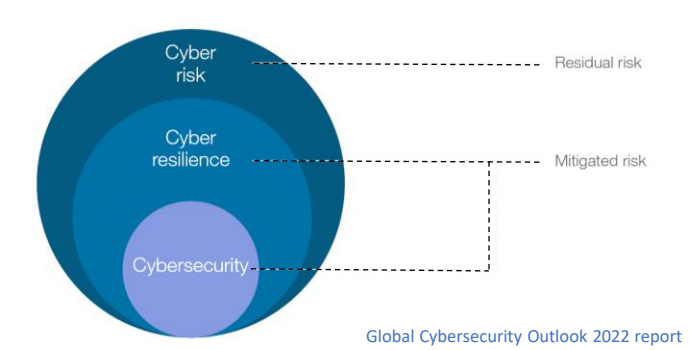
Cyber Risk, Cyber Resilience, Cybersecurity?

Arising from the COVID-19 pandemic, companies are forced to accelerate digitalization of operations, such as adapting to E-meetings, novating into E-commerce and remote working or colloquially termed WFH (Working From Home).

As digitalization advances, so does cybercrimes. Technology in one way or another is vital in our professional and personal lives. However, many of us including companies might be lacking in the department of being "cyber-safe". Based on a survey from the Global Cybersecurity Outlook 2022 report published by the World Economic Forum, 2 out of 5 organisations surveyed had been affected by a 3rd party cyber incident and more shockingly, 6% surveyed were not even aware if they were victims of a cyberattack.

On 31 Oct 2022, Singapore Exchange Regulation ("SGX RegCo") published a Cyber Incident Response Guide ("Guide"), which sets out considerations and good practices that companies can adopt in preparing and operationalising their own Cyber Incident Response Plan which we will discuss below.

Relationship between cyber risk, cyber resilience and cybersecurity



Global Cybersecurity Outlook 2022 report

Cyber Resilience

IT

Organization's capacity to anticipate, respond to and recover from cyber threats

Cyber Security

System & Data Protection

SGX RegCo's Guide on having a Cyber Incident Response Plan

1 Governance for Cyber Resilience

Management should consider various functions across the company that would be involved in handling a swift and effectively response to a cyber incident.

This would form the company's Crisis Management Team ("CMT") and Cyber Incident Response Team ("Cyber IRT") that would be activated in the event of a cyber incident.

Crisis Management Team

Key Decision Makers during a cyber incident

- Should consist of senior management, including C-suite executives and Heads of Departments of all relevant functions
- CMT should be activated based on a structured approach, assessing the scope and severity of the incident. Companies may opt for a phased approach in involving CMT

Cyber Incident Response Team

Executioner of decisions made by CMT

- Should consist of key representatives from all relevant functions
- Responsible for updating CMT on the incident
- Companies can also consider engaging third party service providers that support the company in respect of the incident

2 Cyber Response Procedures (PDRP)

Cyber Response Procedure	Description
Preparation	• Companies can take pre-emptive actions to prepare effective cyber crisis management plans. • This involves development, testing and validation of plans for incident handling preparation or incident prevention.
Detection and Analysis	• Companies should develop procedures for detection and validation of the type of incident. • An analysis of the cyber incident can be performed on the basis of its applicability, relevance and criticality to their IT environment. • Depending on the nature and complexity of their business and IT environments, companies should assess whether there are additional considerations to take into account or additional scenarios they may be susceptible to.
Remediation: Containment/ Eradication/ Recovery	• Based on the findings in the Detection and Analysis phase, companies are able to prepare their incident response plans accordingly. • This includes the procedures to contain and remediate affected areas of the IT environment and actions to contain data breaches, if any.
Post-Incident	• Through the post-incident review, the company can adopt a holistic approach in identifying risk and vulnerabilities in their IT environment and corresponding measures to strengthen their response plans.

3 Having a Crisis Communication Plan

Having a Crisis Comms Team

- Companies can consider forming a Crisis Communication Team ("CCT") that develops/ maintains communication templates, as well as to activate, approve and execute the Crisis Communication Plan during cyber incidents.

Stakeholder Identification

- Companies can identify internal and external stakeholders' point of contact, alternative contacts and document their respective channels of communication. This ensures that the Crisis Communication Plan, information and any updates are disseminated to all relevant parties on a timely basis.

Logistics

- Companies may wish to document in the Crisis Communication Plan: the timeline for the activation of the CCT and follow-up actions to the announcement of the cyber incident. This is to ensure clarity in operations and consistency across the company.

Communication and Engagement

- Companies could consider defining triggers for the activation of the CCT, with reference to the scope and severity of the incident.
- To mitigate reputational risk, companies should obtain details of the incident to confirm the content of messaging to stakeholders, when and how the messaging should be disseminated.
- Timing of external communication would depend on the nature and complexity of the incident and impact to stakeholders. Should companies require more time to investigate, companies could issue a holding statement to acknowledge the issue and assure stakeholders that further updates can be expected when information is available.
- Subsequent updates would keep stakeholders informed and provide closure once investigations have concluded. This would be important to stakeholders who are directly affected by the cyber incident and require prompt assistance. Relevant listing rule obligations on material cyber incidents and updates are illustrated below:

SGX Mainboard Rules Appendix 7.1, Para 23/ SGX Catalist Rules Appendix 7A Para 25

- There is a requirement to disclose the occurrence of cyber incidents via SGXNet if they are material (specifying the maximum impact of the cyber incident)

SGX Mainboard Rules Practice Note 7.1, Para 5.5/ SGX Catalist Rules Practice Note 7A Para 5.5

- The extent of the disclosure is dependent on the materiality of the incident, including the financial impact to ensure that the public can continue trading on an informed basis
- If the company is of the opinion that the status of the incident is unclear, the companies should consider halting or suspending trading until there is greater clarity to be provided

- Companies can engage 3rd party service providers to obtain reports and analyze any relevant news on social media platforms. This allows companies to be apprised of potentially harmful narrative so that early intervention can take place.
- To ensure that a stakeholder notification process is in place, companies should notify all relevant stakeholders and respond to any form of queries. A sample of internal process flow for stakeholder notification can be as follows:

Sample: 10-step Internal process flow for stakeholder notification

Step 1: Triggers for stakeholder notification
Step 2: Who to prepare communications
Step 3: Sources to obtain information from
Step 4: Information to be included in communications
Step 5: Statement of communication (e.g. holding statement, interim updates)
Step 6: Modes of updates/dissemination (e.g. website updates, email, SMS)
Step 7: Stakeholders to update/disseminate communications to
Step 8: Who to review and approve communications before dissemination
Step 9: When to update / disseminate communications
Step 10: Who to perform update / disseminate communications

Content and Messaging

To manage reputational risks that may arise from cyber incidents, companies should assess and communicate the impact of the incident on their financials, operations and customers. Companies may wish to develop key lines of messaging for each cyber scenario, and review them from legal, reputational and financial impact perspectives to ensure clarity is provided to the stakeholders.

Useful References:

SGX RegCo Cyber Incident Response Guide (Please see here)
Sharing on Cyber Incident Response Guide for ListCos (Please see here)
Global Cybersecurity Outlook 2022 report from the World Economic Forum (Please see here)

Please Contact or Find us at:

SAC Capital Private Limited
1 Robinson Road, #21-00 AIA Tower
Singapore 048542
Telephone: (65) 6232 3210
Fax: (65) 6232 3244
www.saccapital.com.sg