Information Technology Security and Data Protection

Office of the Government Chief Information Officer

C K Ng
Senior Systems Manager (Cyber Security)

15.7.2024

Security Threat Landscape

News on security incidents

- Ransomware
- Data leakage
- DDoS attack
- Website defacement

Security incidents reported to HKCERT

HKCERT
Hong Kong Computer Emergency Response Team Coordination Centre

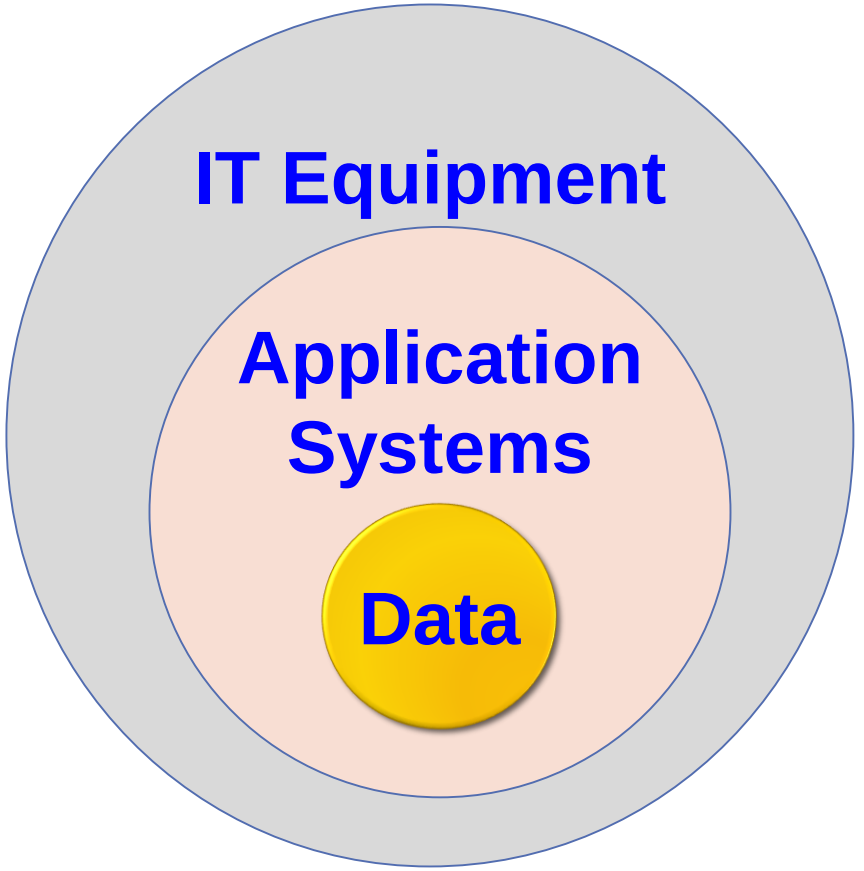
25,392+	21,975+	5,326+	219+	122+	4,183+
Botnet	Phishing	Malware	Web Defacement/Intrusion	Distributed Denial-of-service	Others

Assets for IT

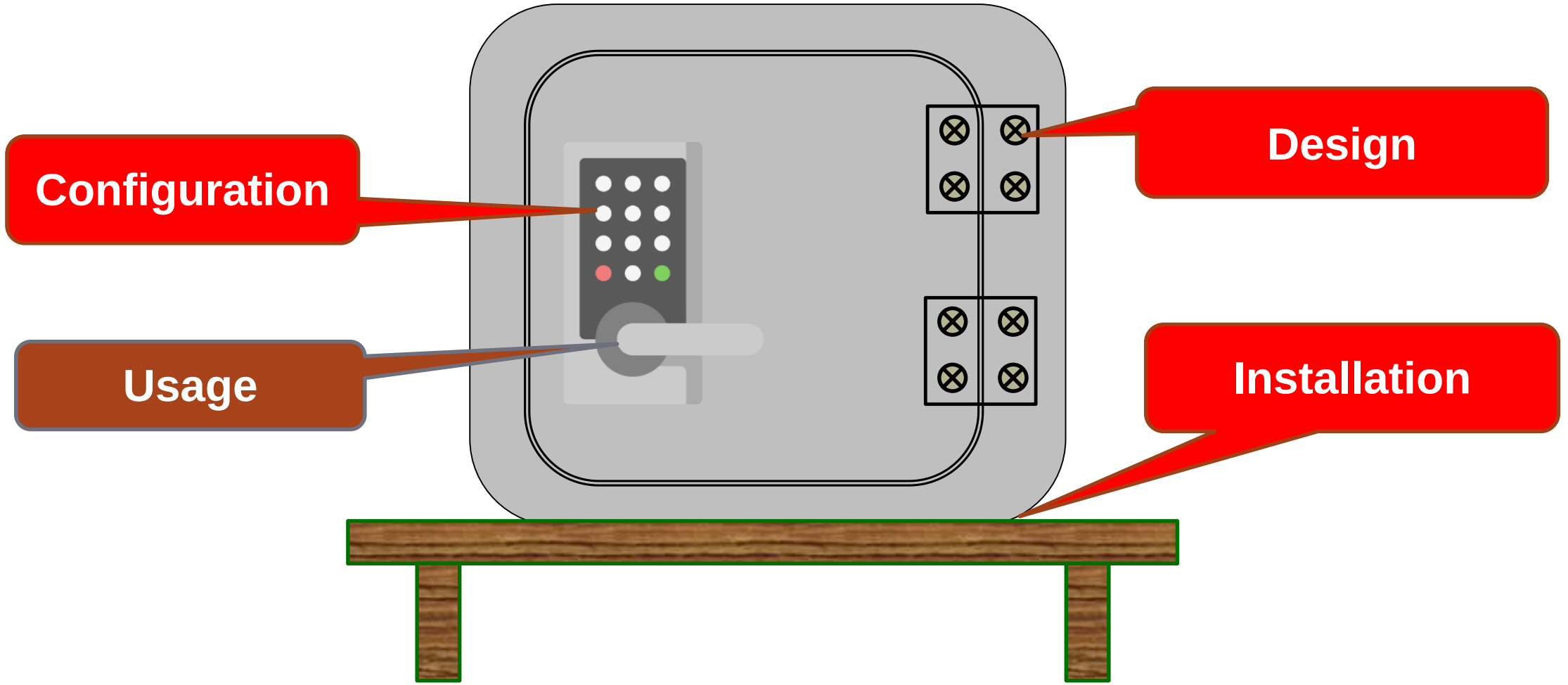
Hardware

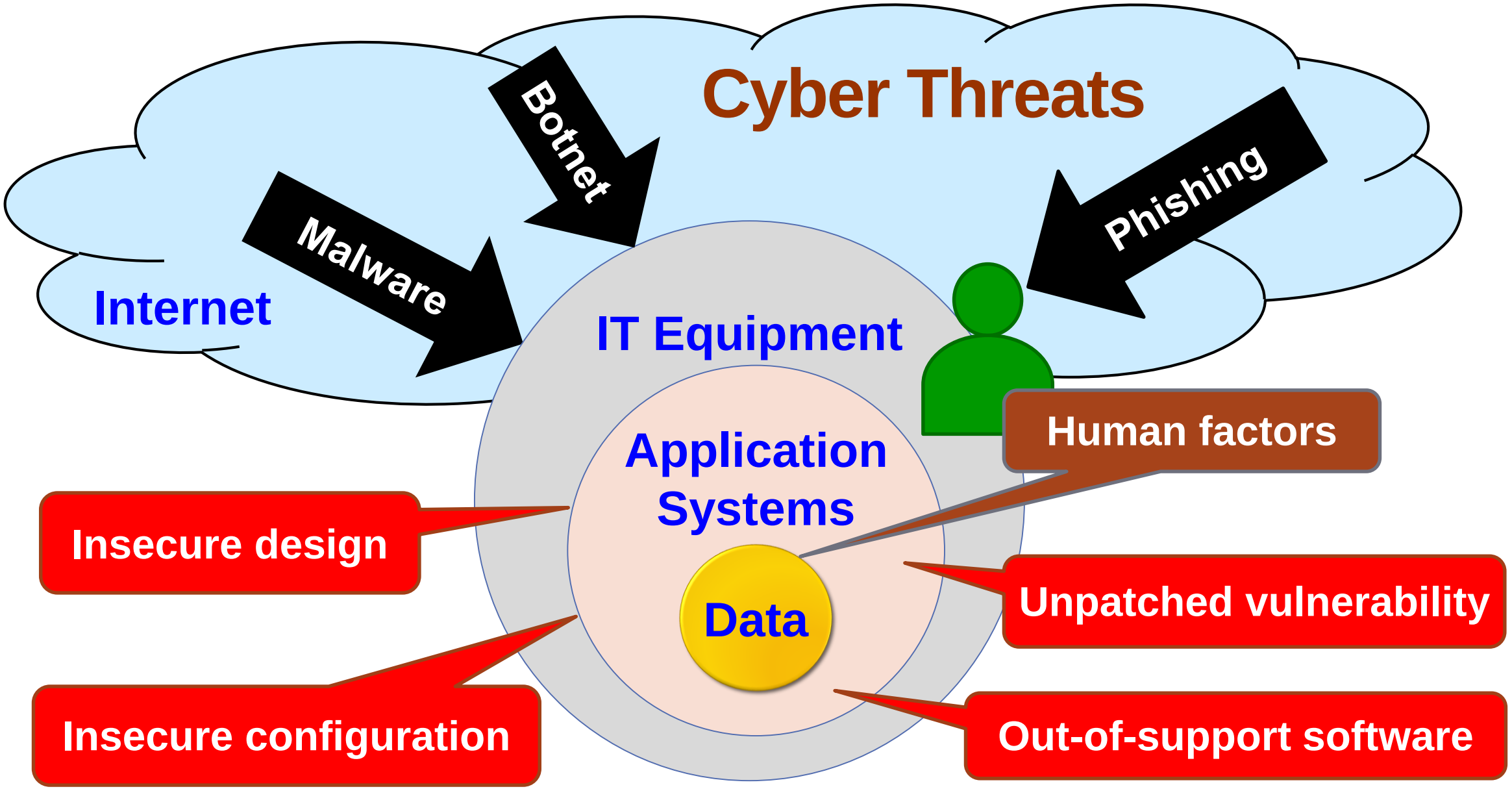
Software

Data



Security Issues



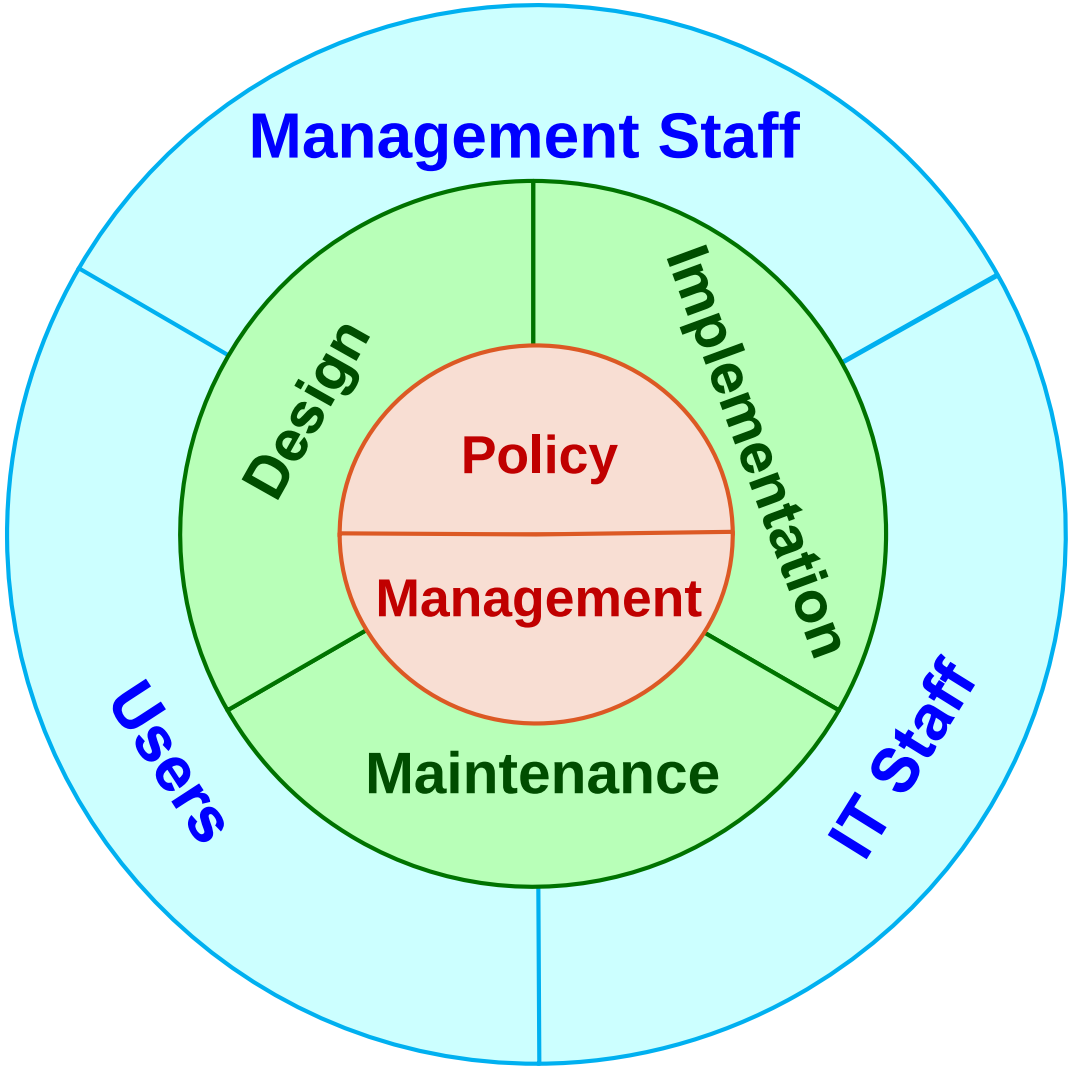

Cyber Threats
Botnet
Malware
Phishing
Internet
IT Equipment
Application Systems
Data
Human factors
Insecure design
Unpatched vulnerability
Insecure configuration
Out-of-support software

Security Framework

Governance

IT System

People



Governance

Security Policy

- Rules and regulations
- Guidelines
- Procedures
- Checklists

Security Management

- Organisation
- Responsibility
- Policy Implementation
- Risk Management

IT System - Design

Design Principle

- Security by Design
- Privacy by Design
- Risk Management

Data Protection

- Classification
- Access control
- Authentication (password, multi-factor)
- Encryption (standard, key length)
- Backup (copies, locations)

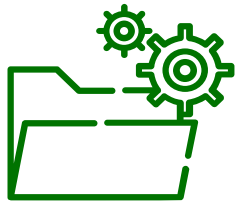
Security Assurance

- Security Risk Assessment
- Privacy Impact Assessment (personal data)

IT System - Implementation

Configuration

- Server hardening guide
- Default setting, user account & password
- Encryption of sensitive data



Tests

- Function test
- Load / stress test
- User acceptance test
- Recovery test & drill
- Reliability test & trial run

Security Assurance

- Security Risk Assessment
- Security Audit
- Privacy Impact Assessment (personal data)

IT System - Maintenance

Preventive measure

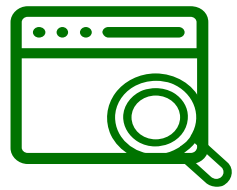
- Software vulnerability
  - Apply patches ASAP
- Software end-of-support
  - Timely upgrade / replace

Periodic exercise

- Security Assurance
- Backup restoration test
- Recovery drill
- Incident response drill

Ongoing activity

- Potential unauthorised access or suspicious activities monitoring
- Log management
- Web scanning
- Cyber security information sharing



People

Management Staff

- Organisation
- Responsibility

IT Staff

- Capability building
- Certification

Users

- Operation
- Awareness

User awareness

Objective

- Be accountable for all their activities
- Follow security mechanism to prevent leakage of and unauthorised access to information

Topic

- Phishing: email, SMS, instant messaging, social media, phone …
- Malicious attachment, website, link, QR code …
- Malware / ransomware
- Handling of personal and sensitive information
- Use of technologies: remote access, IoT, AI, Blockchain …

Format

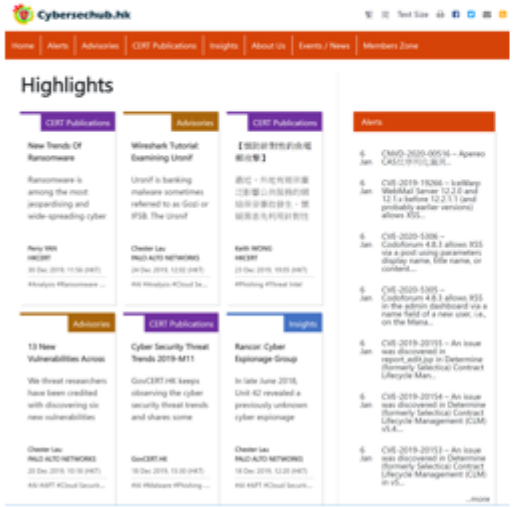
- Training: classroom course, sharing session
- Self-study: interactive online course, quiz, video
- Phishing drill
- Role-based content in training

Useful Resources

GovCERT.HK
www.govcert.gov.hk

Cyber Security Information Portal
www.cybersecurity.hk

Cybersechub.hk
www.cybersechub.hk



InfoSec Website
www.infosec.gov.hk

Useful Resources

HKIRC (www.hkirc.hk)

- Cybersec Training Hub
- Web Scan

HKCERT (www.hkcert.org)

- Seven Habits of Cyber Security for SMEs
- Check Your Cyber Security Readiness Tool
- Incident Response Guideline for SMEs

HKPF CSTCB (cyberdefender.hk)

- Scameter website
- Scameter+ mobile app

PCPD (www.pcpd.org.hk)

- Investigation reports of data breach incidents

The most important

Thank You !!!

- Establish the IT security policy
- Manage the implementation of policy
- Design, implement and maintain IT systems
- Use the IT systems and handle the data