ADVANCING CYBER RESILIENCE:

Are you ready for the next cyber threat?

Paul Yeung
Senior Inspector of Police
Cyber Security and Technology Crime Bureau

AGENDA

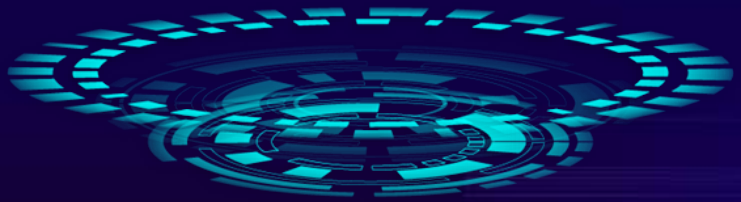
01 Cyber Security Landscape

02 Cyber Threats and Pitfalls

03 What is Cyber Resilience?

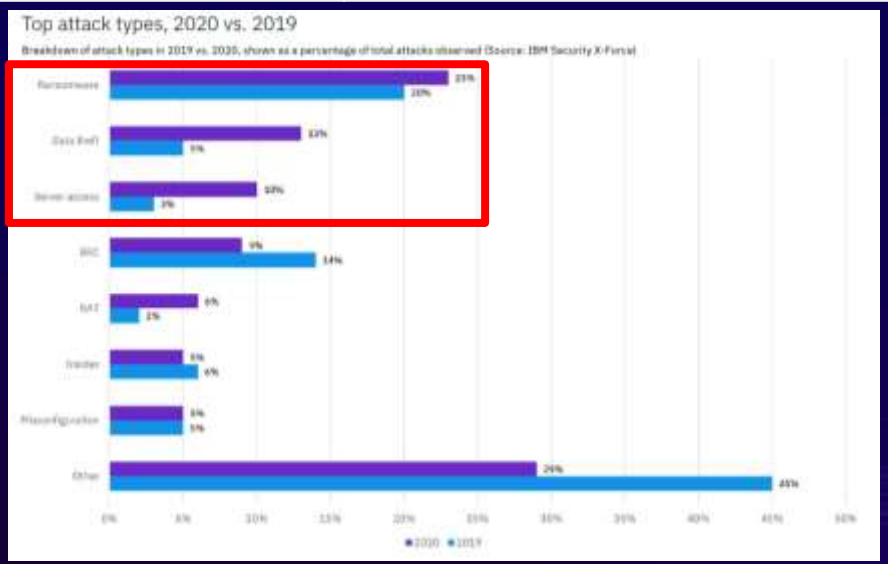
04 How to Build Cyber Resilience?

Cyber Security Landscape



Global Landscape

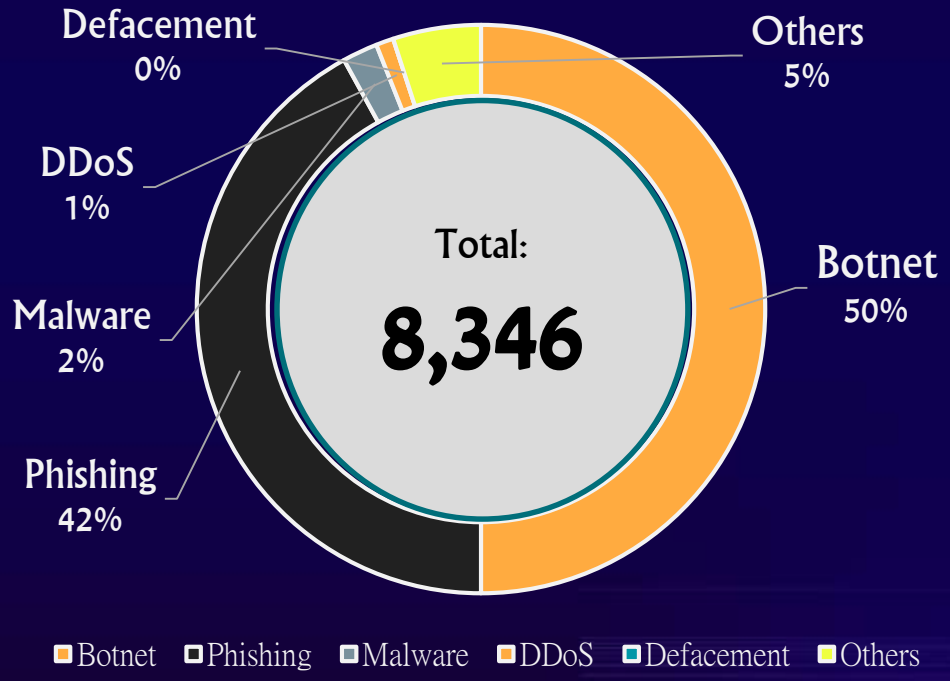
Top 3 attack types	Top 3 initial attack vectors
1. Ransomware (23% of attacks)	1. Scan-and-exploit (35% of attacks vs. 30% in 2019)
2. Data theft (160% increase since 2019)	2. Phishing (33% of attacks vs. 31% in 2019)
3. Server access (233% increase since 2019)	3. Credential theft (18% of attacks vs. 29% in 2019)



Source: IBM Security X-Force Threat Intelligence Index 2021

Local Landscape

Distribution of Incident Reports in 2020



Source: HKCERT Security Incident Report 2020

Global Incidents

Ransomware Hackers Claim To Leak 250GB Of Washington, D.C., Police Data After Cops Don't Pay $4 Million Ransom

Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate

JBS Paid $11 Million to Resolve Ransomware Attack

Meat supplier's U.S. chief says firm paid cybercriminals in bitcoin to avoid more disruptions

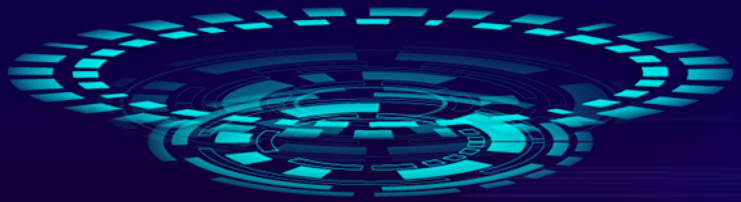
Local Incidents

…reported that its public enquiry email suffered from an email bomb attack…

…reported that phishing emails purportedly to be sent by the GovHK lured the public to provide personal particulars to claim anti-pandemic funds through an attached link

…reported that phishing SMS messages embedded with links purported to be sent by the companies to lure for users' personal particulars and credit card details for bill refund

Cyber Threats and Pitfalls




Cyber Threats
Phishing
Email Scam
Ransomware
Data Breach
Insider Threat
Supply Chain Attack
Different yet interconnected
Human element-emphasized
Sophisticated Attack

Phishing & Email Scam

Phishing

- A way that cybercriminals steal confidential information by sending fraudulent messages
- Use pressure and quick emotional responses to trick the recipient

There has been a scheduled outward PAYMENT of HKD50,000.00. If this was NOT made by you, please CANCEL via: https://hangseng-online.com/signin

Hongkong Post 香港郵政

Dear subscriber ,

Package: HK63 **** 726**

Failed delivery attempt: 28/01/2021 , 09:15
Reason: Incomplete delivery address.

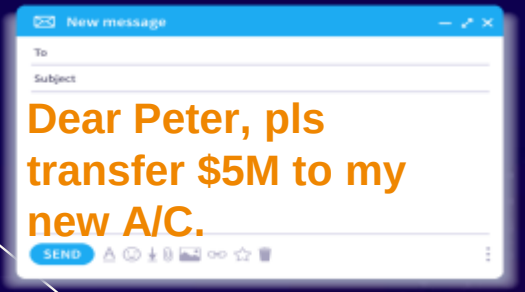
New estimated delivery date : 29/01/2021 - 30/01/2021

To receive your package, we ask that you send us your correct address and pay the new shipping costs (**17 HK$**) at the following link:

COMPLETE MY COMPLETE DELIVERY ADDRESS

Email Scam

- Scam targeting companies who conduct wire transfers and have suppliers abroad
- Rely heavily on social engineering tactics to trick unsuspecting employees



Pseudo Phishing Email Campaign

Pseudo Phishing Email Campaign

INDIVIDUALLY

12%

CLICKED ON THE PHISHING EMAIL

COMPANY-WISE

70%

HAD AT LEAST ONE STAFF MEMBER CLICK ON THE PHISHING EMAIL

Ransomware

- Progressing attack pattern: Double extortion
  - **Triple Extortion**
    - Encrypt data
    - Threaten to publish
    - Demand payments from partners, customers and other third parties
- **Ransomware-as-a-service (RaaS)**

Source: IBM Security X-Force

Data Breach (資料外洩)

Aug 2020

Personal information of over 720,000 customers of an online food ordering website were leaked

Oct 2020

1.2TB size of activity log is exposed in data breach of a VPN provider of HK

Mar 2021

Personal data of 1,644 subscribers of a news agency leaked including credit card information

Apr 2021

A Social Audio App data leak: 1.3 million scraped user records leaked online for free

Data Breach (資料外洩)

250 days

Average time to identify and contain

Healthcare

Highest industry cost

44%

Breaches with customers' info

HK$33 million

Average total cost

HK$1,440

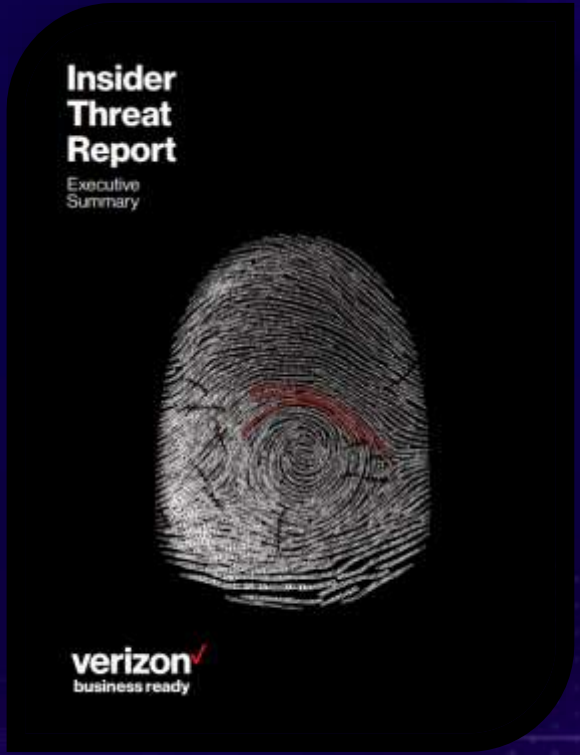
Average cost per customer record

Source: IBM - Cost of a Data Breach Report 2021

Insider Threat (內部威脅)

4 warning signs of a breach

1) Erratic Access
2) Excessive Access
3) No need to know
4) Off-peak access

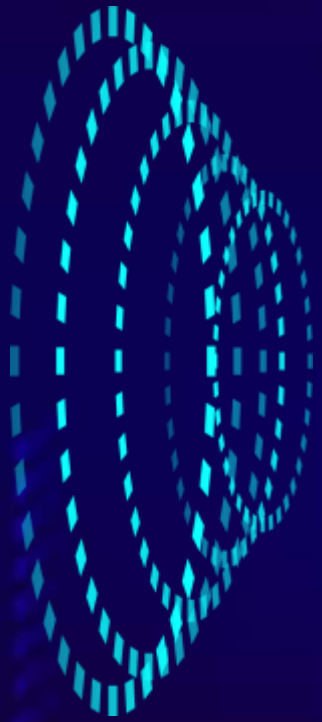


Source: Verizon – Insider Threat Report

Supply Chain Attack (供應鏈攻擊)

- A cyberattack that attempts to inflict damage to a company by **exploiting vulnerabilities** in its **supply chain network**
- E.g. Material supply, manufacturing, assembly, distribution, etc.

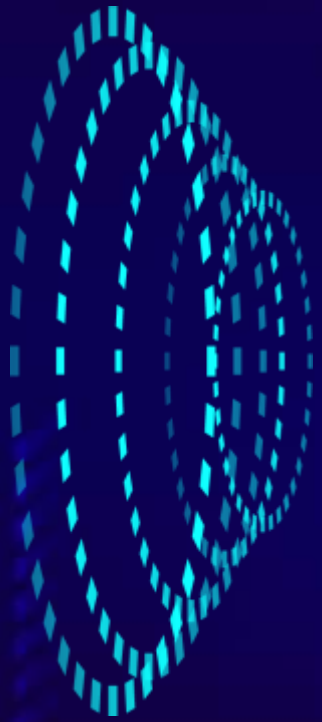
What is Cyber Resilience?



What is Cyber Resilience?

The ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enable by cyber resources.

Source: NIST Special Publication 800-160 Volume 2 “Developing Cyber Resilient Systems: A Systems Security Engineering Approach”



A cyber-resilient posture brings you

- Reduce financial losses
- Meet legal and regulatory requirements
- Improve incident response and business continuity management
- Improve your culture and internal processes
- Protect brand and reputation

Source: IT Governance Ltd - Cyber security solutions

Cyber Resilience (網絡韌性)

Resilience is Key

Protect the best you can, but realize that absolute cyber security is unattainable, so system resilience is the path forward

How to Build Cyber Resilience?

Cyber Resilience (網絡韌性)

Being cyber resilient is:

1) Taking steps to reduce the risk of cyber breaches
2) Making sure that if a breach occurs you know how to respond to ensure:
    - Adequate legal response
    - Responsible public response
    - Business continuity

Cyber Resilience (網絡韌性)

IDENTIFY

- Identify vital security vulnerabilities
- Identify high-value and critical assets

PROTECT

Protect critical infrastructure and services

- Securing business-critical systems
- Protecting endpoints and gateways
- Protecting mobile workforce and customers

DETECT

Implement a detection system for identifying attacks and assessing affected systems

RECOVER

Implement a plan to restore any data or services affected by an attack

RESPOND

Implement a plan to restore any data or services affected by an attack

Source: NIST: Cybersecurity Framework Overview

Case Study (1) – Local (Gov't Dep't)

What happened?

- Unsuccessful login attempts to an online portal for Government Departments to upload information within Government were detected
- Classified and sensitive data were stored in one of the compromised servers in another Gov't Dep't initiating attack

Why it happened?

- Originated from compromised servers of a Gov't Dep't

Case Study (1) – Local (Gov't Dep't)

What were the malpractices?

1) Weak protection on internet-facing servers
2) Weak password protection
3) The testing server is lack of suitable patching
4) Personnel have no knowledge that the testing server is directly exposed to the Internet
5) Poor segmentation policy for the network
6) The firewall policies do not record the incoming traffic of the testing server
7) Personnel could not provide a clear network diagram

Case Study (2) – Local (Gov't Dep't)

What happened?

- A Government department reported a ransomware attack (i.e. REvil) against its internal server in June 2021

How the attack happened?

- Insertion of an infected USB by staff

The impact

1) A number of files with personal data were encrypted
2) Server suspension
3) Unknown threat actor demanding $5.5M-HKD valued cryptocurrency

Case Study (2) – Local (Gov't Dep't)

What could have been done better?

Prevention

- People
- Processes
- Technology

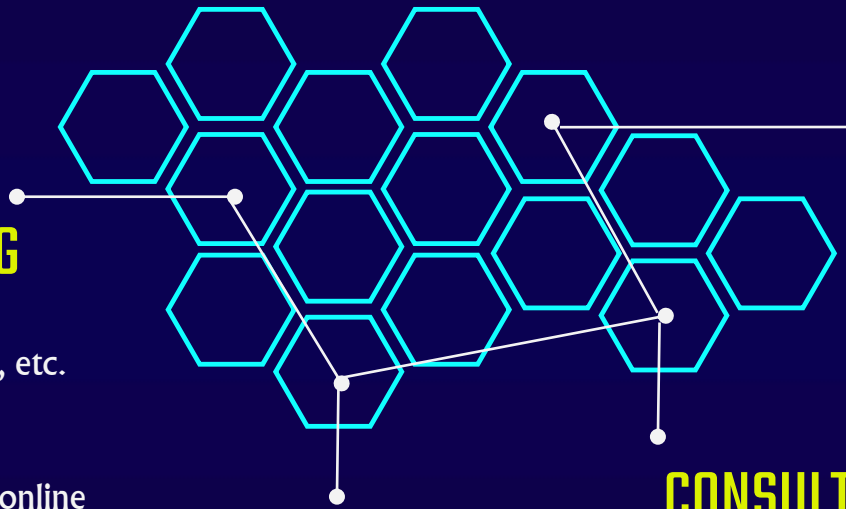
Detection

- Pre-incident
- Real-time
- Post-incident

Response

- Identification
- Containment
- Eradication
- Recovery

Enhancing Preparedness



TRAINING

- Staff awareness, foundation courses, advanced program, etc.
- Internal training team/ Outsourced training
- Live Online and self-paced online training courses

SOFTWARE

Software tools, developed with according needs and requirements, make information security risk and compliance management more applicable to that industry

TOOLKITS

Help organisations adapt quickly and adopt best practice

CONSULTANCY

Consultants can help accelerate the IT GRC projects

Food for Thoughts

To reach high levels of Cyber Resilience:

1) A continuous monitoring of new trends in cyber attacks and update of defence mechanisms
2) Focus not only technology, but consider also processes and people
3) Design and implement both preventive, detective and reactive controls
4) Crucial elements:
   - The identification and prioritization of risks
   - Use of an established framework
   - The risk stemming from third parties and new technologies must be identified and managed

Grand Launch of 'CyberDefender'

- One-stop shop
- Providing timely and comprehensive information on Cyber Security, Information Security and prevention advice of Technology Crime

Grand Launch of 'CyberDefender'

https://cyberdefender.hk/

守網者

THANK YOU

Does anyone have any questions?

ip-sip-col-1-csd-cstcb@police.gov.hk

3661-7712

REFERENCE & CREDITS

- 2018 State of Cybersecurity in Small & Medium Size Businesses, Ponemon Institute
- Cybersecurity Exposure Index (CEI) 2020
- IBM - Cost of a Data Breach Report 2021
- IBM Security X-Force Threat Intelligence Index 2021
- IT Governance Ltd - Cyber security solutions
- MITRE - Cyber Resiliency Case Study
- NIST: Cybersecurity Framework Overview
- NIST Special Publication 800-160 Volume 2 “Developing Cyber Resilient Systems: A Systems Security Engineering Approach”
- NortonLifeLock – The Cyber Resiliency Blueprint
- Slidesgo
- SSH Hong Kong Enterprise Cyber Security Readiness Index Survey 2020
- Verizon – Insider Threat Report
- Verizon- 2020 Data Breach Investigations Report