## The Financial Stability Board (FSB) questions in consultative document for the toolkit in Cyber incident response and recovery (CIRR) activities

**Deadline for submission: 20 Jul 2020**

| ***Questions for each component*** | ***Tahoe Life Feedback*** |
|---|---|
| General | |
| 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? | Yes, as an organisation we learnt to be ever more vigilant as security incidents or pandemics can happen at any time and for prolonged periods. It is crucial that our cyber incident response and recovery practices need to be reviewed on a regular basis. |
| 1.2. To whom do you think this document should be addressed within your organisation? | Risk teams, information security team, and senior management members. |
| 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? | - We have the security incident response team (SIRT) which links the organisation's business and other senior stakeholders.<br>- We follow the NIST cybersecurity framework and make reference to San Top 20 and ISO 27001. |
| 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. | Yes, we do. Our cyber incident response and recovery is structured largely along the seven components. |
| 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). | We largely follow the listed number of tools, no additional. |
| 1.6. Based on your organisation's experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6). | Nothing more to add to the six boxes. |
| 1.7. What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities? | More proactive to case and market intelligence sharing. |
| 1.Governance | |
| 1.1. To what extent does your organisation designate roles and responsibilities asdescribed in Tool 3? Does your organisation identify these roles by business line, technology application or department? | Yes, we do and similarly. |
| 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? | We promote immediate security incident reporting in the organisation even with suspected cases.<br>We have annual security awareness training for all staff and new joiners need to complete the mandatory e-course. |
| 2. Preparation | |
| 2.1. What tools and processes does your organisation have to deploy during the first days of a cyber incident? | We have implemented SIEM and have a dedicated team to analyse the security events. |
| 2.2. Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months. | - We have adopted a number of tools to monitor the internal and external threat.<br>- In addition, we have regular security awareness training for all staff and regular security drill tests. Those exercises contribute and enhance our knowledge and response time. |
| 2.3. How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)? | Yes. We conduct third party security assesments prior to engaging vendors; and have regular performance meetings to gauge their performance and give proactive feedback. |
| 3. Analysis | |
| 3.1. Could you share your organisation's cyber incident analysis taxonomy and severity framework? | We classify by types of incident and severity level.<br>Incident type: disruption of service, social engineering, APT, malicious attacks, unauthorised access, misuse, hoaxes, multiple components.<br>Severity level: informational, low, medium, high. |
| 3.2. What are the inputs that would be required to facilitate the analysis of a cyber incident? | The impact, source of incident, process involved, and affected tools and technology. |

| *Questions for each component* | *Tahoe Life Feedback* |
|---|---|
| 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? | Currently our process is quite manual, it would be good for a list of recommended tools from FSB. |
| 3.4. What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation? | Our staff members join seminars organised by The Hong Kong Federation Insurers (HKFI) to enhance our knowledge in all areas of insurance including cybersecurity. |
| 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? | Our communication with the regulator for continous feedback.<br>Another key consideration is the restoration of the business as soon as possible and reduce the reputation risk towards the customers. |
| 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? | Tools include:<br>- FortiMail Email Security Appliance<br>- IntSights Threat Intelligent Platform<br>- Symantec Endpoint and TrendMicro Deep Security<br><br>Effective practices being: Internal policies and standards, SIEM, latest anti-virus tools & others, and incident reporting process. |
| 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? | We use the following tools for managing the third party<br>-Security risk assessment<br>-Regular Vendor assessment<br>-SLA<br>At the same time, we have the CITIC as the SOC and ATOS as our Data center to manage incident and monitor the security services. |
| 4.4. What additional tools could be useful for including in the component Mitigation? | The suggested list is quite comprehensive, nothing more to add. |
| 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 overlap. |
| 5. Restoration | |
| 5.1. What tools and processes does your organisation have available for restoration? | Back-up technology solutions, disaster recovery site, etc. |
| 5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities? | Disaster recovery plan which documents clear responsibilities and priorities based on incident severity level. |
| 5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data? | We have clear documented process which requires data domain owner sign-off. Prior to that, there is the maker and checker process with authorised staff. In addition, incidents are prioritised based on the severity rating. |
| 6. Improvement | |
| 6.1. What are the most effective types of exercises, drills and tests? Why are they considered effective? | Both are very effective. |
| 6.2. What are the major impediments to establishing cross-sectoral and cross-border exercises? | Trust, legal and different nature of business. |
| 6.3. Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery? | Artificial intelligence (AI) technology tools would help to automate the response process. |
| 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. | No, we do not, all are part of the list of activities. |
| 7.2. How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident? | We have established the call tree and also regular call tree exercise to ensure the communication channel for instant messaging.<br>Other consideration includes WeChat. |
| 7.3. Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities? | What's covered is quite comprehensive, no more to add. |