Blue Cross Insurance

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?

During the COVID-19 pandemic outbreak, we adopted tools to do online meeting and remote access to facility work from home arrangement. We see many incidents from news feed related to such tools. We then re-assessed the security robustness of the tools we are using and issued internal guideline to our staff to follow best practices while using the tools. Examples include verifying participant identity before starting the meeting and set password for joining online meetings etc. We also issued guideline for staff who need working from home. Examples include setting home wifi password, installing proper anti-virus software for home computers etc. Apart from that, we also heard many companies received phishing emails related to COVID-19. Therefore, when new threats are emerging during this period, we need to have a channel to quickly collect information, prepare control measures and update the information to our staffs frequently. We also need to have a communication protocol to quickly collect information from our staffs while they are not in office.

1.2. To whom do you think this document should be addressed within your organisation?

This document should first be addressed to the IT information security team, emergency response team, risk management team and business continuity team.

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 Company's cyber incidents are handled according to the assessment of business impact, which is determined by number of affected customers, financial loss, potential reputational loss, duration of outage of critical systems, whether the incident is caused by internal fraud, or involves any data breach or violation of regulations. The recovery of affected systems is prioritized by the Recovery Time Objective (RTO) defined in the Business Impact Analysis (BIA) by various business departments in the Company.

The Company follows NIST Cybersecurity Framework for incident response and recovery.

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 Company established the Incident Management and Response Guideline with the overall management framework for all types of incidents including cyber security incidents, including roles and responsibilities of different stakeholders, impact assessment of incidents, reporting and communication channels with internal and external parties. Details of response and recovery processes for cyber incidents are documented in a separated

Technology Related Incident Response and Escalation Procedure and Business Continuity Plan (BCP).

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).

Tool 44: Trusted information sharing.

- Organizations that shared information on cyber incidents should be anonymized in the sharing platform, to avoid giving audience a perception that they are susceptible to certain vulnerabilities or cyber attacks.

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: Examples of metrics used by industry

- Metrics to measure impact of a cyber incident
  - Reputational loss
  - Penalty by regulators
  - Potential legal actions by affected customers against the Company
  - Whether the incident is a criminal offense or not
- Performance metrics for incident management
  - Number of cyber security incidents causing financial loss exceeding the threshold

Box 2: Examples of internal and external stakeholders

- Internal stakeholders
  - Risk management team
- External stakeholders
  - Business partners

Box 3: Examples of CIRR taxonomies

- Information to be used when describing cyber incidents
  - Describe the current state of incident (e.g. identified, contained, isolated, eradicated)
  - Describe the scope of impact (e.g. on specific host, limited number of hosts in certain network segments, all computers in the corporate network)

Box 4: Examples of scope and types of test

- Table-top drill to test the preparedness of the Emergency Response Team to react when a cyber incident occurs

Box 5: Examples of information that could be shared

- Impact of incident

Box 6: Type of information that could be included in the cyber incident reporting to provide useful details

- Lesson learnt

1.7. What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?

Authorities can support the Company's cyber incident response and recovery activities by providing guidance of proper collection and preservation of digital evidence that are essential in forensic investigations and future litigation process.

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 Company defined the roles and responsibilities of different internal stakeholders in the Emergency Response Team, including the decision maker, commander, business departments responding the incident, contact points for internal and external communications (e.g. media spokesperson) and incident reporting. However, independent observers are only appointed during annual cyber attack drills. There is nobody in the Company having the observer role during actual incidents.

The Company identifies these roles by department.

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?

The Company promote timely reporting of cyber incidents by regular staff awareness education. As a respect of privacy, the name of employee reporting an incident will not be disclosed.

2. Preparation

2.1. What tools and processes does your organisation have to deploy during the first days of a cyber incident?

Once a cyber incident has been identified, event logs of affected systems are extracted and analyzed by IT to determine the impact of the incident. IT may engage external consultants for professional advice of incident response and digital evidence preservation to support forensic investigations.

2.2. Please provide an example of how your organisation has enhanced its cyber incident response plan over the last 12 months.

The Company has enhanced the remediation procedures in cyber incident response playbook of phishing attacks after improvement areas were identified in the cyber-attack table-top drill last year.

2.3. How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)?

The Company monitors the risks stemming from service providers by regular assessment of their internal controls through questionnaires, interviews or site visits, in accordance to the Company's third party management procedure. For any findings with the risk above the Company's acceptable level, the Company will discuss with service providers for improvement actions in order to mitigate the risk. Any overdue remedial actions mitigating third-party risks are reported to senior management.

3. Analysis

3.1. Could you share your organisation's cyber incident analysis taxonomy and severity framework?

A cyber incident is analyzed according to the type of incident, the actors and route of cyber attack; while its severity is determined by:

- estimated number of affected customers,
- negative media coverage affecting the Company's image,
- duration of disruption on critical systems,
- whether the incident is an internal fraud,
- whether the incident involves data breach,
- whether the incident cause non-compliance with regulatory requirements, and
- estimated financial loss to the Company or customers.

3.2. What are the inputs that would be required to facilitate the analysis of a cyber incident?

System and transaction logs, symptoms reported by affected users and cyber threat intelligence information are required for analysis of a cyber incident.

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?

Red team exercises are useful to test an organization's capability to respond to cyber incidents and the effectiveness of the incident response plan. The effectiveness of recovery activities can be tested by regular disaster recovery drills.

The severity, impact and root cause of cyber incidents can be analyzed by referencing historical events of similar incidents happened in the organization.

3.4. What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation?

The Company subscribed several cyber threat intelligence sources with the latest cyber threat or incident information shared by regulators, vendors and Computer emergency Response Team (CERT). The Company is benefited by learning from cyber incidents in other companies to get better prepared for similar incidents that may happened in the Company.

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?

Validation after implementation of the mitigation measures and monitoring the security event logs are also important to ensure a cyber incident is properly handled, contained or eradicated in the mitigation phase.

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?

The Company activates the containment and isolation measures, such as blocking malicious network traffic by firewall rules, blacklisting malware hashes by anti-virus or anti-APT solution, or temporarily switching off the affected machines, to mitigate the impact to business from data breaches, loss of data integrity and ransomware infection.

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?

Having a good understanding of the roles and responsibilities of third-party service providers in incident response and handling and a clear communication channel with service providers would be effective to save the efforts of the Company and service providers in mitigating the impact of a cyber incident.

4.4. What additional tools could be useful for including in the component Mitigation?

Monitoring the effectiveness of mitigation measures could be useful to ensure a cyber incident is properly handled, contained, isolated or eradicated, and the situation would not get worse.

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, the mitigation and restoration activities of the Company are performed sequentially.

5. Restoration

5.1. What tools and processes does your organisation have available for restoration?

The Company follows the restoration procedures defined in the BCP to restore the systems impacted by cyber incidents. Impacted systems are recovered by restoring from offsite data backups stored in third party service providers that have no direct network connection with the Company. Recoverability of data backup is tested regularly to ensure the impacted systems can be recovered when needed.

5.2. Which tools, plans, practices and metrics does your organisation use to prioritise restoration activities?

The Company prioritizes the restoration activities according to the criticality of systems and their RTOs defined in the BIA by business departments, which are reviewed by system owners annually.

5.3. How does your organisation minimise undesirable outcomes of restoration activities, such as restoring affected data?

The Company performs data restoration tests to ensure the integrity of data backups and the recoverability of affected systems while the data of unaffected systems are not corrupted by the restoration activities.

6. Improvement

6.1. What are the most effective types of exercises, drills and tests? Why are they considered effective?

Red team exercise is the most effective to test the effectiveness of the incident response program that covers all people, technologies and processes involved in the incident response and recovery processes, under simulated cyber attack scenarios. It provides organizations a better visibility on the deficiencies in their incident management framework.

6.2. What are the major impediments to establishing cross-sectoral and cross-border exercises?

Variance of regulations between different sectors or countries drive different incident response and recovery requirements in different business units. It is a challenge for large organizations, especially with cross-sector or cross-border business operations, to establish a company-wide incident management program.

6.3. Which technological aids and tools does your organisation consider most useful to improve cyber incident response and recovery?

Honeypots and sandboxes would be most useful technologies for the Company to analyze the pattern of cyber attacks and the capability to detect and respond to such incidents.

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.

Communication refers to information exchange between different parties, while a "coordinator" defined in the Company's incident response framework refers to a focal point who manages the flows of messages to be communicated between different parties.

7.2. How does your organisation address the possibility that email or traditional communication channels will be unavailable during a cyber incident?

In case of unavailability of email or other traditional communication channels during a cyber incident, short message service ("SMS") or WhatsApp message will be used as an alternative channel for internal reporting based on emergency contact list of the Company.

7.3. Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities?

Lesson learnt from incident by the Company would be useful for other organizations in the industry to prevent similar incidents from happening or prepare themselves for a better handling of similar incidents in future.