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.

Questions	Answers
Information about the respondent	
A. Name of respondent institution/firm	Deutsche Börse Group (DBG)
B. Name of representative individual submitting response	Jan Wolfgang Doser
C. Email address of representative individual submitting response	Jan.wolfgang.doser@deutsche-boerse.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.*	Click here to enter text.
E. Would you like your response to be confidential (i.e. not posted on the FSB website)?	Choose an item.

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?	It is important to differentiate COVID-19 from normal circumstances. Due to COVID-19 we saw high volatility and extreme usages of our IT-systems, but did not see any cyber incident. We experienced that critical mission areas functioned well, even when most of the staff worked in remote/home office situation. DBG has set-up an incident management committee to tackle such issues, apply emergency plans, tracking information, develop templates and develop lessons learnt etc. We think well established business continuity management and communication is key.
2. To whom do you think this document should be addressed within your organisation?	If external stakeholders would like to approach us, we would see the group CISO to be addressed, who may then inform the respective CISOs/BISOs of the respective business entities.
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?	We have incident management and crisis management teams on the business side in place. We incorporate a lot of international standards and regional/national regulation coming from different authorities already today: e.g. EU legislation on NIS, MAR; banking rules as well as ISO standards like 27035. Further, we develop our own standards according to specifics of financial market infrastructures (FMI) based on suitable existing frameworks.

Questions	Answers
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.	Yes, we do apply the components set-out in the FSB toolkit. The components should ideally align to ISO 27000, which is a very good reference and covers many of the mentioned components in detail.
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).	Click here to enter text.
6. Based on your organisation's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6).	Click here to enter text.
7. What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?	We would propose to establish channels going both ways with regard to "reporting and sharing". If authorities would share the conclusions and results of the analysis of the reported data, this would help regulators and the industry. Coordination on a broader level would also help to share experiences, exchange views, learn from best practices etc.
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?	We have established recurring channels/processes on external communication, which is not related to a particular/specific topic. As we do not focus on retail clients, we have different channels available to address our B2B customers (technical information exchange etc.).
1.2 How does your organisation promote a non-punitive culture to avoid "too little too late" failures	Information sharing is very important in our company. We have established continuous improvement measures, to adapt to new circumstances, assess risks and

Questions		Answers
	and accelerate information sharing and CIRR activities?	opportunities regularly. KPIs are available, however they are further adjusted each entity within the group.
2.	**Preparation**	
2.1	What tools and processes does your organisation have to deploy during the first days of a cyber incident?	We use different tools, depending on the incident (e.g. forensic tools).
2.2	Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months.	We analyse on a regular basis threat profiles, adjust to new threats accordingly and update our risk management tools.
2.3	How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)?	We have established control mechanisms within the „material change processes“, according to EBA guidelines on outsourcing to third party service providers. Please note that ESMA on the European level is currently working on this topic as well.
3.	**Analysis**	
3.1	Could you share your organisation’s cyber incident analysis taxonomy and severity framework?	We have developed internal standards on incident reporting.
3.2	What are the inputs that would be required to facilitate the analysis of a cyber incident?	There are several tools: correlation tools, incident data base, system logs etc.
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?	We would propose tools like vulnerability handling, CERT alerts, KPI measures, reducing risks/vulnerabilities from the start, continuous improvement and stress testing.
3.4	What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation?	We are member in many associations where such topics are being discussed (e.g. Bitkom, WFE, EACH, ECSDA).

Questions		Answers
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?	Click here to enter text.
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?	Click here to enter text.
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?	Click here to enter text.
4.4	What additional tools could be useful for including in the component Mitigation?	Click here to enter text.
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.	Click here to enter text.
5.	**Restoration**	
5.1	What tools and processes does your organisation have available for restoration?	Different business entities have their unit recovery plans and processes to update those plans. This is supplemented by IT disaster recovery plans, e.g. to make processes or resources available and other emergency planning (e.g. back-up locations, remote working etc.). Restauration is rather used in the context of data which can be restored. In the IT area the focus is rather on recovery. Those teams are often separated: either focusing on getting e.g. the data back while the other teams focusing on rather physical recovery of systems.
5.2	Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?	See above.

Questions		Answers
5.3	How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?	We use many different tools depending on the necessary activities. For example, we apply multiple data center strategies (split/divide workload to different data centers; double work processes which allow for restoration in parallel).
6.	**Improvement**	
6.1	What are the most effective types of exercises, drills and tests? Why are they considered effective?	As we do not focus on retail clients, our threat profile is different. With regard to testing, we do this not only on a service level, but also on complete scenarios.
6.2	What are the major impediments to establishing cross-sectoral and cross-border exercises?	We worked in many international/European bodies: the main impediment is the overarching communication/missing single point of contact to organise e.g. for tests of overarching threat scenarios /continuous established structures to deal with issues.
6.3	Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery?	Click here to enter text.
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.	Yes, we do distinguish between "coordination" and "communication" activities. The first e.g. is aligning internally the existing views of the several business entities and the second is communicating -if agreed on how and what - towards external stakeholders in the appropriate manner.
7.2	How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident?	In some cases, we still use fax as this is legally accepted. BCM developed emergency scenarios with regard to information and communication technology (business phones, simplify devices, WebRAS, modern communication tools, evacuation working spaces etc.)
7.3	Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities?	See above with regard to reporting and sharing.