POSITION PAPER

MMA

Effective Practices for Cyber Incident Response and Recovery: Financial Stability Board Consultation

WSBI-ESBG (World Savings and Retail Banking Group / European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

ESBG Transparency Register ID 8765978796-80

July 2020

WSBI ESBG

Instructions

1 Background for this consultation

The Financial Stability Board (FSB) is seeking comments on its consultative document on *Effective Practices for Cyber Incident Response and Recovery*.

Enhancing cyber resilience has been a key element of the FSB's work programme to promote financial stability. In 2017, the FSB took stock of financial sector cyber security regulations, guidance and supervisory practices[1]. This work identified, among other things, a need to enhance communications between authorities and the private sector. To facilitate more effective communication, the FSB developed a Cyber Lexicon in 2018 to support the work of the FSB, standard-setting bodies, authorities and private sector participants to address financial sector cyber resilience[2].

Given the interconnectedness of the financial sector, the FSB agreed in 2018 to develop a toolkit to provide financial institutions with a set of effective practices to respond to and recover from a cyber incident to limit any related financial stability risks.

2 Questions for public consultation

The FSB invites comments on the consultative document and provides the following specific questions as a guide. Please provide details and supporting information where possible.

Introduction

We appreciate the FSB's initiative to propose a document on Effective Practices for Cyber Incident Response and Recovery. ESBG members advocate for the need of coordinating cybersecurity issues at an international level, we consider that this document is a first step which can served as a starting point for all jurisdictions. In this path, we can achieve a higher-coordination in the field.

General questions

1.1. Have you learnt any lessons from the COVID-19 pandemic and related cyber activity that will contribute to your cyber incident response and recovery practices?

[1] FSB, Summary Report on Financial Sector Cyber security Regulations, Guidance and Supervisory Practices, October 2017.

[2] See FSB, Cyber Lexicon, November 2018.

For financial entities, having an ICT and risk security management frameworks in place is today a hygiene factor but there are many specific risks that require mitigation solutions. However, as the financial sector becomes increasingly dependent on digital technologies, ensuring its resilience while tackling ever growing cyber threats is becoming an important concern, cybersecurity might represent a threat to the stability of the financial system.

The COVID-19 pandemic increased the dependence of financial institutions on digital technologies. Cyber-attacks and incidents have increased in number and sophistication since the start of the COVID-19 pandemic and pose a substantial risk to the stability of the overall financial sector. Each and every financial institution must commit to the proper identification, protection and detection, response and recovery of cyber incidents.

Business continuity plans for a pandemic and business continuity plans as a result of cybersecurity incidents cover different emergency scenarios and involve different measures. Cybersecurity measures must also be implemented continuously during the COVID-19 pandemic. Cybercriminals are increasingly taking up known patterns of action in the context of the Corona Map. In particular, phishing mails are in circulation and social engineering is mainly used. Against this background, clear communication with bank employees and end customers is particularly important as a preventive measure.

Overall, the attacks on bank IT during the corona pandemic are at a normal level and could be handled with the usual precautionary measures and defence mechanisms. Therefore, there is no additional information on reaction and recovery practices. The response and recovery practices are tested at regular intervals regardless of the pandemic.

The primary task during the pandemic is to maintain stable operations in the event of restrictions on presence at the institute and IT service provider locations on site in conjunction with remote working. The communication and reaction procedures described in the course of the business continuity management scenarios and practised in tests have proven their worth.

1.2. To whom do you think this document should be addressed within your organisation?

This Toolkit, to be effective, needs to be addressed to all employees involved in the identification, protection and detection of cyber incidents.

For consultation purposes, we are in contact with member banks, with representatives for information security/ CISO (2nd line of defence) and with IT-managers (1st line of defence).

1.3. How does your organisation link cyber incident response and recovery with the organisation's business? Does your organisation follow international standards or common frameworks? If so, which international standards or common frameworks?

A member of ESBG follows the required three lines of defence model. ICT risk management is part of the first line of defence including the information security function and is the owner of the process and the actor who operates each risk taxonomy (Availability, Operation&Change, Information Security, RDA and Strategy). The second line of defence is an independent party who challenges processes and Key Performance Indicators and guarantees that regulations are taken into account. Third line of defence is Internal Audit.

The number of incident reporting requirements is rapidly increasing, and varies from country to country. For an organisation with common business infrastructure supporting operations in several countries, this means that a single incident triggers several incident reports to multiple authorities in many different countries. Regulators should reduce compliance complexity by integrating regulatory guidance, expectations and requirements.

ESBG believes that cybersecurity needs to be coordinated at international level due to the international dimension and the only way to resolve is increasing the cooperation within the EU and at international level.

1.4. Does your organisation structure its cyber incident response and recovery activities along the seven components set out in the FSB toolkit? Please describe any additional components your organisation considers.

The activities mentioned in the components generally play a role in the management of security incidents in our member institutions. Since many banks in Europe have outsourced their IT to full-service providers, the activities are divided into parts provided by the IT service provider and activities that the bank implements itself.

1.5. Based on your organisation's experience, please provide any additional effective practice(s) for any of the tools. Please list the number of the tool (e.g. Tools 1 – 46) and describe the effective practice(s).

Third-party risk management is an important element for each of the main functions of cybersecurity (identify, protect, detect, respond, recover) and essential as firms progress down digitalization journeys. The FSB practices no. 17 (Supply chain management), no. 23 (business continuity measures) and no. 28 (monitoring) briefly touch on third-party related considerations. Overall, we recommend that the FSB should broaden its coverage of third-party aspects to highlight additional considerations and effective practices that address indirect threats from service providers and mitigating third-party risk when an incident is live.

Often, new serious threats or vulnerabilities become generally known before the own organization is affected by actual incidents, e.g. because serious weaknesses in standard software/multiple-use software become known. The communication plans therefore start to respond to suspected or actual serious threats or vulnerabilities before the organization is affected by an actual incident.

1.6. Based on your organisation's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6).

We would like to take the example of the German banking sector. Due to national and European law and the resulting regulatory requirements of supervision, certain practices must be implemented by all German banks. The "minimum requirements for risk management" and the "banking supervisory requirements for IT (BAIT) specify the German Banking Act (KWG) with detailed and technical requirements. These requirements also include cyber risks.

At European level, cyber and ICT security requirements are specified by technical standards and guidelines of the European Banking Authority (EBA). Important aspects of cyber security are set out in the "Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)"/ "Guidelines on ICT and security risk management"/ EBA/GL/2019/04 and the "Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)".

1.7. What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?

The ESBG believes that authorities should contribute to monitor and promote cyber-resilience to all types of entities. As the European Parliament stated in its FinTech Report "a connected system is only as safe as it weakest element". Therefore, the ESBG believes that cyber-resilience must be prevented not only from critical market operators and financial entities but from all types of entities. A connected system is only as safe as its weakest element and due to the interconnectedness of the financial sector, it is essential that every institution, regardless their size, nature or activity, acquires the same level of cybersecurity.

ESBG emphasizes that cybersecurity should not be treated nor regulated with proportionality criteria. Cyber-attacks must be prevented to all companies without taking into account the size, complexity or business model of the different players. Hackers will attack the weakest link in the chain in the ecosystem to gain access to customer's and proprietary data, this can in several cases be through third-parties who might not have the same level of security.

In particular, prosecution by the competent authorities (usually police) is essential, as this cannot be done by private companies and is necessary to deter the perpetrators. According to our findings,

efficient and effective cross-border criminal prosecution occurs too rarely, especially when perpetrators act from abroad - in this case, consistent administrative assistance is required. In addition, authorities could offer assistance in eliminating the threat, e.g. by insisting that other companies in European and non-European countries comply with conventions, or, more specifically, in containing threats via infrastructure from abroad.

Additionally, authorities can play a role in the response activities by issuing warnings to other potential affected parties from the information received in the context of reporting obligations.

1. Governance

1.1. Have you learnt any lessons from the COVID-19 pandemic and related cyber activity that will contribute to your cyber incident response and recovery practices?

While the board has overall responsibility with respect to CIRR, the allocation of responsibility for the related tasks varies from institution to institution, due to considerations of size, structure and footprint considerations, among others. A special aspect is the division of tasks between the bank and IT service providers, in particular full-service providers. For example, the role of incident owner is taken by the IT service provider. Communication with customers and the press is carried out by the bank or, in the case of incidents involving more than one company, e.g. in the case of affiliated groups or joint products (girocardsystem), centrally. Independent observers are located both on the side of the IT service providers and on the side of the bank (Information Security Officer/ CISO).

Note on Practice no. 2 / 3:
Overall, the tasks of the roles mentioned in the FSB Toolkit appear to be target-oriented, but should be adapted to the respective existing organisation in order to avoid unnecessary overhead. We recommend that this be made clearer in the text so that the allocation of specific roles and responsibilities better allows for proportionality and scaling across a number of institutions. In addition, it should be made clear that in relation to the board, overall responsibility for the CIRR is meant, not responsibility for operational activities.

Not for all roles is the naming of 'named individuals' appropriate. In the case of the operationally pronounced roles, it has proven to be best to assign them to functional units/teams which have equal access to all information. Depending on the severity of the incident, several interlinked processes with different decision-makers can be triggered, so that the assignment of responsibility for incident handling is not restricted to a single incident owner. For incidents that are classified as crises, crisis teams/units have proven their worth.

1.2. How does your organisation promote a non-punitive culture to avoid “too little too late” failures and accelerate information sharing and CIRR activities?

Within the measures on safety and risk awareness, for example, realistic examples raise awareness of being vigilant and reporting unusual observations. The handling of specific serious incidents is carried out within crisis teams, which are composed of different affected areas and with their complementary competences avoid "blind spots" or too late reactions.

2. Preparation

2.1. What tools and processes does your organisation have to deploy during the first days of a cyber incident?

One ESBG member has deployed the following tools during the first days of a cyber incident:

- Identification.
- Detection
- Respond
- Recovery
- Learning and evolving

A selection of often used processes and instruments (without claiming to be complete) are:

- Technical processes (analysis, immediate measures (if necessary workaround), restoration of normal status)
- Coordination up to a crisis unit in the event of major incidents
- Communication tools and processes - internal and external
- Meet reporting requirements for public authorities/ banking supervision

2.2. Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months.

Exercises performed and real incidents are continuously evaluated by our institutes in the sense for lessons learned. For more examples, see 6.3.
Stress tests play an important role in the institutions' cyber resilience efforts and consist of a series of exercises with different design and participation.

Note on Practice No 12: Scenario planning and verification.
The final sentence for this practice could imply that "important external stakeholders" should be involved in each exercise. In our practice, scenario testing covers a wide range of exercises – from purely internal to exercises with external participation. We recommend that you revise the sentence accordingly.

2.3. How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)?

The current regulatory framework in place, the EBA (European Banking Authority) in its Outsourcing Guidelines, set some obligations for banks, which can hardly be met. For example, auditing rights, data location, etc… as the negotiating position of European banks towards cloud service providers is fairly weak.

In the framework of ESBG, we are working on an official certification scheme for Cloud, with boxes that cloud service providers need to tick and requirements that they need to meet, in order for, them to offer their services in the European banking market. The certification should assess and validate standard regulatory requirements such as technical/security/legal/ compliance issues, which are imposed by the EBA Guidelines on Outsourcing.

We believe that this certification could contribute to minimize technical, operational and security risks, and at the same time would contribute to the compliance of the Guidelines.

To mitigate the risks posed by third-party services (IT service providers, cloud providers, suppliers of software and hardware components), the following measures are used, among others:
- Contractual agreements to transfer security standards to downstream service providers, to provide immediate information on security incidents
- SLA agreements (including KPI RTO and RPO)
- Coordinated emergency concepts, consideration of outsourcing in bank contingency plans, emergency contacts
- Coordinated technic measures (such as firewalls, prohibition of connecting foreign clients directly to the company network, jump servers)
- Monitoring and control of IT service providers

3. Analysis

3.1. Could you share your organisation's cyber incident analysis taxonomy and severity framework?

Various reporting obligations to national and European authorities must be taken into account in the Bank's taxonomy in order to fulfil these obligations. As a result, information is already standardized and can be shared in principle for these cases.

Voluntary exchange of information is already of great importance for both the prevention and containment of cyber-attacks. This is usually organised informally and is based on the trusting and cooperative cooperation of the parties involved. An essential prerequisite for the exchange of information is a mutual knowledge and a resulting basis of trust. Taxonomies play a minor role here, more important is the (often informal) exchange on the mode of action of cyberattacks, danger situation and defense mechanisms. Since the classification as a security incident depends on institutionally specific criteria (business model, risk detection ...), however, there are limits to the standardized sharing of taxonomy and severity.

3.2. What are the inputs that would be required to facilitate the analysis of a cyber incident?

It is important that all stakeholders involved agree on what the purposed of the reporting is and thus, what needs to be reported. That is the reason why we have always advocated that incident reporting should include materiality thresholds.

For entities, it is challenging to report any kind of incident. It is desirable to establish materiality threshold regarding impact on customer or in the market. Financial institutions do not have the capacity in terms of human resources, budget to report any incident.

The reporting obligation on financial institution must be relevant and fit for the purpose. Reporting all incidents is not productive for any party involved. Finally, we would like to stress that the burden shall not be on the financial institutions to provide differentiated reports to regulators, it should be the burden of regulators to harmonize the report requirements.

In the case of cyber incidents, the precise description of attack vectors and exploited vulnerabilities is especially useful for other organizations to prevent similar attacks.

3.3. What additional tools could be useful to analyse the effectiveness of cyber incident response and recovery activities and the severity, impact and root cause of cyber incidents?

The ESBG advocates to introduce new tools in order to increase the effectiveness of cyber incident response and recovery activities. As a first step, we believe that it is needed to share best practices among peers, this framework, to be effective, should be compulsory for all players. This framework should be designed on two pillars:

i) sharing good practices between peers. For the time being, sharing good practices takes place through informal channels. In order to provide confidence, it is important that regulator design and establish these frameworks.

ii) receiving feedback from authorities to improve our internal practices. Authorities require us enormous information, not always essential, however we do not receive any feedback from them. We believe that there should be a two-way flow of information that will allow financial entities to improve our effectiveness.

We are aware that many times financial entities are reluctant to share good practices with peers. For this reason, the framework to share good practices between peers, to be helpful, should be mandatory always ensuring safe data sharing.

A variety of instruments are used by institutions and IT service providers. If an analysis requires cooperation with law enforcement authorities, regional, federal and national structures sometimes make it difficult to make effective contact and processing.

3.4. What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation?

Some ESBG members participate in an initiative launched by the European Union Agency for Cybersecurity (ENISA) to set up frameworks to share information between peers. We encourage initiatives, similar to those launched by ENISA and we hope that it will soon become operational.

The leading German sector associations represented in the GBIC offer exchange platforms for banks as well as platforms for exchanges between associations. The exchange of attack scenarios on critical infrastructures is in UP KRITIS – a public-private partnership in this field of great importance. Direct contacts and SPOC structures, e.g. BSI location center, are used as an interface. In addition, some institutions use other information sharing organisations, e.g. G4C (Germany) and FI-ISAC and FS-ISAC (international). The IT service providers are represented in a variety of national (e.g. BITKOM) and international industry organisations (Eurofite) and exchange directly within the industry. Other tools: International Cert exchange, cooperation with Microsoft/ Google Save Browsing Initiative, cooperation with antivirus laboratorie= for concrete exchange.

4. Mitigation

4.1. Besides reducing impact to business and system security, what are other considerations that need to be taken into account during mitigation?

The concern of customers/reputation is another important framework condition -> cf. 7.

Note on Practice No 23 Business Continuity Measures:
The current wording implies that every cyber incident triggers business continuity plans (BCP). The activation of BCP however will depend on the severity of the incident, among other factors. We recommend to highlight that BCP may be triggered by the Incident Manager or other responsible party, depending on the incident's severity and expected impact.

4.2. What tools or effective practices does your organisation have related to mitigating the impact from: (i) data breaches (ii) loss of data integrity and (iii) ransomware events?

A complete, comprehensive set of instruments for ISMS / DMS with extensive controls is available. This serves both to manage the risks arising from the institutions' own interests and at the same time to meet the extensive requirements of the EU GDPR and the regulatory requirements for information security. Within this process, considerable importance is attached to the analysis and documentation of threats and measures in order to secure business processes preventively and to be able to continue them in case of a response.

4.3. What tools or practices are effective for integrating the mitigation efforts of third- party service providers with the mitigation efforts of the organisation?

The most important practice is to prepare for such situations – through contractual agreements, SLAs, coordinated contingency and emergency plans and the coordination of technical measures and organisational processes. Best Practise is in particular to provide for direct personal communication, i.e. exchange between those affected at the institution and those involved at the third-party provider via dedicated contact channels.

4.4. What additional tools could be useful for including in the component Mitigation?

Practises 22.-25. describe the instruments well, in addition, interfaces and interactions with other organizations must be taken into account, e.g. financial market infrastructures (payment transactions, WP business).

4.5. Are there situations in which effective practices for mitigation and restoration activities of the organisation are the same or overlap substantially? If yes, please provide examples.

In the case of a Denial Of Service attack with an impact on availability, the measure consists of identifying and mitigating the attack vector and thus restoring the service.

5. Restoration

5.1. What tools and processes does your organisation have available for restoration?

One ESBG member has a Contingency Technological Governance framework designed and developed, and certified, in accordance with the acknowledged and prestigious international ISO 27031 standard, the operation of which ensures the implementation of best practices in ICT Readiness for Business Continuity (IRBC) areas.

This framework has been developed in a specific regulatory corpus.

- This corpus defines, among other topics, a method to assign the criticality for IT services. This method is transposed into a questionnaire that must be completed by the owner of each IT service and it is divided into the following areas:
  - Data Protection Law.
  - Information Security.
  - Business Continuity.
  - Reliability of Financial Reporting.
  - Physical Security.
  - Labour Relations.
  - Business.
  - Operational Risk.
  - Business Critical Processes (new in 2019).
- This criticality obtained is represented in four levels:
  - Platinum (type A).
  - Gold (type B)
  - Silver (type C)
  - Bronze (type D)
- Identify the indicators to be monitored for each one of the types of critically:
  - Recovery Time Objectives (RTO)
  - Recovery Point Objetive (RPO)
  - Detail/scope of the documentation.
  - Test type
  - Test frequency.
- The restore procedures are defined according with criticality of the services.

The institutes use extensive redundancy concepts for the infrastructures and mirroring / security systems during normal operation, which can be even used in the event of an incident.

5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?

The organization maintains detailed business continuity plans. Priorities are set by means of business impact analyses. For prioritization, the common metrics recovery time objective (RTO) and maximal tolerable time period during which data loss can be tolerated (Recovery Point Objective / RPO) are used.

5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?

In the event of an emergency, a quick and at the same time safe restart/recovery of the business processes has priority. Coordinated control of recovery activities, e.g. by crisis teams, minimizes undesirable results.

6. Improvement

6.1. What are the most effective types of exercises, drills and tests? Why are they considered effective?

Regarding reporting requirements, supervisors have reacted with a proliferation of cybersecurity frameworks and regulations of reporting. However, definitions and approaches used by supervisors vary which creates significant inefficacies and conflicting direction to financial institutions, particularly, to the global ones. This fragmentated approach also diverts precious resources away from securing the firm to addressing numerous and disparate supervisory requirements. CISOs spend a significant portion of time on compliance activities addressing similar concerns form different supervisors but needing to tailor each request. Under this situation, the ESBG considers it is key to introduce a comprehensive, harmonised system of ICT incident reporting requirements for the financial sector. This will help entities to report accurate and timely information to competent authorities, in order to allow entities and authorities to properly log, monitor, analyse and adequately respond to ICT and security risks. We propose to standardise templates, taxonomy and timeframes. Currently, one of our main challenge is the relationship with existing incident reporting requirements which usually overlap among them; PSD2, GDPR and the NIS Directive. We also believe that it will be more effective to establish an only authority which receives all reporting`s from financial institutions. This authority will be in charge of reporting to each competent authority depending on the issue and the country. Institutes perform a variety of reviews and exercises, including tabletop exercises, the practice of realistic scenarios and complex crisis staff exercises. IT stress and/or red teaming tests by the institutes or IT service providers complement the crisis staff exercises of the institutes on a technical basis. In addition, to report an example from a Member State, cross-sectoral crisis management exercises are conducted in Germany, e.g. under the coordination of the Federal Office for Civil Protection and Disaster Relief (BBK) (LÜKEX exercises).

6.2. What are the major impediments to establishing cross-sectoral and cross-border exercises?

ESBG highlights the negative effects of the current overlapping of reporting obligations regarding cyber incidents. Supervisors have reacted with a proliferation of cybersecurity frameworks and regulations of reporting. This created significant inefficiencies and conflicting direction to financial institutions. The burden shall not be on the financial institution to provide differentiated reports to regulators it should be the burden of regulators to harmonise the report requirements. Furthermore, this fragmented approach diverts precious resources away from securing the firm to addressing numerous and disparate supervisory requirements.
Cross-sectoral and cross-border exercises cause a high organisational and coordination effort, which increases exponentially with the number of participants. Cross-sector know-how for building realistic scenarios is necessary, but is often not readily available.
As a result, the participants in such exercises often have an inadequate cost-benefit ratio. Especially for participants who already meet a high standard, the knowledge value is limited from the exercises due to the often very general scenarios. The added value is not directly visible, as many sectors are in the process of building or expanding their own cyber defense capacities and thus the narrower focus currently offers greater cost efficiency.

6.3. Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery?

The tools differ from institute to institute. The decisive factor is not the tool by itself, but the coordinated interaction between organization, processes and existing technical tools in the event of an incident.
For example, a good practise is the use of high specialized teams e.g. 24x7 cyber security operations center (SOC)/ cyber defense center to prevent from cyber incidents.

7. Coordination and communication

7.1. Does your organisation distinguish "coordination activities" from broader "communication" in general? If yes, please describe the distinct nature of each component.

Both topics go hand in hand: a coordination team provides information as a basis for broader communication (newsroom) and informs the management board and defined departments responsible for target group-specific preparation, e.g. for affected specialist departments, end customers, press, authorities, etc.

7.2. How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident?

For this purpose, there are more redundant contact channels in the emergency contact directories (e-mail, telephone stationary and mobile, chat, addresses) and exist different communication channels (e.g. separate telephone connections or Internet access, VPN dial-ins for emergencies).

7.3. Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities?

ESBG believes that a standing mechanism to exchange incidents reports among competent authorities is needed to share best practices among financial players, this framework should be compulsory for all players to be effective. This framework should be designed on two pillars: i) sharing good practices between authorities which help to their supervisory powers and ii) receiving feedback from authorities to improve our internal practices. Currently, there are legal and regulatory obligations for cyber incidents to be reported to different authorities on the basis of different, rigid reporting schemes on national and in some cases on European level. We support the FSB's focus on "significant" cyber incidents for reporting purposes. Materiality thresholds should be risk-based and should not be set according to fixed, specific criteria (e.g. number of customers or transactions) so that they can be applied to companies of different types and sizes to cover only significant security incidents. We consider the disclosure of information on security incidents to be useful if they are relevant to a situation picture for critical infrastructures, e.g. cyber security incidents involving systems that affect the stability of the financial system or guarantee the supply to the population or which may have serious effects on other market participants (e. g. new attack vectors). To this end, competent

authorities need comparable data on significant cyber incidents across the whole range of market participants.

About ESBG (European Savings and Retail Banking Group)

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ▪ B-1000 Brussels ▪ Tel: +32 2 211 11 11 ▪ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ▪ www.wsbi-esbg.org

Published by ESBG. [Date]