FSB FINANCIAL STABILITY BOARD

20 April 2020

Effective Practices for Cyber Incident Response and Recovery

Public Consultation - Optional Response Template

Instructions:

The FSB invites comments on the consultative document on Effective Practices for Cyber Incident Response and Recovery that includes a list of specific questions as a guide. To help respond to the public consultation, this optional response template is provided.

The template has been designed to be completed as a form in Microsoft Word. To assist with automated compilation of answers, respondents are only able to make changes in the spaces set aside for answers.

For the context of any question or for defined terms, please refer to the relevant parts of the consultative document.

Please save and submit the completed questionnaire as a Microsoft Word document, rather than converting it to a PDF. A password may be applied; in that case you should communicate the password by separate email or by telephone conversation arranged by email.

The FSB invites stakeholders to provide their responses by Monday 20 July 2020 by e-mail to CIRR@fsb.org with "CIRR" in the e-mail subject line. The feedback received will be taken into account in the FSB's development of the final toolkit of effective practices, which will be published in October.

You may choose to leave answers blank – in that case it is acceptable to leave the answer reading "Click here to answer text".

Should you wish to obtain an unlocked version of this template in order to facilitate sharing of draft answers in your organisation, please contact the FSB Secretariat on the e-mail address above. In that case, you would still be requested to copy your answers to the locked version on the template to ensure accurate processing of the data.

Intesa Sanpaolo Banking Group responses to CIRR Consultation

Questions	Answers
Information about the respondent	
A. Name of respondent institution/firm	Intesa Sanpaolo Group
B. Name of representative individual submitting response	Federico Orsi
C. Email address of representative individual submitting response	federico.orsi@intesasanpaolo.com
D. Do you request non-publication of any part(s) of this response? If so, which part(s)? *Unless non-publication (in part or whole) is specifically requested, all consultation responses will be published in full on the FSB's website. An automated e-mail confidentiality claim will not suffice for these purposes.*	No
E. Would you like your response to be confidential (i.e. not posted on the FSB website)?	No

Questions	Answers
Consultation questions	
General questions	
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?	Lessons learned, in particular in the digital work area, regard: • Accountability of personnel, delegation; • Flexibility and adaptability, use of time; • Focus on results, specific objectives; • Working groups more cross-structures; • Focus on stakeholders and work on clear communication; • Strengthening of security controls on existing digital services (e.g. VPN infrastructure); • Implementation of new security devices on new digital services made available for the management of the COVID-19 emergency; • Strengthening awareness initiatives on cyber risks related to the emergency.
2. To whom do you think this document should be addressed within your organisation?	• Cybersecurity functions, including Incident Management (SOC, CSIRT and CERT); • Other Incident Management Teams (IT Department, Privacy, Physical Security, etc.); • External communication department; • Treasury department/structures involved in payment processes; • Control Functions (risk, compliance, audit): • International Public Affairs - Institutional Relations Office.

Questions	Answers
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?	With reference to the connection of the response and recovery activity to the business of the organization, as soon as CSIRT receives the report relating to the current critical event, it contacts and engages all the structures concerned by the event to understand its severity. Once the necessary preliminary information has been collected, it convenes a first alignment meeting involving all the necessary entities for the management of the event. The constant involvement of the business also allows it to be kept aligned on the evolution of the event and the possible impacts. In addition, the organisation adopts an incident management process that incorporates the main international standards and common frameworks such as NIST Framework for Improving Critical Infrastructure Cybersecurity and ISO 27001/ISO 27002.
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.	Cyber incident response and recovery activities are structured on the basis of the seven components indicated in the FSB toolkit. In particular: • The definition of tasks and responsibilities within the company regulation (tools 3 and 9). • The definition of a runbook for the management of possible event scenarios (tool 10), and a set of communication templates to be used (tool 11) are being addressed within the organization. • The definition of cyber incidents taxonomy that contributes to a rapid and homogeneous classification of events at corporate level (tool 19). • Once a critical event has been identified, the coordination of activities by CSIRT towards all involved functions, aimed at mitigating the effects of the event itself (tools 22-25) and identifying recovery actions (tools 26-33). • The tracking of lessons learned and possible improvements in the management of specific events (tool 40).

Questions	Answers
	• The information sharing always carried out reliably and quickly (tool 44) to guarantee a timely escalation within the organization for the management of events (tool 41). • Finally, the periodic and continuous alignment meetings on the event with CSIRT and involved functions to provide regular updates on the evolution of the activities, and actionable, accurate, timely and concrete information (tool 42).
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).	We do not have any further practice to add.
6. Based on your organisation's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6).	We do not have any further practice to add.
7. What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?	Authorities should play both a Threat Intelligence role - warning of immediate or upcoming threats to the organization or, more extensively, to industry - and a supporting role to help investigate cyber incidents when requested by organizations as the authorities have the ability to provide insight and bring additional resources and intelligence for accurate incident resolution. They can also perform a coordination function to ensure cross-sectorial and cross-border cooperation among the different competent authorities. However, a single incident might entail the need to report to different Supervisory Authorities complying with different regulations; all these different criteria and patterns cause fragmentation with respect to the overall incident reporting requirements and can subtract resources from the handling of the incident itself.

Questions	Answers
	At this regard, it would be helpful for the different authorities to cooperate for a clear set of harmonized and shared requirements and standards.
1. Governance	
1.1 To what extent does your organisation designate roles and responsibilities as described in Tool 3? Does your organisation identify these roles by business line, technology application or department?	The involvement of the different competent functions is assessed according with the specific nature of the incident and its severity, and all the identified stakeholders are included in periodic alignment meetings throughout the incident management evolution and the recovery activities definition.
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?	All company functions that could be affected by a potentially critical event are aware that they must alert the competent cybersecurity and/or incident management functions as soon as they detect the event. If the event is considered critical, the CSIRT starts organising meetings between stakeholders. This allows to speed up information sharing and to sensitise all the functions involved.
2. Preparation	
2.1 What tools and processes does your organisation have to deploy during the first days of a cyber incident?	Our organisation adopts an incident management group process that allows, based on the specificity and severity of the incident, to activate the appropriate internal escalation and decision-making process leading, if necessary, to the activation of the crisis management model. These practices allow not only the correct coordination and internal collaboration but also the fulfilment of reporting obligations to the competent authorities in an effective and efficient way. The most suitable strategy is defined on the basis of the information, promptly and accurately collected, and the impacted processes.
2.2 Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months.	• Update of the rules for the business continuity plan to include all possible scenarios and enhance cyber events'one; • Update of the process for critical event management;

Questions	Answers
	• Review and update of the crisis management model; • Start of "critical event readiness" project for the identification and formalisation of contingency solutions relating to the organisation's digital services; • Participation in external cyber exercises (e.g. G7 Simulation for Cross-border Coordination) and organization of internal crisis simulation (table-top exercise); • Internal re-organisation for segregation of tasks between the event's phases of classification, management, mitigation and lessons learned, analysis, intelligence.
2.3 How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)?	In order to strengthen and extend the monitoring activities to all the suppliers for all the Group, within the organisation there is a dedicated team carrying out monitoring and controlling activities against suppliers identified as cyber-relevant We also reviewed the contracts to assess suppliers also through on-site audits, and defined specific procedures to be activated when a cybersecurity event is first detected for third party risk mitigation. Furthermore, high-level assessment is conducted on the main providers (identified with a risk based approach), checking effective implementation of the main security measures, alignment with the organisation's policies and establishing procedures in case of non-compliances.
3. Analysis	
3.1 Could you share your organisation's cyber incident analysis taxonomy and severity framework?	Our organisation contributed to FSB's Common Taxonomy, and we use it for CIRR's activities. Moreover, we follow standard such as NIST Framework for Improving Critical Infrastructure Cybersecurity and ISO 27001/ISO 27002.

Questions	Answers
	Finally, for assessing the severity of cyber incidents, reference we refer to the type of incident/event (for example if it is an ordinary incident or a complex event) to involve the correct functions within the organisation.
3.2 What are the inputs that would be required to facilitate the analysis of a cyber incident?	The timely collection of information relating to the impact perimeter (which/how many devices, tools and/or systems involved) and its severity concerning reputation, regulations and economic effects, and the promptness of such information allow to start the analysis of the incident and define the appropriate response action.
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?	• Implementation of tools that solve the challenges of managing multiple and fragmented requirements in an efficient mandatory incident reporting process, and the implementation of prevention and monitoring tools in order to limit the risk of the incident occurring. • Establishment of a shared database including all cyber incidents and the possible root cause of these incidents would be useful.
3.4 What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation?	The main collaboration we have are with: • CERTFin and ABI (Italian Banks Association) at Italian level; • EBF, AFME and ECSO (not only sectoral) at European level; • IIF at international level. Constant updating on the main cyber risks, sharing of best practices, and advocacy activity are the main benefits we accrue in participating in these associations.
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?	We deem fundamental the mitigation of reputational and economic impacts, the mitigation of the impacts that any inefficiencies can bring to customers, as well as

Questions	Answers
	the management of the external communication (Media, Customers, Thirds parties, Authorities).
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?	Our organisation has developed a tool with contingency measures (IT, Operational and Communication) to guarantee the continuity of customer service, and to mitigate any regulatory and reputational impacts deriving from cyber and/or business continuity incidents so to guarantee the continuity of digital service.
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 continuous interaction between the different functions (e.g. Procurement, Cybersecurity) dealing with suppliers/third parties is essential to enhance third party risk mitigation. In order to mitigate the reputational impacts, our organisation has also developed a tool providing ready-to-use internal and external communication templates to be used when incidents occur.
4.4 What additional tools could be useful for including in the component Mitigation?	Communication is an additional tool worth including in the Mitigation component. Furthermore, prevention tools should be improved as much as possible, because, once the incident occurs, all necessary measures must be activated for incident management: Detect, Protect, Identify, Respond and Recover. Once the situation is resolved, a Post-Incident Analysis is required.
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.	No: remediation solutions aim to restore the service while mitigation ones aim to guarantee the continuity of services until their total restoration.
5. Restoration	
5.1 What tools and processes does your organisation have available for restoration?	The organisation has tools with detailed evidence relating to the criticality and relevance of operating and business processes. Each process has a pre-defined business continuity solution, to be activated according to the occurred scenario.

Questions	Answers
5.2 Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?	The organisation has a specific tool for managing business continuity and for activating solutions. The main metric for assessing recovery priorities is the RTO associated with processes.
5.3 How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?	Our organisation constantly monitors the operating trend during the incident management activities (service levels, operating volumes, system cut-off compliance, data integrity) by adopting the appropriate technical and organizational countermeasures when alarming situations are detected. The restoration of post-emergency operations is specifically defined in the Restoration Manuals (both for technological and organisational solutions).
6. Improvement	
6.1 What are the most effective types of exercises, drills and tests? Why are they considered effective?	• In our opinion, the most effective exercises should be done periodically and should also: o on one hand, test business continuity plans and, on the other, evaluate those relating to the management of complex events, also arriving at emergency / crisis scenarios (e.g. with table-top simulations); o include more operational simulations both related to business continuity solutions and to red teaming, to evaluate technological responses; o evaluate the effectiveness of awareness and training activities provided to employees, both through post-courses tests, and through simulations such as ethical phishing campaigns. • Exercises' plans are essential to improve readiness in responding to cyber incidents and crisis management and should be constantly improved by organisations. To improve the effectiveness of tests and exercises, there is

Questions	Answers
	a strong need to define common regulations regarding what can be done so that all players, and in all States, have the same opportunities. • Finally, the use of a shared threat-led penetration testing framework for more operational exercises such as red teaming should be pushed, to simplify joint exercises at financial or even wider ecosystem level, as well as to make the test results comparable.
6.2 What are the major impediments to establishing cross-sectoral and cross-border exercises?	The major impediments to cross-sectoral and cross-border exercises are the fragmented regulatory landscape, and the lack of a cooperative approach to cyber defence. Also, cross-sectoral and cross-border exercises are onerous activities, in terms of time and effort, so a strong cultural change would be needed to push organisations to see the added value.
6.3 Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery?	One of the most delicate activities in the management of serious cyber security incidents is the Incident Reporting due to the fragmented nature of the current legislation by different authorities. Harmonization of Incident Reporting regulations would make reporting incidents to authorities more effective and less costly.
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.	• During coordination activities, communication is made gradually with the structures involved based on the classification level of the event. • Broader communication activities are addressed: o Towards the top management; o To different external stakeholders such as media, social media, authorities, customers, providers, etc.; o Internally to employees and structures in direct contact with customers.

Questions	Answers
7.2 How does your organisation address the possibility that e-mail or traditional communication channels will be unavailable during a cyber incident?	In case e-mail or traditional communication channels (Skype, Outlook) are not available during a cyber incident and, specifically, an emergency or a crisis, alternative dedicated communication channels are activated, including the External Call Conference and satellite communication systems.
7.3 Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities?	• About Cyber incident response, high level overview of the main countermeasures activated. For Cyber Incident recovery: high level overview of root cause analysis (non-technical) and remediation plan. • Specific, detailed and technical information regarding the incident are shared only with competent authorities, according to the regulatory requirements in force or when expressively required; in addition, information on ongoing threats/incidents is already being shared with authorities and key stakeholders from a collaboration perspective (e.g. CERTFin, FIRST, FS-ISAC, etc.).

For further issues concerning this consultation please contact:

Intesa Sanpaolo
International Relations
Piazza di Montecitorio, 115 - 00186 Rome, Italy

– Alfonso Siano - e-mail alfonso.siano@intesasanpaolo.com
– Federico Orsi - e-mail federico.orsi@intesasanpaolo.com