## Effective Practices for Cyber Incident Response and Recovery
## ( 2020 Consultative Document )

| Category | Item | Item Description | Reply |
|---|---|---|---|
| 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? | Enhanced the process to identify and mitigate any phishing email<br><br>Included more restricted security configuration when using video conference tool |
| | 1.2. | To whom do you think this document should be addressed within your organisation? | Head of Risk Management and AVP Risk and Control |
| | 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? | Operational Risk and Reputation Committee (ORRC) oversight of operational and reputation risks, including cyber security risk<br><br>Security Incident Management Team (headed by CTO) is defined to response and recovery cyber attack<br>Yes, NIST Cybersecurity and ISO 27001 Frameworks are using |
| | 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. | We use NIST cybersecurity framework which should be compatible to FSB Toolkit at high level<br><br>In between the "Preparation" and "Analysis" components, it may have an "Identification" component to identify if there is any area for cyber attack. It may have Risk assessment, Data security, Asset management and Identify access management (Refer to NIST Cybersecurity framework for detail)<br><br>The "Coordination and communication" component should work with "Mitigation" component together. During the mitigation, the formal communication is mandatory to update the stakeholder till resolution<br><br>Restoration could be part of Mitigation. The objective is to resume normal operation after the mitigation<br><br>The "Improvement" component is mainly post review and lesson learnt to make further enhancement. It should be the last component in the framework |

| Category | Item | Item Description | Reply |
|---|---|---|---|
| | 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). | Tools 3: Roles, responsibilities and accountabilities for CIRR<br>The roles can be extended to the incident management team from various areas, such as forensic, remediation and recovery teams<br><br>Tool 7: Human resources<br>In general, it is seldom to have internal job rotations on cyber security issue. It requires specialist to deal with the attack immediately<br><br>Task 15: Forensic capabilities<br>Instead of building own technical and forensic capabilities, more companies will subscribe professional service for forensic investigation purpose. The company may build its alert capability to identify for any cyber attack and invoke forensic investigation service upon confirmation<br><br>In between "Preparation" and "Analysis" components, it may have additional practices for "Identification" component. It may have<br>- Risk assessment<br>- Data security<br>- Asset management<br>- Identify access management<br>(Refer to NIST Cybersecurity framework for detail)<br><br>Restoration could be a part of Mitigation. Identify->Contain->Eradicate->Restore back to normal operation<br><br>Task 23: Business continuity measures<br>The KRI is pre-defined under "Preparation" component. The Eradication is execution of the KRI when exceeding the threshold<br><br>Task 24: Isolation<br>Under task 22: Containment already isolate the infected systems and task 25: Eradication is to build the clean environment to resume the operation. Hence, the isolation is already included in both tasks<br><br>Task 26 Prioritisation to Task 29 Approved restoration procedures<br>These tasks should be defined under "Preparation" component. During recovery, it is to validate and resume the normal operation after cyber security attack |

| Category | Item | Item Description | Reply |
|---|---|---|---|
| | 1.6. | Based on your organisation’s experience, please provide additional examples of effective practices listed in the boxes (e.g. Boxes 1-6). | Box 1: Example of metrics used by industry<br>Performance metrics are hard to define by incident volume. RPO/RTO is not always applied as it may not trigger BCP. It is recommended to measure by time of incident discovery, lead time to identify the cyber attack, contain, eradicate and restore the operation environment. The forensic investigation sometimes take longer and with other professional service support<br><br>Box 2: Example of internal and external stakeholders<br>CIRR should define the severity/criticality of cyber incident and inform the corresponding external stakeholders where necessary<br><br>Box 3: Example of CIRR taxonomies<br>The attack/infected period and customer impact (financial, PII) should be included<br>CIRR should define the severity category according to regulatory/company requirement and take the corresponding action defined under the framework<br><br>Box 4: Example of scope and types of test<br>There are two areas for test<br>- The readiness of CIRR team which can enhance via regular table top review and drill of "cyber attack"<br>- The readiness of operational environment via Red team and Blue team testing. Red team testing is more on the vulnerability scanning and penetration testing while Blue team testing is more on the cyber attack simulation, such as malware/virus/DDoS attack to validate the infrastructure capability<br><br>Box 6: Type of information that could be included in the cyber incident reporting to provide useful details<br>The following action should be included additionally<br>- Mitigation actions performed<br>- Lesson learnt and improvement performed<br>- Prevention or detection mechanism trigger to prevent/detect the re-occurrence in future |
| | 1.7. | What role, if any, should authorities play in supporting an organisation’s cyber incident response and recovery activities? | The authorities can examine the completeness of remediation actions taken. It can also issue regular security awareness program to draw public awareness |
| 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? | Yes, the security incident management team leaded by CTO with corresponding IT function lead to support cyber security incident. The business unit heads and senior management are involved to handle internal/external communication |
| | 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? | There is not definition for "enough" preventive action from incident occurrence. In fact, the company has lesson learnt process to keep on improving its actions to minimize the recurring of incident in future |
| 2. Preparation | 2.1. | What tools and processes does your organisation have to deploy during the first days of a cyber incident? | There is a defined processes under security incident management policy<br>Identify & Triage -> Analyse -> Contain -> Eradicate -> Restore |
| | 2.2. | Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months. | We have started the 24x7 SOC service (via Ensign) to monitor all critical firewall/servers activities. We shall receive alert whenever any suspicious traffic is found |
| | 2.3. | How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)? | The similar SOC service are setup for various service providers, such as Tencent Cloud and Aviva Group. We shall also receive alert whenever any suspicious traffic is found |
| 3. Analysis | 3.1. | Could you share your organisation’s cyber incident analysis taxonomy and severity framework? | The information needed for each incident is likely to include:<br>• Unique reference number<br>• Incident Priority<br>• Date/time recorded<br>• Descriptions of symptoms<br>• Name/department/phone/location of user<br>• Application Name<br>• Incident Urgency<br>• Incident Impact<br>• Line of Business<br>• Incident Support Team |

## Effective Practices for Cyber Incident Response and Recovery
## ( 2020 Consultative Document )

| Category | Item | Item Description | Reply |
|---|---|---|---|
| | 3.2. | What are the inputs that would be required to facilitate the analysis of a cyber incident? | Those items under 3.1<br>Firewall and servers log information |
| | 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? | Firewall and servers log with SOC (IBM QRadar)<br>Akamai/Checkpoint with Threat Prevention feature<br>Nexpose to validate the fixing of the vulnerabilities<br>Forensic analysis professional service will be under on need basis |
| | 3.4. | What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation? | The Hong Kong Federation of Insurers. We regularly receive updates about topics that are of interest to insurers in Hong Kong. |
| 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? | Add-on alternatives, such as better firewall feature, virtual patching, reverse proxy |
| | 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? | i) Symantec DLP,<br>ii) Access restriction, database access protection<br>iii) Sophos endpoint security, Cisco AMP for Endpoint |
| | 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? | Service level meeting to review all related incident with mitigation effort till completion<br>Workflow software (such as IBM OpenPages) to record any issue and timely review |
| | 4.4. | What additional tools could be useful for including in the component Mitigation? | Veeam backup and replication solution |
| | 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. | Not applicable |
| 5. Restoration | 5.1. | What tools and processes does your organisation have available for restoration? | Veeam backup and replication solution |
| | 5.2. | Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities? | The prioritization of restoration activities is defined based on the application criticality and also the RPO and RTO requirements |
| | 5.3. | How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data? | Veeam backup and replication solution has defined the backup versioning |
| 6. Improvement | 6.1. | What are the most effective types of exercises, drills and tests? Why are they considered effective? | Yes,<br>Tests can verify the integrity in more frequent, while drill can only be performed annually. Both of them are required |
| | 6.2. | What are the major impediments to establishing cross-sectoral and cross-border exercises? | The data will be stored offshore while it is not mandatory for local based company |
| | 6.3. | Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery? | SSL VPN which provide more virtual connection from business users to support verification<br><br>Zoom with remote access to connect oversea forensic analysis professional to assist in the cyber security incident |
| 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. | Task 41 (Timely escalation), Task 42 (Regular updates with actionable messages) and Task 43 (Cross-border coordination) are coordination activities which are helping to complete the mitigation<br><br>Task 44 (Trusted information sharing), Task 45 (Trusted communication channels) and Task 46 (Cyber incident reporting) are grouped as communication with authority and internal/external stakeholders on the security incident in a timely manner |
| | 7.2. | How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident? | The company will switch to Microsoft M365 which to prevent the shutdown of traditional communication channels during cyber incident or disaster |
| | 7.3. | Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities? | The company will share the mandatory information only. Additional information will be provided subject to the request from authorities and the availability of the other information |