Cybersecurity in Healthcare
醫療保健業的網絡安全

Fuller Yu
Chief Information Security Officer, Hospital Authority
Co-Chair of Cyber Security Work Stream, Global Digital Health Partnership (GDHP)

October 2021

Healthcare Industry is an attractive target of cyber attacks

"Low hanging fruit" target

High value of patient records

Scarce cybersecurity resources

Increasing digital transformation

Cybersecurity Challenge in Healthcare Organisation

IT&HI

Cybersecurity Challenge in Healthcare Organisation

- Huge volume of medical data need to be protected
- Extended data exchange with increased third parties

- Clinical IT systems as mission critical
- Medical devices with inadequate security controls
- Risks of emerging technologies (Cloud, AI, 5G, Big Data)

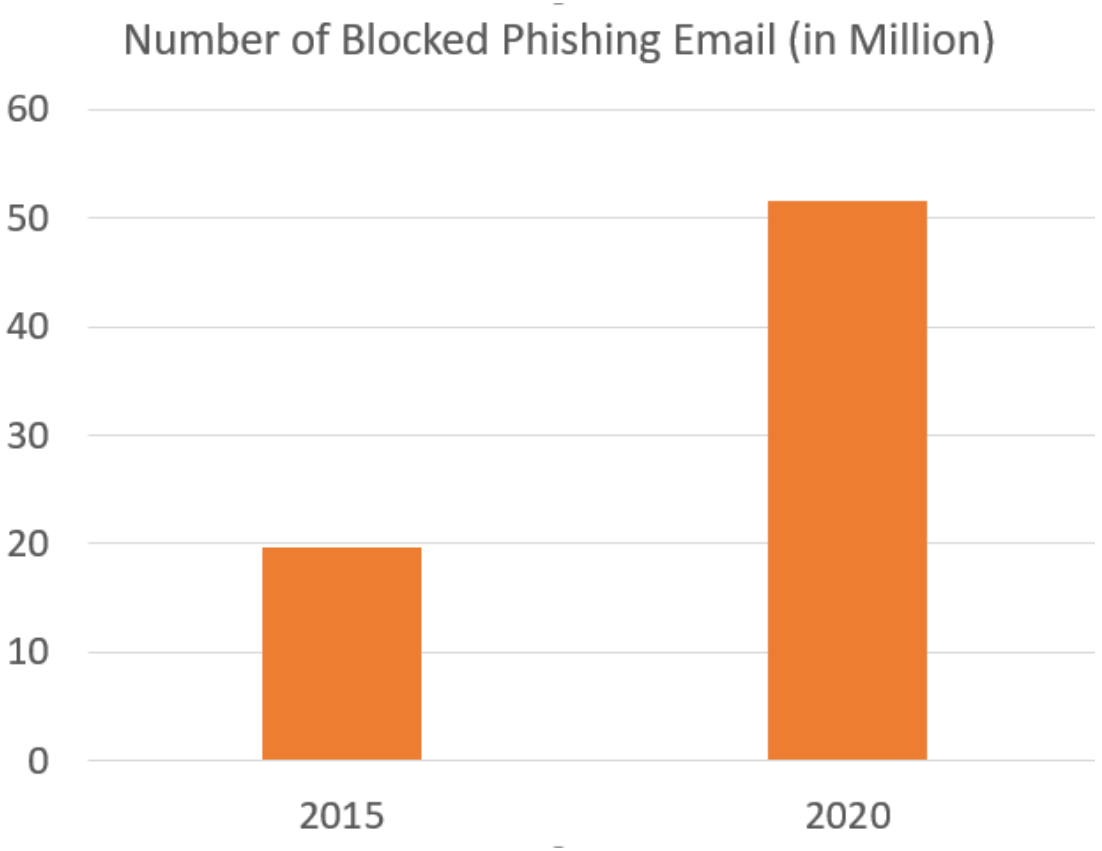
- Insufficient awareness training among healthcare workers
- High demands for anytime anywhere access

IT&HI

Phishing Attacks to End User - the Weakest Link

COVID-19 Themed Phishing Email Attack

- Scams (sell mask, vaccine, cures)
- Credential Theft
- Malware
- Ransomware



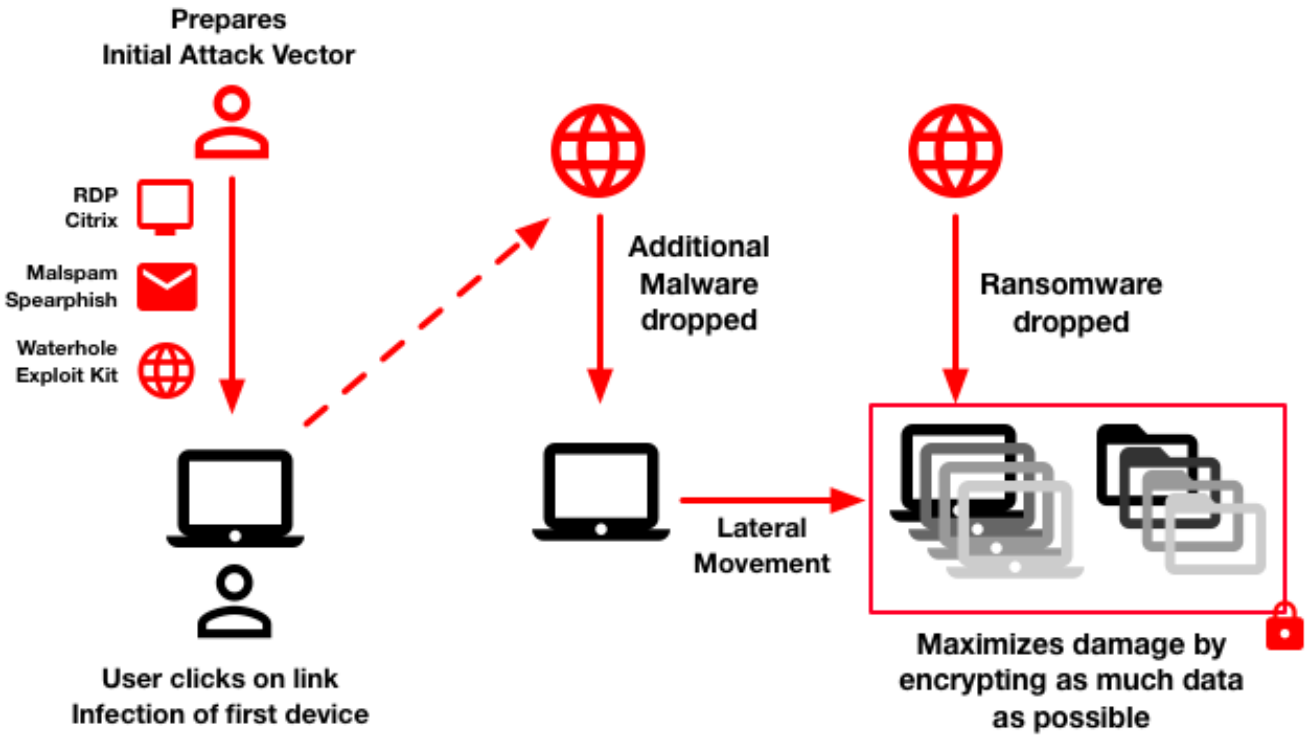
Source: HA Information Security Office

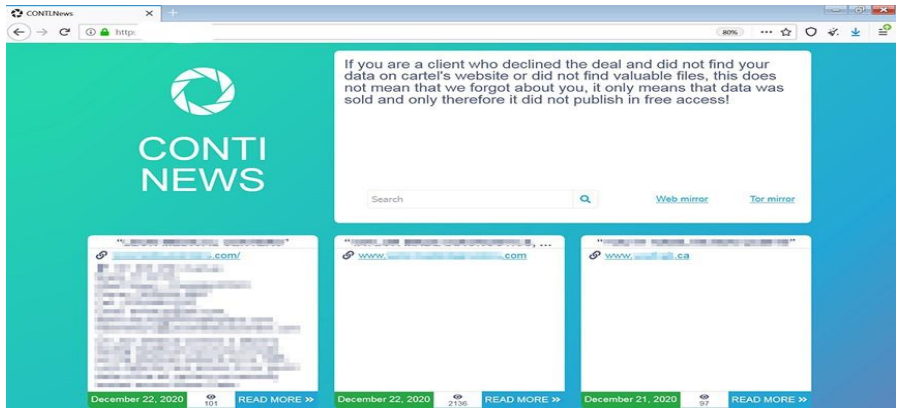
Ransomware is a key cyber threat for healthcare

- Increased ransomware attacks globally
- Clinical services were impacted seriously
- German reported the first patient death case due to ransomware attack in 2020
- US UHS lost USD$67 million due to ransomware attack in 2020
- Ireland HSE hit with USD$20 million ransomware demand in May 2021
- HA blocked several ransomware attack attempts

The Ransomware behind the attacks – Conti

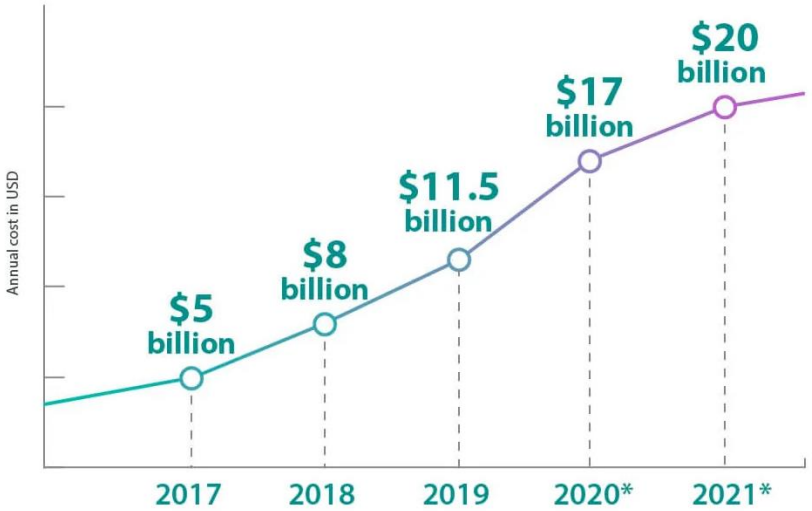
- Ransomware-as-a-service (RaaS)
- End-users are highly targeted
- Lateral movement for days
- Steal & encrypt data
- Double Extortion
- USD$10-40 million ransom





Ransomware would continue to hit the world

- Damage predicted to reach US$20 billion by 2021



Source: Cybersecurity Ventures

Defense Strategy

- Get the basic right (Hardening, Backup, etc)
- Assume the bad guys are already in
- Focus on detection and response capability
- Threat Intelligence from dark web
- Multiple layered approach - Defense in depth
- Cybersecurity & Cyber Resilience

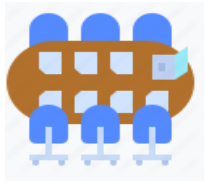
Source: peraton.com

IT&HI


KEEP
CALM
AND
BE
PREPARED

Opportunity to improve Cybersecurity in Healthcare

Cybersecurity is treated as a patient safety issue



Cybersecurity risk is a board level agenda and priority

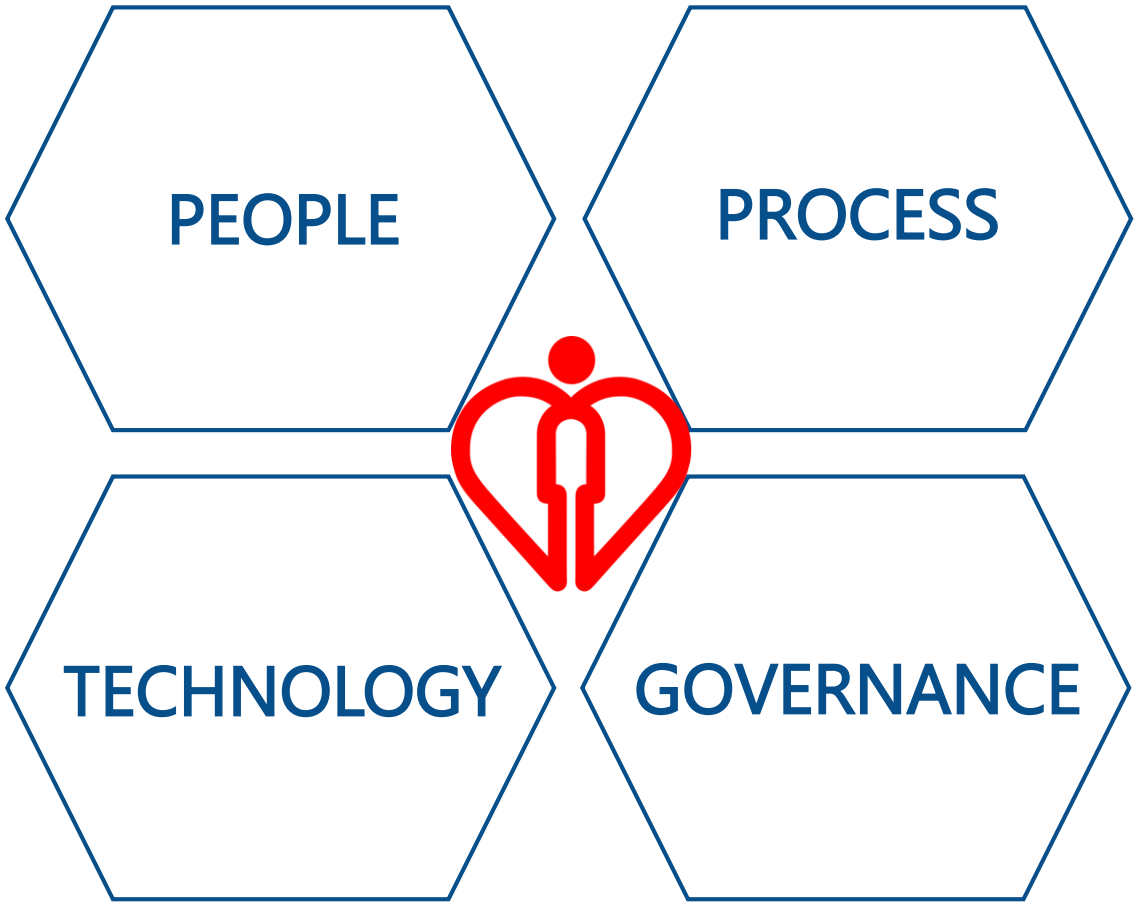
End users are more aware of cyber incidents and their impacts

More security measures being developed for medical devices

Increased local and global cyber intel sharing network platforms

Start with a sound and practical Cybersecurity Strategy

- Culture
- Awareness
- All Staff Engaged

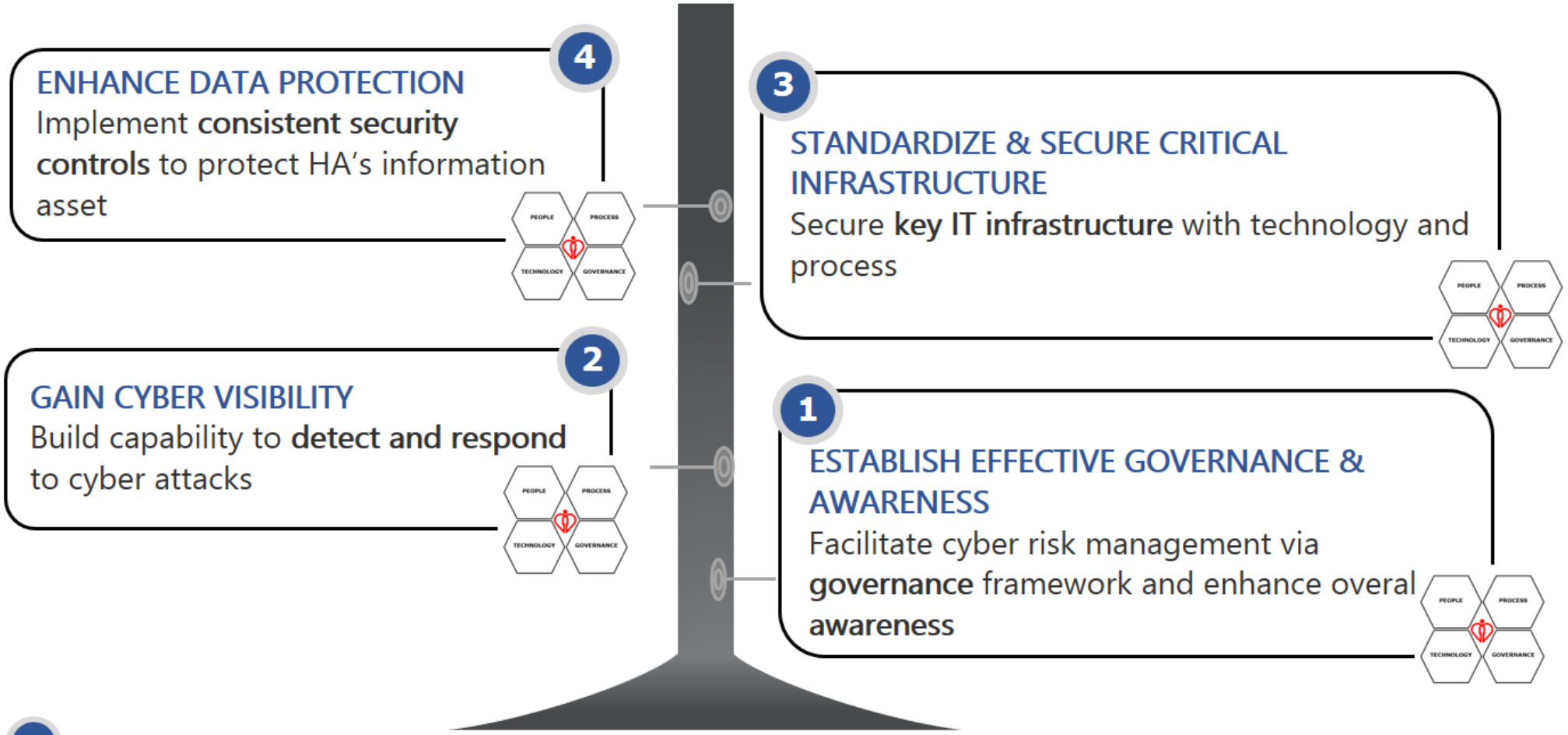


- Centralized
- Standardized
- Closed Loop

- Prevention
- Detection
- Response

- Dedicated Function
- Targeted Ops Model
- External Collaboration

Start with a sound and practical Cybersecurity Strategy

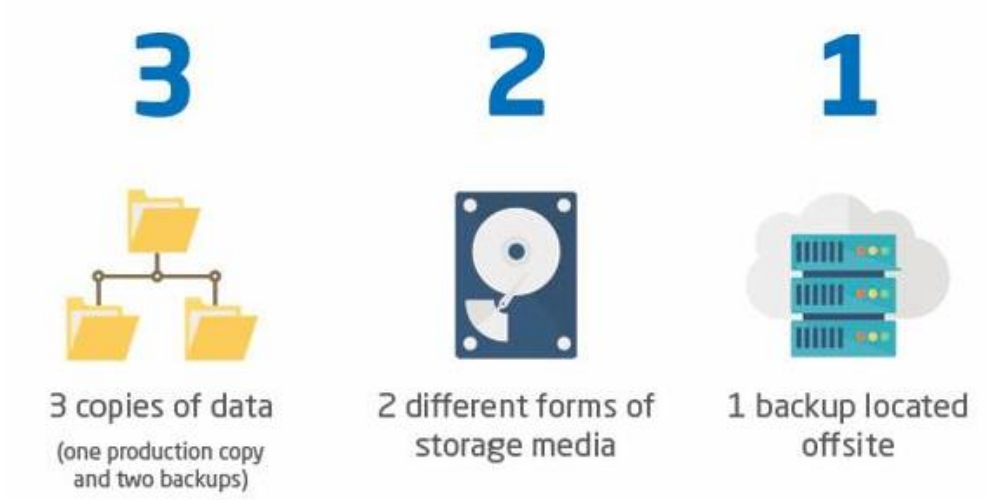


Get the basic right to avoid being low hanging fruit

Source: HKCert.org

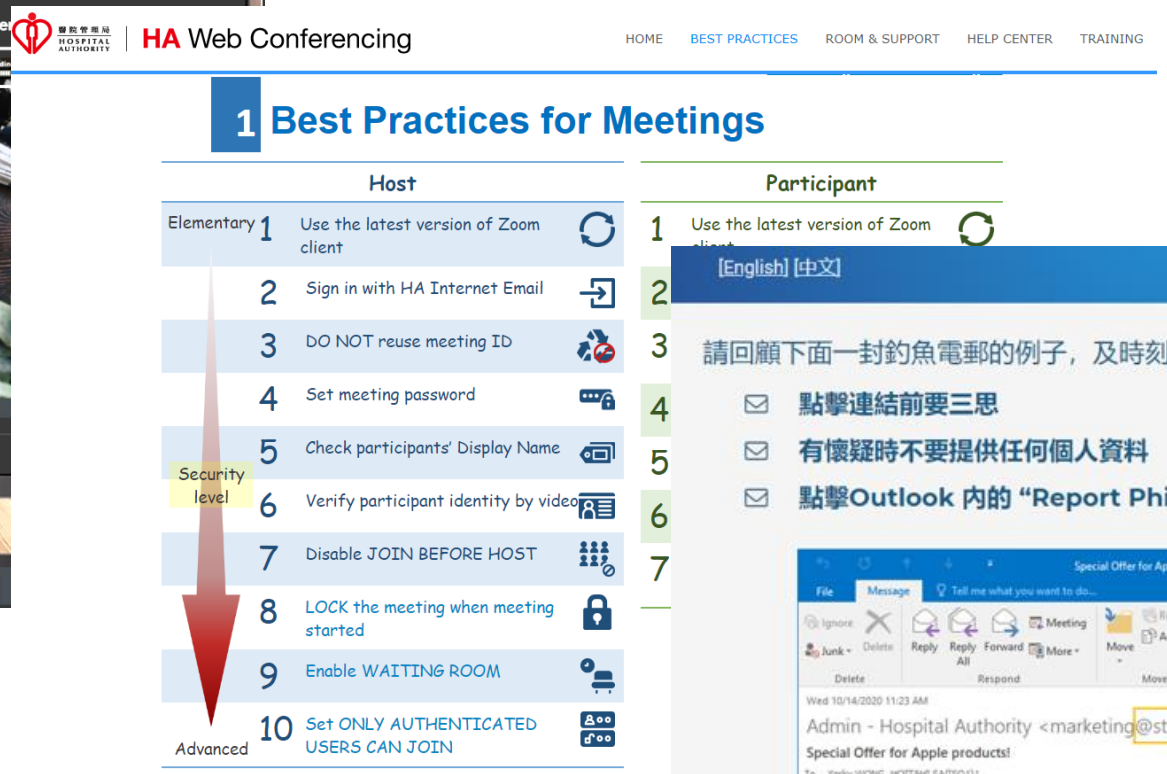
Plan and prepare for the worst

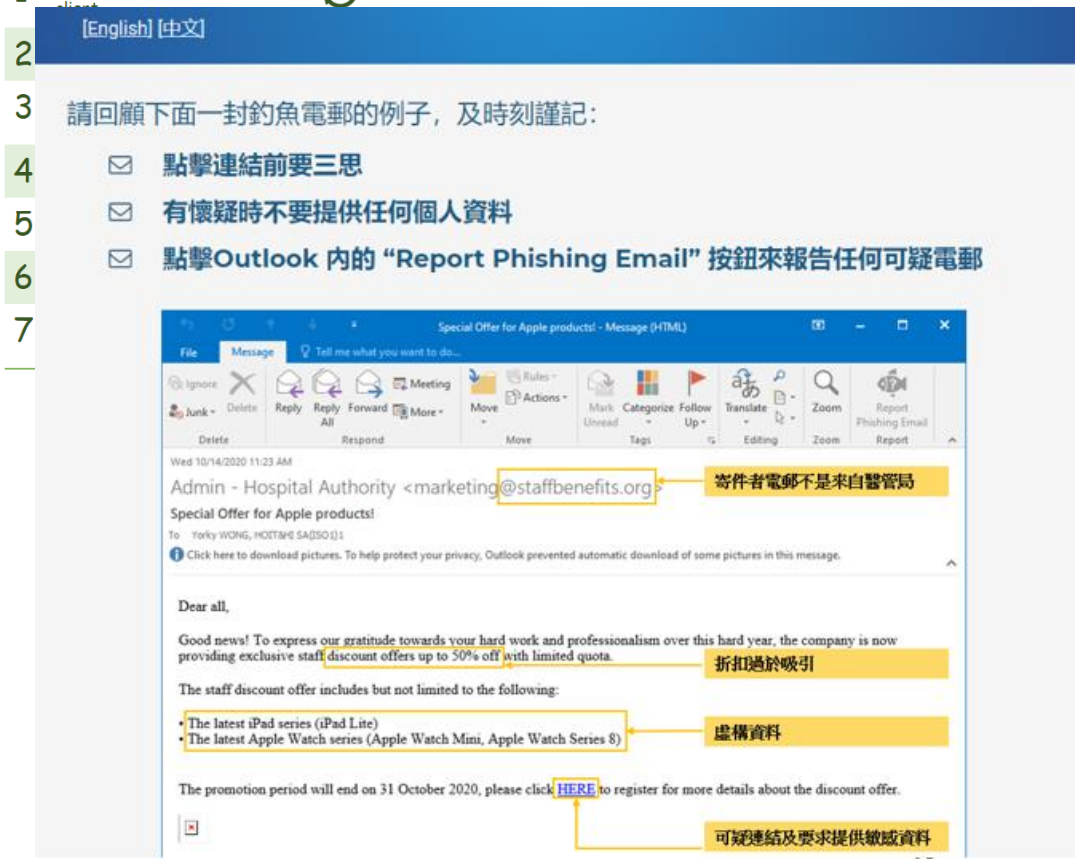
- Implement 3-2-1Backup
- Establish a Business Continuity Plan (BCP)
- Drill the BCP plan regularly
- Engage business and users (e.g. PR)



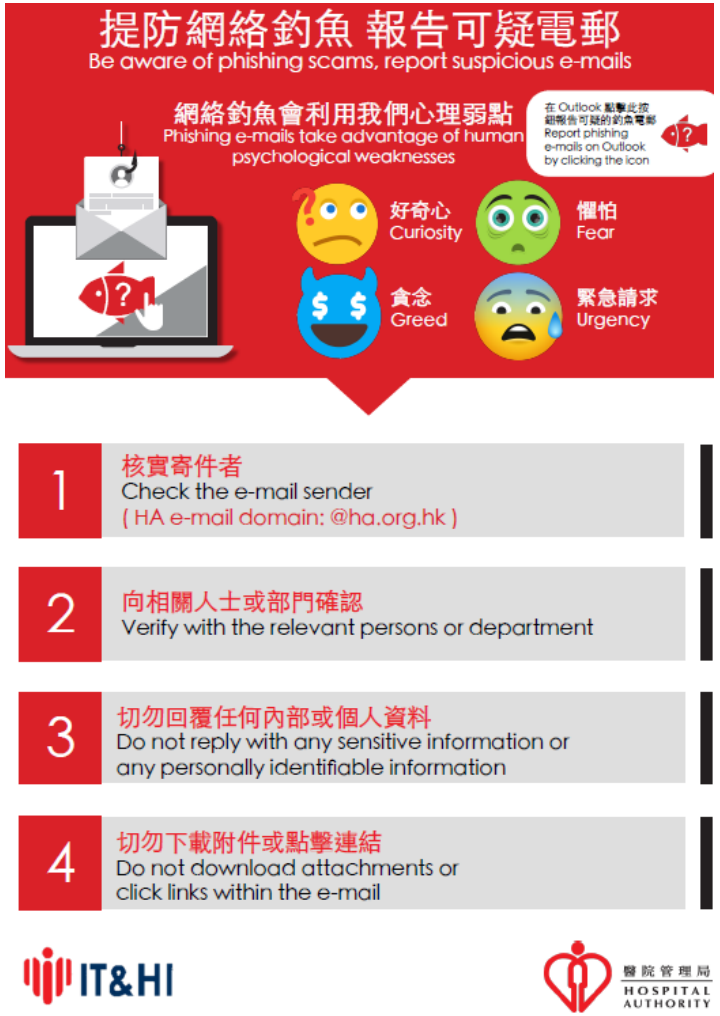
IT&HI

Cultivate a cyber risk aware culture focusing on cyber hygiene





Cultivate a cyber risk aware culture focusing on cyber hygiene



IT&HI

Cultivate a cyber risk aware culture focusing on cyber hygiene

Source: HKCert.org

Cybersecurity is a Team Sport

Everyone has a role to play

IT&HI

Thank you!