AIMA Hong Kong Seminar: Cyber Security
30 January 2019

AIMA

THE ALTERNATIVE INVESTMENT MANAGEMENT ASSOCIATION

Opening Remarks:

Ling Ho, Partner, Clifford Chance

AIMA

THE ALTERNATIVE INVESTMENT MANAGEMENT ASSOCIATION

AIMA Hong Kong Seminar: Cyber Security

30 January 2019

Panellists:

Daniel Kolbe, Founder & Managing Director, ITCS Group Limited

Carolyn Camoens, Managing Director, Asia, Hume Brophy

Lijun Chui, Counsel, Clifford Chance Pte Ltd

Linden Reko, Client Manager for Cyber Practice Asia, Marsh Singapore

William Wong, Consultant, Clifford Chance Hong Kong

Vishal Lanjekar, Principal Consultant & Lead, Mandiant Services, Hong Kong, Macau, & Taiwan, FireEye

Moderator: Kher Sheng Lee, Managing Director and Co-Head of APAC, AIMA

AIMA

THE ALTERNATIVE INVESTMENT MANAGEMENT ASSOCIATION

AIMA

THE ALTERNATIVE INVESTMENT MANAGEMENT ASSOCIATION

AIMA Cyber Security Resources

Cyber Security Resources

The resources included below and within each of the linked documents are a sample of the available resources. Other resources are also available. Appearance of a resource in these documents should not be taken as a representation or warranty of fitness for any purpose and users must make their own judgments about whether to use any of the resources linked through the documents included in the resources below.

Cyber Security Resource

AITEC-AIMA DDQ Change Tracker 2016 v 2019

DDQ TOOLS
CYBER SECURITY RESOURCE

AITEC-AIMA DDQ for Vendor Technology and Cyber Security (Long Form) (2019)

OTHER DDQS
CYBER SECURITY RESOURCE

AITEC-AIMA DDQ for Vendor Technology and Cyber Security (Short Form) (2019)

OTHER DDQS
CYBER SECURITY RESOURCE

Guide to Sound Practices for Cyber Security 2.0

AIMA GUIDES TO SOUND PRACTICES
CYBER SECURITY RESOURCE

Cyber Security Checklist

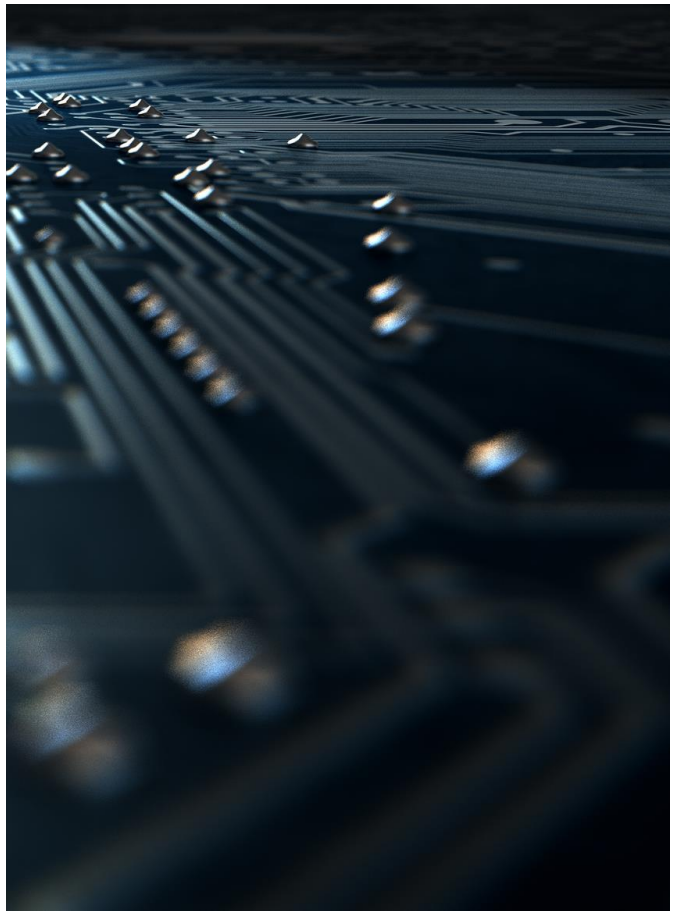
CYBER SECURITY RESOURCE

Sample Personal Security Guidelines Presentation

CYBER SECURITY RESOURCE

Cyber Scenario – Health Warning

- The following slides represent a fictional (yet plausible) scenario.
- You will be provided with incomplete information about a possible incident, just like you would have in a real life incident.



Cyber Scenario

- The scenario involves a fund manager, **Fragrant City Capital (FCC)**.
- FCC is based in Hong Kong and has offices in Singapore, China and London.
- It has a cybersecurity plan and an Emergency Management Team (EMT).

- Late one Tuesday afternoon, an individual arrives at FCC's premises in Hong Kong and says that the building management has sent him to check a problem with the air-conditioning system in the office.
- He asks the receptionist if she has noticed any problems with the air-conditioning system and asks to enter the premises to check.
- He further asks to enter the server room to check the air-conditioning system there. He says that it will take a while to complete the checks and is left alone in the server room for a substantial period of time.
- He eventually leaves the office premises and says that no further action or follow-up is needed.

Cyber Scenario

Several weeks later, Julia Chan, a portfolio manager with FCC based in Hong Kong, notices that the firm's algorithmic trading strategy has suddenly become less effective.

She speaks to the traders and contacts Eddie Lau, the Chief Technology Officer in FCC, about the delays.

After some informal investigation, they discovered an unexpected lag time between when they were issuing trade orders and when those orders were executed. The delays ranged from hundreds of microseconds to the low-single-digit milliseconds.

Question 1

What else should Eddie do to investigate the delay?

Cyber Scenario

While investigating the delay, Eddie and his team detects suspicious behavior on the FCC computer network—files being moved on the system in ways that couldn't be explained by normal business operations.

FCC activates its EMT.

Question 2

Should the EMT have been activated at this point?

Cyber Scenario

As the investigations are underway, Julia suddenly receives the following email from an entity called "Ace Consulting":

"**Your important files have been encrypted: photos, videos, documents etc. Here is a complete list of encrypted files, and you can personally verify this.**

Encryption was produced using a unique public key RSA – 1234 generated for this compute. To decrypt the file you need to obtain the private key."

"The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files..

To obtain the private key for this computer, which will automatically decrypt files, you need to pay XXX USD.

Click <<NEXT>> to select the method of payment."

Cyber Scenario

Question 3

Would you pay the "consultant"?

Question 4

Would you involve law enforcement?

Cyber Scenario

Before a decision is made as to whether to pay the ransom, a junior trader who was assisting with the investigation, sends an email to several of his closest colleagues. His email reads:

"This is terrible! Julia's computer has been hacked!!! This is on top of all the funny things going on. I can't believe we waited this long to do anything – now we have a MASSIVE BREACH on our hands! I'm very worried…. Is the fund going down?"

Question 5

What can be done about the unhelpful email sent by the junior trader?

Cyber Scenario

The team finds that malware had been inserted into FCC's servers and programmed to insert a random lag into the firm's order entry system of just a few milliseconds. The malware also recorded the details of those orders.

In addition, they find that it is not just Julia's computer which has been compromised. The computers of 3 other employees who frequently work with Julia have also been breached, and data stolen from their computers.

The employees include:

(1) **John Goldsmith**, an execution trader, who works very closely with Julia. He is also based in Hong Kong.

(2) **Rebecca Lai**, an investor relations manager whose clients include several high net worth individuals resident in London and China.

(3) **Devi Saram**, a research analyst who has been working on a new trading strategy and was going to present the new strategy to Julia in about two weeks' time.

There are 10 other employees in Hong Kong whose computers and emails have not been investigated. Employees of FCC in the other jurisdictions total 60.

Cyber Scenario

Question 6

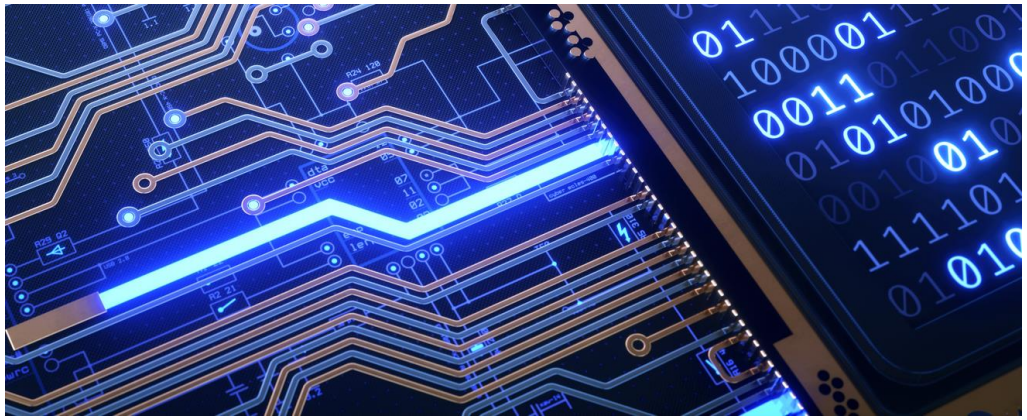
Should a review of the content of all the computers of FCC's employees be undertaken?

Question 7

Should any regulators be notified at this stage?

Question 8

Should any investors be notified?



Cyber Scenario

The decision is taken to review the contents of the computers for **all** employees of FCC. The review takes approximately XX days to complete.

It is established that the computers of a total of 6 employees have been compromised. The data copied out from the network includes:

1) Some, but not all, of FCC's trading algorithms which these employees had access to.
2) Client data of approximately 5 institutional investors in USA, 8 HNW individuals resident in London and 23 HNW individuals resident in China.
3) The access details for FCC's trading account with the funds' prime brokers.
4) The details for 3 of FCC's bank accounts with Goliath Bank in Hong Kong, Singapore and China.

Cyber Scenario

Question 9

Which of the parties should be notified?

(A) The affected institutional investors

(B) The affected HNW individuals

(C) The prime brokers

(D) Goliath Bank

(E) Regulators in US, Singapore, Hong Kong, China and England

(F) All of the above

Question 10

When should the affected institutional investors and HNW individuals be notified, and how should they be notified?

Cyber Scenario

It is discovered that the breach was perpetrated by a disgruntled former employee, Lucius Draco. He was let go for underperforming and had master-minded the entire attack to get back at the fund manager.

It turns out that he had arranged for that individual to use a USB drive to install a rootkit on FCC's servers while in the server room.

FCC, with the help of local law enforcement, manages to track Lucius down. He is arrested and currently in remand.

Question 11

What actions can FCC take against Lucius Draco?

Cyber Scenario

FCC has mostly concluded its remediation efforts, although **certain vulnerabilities still exist**.

In addition, notification letters have been sent out to investors, counterparties and regulators, as appropriate.

After receiving the notifications, several HNW investors sent letters demanding compensation for the compromise of their information. They have not yet commenced formal legal proceedings.

Regulators receiving a notification letter contact FCC with follow up inquires.

The Chinese regulator CSRC requests documents from FCC regarding the incident, including communications in the immediate aftermath of the breach.

Additionally, the Hong Kong SFC asks for information regarding FCC's remediation efforts to ensure the underlying vulnerabilities have been addressed and no longer exist.

Cyber Scenario

Question 12

How should FCC respond to the Chinese regulator's request for documents?

Question 13

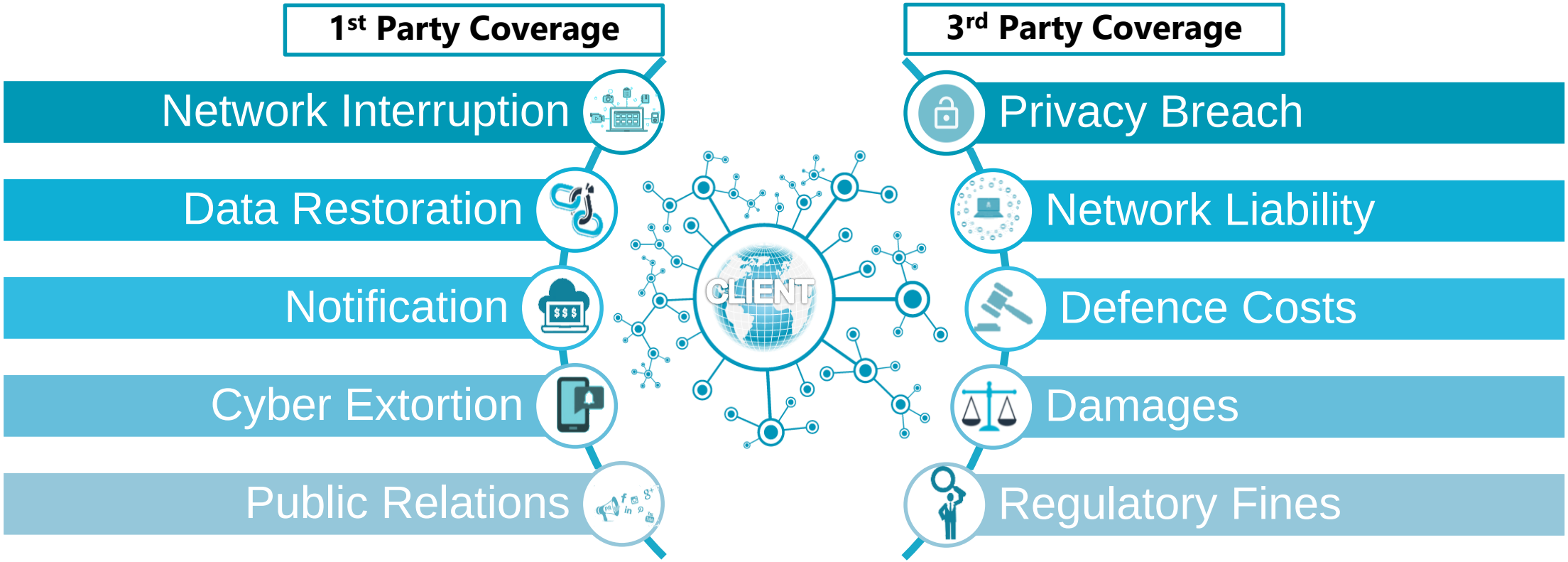
How should FCC address the Hong Kong regulator's concerns regarding remediation given there are still some existing vulnerabilities?

AIMA

THE ALTERNATIVE INVESTMENT MANAGEMENT ASSOCIATION

Cyber Insurance

Cyber Coverage Overview
Scope Of Cover



The above represents cyber insurance in a broad context for presentation purposes and does not guarantee any indemnities or warranties.

Please refer to the insurers terms and conditions for coverage.

First Party Cyber Coverages

COVERAGE	DESCRIPTION	COVERED COSTS
Network Business Interruption	Interruption or suspension of computer systems due to a network security breach. Coverage may be limited to security attacks or broadened to include general system failure.	▪ Loss of income. ▪ Costs in excess of normal operating expenses required to restore systems. ▪ Forensic expenses to value a loss. ▪ May include contingent business interruption as well.
Data Restoration	Costs to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed by a cyber attack.	▪ Restoration of corrupted data. ▪ Vendor costs to recreate lost data.
Event Management/Breach Response	Costs resulting from a network security or privacy breach.	▪ Forensics. ▪ Notification. ▪ Credit monitoring. ▪ Call center. ▪ Public relations. ▪ Sales discounts.
Cyber Extortion	Threat to compromise network or data if ransom not paid.	▪ Forensics and related investigation costs. ▪ Costs to negotiate and pay any ransoms demanded.

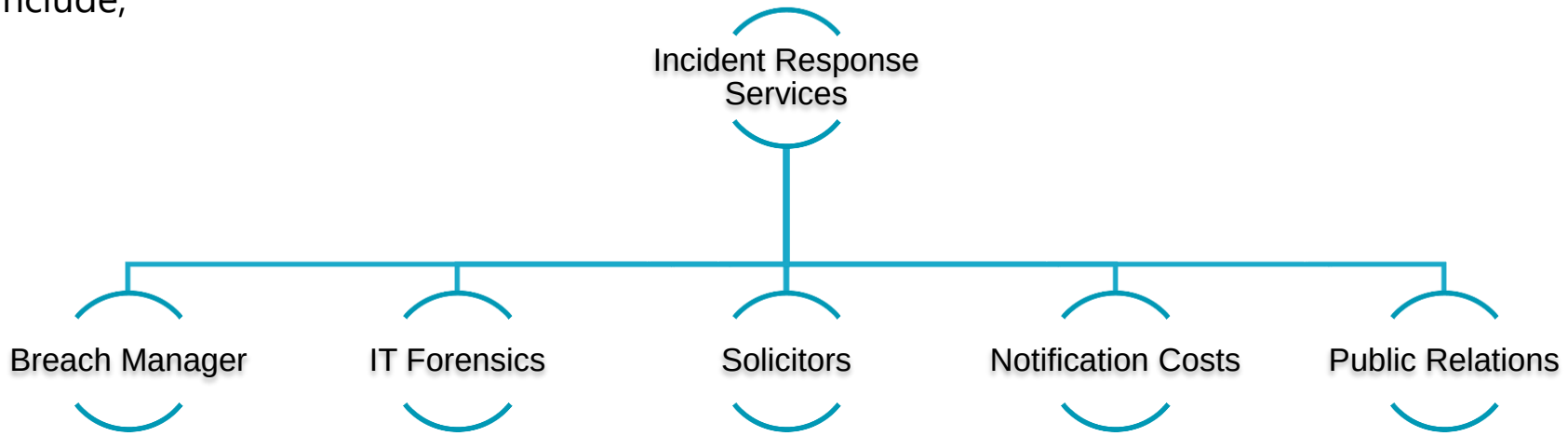
Third Party Cyber Coverages

COVERAGE	DESCRIPTION	COVERED COSTS
Privacy Liability	Failure to prevent unauthorized access, disclosure or collection, or failure of others to whom you have entrusted such information, for not properly notifying of a privacy breach.	▪ Liability and defense costs. ▪ Commercial litigation – e.g., bank suits. ▪ Consumer litigation – e.g., class-actions. ▪ Third-party costs for notification and investigation. ▪ PCI fines and penalties.
Network Security Liability	Failure of system security to prevent or mitigate a computer attack. Failure of system security includes failure of written policies and procedures addressing technology use.	▪ Liability and defense costs. ▪ See above.
Privacy Regulatory Defense Costs	Privacy breach and related fines or penalties assessed by Regulators.	▪ Liability and defense costs. ▪ Regulatory investigations. ▪ PHI fines and penalties. ▪ Prep costs to testify before regulators.
Media Liability	Defense and liability for online libel, slander, disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, negligence in content to those that relied on content.	▪ Liability and defense costs. ▪ Commercial litigation – e.g., bank suits. ▪ Consumer litigation – e.g., class-actions.

Cyber Insurance As A Service
Breach Response Management

Cyber liability insurance policies are unique, one of the key advantages is the 24/7 incident response services. Preferred insurers have partnered with industry experts who will be your first responders to help guide you in the event of a cyber breach.

These services can include;



The inclusion of these services ensures that claims are contained, mitigated and resolved in an expedient manner, as well as provides cost-effective end-to-end solutions for both the insureds and the insurers.

The above is for presentation purposes only, vendors may differ from insurer to insurer

The Policy Spectrum

STANDARD

E.g. most carrier forms

- Includes full limit for standard coverages:
  - Privacy & network security liability
  - Breach response costs
  - Media liability
  - Data restoration
  - Cyber extortion
  - PCI fines & penalties
  - Business interruption
- Business interruption is limited to a security failure of insured's network

BETTER

E.g. modified carrier forms

- Adds broader business interruption triggers, such as:
  - System failure
  - Contingent security failure
  - Contingent system failure
- Other as-needed, risk-specific enhancements such as:
  - Broad GDPR coverage
  - Contingent bodily injury/property damage
  - E&O

BEST

E.g. Cyber CAT

- Business interruption is further enhanced:
  - Contingent coverage expanded from IT providers to suppliers
  - Voluntary shutdown
  - Year-long period of restoration vs. 90-day standard
- Forensic claims preparation costs included

Contact

Carolyn Camoens
Managing Director, Asia, Hume Brophy
carolyn.camoens@humebrophy.com

Lijun Chui
Counsel, Clifford Chance Pte Ltd
Lijun.Chui@CliffordChance.com

Linden Reko
Client Manager for Cyber Practice Asia, Marsh Singapore
linden.reko@marsh.com

William Wong
Consultant, Clifford Chance Hong Kong
William.Wong@CliffordChance.com

Vishal Lanjekar
Principal Consultant & Lead, Mandiant Services, Hong Kong, Macau, & Taiwan, FireEye
vishal.lanjekar@FireEye.com

Daniel Kolbe
Founder & Managing Director, ITCS Group Limited
daniel.kolbe@itcs-group.com