BrokerFabrik Next generation retail stock trading.

www.brokerfabrik.com

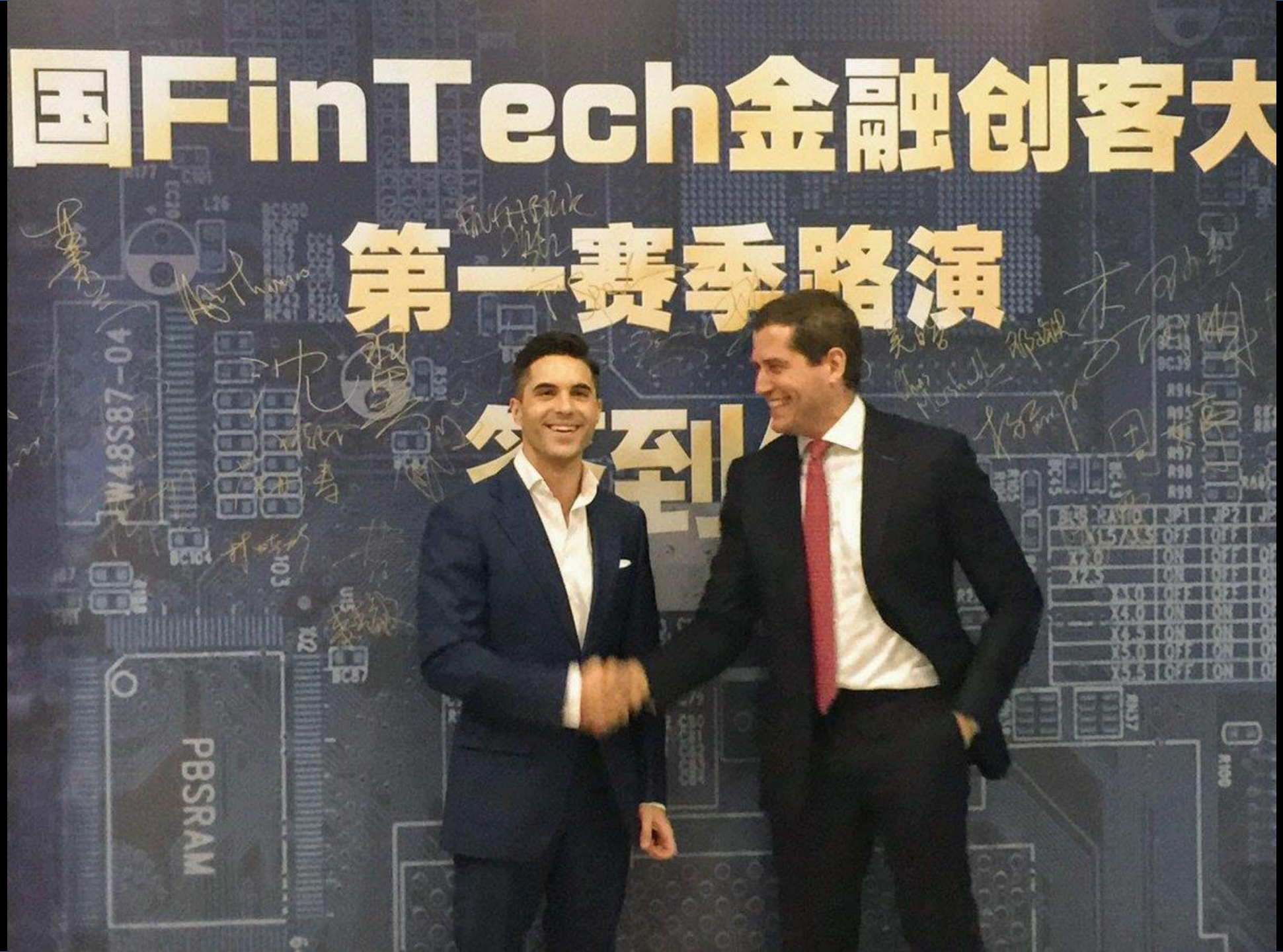
FinFabrik

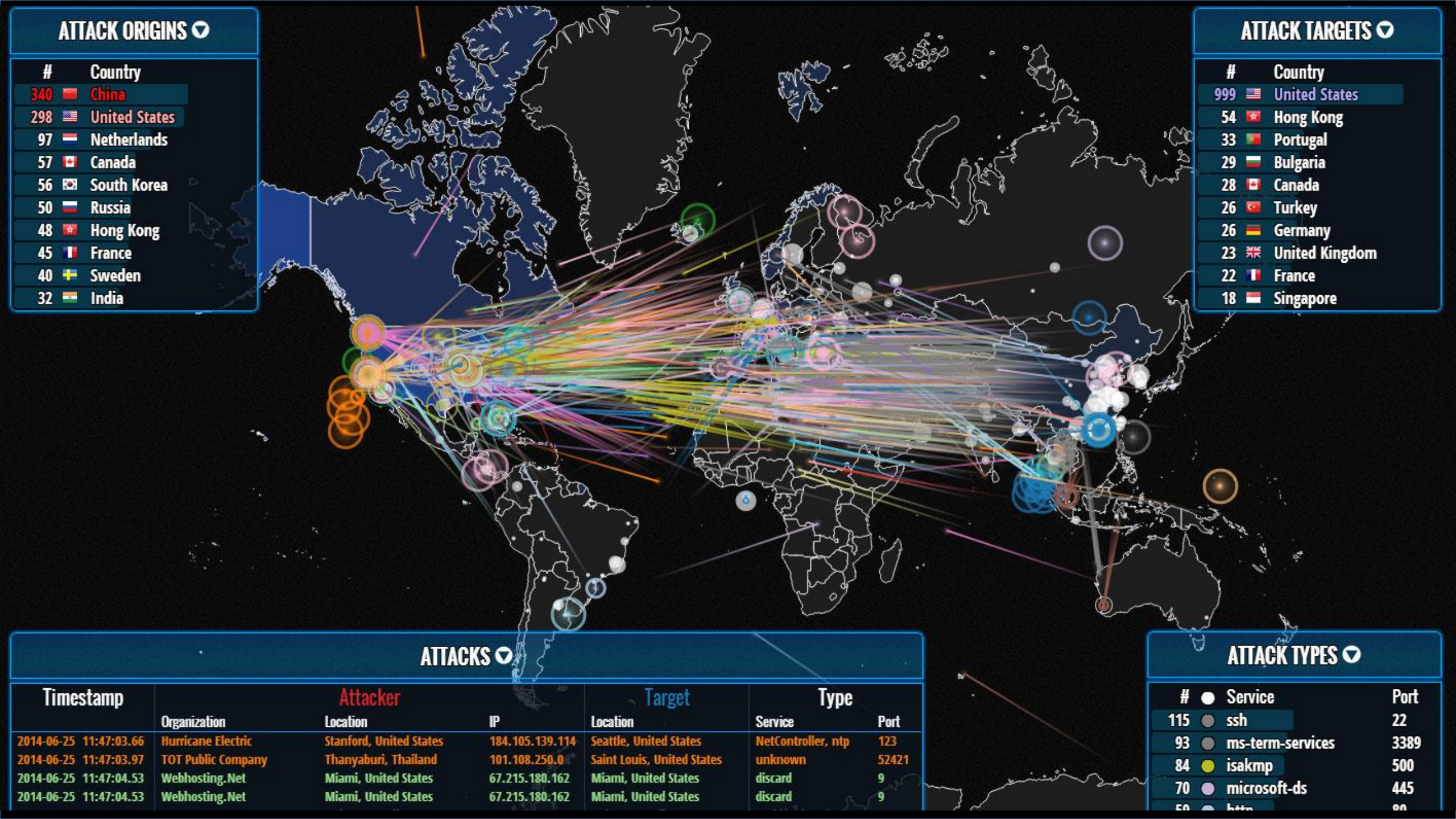
ONC Lawyers 柯伍陳律師事務所

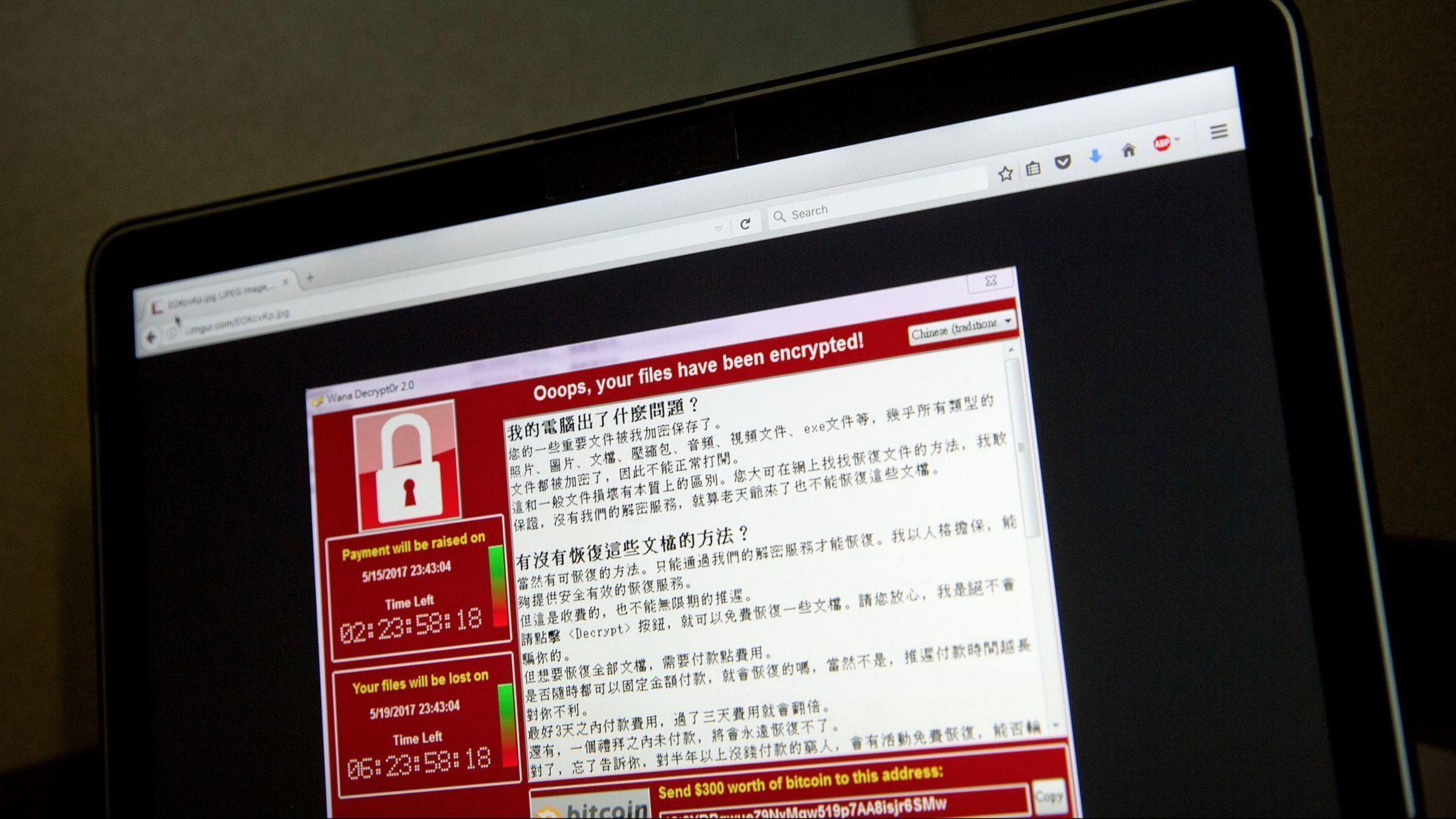
BLUE DRAGON

Online Broker Cybersecurity: Insights & Strategies from Practitioners

Friday, 14 July 2017


国FinTech金融创客大
第一赛季路演
PBSRAM


ATTACK ORIGINS
Country
340 China
298 United States
97 Netherlands
57 Canada
56 South Korea
50 Russia
48 Hong Kong
45 France
40 Sweden
32 India
ATTACK TARGETS
Country
999 United States
54 Hong Kong
33 Portugal
29 Bulgaria
28 Canada
26 Turkey
26 Germany
23 United Kingdom
22 France
18 Singapore
ATTACKS
Timestamp
Attacker
Organization
Location
IP
Target
Location
Type
Service
Port
2014-06-25 11:47:03.66 Hurricane Electric Stanford, United States 184.105.139.114 Seattle, United States NetController, ntp 123
2014-06-25 11:47:03.97 TOT Public Company Thanyaburi, Thailand 101.108.250.0 Saint Louis, United States unknown 52421
2014-06-25 11:47:04.53 Webhosting.Net Miami, United States 67.215.180.162 Miami, United States discard 9
2014-06-25 11:47:04.53 Webhosting.Net Miami, United States 67.215.180.162 Miami, United States discard 9
ATTACK TYPES
Service Port
115 ssh 22
93 ms-term-services 3389
84 isakmp 500
70 microsoft-ds 445


Search
Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
Chinese (traditiona
我的電腦出了什麼問題？
您的一些重要文件被我加密保存了。
照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的
文件都被加密了，因此不能正常打開。
這和一般文件損壞有本質上的區別。您大可在網上找找恢復文件的方法，我敢
保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。
有沒有恢復這些文檔的方法？
當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能
夠提供安全有效的恢復服務。
但這是收費的，也不能無限期的推遲。
請點擊 <Decrypt> 按鈕，就可以免費恢復一些文檔。請您放心，我是絕不會
騙你的。
但想要恢復全部文檔，需要付款點費用。
是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長
對你不利。
最好3天之內付款費用，過了三天費用就會翻倍。
還有，一個禮拜之內未付款，將會永遠恢復不了。
對了，忘了告訴你，對半年以上沒錢付款的窮人，會有活動免費恢復，能否輪
Payment will be raised on
5/15/2017 23:43:04
Time Left
02:23:58:18
Your files will be lost on
5/19/2017 23:43:04
Time Left
06:23:58:18
Send $300 worth of bitcoin to this address:
bitcoin
Copy

[redacted]

13 July 2016 at 9:38 AM

IJ

To: [redacted]

Reply-To: [redacted]

Payment

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile

FinFabrik

ONC Lawyers 柯伍陳律師事務所

BLUE DRAGON

Online Broker Cybersecurity: Insights & Strategies from Practitioners

Friday, 14 July 2017

Agenda and speakers

REGULATION 1

Legal and regulatory perspectives on Cybersecurity in Hong Kong

JP Reimann
Regulatory Lead
FinFabrik

PREVENTION 2

Vulnerability Assessment & Penetration Testing

Dominic Wai
Partner
ONC Lawyers

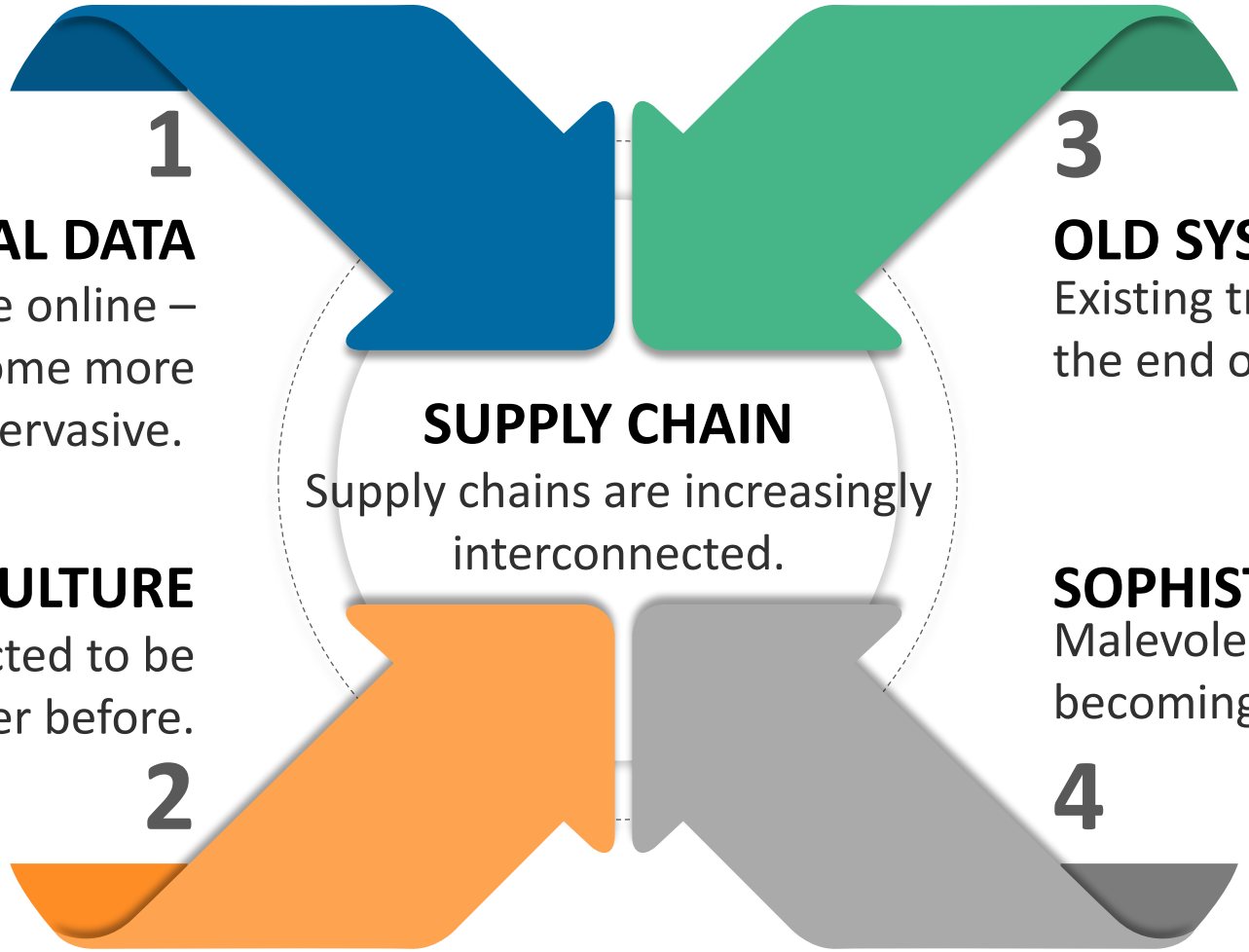
Dmitri Hubbard
General Counsel
Blue Dragon

STRATEGIES 3

Practical strategies to maintain a compliant, cyber resilient business

Dr. Florian M Spiegl
Co-Founder
FinFabrik

Cybersecurity as a major topic in brokerage



1

DIGITAL DATA

Value continues to migrate online – digital data has become more pervasive.

3

OLD SYSTEMS

Existing trading systems are at the end of their lifecycle.

SUPPLY CHAIN

Supply chains are increasingly interconnected.

CORPORATE CULTURE

Corporations are expected to be more ‘open’ than ever before.

2

SOPHISTICATED CRIMINALS

Malevolent actors are becoming more sophisticated.

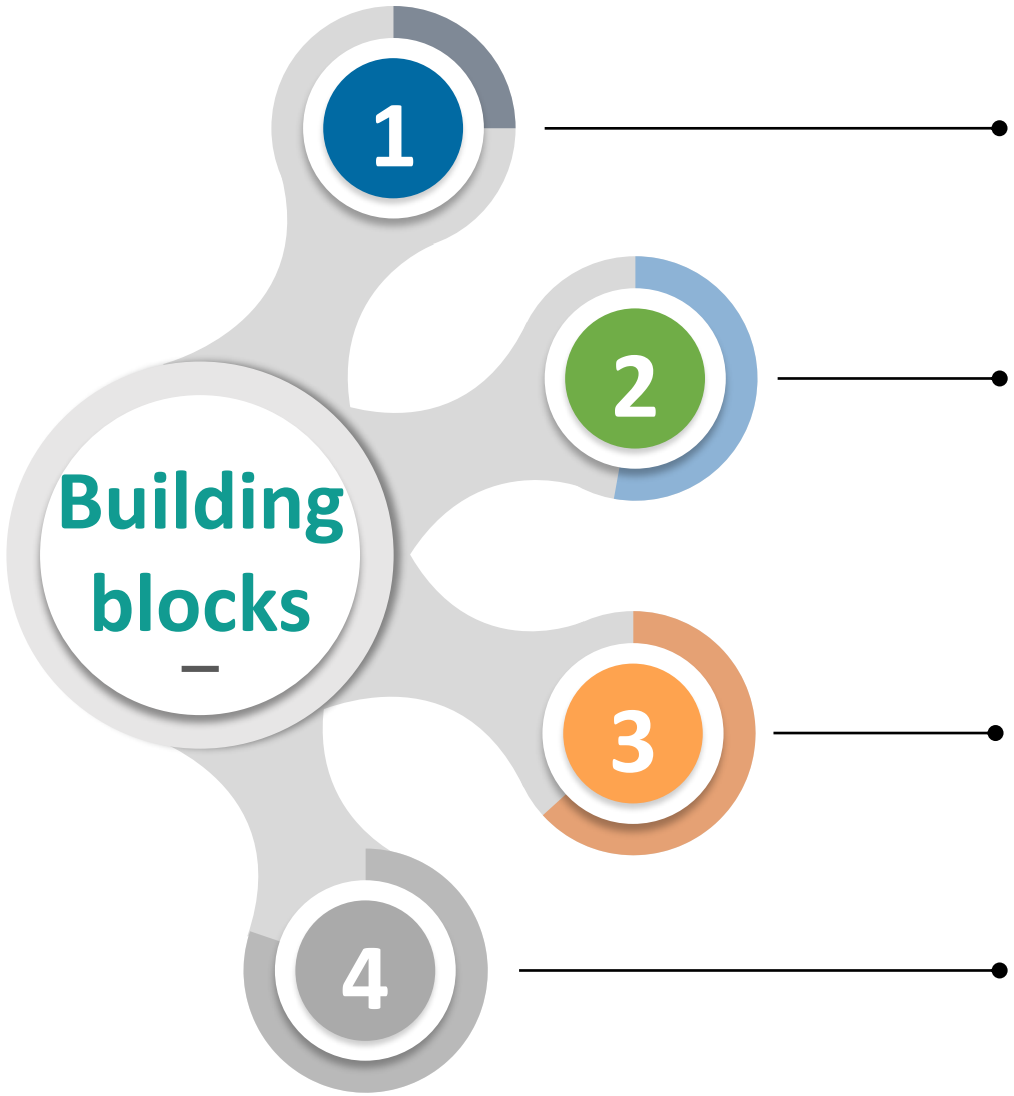
4

Regulation and Cybersecurity in HK

Dominic Wai
Partner at ONC Lawyers

+852 9385 6984
dominic.wai@onc.hk

Regulation and cybersecurity in HK

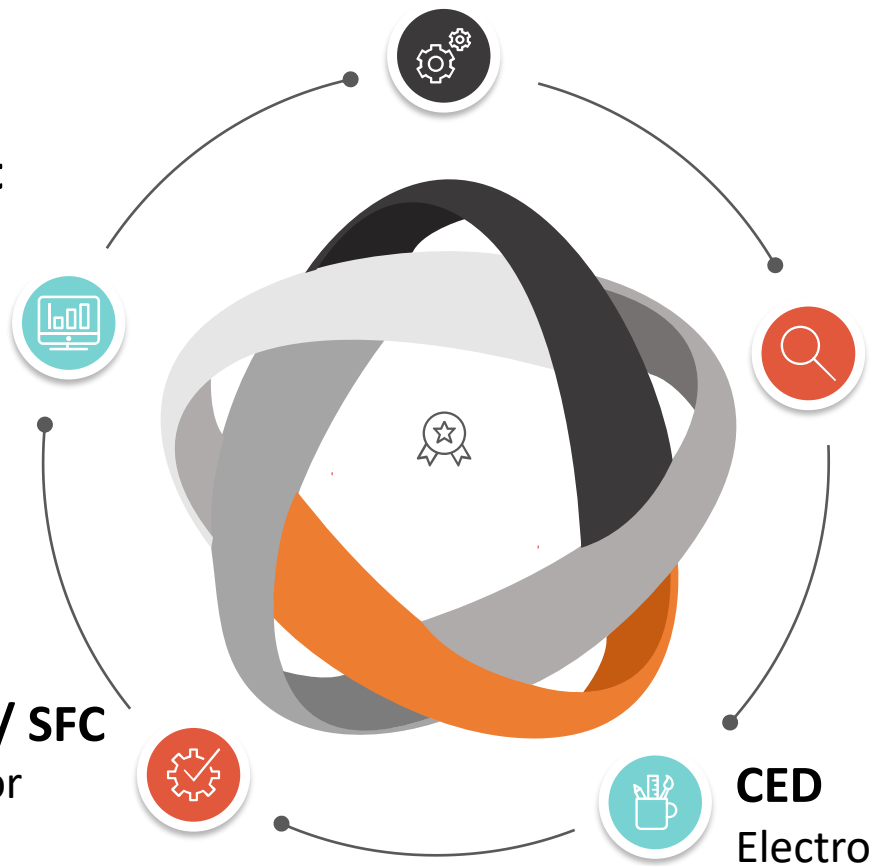


1. Laws and regulations concerning cybersecurity in Hong Kong
2. Latest consultations and covered topics
3. Case study
4. Expected near-term changes to cybersecurity regulatory environment

HK Cybersecurity Regime

Police

Cyber Security and Technology Crime Bureau (CSTCB)(GOV:SB)



Government

Office of the Government Chief Information Officer (OGCIO)(GOV:ITB)

1) Cyber Security Information Portal (CSIP)

2) www.cybersecurity.hk

Statutory Bodies

1) Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)(HKPC)(Statutory Body)

2) Centre for coordination of computer security incident response for local enterprises and internet users.

Government / SFC

1) Office of the Privacy Commissioner for Personal Data (GOV:CMAB)

2) Securities and Futures Commission (SFC)

CED

Electronic Crime Investigation Centre

Criminal and Civil Responses (I/V)

- **Offences**
  - "Unauthorised access to a computer by telecommunications" (s.27A of the Telecommunications Ordinance)(Cap 106)
  - "Access to a computer with criminal or dishonest intent" (s.161 of the Crimes Ordinance)(Cap 200)
  - "Disclosing Personal Data Obtained without consent from Data Users"
    - with an intent to obtain gain in money or other property, whether for the benefit of the person or another person; or
    - To cause loss in money or other property to the data subject. (s.64 of the PDPO)(Cap 486)
  - DPP4 – data users should take all practical steps to ensure that personal data held by the data user are protected against unauthorised or accidental access, processing, erasure, loss or use.

Criminal and Civil Responses (II/V)

- Criminal damage – destroying or damaging property (Crimes Ordinance, ss 59(1A), 60(1))
- To destroy or damage any property in relation to a computer includes the misuse of a computer.
- Misuse of a computer –
  - To cause a computer to function other than as it has been established to function by or on behalf of its owner, notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;
  - To alter or erase any program or data held in a computer or in a computer storage medium;
  - To add any program or data to the contents of a computer or of a computer storage medium.
  - And any act which contributes towards causing the misuse of a computer as described above shall be regarded as causing it.

Criminal and Civil Responses (III/V)

- But no definition of a computer in the relevant ordinances.
- Recent cases ruled mobile phones and smartphones are “computers” under s.161 of Crimes Ordinance.
- Meaning of “computer” – s.22A of Evidence Ordinance (Cap 8) – documentary evidence from computer records
  - *“Any device for storing, processing or retrieving information, and any reference to information being derived from other information is a reference to its being derived therefrom by calculation, comparison or any other process.”*

Criminal and Civil Responses (IV/V)

- Police investigation
  - CED for Copyright Ordinance against providing device or services for “jail breaking” s.273C(1)(d)(Cap 528)
- Online report of cybercrime
- Interpol - Global Complex for Innovation (Singapore)
- Mutual Legal assistance on criminal matters
- The relevant ordinances on cybercrime mainly are not extraterritorial.
  - Save for CJO (Cap 461) for Theft

Criminal and Civil Responses (V/V)

- <u>Law Enforcement</u>
- Companies should maintain a close connection with various law enforcement representatives to discuss before an incident occurs:
  - When should the company report the incident to them.
  - How the reporting should be performed.
  - What evidence is needed.
  - How evidence should be collected.

Unauthorised stock trading (I/VI)

"Hacking of internet trading accounts is the most serious cybersecurity risk faced by internet brokers in Hong Kong.

If you ask regulators in the industry what is the number one threat, not surprisingly it's all about cyber attacks.

We've seen that happen not only in banking but also at brokers in Hong Kong, in particular recent attacks to do with basically hijacking share trading accounts."

Reuters - Ashley Alder, CEO of the SFC and chairman of the International Organization of Securities Commissions, in a LegCo speech, February 2017.

Unauthorised stock trading (II/VI)

- On 8 May 2017, SFC launched a 2-month consultation on proposals to reduce and mitigate hacking risks associated with internet trading
  - *For the 18 months ended 31 March 2017,12 licensed corporations (LCs) reported 27 cybersecurity incidents, most of which involved hackers gaining access to customers internet-based trading accounts with securities brokers resulting in unauthorised trades totalling more than $110 million when some others involved DDoS attacks targeting their websites accompanied by threats of extortion.*

Unauthorised stock trading (III/VI)

- Hacking incidents and potential root causes
- The hacking incidents reported by licensed internet brokers remain under Police investigation. However, the Police shared case studies suggesting that hackers used compromised internet trading accounts to carry out a pump-and-dump scheme which could lead to substantial financial losses. Such schemes typically follow these steps:
  - (a) Hackers first gain control of clients' internet trading accounts (hacked accounts) which enables them to log into the accounts "legitimately" to effect unauthorised transactions;
  - (b) Hackers then employ people to open other internet trading accounts to accumulate penny stocks;

Unauthorised stock trading (IV/VI)

- (c) Using the cash in the hacked accounts, or cash raised by selling off existing stock holdings in the hacked accounts, hackers then buy these penny stocks in order to pump up their stock prices; and
- (d) After the prices of the penny stocks go up, hackers off-load them and make a profit, leaving the owners of the hacked accounts to suffer significant losses.

Unauthorised stock trading (V/VI)

- SFC's proposal in the consultation:
  - Propose to incorporate new guidelines which set out baseline cybersecurity requirements for internet brokers to address hacking risks and vulnerabilities and to clarify expected standards of cybersecurity controls.
  - Key proposed requirements include 2-factor authentication for clients' system login and prompt notification to clients of certain activities in their internet trading accounts.

Unauthorised stock trading (VI/VI)

- In addition, the SFC proposes to expand the scope of cybersecurity-related regulatory principles and requirements which now apply to electronic trading of securities and futures on exchanges to cover the internet trading of securities which are not listed or traded on an exchange. This includes authorised unit trusts and mutual funds because they are subject to the same hacking risks.
- The SFC also proposes to update the definition of “internet trading” to clarify that an internet-based trading facility may be accessed through a computer, mobile phone or other electronic device.

Case study - Unauthorised stock trading – 2016 (I/II)

- P is a HK company engaged in the trading of securities, options and futures contracts, and investment holding.
- D is a corporation licensed to carry on Type 1 (dealing in securities) regulated activities under SFO (Cap 571) and also an Exchange Participant of the Stock Exchange of Hong Kong Limited and Hong Kong Futures Exchange Limited.
- P has a securities account with D that can be operated online with the use of specified user ID and password for online access to the account for the purpose of carrying out transactions for the sale and purchase of securities. According to P, there are only 3 persons in the company who are authorized to access and operate the account with D and conduct online securities transactions with the account.

Case study - Unauthorised stock trading – 2016 (II/II)

- On 23 Sept 2016, between 14:40 and 15:22, unauthorized person(s) logged into P's account with D with a valid user ID and password from an IP address and in the space of 18 minutes, bought a total of 49.2m shares in a Listco from a total of 76 selling brokers at a purchase cost of HK$37.69m (including fees and levies), draining almost all of the HK$37.85m cash in the account.
- The 49.2m shares represent 4.92% of the Listco's shareholding at an average price of HK$0.7636 per share, 36% above the previous day's close.
- There was a huge spike in the volume and price of the Listco on 23 Sept 2016: the traded volume was 92.568m shares or 9.26% of the ListCo and the price at one point reached HK$0.88, up 57.1% on the previous close of HK$0.56, before closing at HK$0.66, up 17.9%.

Expected near-term changes to cybersecurity regulatory environment (I/II)

Baker, 2016

Expected near-term changes to cybersecurity regulatory environment (II/II)

- Cybersecurity regime
  - No centralised arrangement or policy initiative to tackle cybersecurity and no plan to change the existing arrangement [see response of ITB to LCQ8: Cyber security, 7 Dec 2016]

Trends and challenges

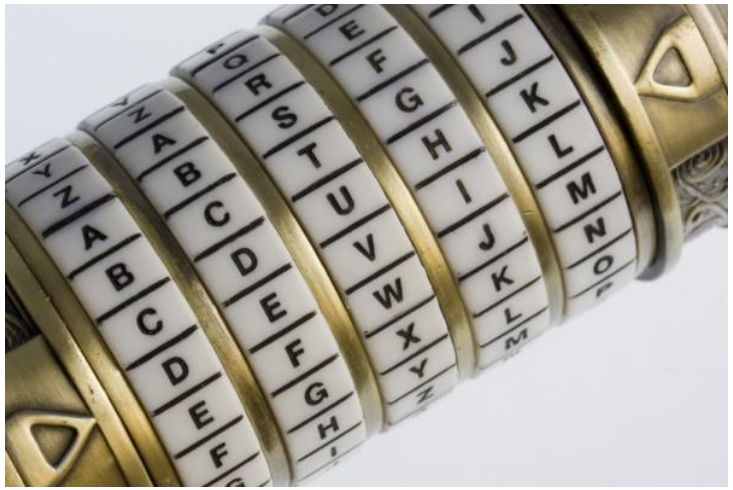
- **Emails**
- **Attack Trends**
  - Against less mature financial services organisations
  - ATM attacks
  - Nation-states hunting for PII
  - Espionage targets on China's periphery
- **Target Industries**
  - Construction and engineering
  - Financial Governments
  - High Tech and Electronics

Vulnerability Assessment & Penetration Testing

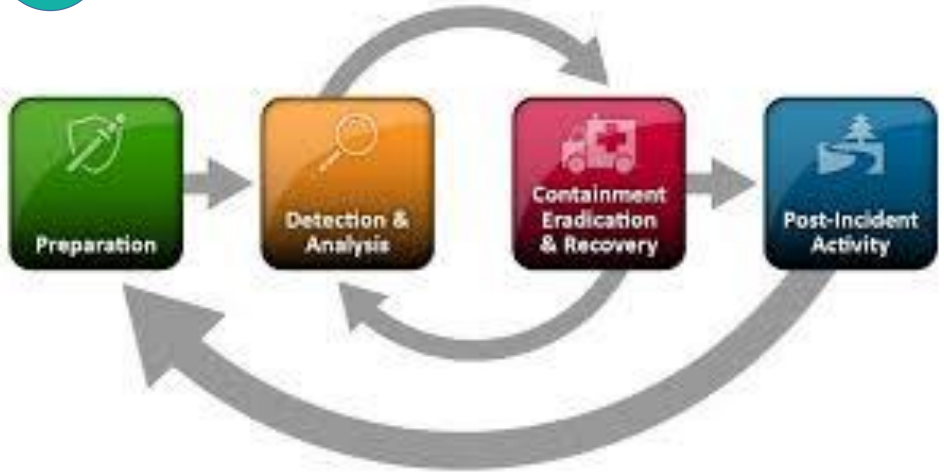
Dmitri M A Hubbard
General Counsel at Blue Dragon Asia

dmitri@bluedragon.com.hk
+852 9028 6677

Making security part of broker business



1 **Case One** – the secret wifi network



Avoid "Security by obscurity"

Offence informs defence

2 **Case Two** – the enemy within

3 **Case Three** – the invisible man

SFC Suggestions – March 2016

i. Establish a strong **governance framework** to supervise cybersecurity management;

ii. Implement a formalised **cybersecurity management process** for service providers;

iii. Enhance **security architecture** to guard against advanced cyber-attacks;

iv. Formulate **information protection programs** to ensure sensitive information flow is protected;

v. Strengthen **threat**, intelligence and **vulnerability management** to **pro-actively identify** and remediate cybersecurity vulnerabilities;

vi. Enhance **incident and crisis management procedures** with more details of latest cyber-attack scenarios;

vii. Establish adequate backup arrangements and a **written contingency plan** with the incorporation of the latest cybersecurity landscape; and

viii. Reinforce user access controls ensuring **access to information** is granted to users on a need-to-know basis.

Cyber Response along predefined steps

1	**Prevent**	What security controls do we need?	***What threats have been identified by us, our industry and the HKSFC?***
2	**Detect**	Can you protect client trading accounts, infrastructure?	***What are our vulnerabilities? Platform and human…***
3	**Respond**	Who does what when and how when a crisis occurs?	***Contingencies, roles, communication.***
4	**Investigate**	How can we simulate and crisis to prepare?	***Penetration testing Social engineering Spear phishing***
5	**Recover**	Knowing our weakness, how do we move on?	***Implementation of improvements***

Blue team vulnerability assessment

1	Cyber risk assessment	Identify risks	**HKSFC** **Cyber threat intelligence** **SANS 20**
2	Service providers and third parties	Control risks outside	**Due diligence** **Supplier vetting** **Encryption**
3	Cybersecurity awareness	Enhance understanding inside	***Staff knowledge*** ***Staff behaviour*** ***Mgmt approach***
4	Incident response	Contingency planning	***Penetration testing*** ***Social engineering*** ***Spear phishing***
5	Data protection	Identify personal information, crown jewels	***Implementation of improvements***

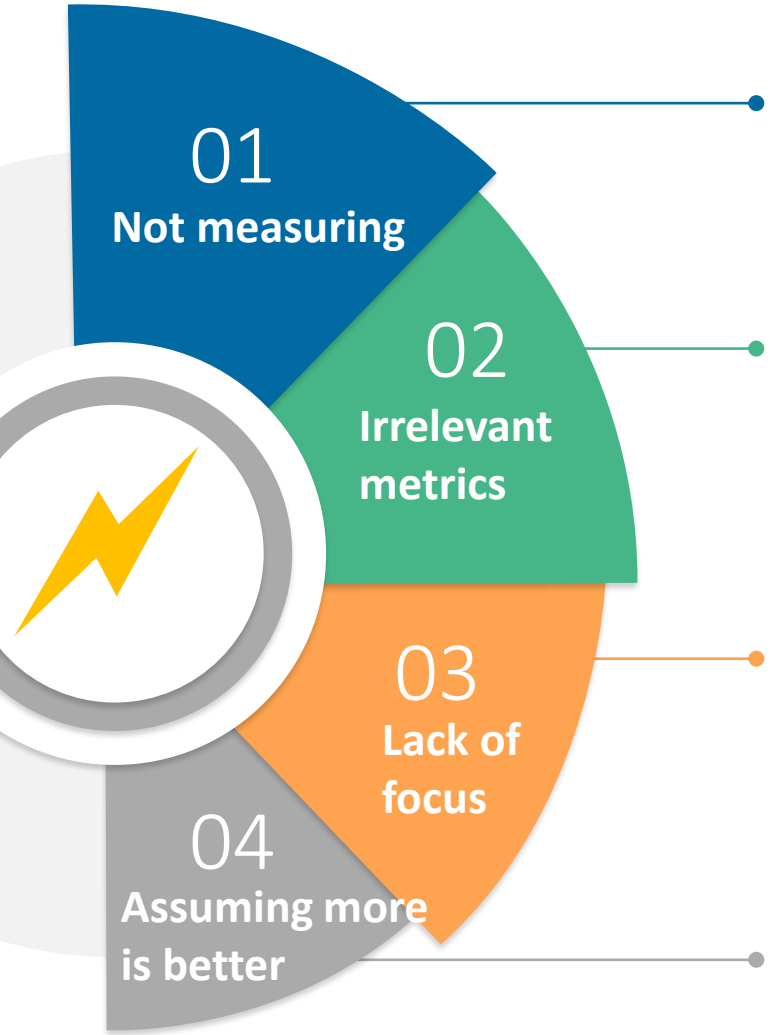
Red team penetration assessment

Lois Lane, 1972

1	Social engineering	Human exploitation has proved the easiest means of cyber breach.	***52% of cyber attacks involve social engineering***
2	Security	***Prank call*** ***Prank visit*** ***Prank USB***	***40% of cyber attacks involve insiders***
3	Phishing	***Spear phishing*** ***Whaling*** ***Before-after***	***39% involve APTs (advanced persistent threat)***
4	Pen testing	***Trading platform*** ***Network*** ***Wifi***	***Vulnerabilities in your network, website and wifi network***
5	Follow up	Knowing our weakness, how do we move on?	***Implementation of improvements***

Strategic approaches to build compliant cyber resilience

Cybersecurity needs to be focused: pitfalls in security assessments



Cybersecurity performance can be managed, but only if measured.

Tiny percentage of sophisticated attacks represent true risk, rather than the millions of attacks from “script kiddies”.

Lagging indicators vs leading indicators: attacks vs extend of encryption.
Looking at cybersecurity organisation vs enterprise resilience.

Easy to incur too much cost and create too much complexity.
Encryption of every piece of data and 2FA to every system.

High spend does not equal high security

Budgeting

Start with holistic and comprehensive risk assessment.

ROI

Spending millions on security technology can make executives feel safe without real impact.

Controls

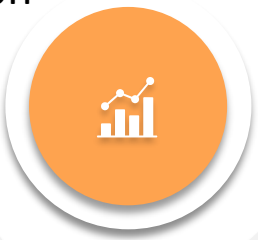
Assure appropriate, efficient and continuous risk mitigation.

Humans

Major sources of cyber threats are human brain (curiosity, ignorance, apathy etc).

Spending

Cybersecurity spending to hit USD 170 billion by 2020.



Defence

First and last line of defense are prepared leaders and employees, whether inside an organisation or of the supply chain.

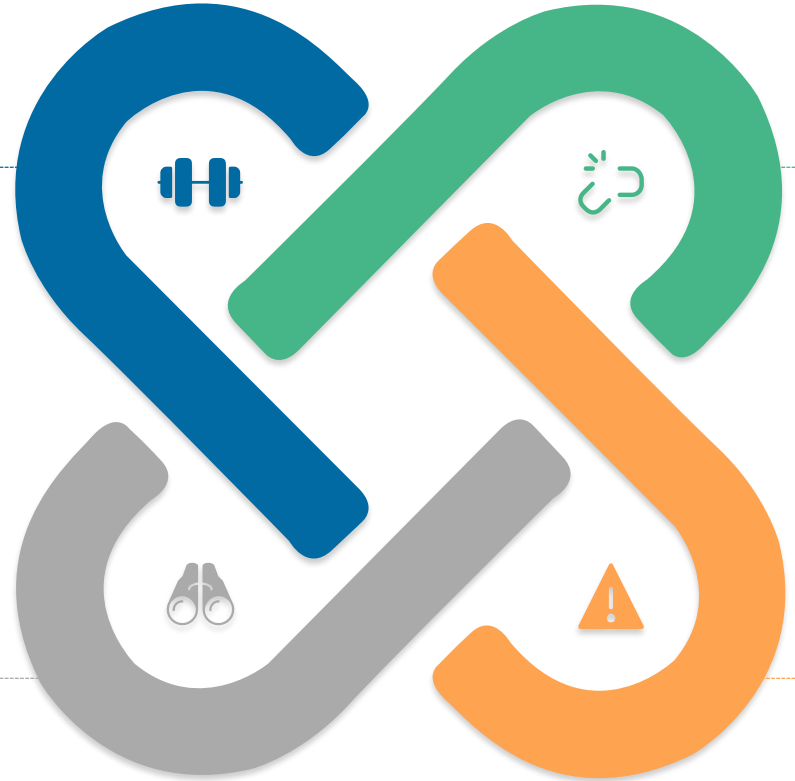
Cybersecurity needs to be business-driven: protect without slowing innovation & growth

SOFTWARE

Slow security software can cause employees to abandon corporate laptops and e-mail services for personal devices and web-mail..

CONTROLS

Overly stringent controls can get in the way of doing business or have other adverse effects..



PROTECTION

Protecting technology assets from malicious damage requires intelligent constraints.

THREATS

Insufficient safeguards result in loss of critical data.

An integrated, broad approach works best

01

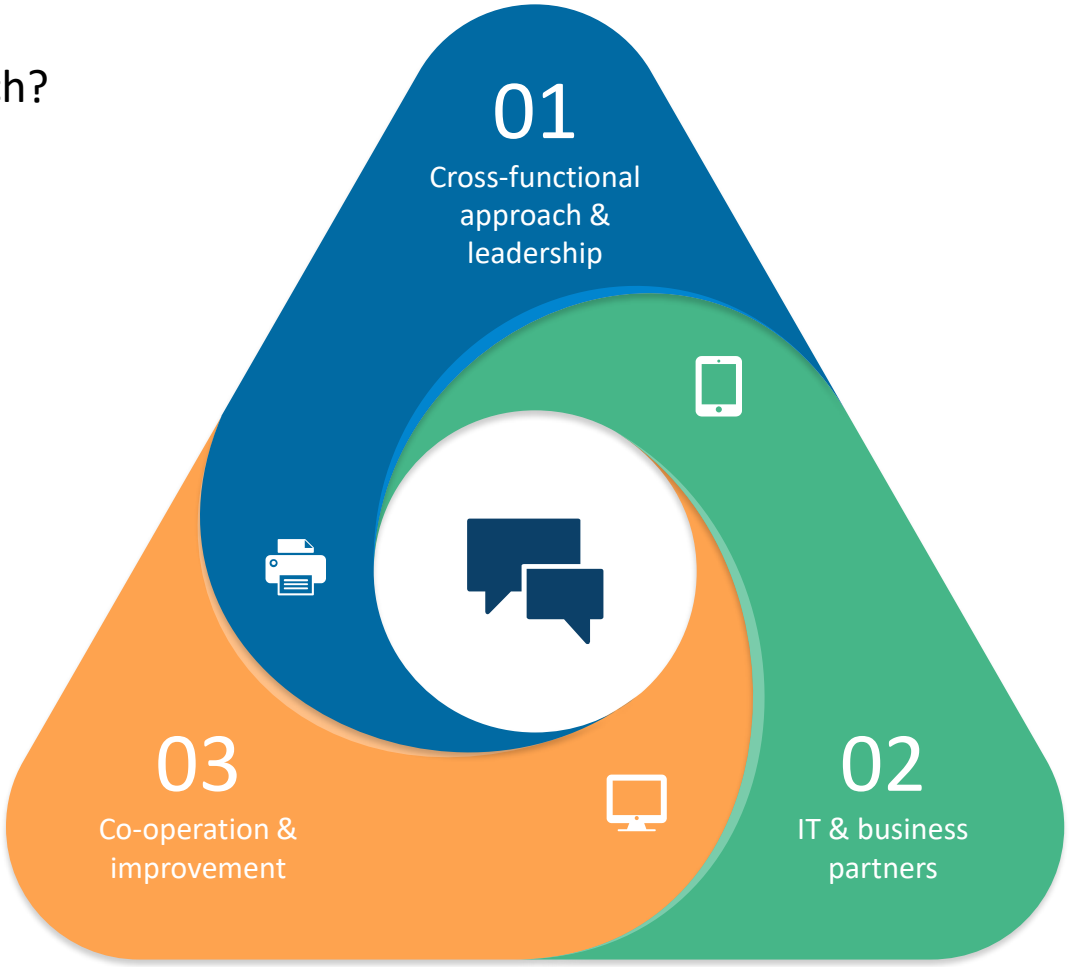
- Who is responsible for cross-functional approach?
- Are business leaders (as opposed to IT or risk executives) owning this topic?

02

- Which information is most critical, and what is “value at stake” in event of breach?
- How are we using technology and business processes to protect critical information?

03

- How does our approach compare with peers and best practices?
- Is our approach evolving and changing?
- As an industry, are we working together and with government entities to reduce cybersecurity threats?

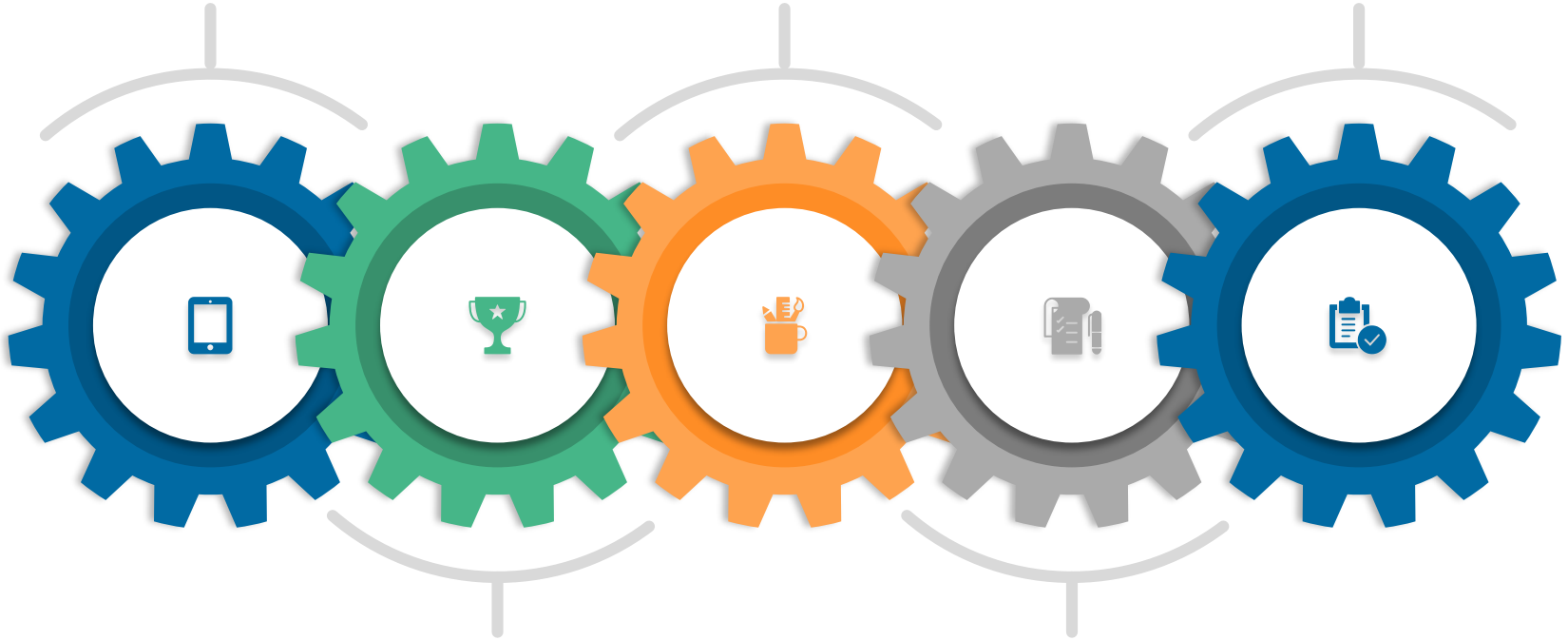


Steps in control functions - resilient approach

STEP 1
Implement multiyear programs to classify corporate data.

STEP 3
Evaluate cyberrisk profile across the full value chain.

STEP 5
Make cybersecurity a core part of the customer value proposition, establishing an ongoing dialogue.

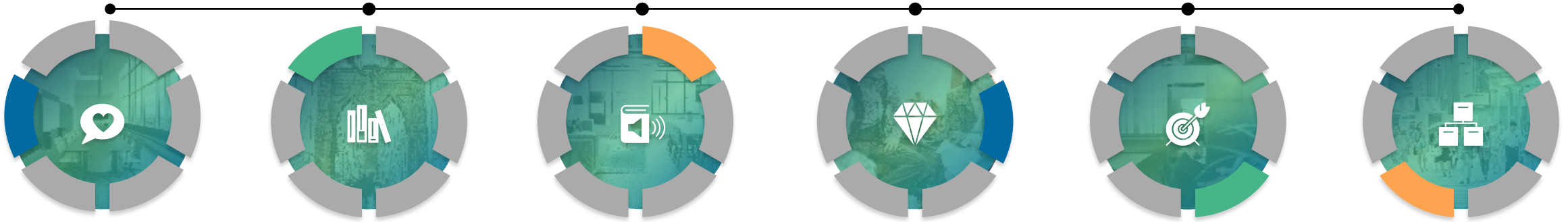


STEP 2
Protect most critical business assets or processes (such as customer credit card information)— a “business-back” approach.

STEP 4
Clarify expectations with vendors and enhancing collaboration with key business partners.

Cybersecurity is a business opportunity - convenient and secure end-to-end customer experiences.

Concrete first steps: get clarity on your cyber resilience and raise awareness



Prepare your workforce: build awareness, offer tailored training, drill your technical staff

Run a cybersecurity health check: assess security controls and capability maturity of organisation and processes

Perform a training session to enable C-suite: tabletop simulation or war-gaming exercise

Ensure that training and communication agenda includes cybersecurity-related offerings

Develop or check attack response plans, and verify external vendor readiness

Start to build a cybersecurity management system, or launch a review of your existing one.

Taking a step back

- Avoid common pitfalls
- Focus spending where it is most effective
- Choose a broadly integrated approach: enterprise resilience over cybersecurity organisation
- Start with concrete, focused steps: get your technology right

Technology in brokerage cybersecurity: a deep dive excursion

Marcel van der Vliet
CTO, FinFabrik

Application Topology Diagram
Infrastructure Diagram
Level 3 network Diagram
VLAN and VM Diagram
Load Balancers and Firewalls

Technical diagrams as shown in the live presentation available on request

Q&A

www.finfabrik.com

www.brokerfabrik.com