Legal Clinic – Cyber Risks and Civil Liability

Webinar with ISCA on 23 July 2020

Sharon Lin
Partner, Litigation & Arbitration

Withers KhattarWong LLP

About the Speaker (Civil and Regulatory Liability)

- More than a decade in litigation practice
- Advised and acted as counsel in various professional negligence/ indemnity and liability disputes in related civil proceedings and mediation/ arbitration, as well as in investigatory/ disciplinary proceedings across key professional practices

Sharon Lin
t +65 6238 3364
e sharonlin@witherskhattarwong.com
Partner, Litigation & Arbitration
Withers KhattarWong LLP

Roadmap

- Cyber liability insurance and its coverage
- What to do when faced with a civil or regulatory claim
- Case studies

Disclaimer:

The information provided in these slides and this presentation does not, and is not intended to, constitute professional legal advice. All information, content and materials are available only for general informational purposes only. The author assumes no responsibility or liability for any errors or omissions in the content of these slides. Proper legal advice should be sought in respect of any particular legal matter.

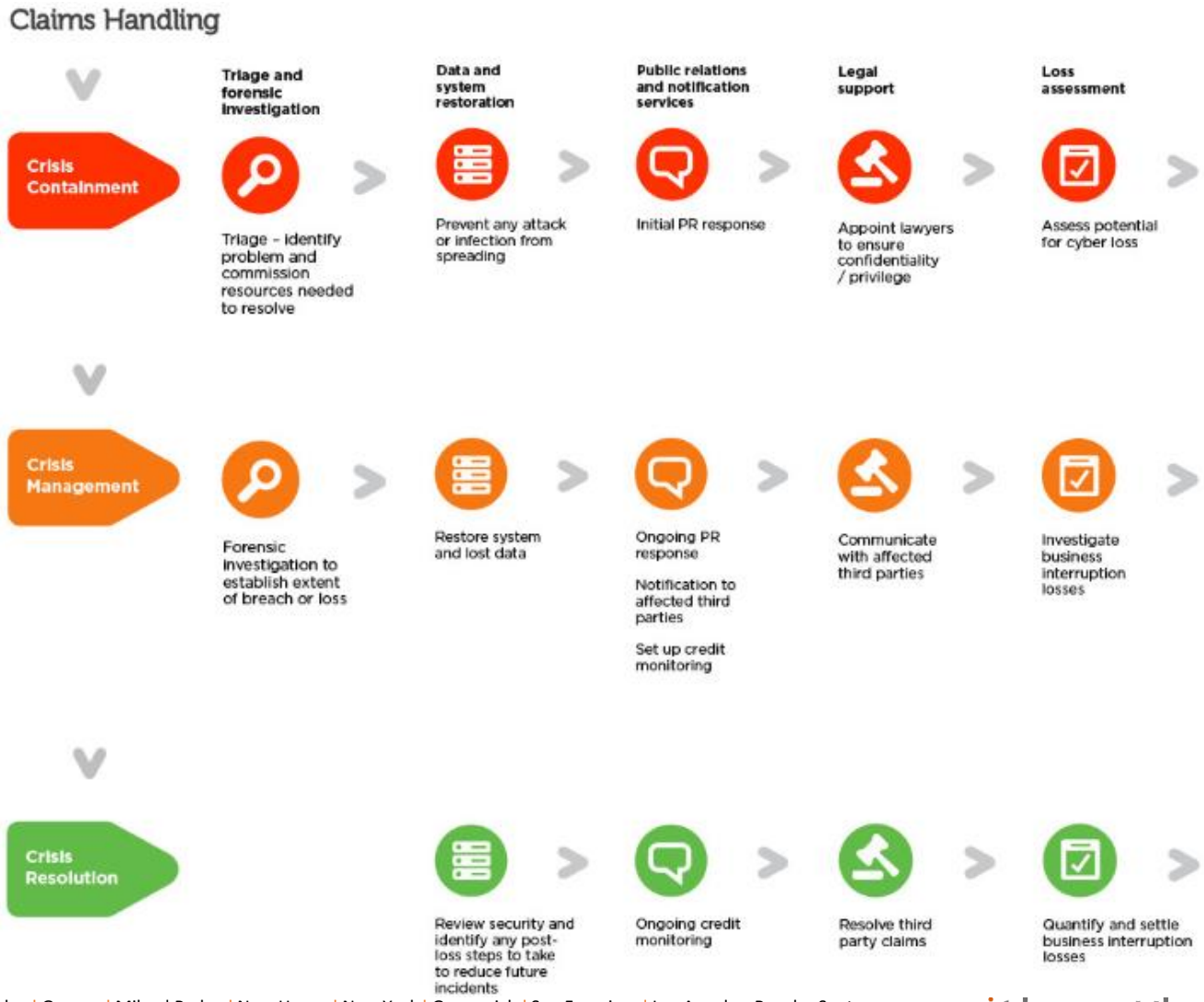
Cyber Liability Insurance and its Coverage

What is Cyber Liability Insurance

- Generally, protection against third party liability and costs associated with cyber risk exposure and/ or recovery after cyber-related security breaches or similar events
    - e.g. sensitive data breach, computer hacking, dumpster diving, computer viruses, pilferage of information, security failures, business interruption and identity theft etc.
- Coverage varies for different policies offered by different insurers

Main coverage of a policy

Source: Delta Insurance (https://deltainsurance.sg/cyber-risk-management/claims-handling-2/)



Main coverage of a policy

- **Crisis Containment/ Management**
  - Data Forensic Expenses
  - Breach Consultation Costs
  - Costs to Restore
  - Breach Response Services
  - Public Relation Expenses
- **Business Interruption Costs**
- **First party Coverage**
  - Hacker Theft Cover
  - Network Extortion Coverage
  - Loss Adjustor Costs

Coverage is subject to applicable exclusions, limits of liability, policy excess and other terms of the policy.

Main coverage of a policy

- **Third Party Liability**
  - Third Party Liability
  - Regulator Liability
  - Investigation Liability
  - Payment Card Industry Data Security Standard ("**PCI DSS**") Cover
  - Consumer Redress Fund
- **Automatic Extensions**
  - Emergency Costs, Loss Mitigation Costs, Network Improvement, Personal Reputation Cover, Network Failure

Coverage is subject to applicable exclusions, limits of liability, policy excess and other terms of the policy.

Facing a Civil or Regulatory Claim

Condition precedents under a policy and general tips

Some condition precedents for policy coverage

- **Written Notice**: Written notice must be given to the underwriters of the policy about any claim made against the insured or any matter for which coverage is provided under the policy *as soon as practicable* after an executive officer first becomes aware of such claim or when such matter first arises
  - Either by certified mail/ prepaid courier to address stated in the Schedule of the policy; or
  - By electronic mail to e-mail address listed in the Schedule of the policy
- **No Admission of Liability without Prior Consent**: Without the prior written consent of the underwriters of the policy, the insured shall not admit or assume any liability, enter into any settlement agreement, or consent to any judgment or incur any legal fees or any other amounts covered under the policy

General tips when facing or in anticipation of a claim

- Take immediate step to contain the breach
- Preserve the evidence
- Alert your company's appointed Data Protection Officer
- Notify your insurers/ broker
- Consult a lawyer to obtain preliminary legal advice

Case studies

(1) Singapore Health Services (SingHealth) and Integrated Health Information Systems (IHiS) [2019] SGPDPC 3

FACTS :

- Cyber attack on Singhealth patient database system, resulting in personal data of 1.5 million patients and outpatient prescription records of nearly 160,000 patients exfiltrated
- Attacker gained initial access to the database system in August 2017 by infecting a user's workstation, likely through an *email phishing attack*, which led to customized malware and hacking tools subsequently being installed and executed on the user's workstation – to gain subsequent remote access to and control of other workstations
- PDPC found that IHiS failed to take adequate security measures to protect personal data in its possession; financial penalty: **$750,000**
- PDPC found that SingHealth as the owner of the patient database system, did not have personnel handling security incidents who were familiar with the incident response process, but were instead overly dependent on IHiS. They also failed to understand and take further steps to understand the significance of the information provided by IHiS after it was surfaced; financial penalty: **$250,000**

TAKEAWAYS:

- Even if organisations delegate work to vendors/ intermediaries, organisations as data controllers/ owners must still take responsibility for the personal data that they have collected from their customers
- Importance of having strong cyber defence capabilities, as well as personnel handling security incident to be familiar with incident response processes, including taking further steps to investigate and understand reports on suspicious activities
- Highest financial penalty imposed by PDPC to-date: given that it was the largest breach experienced, and the sensitive and confidential nature of the patients' data

(2) Horizon Fast Ferry [2019] SGPDPC 27

FACTS :

- Complainant informed PDPC that by entering her passport number in the booking form on the organization's website, her name, gender, nationality, date of birth and passport expiry date were automatically populated in the corresponding fields on the form on the booking site without any requirement for further authentication.
- In May 2017, the organization had engaged an independent contractor *informally* to revamp its booking site, specifically to improve the user interface and user experience. Unbeknownst to the organization, the contractor replicated the auto-retrieval and auto-population feature (previously only used in the internal system) in the booking site as part of the website revamp.
- Organisation failed to conduct proper user acceptance tests before launching the revamped booking site, and was thus not aware of the function until it was notified by the complainant.
- At the time of the investigation, there were a total of 444,000 personal data sets stored in the organization's database.
- PDPC found a blatant disregard for its data protection obligations, as among other things, it did not designate any individual to be its data protection officer; financial penalty: **$54,000**

TAKEAWAYS:

- Importance of designating a DPO to be responsible in ensuring the organization's compliance with the PDPA
- Importance of having internal guidelines setting out actual practices or processes to protect personal or sensitive data in the organization's possession
- Importance of emphasizing need for personal data protection to IT vendors/ intermediaries, by making it part of their contractual terms and/ or setting out clearly the responsibilities of the IT vendors with respect to PDPA

Thank you.

Q & A Session