German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

FSB "Effective Practices for Cyber Incident Response and Recovery"
Consultative Document

Register of Interest Representatives (EU)
Identification number in the register: 52646912360-95

Contact:
Berit Schimm
Telephone: +49 30 2021-2111
Telefax: +49 30 2021-19 -2100
E-mail: b.schimm@bvr.de

Berlin, 20-07-17

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent approximately 1,700 banks.

Coordinator:
National Association of German Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-dk.de

Comments: FSB "Effective Practices for Cyber Incident Response and Recovery" - Consultative Document

General

General notes
The toolkit demonstrates best practices without claiming to be exhaustive. Institutions can use these identified practices for guidance and to mirror their own practices and processes.
The toolkit does not claim to meet regulatory requirements. In our opinion it should not be adapted for this purpose either, because regulatory requirements should be much more principle based to match proportionality.

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?
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 BCM scenarios and practised in tests have proven their worth.

1.2. To whom do you think this document should be addressed within your organisation?
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?
The national supervisory authorities require banks in Germany to take the design of IT systems and associated IT processes into line with current standards, e.g. ISO2700x. The emergency management of the institutions is often based on business continuity management (ISO 22301) and IT service continuity management (ISO 27031) and/or national standards.
In addition, banks use frameworks or knowledge bases, e.g. MITRE ATT&CK ("Adversarial Tactics, Techniques, and Common Knowledge") or the NIST Cybersecurity Framework to support their cyber defenses.

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 Germany 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 Broadens 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).
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?
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. 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?
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 (girocard payment system), 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?
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 institutions 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:

Comments: FSB "Effective Practices for Cyber Incident Response and Recovery" - Consultative Document

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)?
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?
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?
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?
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 laboratories 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 in integrating third-party service efforts into the organization's mitigation efforts?
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, securities 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?
Institutions 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?
Institutions 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 institutions or IT service providers complement the crisis staff exercises of the institutions on a technical basis.
In addition, 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?
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

Comments: FSB "Effective Practices for Cyber Incident Response and Recovery" - Consultative Document

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?
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 (Germany) 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.