communicating via e-mail, encrypted email, or a secure platform.

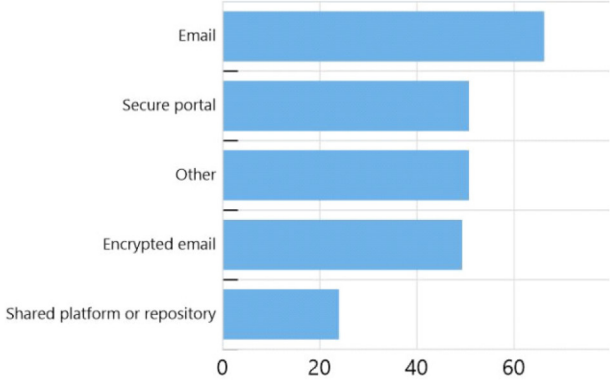
Fragmentation in reporting timeframes and communication channels

Percent of survey respondents **Graph 2**

Timeframe for financial institutions to report a cyber incident once identified



Communication channels used by financial institutions to report a cyber incident



Source: FSB.

However, most authorities prefer that more than one communication channel be used to report a cyber incident, such as telephone, meetings and written report. Only some authorities require financial institutions to authorise particular personnel to report an incident, such as the Chief Information Security Officer (CISO) or Chief Information/Technology Officer (CIO/CTO). Some authorities also set different protocols and/or templates for cyber incident reporting based on

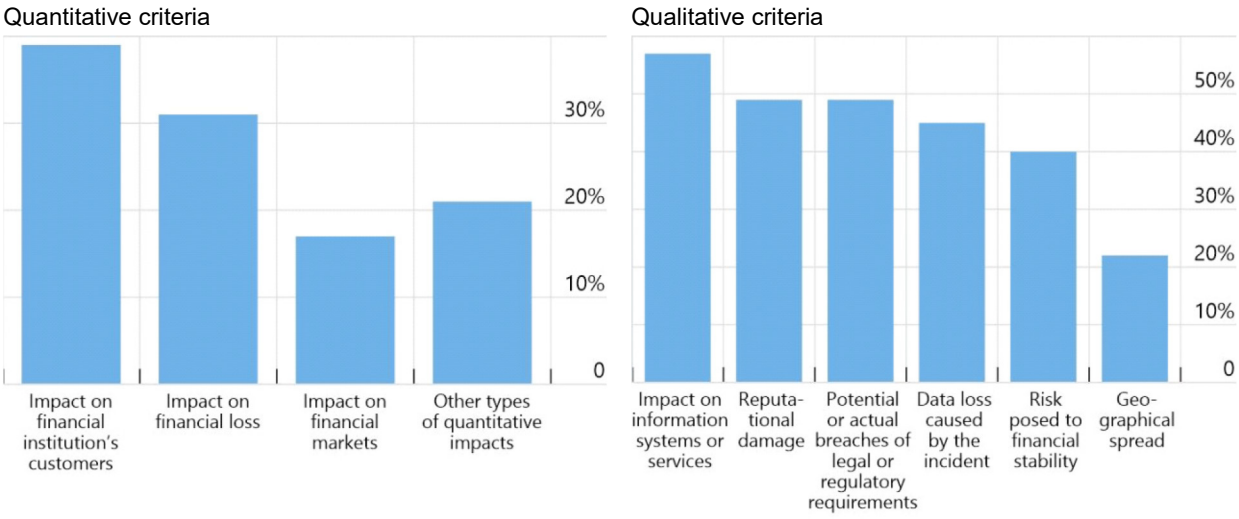
certain features of financial institutions. Such features include: industry and sectors; type of license financial institutions hold or activities financial institutions are involved in; and size or systemic importance of a financial institution.

2. Criteria for reporting and characteristics of reportable cyber incidents

Most authorities set quantitative and qualitative thresholds for reporting cyber incidents (Graph 3), but do not have an established methodology for determining the impact and severity of a cyber incident. This may be due to the inherent difficulty in determining the impact of cyber incidents, which can change over the lifetime of the incident as well as financial institutions having discretion in defining the cyber incidents to be reported but under guidance from the relevant authorities. Of those authorities that have an established methodology, many include quantitative thresholds to measure the impact and severity of a cyber incident based on 'impact on the financial institution's customers' and 'impact and severity of financial loss', although detailed definitions differ. Most authorities allow financial institutions to submit voluntary notification reports on the impact and severity of an incident.

Criteria for reporting cyber incidents

Percent of survey respondents **Graph 3**

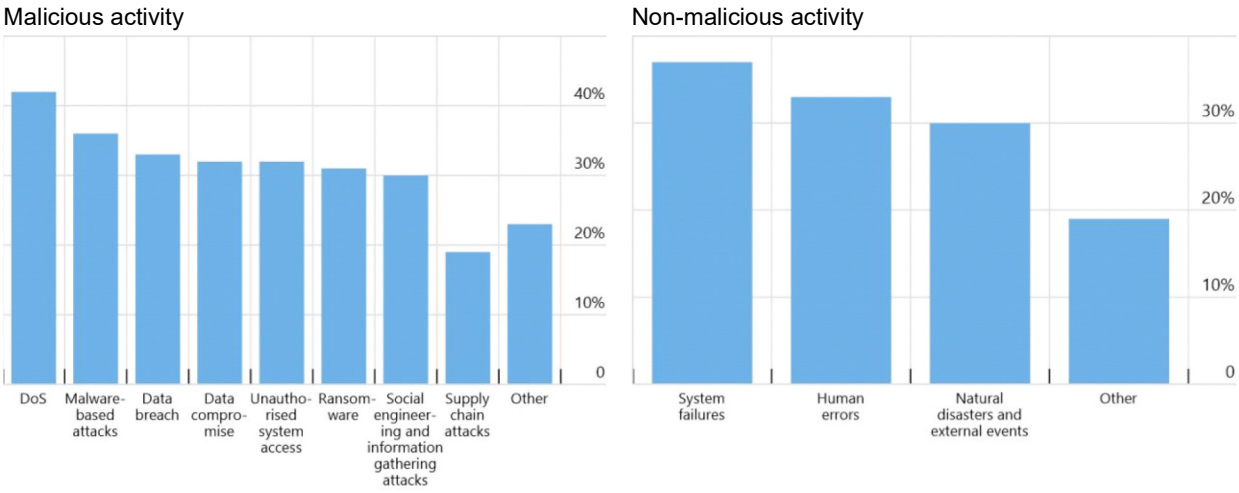


Source: FSB.

Many authorities have developed a taxonomy to designate a cyber incident, and a majority use a hybrid of a self-derived lexicon and a market or industry standard that is prevalent in their own jurisdiction. Most taxonomies distinguish cyber incidents from other types of operational incidents, and between cyber incidents that originated at a financial institution or at a third-party service provider. The scope of the taxonomy largely applies to confirmed cyber incidents and most taxonomies include categories for malicious and non-malicious activities (Graph 4).

Scope of a cyber incident

Percent of survey respondents **Graph 4**



Notes: DoS = Denial-of-Service; System failures = e.g. hardware failure, network failure, database issues, software/application failure, physical damage; Human errors = e.g. unintended errors, inaction, insufficient resources.

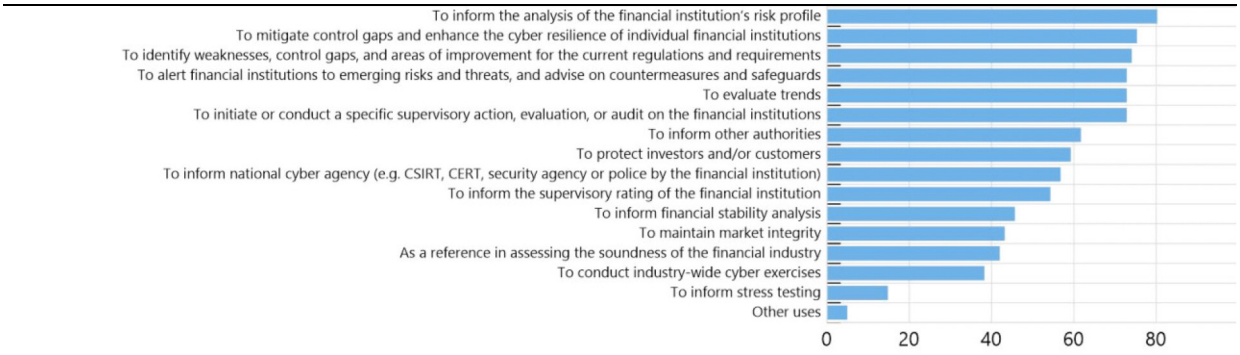
Source: FSB survey

3. Usage of the reported information by financial authorities

Cyber incident reporting data are primarily used to inform the analysis of the financial institution's risk profile, and authorities take a range of actions following a reported cyber incident (see Graph 5). Examples of actions taken include: supervisory or regulatory actions involving the affected institution; updates to regulations and guidance; incorporating the incident data into monitoring and analysis of trends; and information sharing with other authorities (although it may be limited due to legal limitations or confidentiality constraints within each jurisdiction). Many authorities also use reported information for their financial stability analysis, including for stress tests. However, including cyber incident information in stress tests is still not a common practice.

Financial authorities' policy objectives for cyber incident reporting

Percent of respondents **Graph 5**



Source: FSB.

4. Cooperation and coordination

Some authorities share the outcomes of a cyber incident with other agencies (e.g. national cyber agencies), other financial institutions and with the public. The information shared includes items that are of public interest and where public awareness is necessary. This information is typically anonymous, and do not include sensitive details. The information shared could include incident root causes, lessons learnt and remedial actions as well as attack modus operandi, indicators of compromise (IOCs), technical details of malware and attack vectors.

Many authorities have a shared responsibility[8] with other authorities within their jurisdiction related to cyber incidents and share information about incidents with them on a bilateral, multilateral or informal basis. Notification via email is the preferred method of information exchange among authorities, with encrypted emails also commonly used. The criteria for sharing information with cross-sectoral authorities include whether the incident was significant, could threaten financial stability or could otherwise affect another authority's mandate.

Many authorities are members of industry-wide information-sharing groups related to cyber incidents. The most commonly cited such industry-wide information-sharing groups include: (i) Computer Emergency Response Team (CERT); (ii) Financial Services Information Sharing and Analysis Center (FS-ISAC); (iii) Operational Security Situational Awareness Teleconference (OSSAT); (iv) Computer Security Incident Response Team (CSIRT); (v) Cyber Information and Intelligence Sharing Initiative (CIISI); (vi) Central Bank and Regulatory and Supervisor Forum; and the (vii) Financial Services Sector Coordinating Council.

Internal information classification systems are prevalent among authorities; however, these systems tend to be for broader purposes than cybersecurity and they may not necessarily be aligned to industry protocols such as the Traffic Light Protocol (TLP). The TLP may be a starting position in determining how to classify the information to be shared based on each unique information-sharing arrangement, as sufficiently sanitised information and trend data can be aligned to TLP standards. For example, information shared with cybersecurity information sharing groups can be sanitised to only include IOCs and other Tactics, Techniques and Procedures (TTPs) data that may be used by other organisations to identify and prevent or respond to an attack.

Some authorities map their own information classification system to those existing at other institutions or cross-check their internal information classification system against respective industry protocols, prior to sharing the cybersecurity information. The confidentiality of information needs to be reviewed on a case-by-case basis and is subject to legal requirements. In many cases, sharing requires prior authorisation (e.g. by the owners of the information or by a particular Executive Committee).

---

8 This refers to situations where authorities collaborate with each other to manage a cyber incident. For instance, if a cyber incident occurred at a financial institution that is under the supervision of both a banking and securities regulator, the two regulators would likely collaborate and share information with each other on that incident.

5. Challenges in implementing cyber incident reporting regimes

While most authorities consider their current cyber incident reporting regime to be effective, a wide range of challenges in their implementation were highlighted. These include:

- sharing of information and enhanced coordination on cyber incidents with other authorities across jurisdictions as well as sectors (to avoid under-reporting and over-reporting), for example, due to confidentiality and legal/regulatory constraints;
- operational burden for financial institutions and authorities;
- setting appropriate and consistent quantitative and qualitative criteria/thresholds for reporting;
- establishing appropriate culture/behaviour among financial institutions to report cyber incidents in a timely manner;
- difficulty in making accurate assessments and informed decisions during the early stage of cyber incidents based on the reported information as incidents develop over time;
- inconsistent definitions and taxonomy related to cybersecurity across financial institutions, as they tend to have internally-developed definitions and taxonomy;
- establishing a secure method of communicating about cyber incidents; and
- building appropriate skills and capacity among staff at the relevant authorities.

The authorities that view their regime to be less effective attribute this to: inconsistent requirements across financial sectors; the lack of aggregation, trend analysis and archiving; lack of specific reporting requirements for cyber incidents in existing cybersecurity reporting regimes; and the lack of structure and clear process.

6. Use of the FSB Cyber Lexicon

Many authorities use the FSB Cyber Lexicon in their guidance or internal reports, and to lesser extent, in their discussions with financial institutions. In a few cases, the Lexicon is considered in drafting cyber-related risk alerts, policies, procedures and guidance, as well as in supervisory and regulatory assessments. The Cyber Lexicon is generally well recognised by financial institutions and many terms are used by national authorities in their communications and discussions with financial institutions. However, financial institutions do not necessarily use it for their internal risk management purposes as they rely on terminologies and definitions used in the cybersecurity standards they adopt.[9]

More specifically, only a few authorities use the Cyber Lexicon definition for ‘cyber incident’. All other authorities use their own definition, which is typically set out in regulations or guidelines.

[9] Financial institutions seem to generally consider the Cyber Lexicon a useful tool for educating their management and small institutions.

These range from high-level definitions, such as ‘an actual or potential compromise of information security’, or ‘any type of disruption of the provision of services under licensing obligations’, to more complex and detailed definitions.

Some authorities see the need to update the Cyber Lexicon to keep current with the evolving cyber landscape and development of information technology. For instance, given the rise in cyber threats due to prolonged remote working arrangements in light of COVID-19 and increased dependencies on third-party service providers, several authorities suggested including terms such as ‘phishing’, ‘ransomware’, ‘proof of concept’ and ‘supply chain’, along with other terms related to third-party dependencies and operational resilience. Improvements in existing definitions for ‘information assets’ and ‘ICT assets’ may also need to be considered. At the same time, authorities also recognised that when considering whether to update the Cyber Lexicon, due consideration should be given to other lexicons emerging[10] and efforts should be made to establish that updates, if any, to the Cyber Lexicon are aligned and do not inadvertently contribute to further artificial differences that contribute to fragmentation. Furthermore, there was also discussion on whether it may be more appropriate for the Cyber Lexicon to be updated by other public or private-sector bodies. Overall, while there are multiple bodies that could update the Cyber Lexicon, the FSB could still play a leading role in this respect.

[10] For example, in the areas of third-party risk management and operational resilience,

Annex 2: Respondents to the Cyber Incident Survey

(* denotes RCG member jurisdictions)

Jurisdiction	Authority
Argentina	Central Bank of Argentina
Australia	Reserve Bank of Australia Australia Prudential and Regulatory Agency Australian Securities and Investments Commission
Austria*	Oesterreichische Nationalbank Financial Market Authority
Bahamas*	Central Bank of the Bahamas
Belgium*	National Bank of Belgium
Brazil	Banco Central Do Brasil
Canada	Office of the Superintendent for Financial Institutions
Cayman Islands*	Cayman Islands Monetary Authority
China	China Banking and Insurance Regulatory Commission People's Bank of China
Colombia*	Financial Superintendence of Colombia
Costa Rica*	Superintendencia General de Entidades Financieras
Czech Republic*	Czech National Bank
Denmark*	Danish Financial Supervisory Authority
European Union	European Central Bank European Commission European Central Bank Single Supervisory Mechanism European Insurance and Occupational Pensions Authority European Banking Authority European Securities and Markets Authority Single Resolution Board
Finland*	FIN-Financial Supervisory Authority
France	Autorité des Marchés Financiers Banque de France
Germany	Deutsche Bundesbank Bundesanstalt für Finanzdienstleistungsaufsicht
Guatemala*	Superintendency of Banks of Guatemala
Honduras*	Central Bank of Honduras
Hong Kong	Hong Kong Monetary Authority Securities and Futures Commission

Jurisdiction	Authority
Hungary*	Magyar Nemzeti Bank
Iceland*	Central Bank of Iceland
India	Reserve Bank of India Securities and Exchange Board of India International Financial Services Centres Authority Pension Fund Regulatory and Development Authority
Indonesia	Bank Indonesia Financial Services Authority
Ireland*	Central Bank of Ireland
Israel*	Capital Market, Insurance and Saving Authority
Italy	Banca d'Italia Ministry of the Economy and Finance Commissione di vigilanza sui Fondi Pensione Institute for the Supervision of Insurance
Japan	Bank of Japan Financial Services Agency
Korea	Financial Services Commission
Lebanon*	Banque du Liban
Luxembourg*	Central Bank of Luxembourg
Mexico	Central Bank of Mexico
Namibia*	Bank of Namibia
New Zealand*	Reserve Bank of New Zealand
Norway*	Norges Bank
Pakistan*	State Bank of Pakistan
Portugal*	Bank of Portugal
Russia	Central Bank of the Russian Federation
Saudi Arabia	Saudi Central Bank Capital Markets Authority of Saudi Arabia
Singapore	Monetary Authority of Singapore
South Africa	South African Reserve Bank
Spain	Bank of Spain Dirección General de Seguros y Fondos de Pensiones
Sweden*	Swedish Financial Supervisory Authority
Switzerland	Swiss Financial Market Supervisory Authority
Thailand*	Bank of Thailand
Trinidad and Tobago*	Central Bank of Trinidad & Tobago

Jurisdiction	Authority
Turkey	Central Bank of the Republic of Turkey Banking Regulation and Supervision Agency Capital Markets Board of Turkey
Ukraine*	National Bank of Ukraine
United Arab Emirates*	Central Bank of the UAE
United Kingdom	Bank of England (BoE) Financial Conduct Authority Prudential Regulatory Authority
United States	Board of Governors of the Federal Reserve System Securities Exchange Commission Financial Crimes Enforcement Network National Association of Insurance Commissioners
West Africa*	Central Bank of West African States