



Cyber Security Management Training for Welfare Sector

SC LEUNG | Summ CHAN | 2020/2021

Background

- This management training is one deliverable of **The Pilot Project of Information Technology Security Audit for Non-governmental Organizations of the Welfare Sector in Hong Kong (The Pilot Project)**
- The Pilot Project aims to raise the participating NGOs' awareness and knowledge of IT security, also enhance NGO's IT security level.

22 Participating NGOs of the Pilot Project

8 "Large NGOs"
(>1,000 staff members)

6 "Medium NGOs"
(400-999 staff members)

8 "Small NGOs"
(<400 staff members)

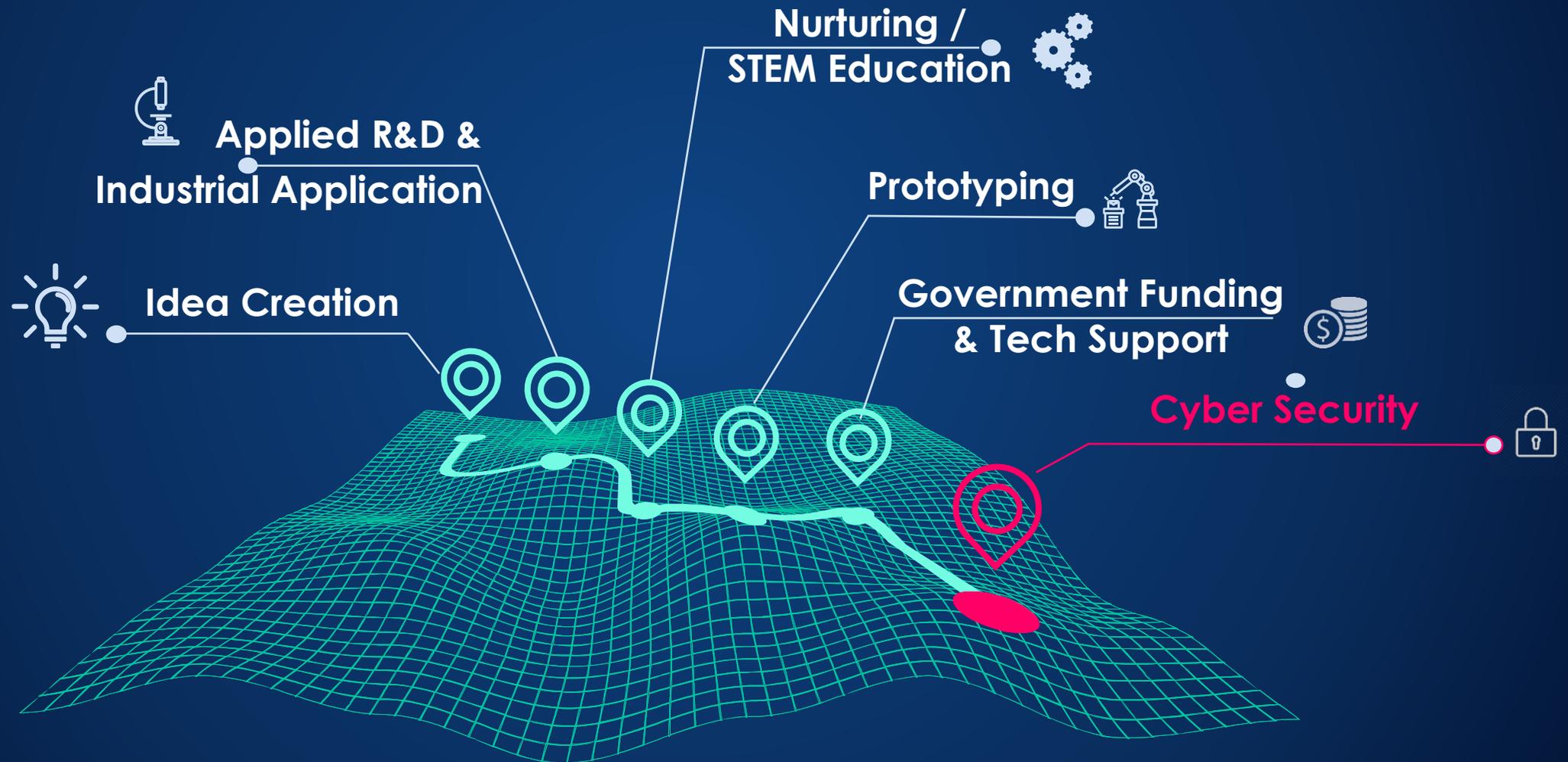
Who am I?

- **Senior Consultant**
 - @HKCERT since 2001
 - International and local liaison, strategic planning, supervision of CERT operation
- **Security Designations**
 - CISSP, CCSP, CISA, CBCP
- **Previous industrial experiences**
 - ISP & Telecommunication
 - Multinational Banking
 - Multinational IT Consultancy
 - Software Distribution



SC Leung

What HKPC Does





01

Security Alert Monitoring
and Early Warning

www.hkcert.org

02

Report and Response

Hotline: **8105 6060**

03

Publication of Security
Guidelines and Information

04

Promotion of Information
Security Awareness



Objective of the training

- To raise information security **awareness**
- To learn the **best practices** of information security management policies and workflows
- To learn to consider **resources input and allocation priority**
- To understand the **IT Security Practice Guide for the Social Welfare Sector**
- To allow an **interactive exchange** of experiences and problems

Training Flow (PM)

Time	Activity
2:30pm – 3:15pm	Cyber Security Training – Part 1
3:15pm – 3:25pm	Break
3:25pm – 4:10pm	Cyber Security Training – Part 2
4:10pm – 4:30pm	Q & A and Sharing Session

Agenda (1)

1. Overview Cyber Security for Management

- Cyber Security Landscape of Social Welfare Sector in Hong Kong
- Cyber Security Threats and Trends
- Security Risk and Risk Management

2. Case Study

- New Ransomware Threat
- SingHealth Data Breach
- “Missing USB Drive” incident of Local NGO

Agenda (2)

3. Cyber Security Oversight: Role of Board & Senior Management

- Ensuring the Board's Security Consciousness
- Governance, Accountability and Ownership
- Building a Cyber Security Culture in Your Organisation

4. Steps to Cyber Security for Social Welfare Sector

- International reference: NIST cyber security framework
- IT Security Practice Guide for the Social Welfare Sector



Cyber Security Landscape of NGOs in Hong Kong

Overview of Compliance Status in Different Security Domains

	Security Program	Security Policy	Training & Awareness	Personal Security	Physical Security	Network Security	Logical Access	Operations Management	Incident Management	Business Management	Continuity Management	Asset Management
Compliant	21	11	14	19	17	10	11	5	15	11	9	
Partially Compliant	1	11	8	3	4	12	11	17	7	11	13	
Non-Compliant	0	0	0	0	0	0	0	0	0	0	0	
Non-Applicable	0	0	0	0	1	0	0	0	0	0	0	

Source: Result of IT security audit, scanning (pre-scanning), penetration test for reviewed pilot NGOs

Cyber Security Snapshot of Reviewed Pilot NGOs

Top 5 Common Weaknesses found in Security Audit

- **Operations Management**

- Change Management
- Security Monitoring

- **Network Security**

- Vulnerability Assessment

- **Asset Management**

- Information Classification

- **Logical Access**

- Identity Management

Addressed in Practice Guide

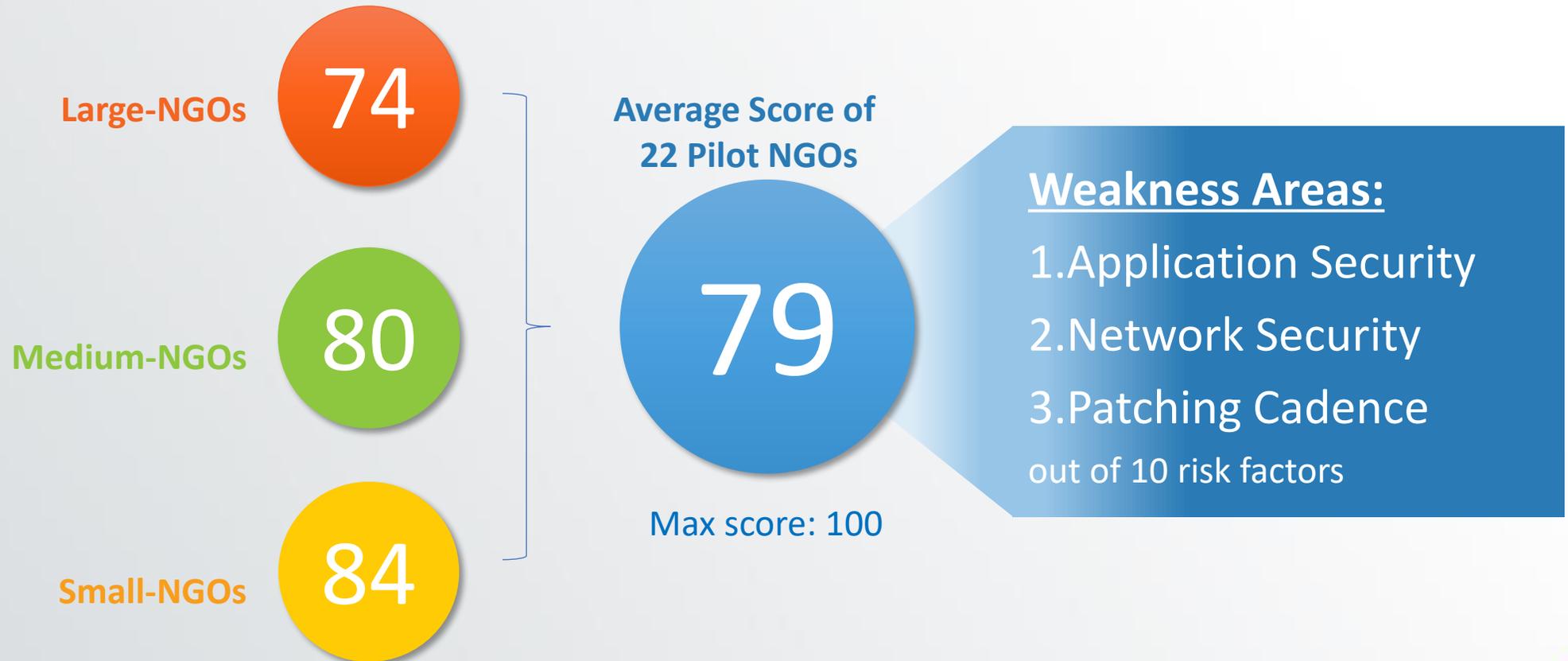
- 6.1.5 Configuration Management
- 6.1.6 Log Management and Monitoring

- 6.1.2 Asset Management
- 6.11 Security Risk Assessment and Audit

- 6.2.13 Information Classification

- 6.2 Password Control and Authentication

Cyber Security Scoring * Result over Reviewed Pilot NGOs



Source: Security Scorecard result of 22 Reviewed Pilot NGOs. Score is based on security exposure of digital footprints of the organisations

SSH Hong Kong Enterprise Cyber Security Readiness Index Survey 2020

May 2020

Source: SSH Hong Kong Enterprise Cyber
Security Readiness Index Survey (May 2020)
by HKPC

<http://u.hkpc.org/ssh2020>

Hong Kong Enterprises Top Cyber Attacks

Type of Incidents	
External Attacks (e.g. Phishing Email, Ransomware, Malware)	56%
Internal Incidents (e.g. Loss of equipment, abuse of usage, unintended mistake)	10%
Incidents caused by External Partners (e.g. abuse of usage, data leakage)	6%

SSH Hong Kong Enterprise Cyber Security Readiness Index Survey 2020

May 2020

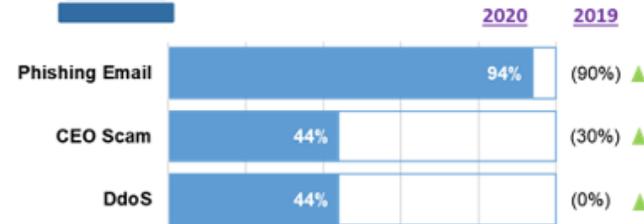
Source: SSH Hong Kong Enterprise Cyber Security Readiness Index Survey (May 2020) by HKPC

<http://u.hkpc.org/ssh2020>

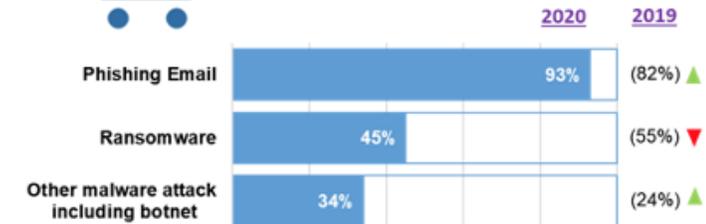
Top Cyber Attacks (by business category)



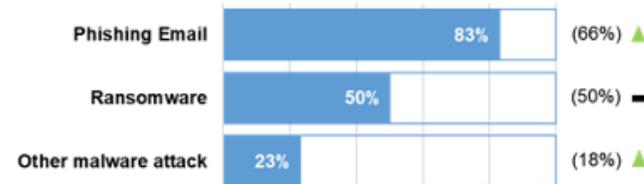
Financial Services



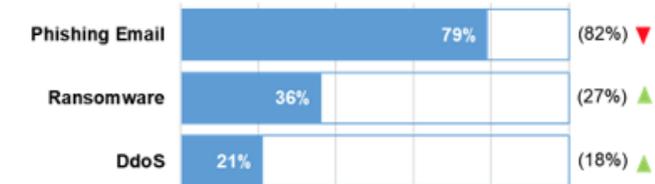
Retail and Tourism Related



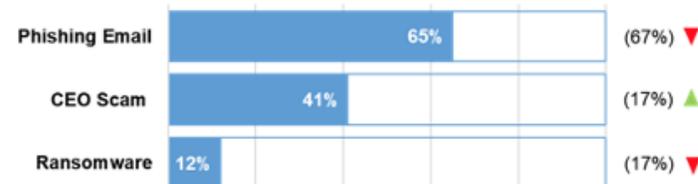
Manufacturing, Trading and Logistics



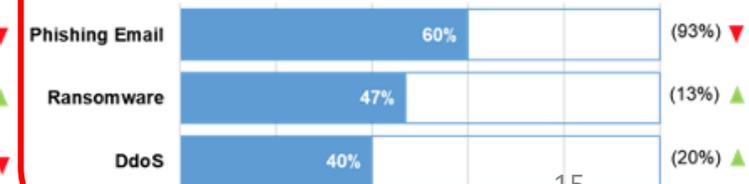
Information and Communication Technology



Professional Services



NGOs, Schools and Others





Cyber attacks against NGOs amid pandemic

- Attackers aimed to benefit from money intended for the pandemic response and capitalize on weaknesses caused by the disruption.
 - **International Red Cross** experienced spike of attack
 - **Mercy Corp.** experienced increase in **phishing** on donations and chances to apply government funding
 - **WHO** experienced double amount of cyber attacks by **fraudulent email and Whatsapp messages** targeting to steal money and information

Highlights on Microsoft Digital Defense Report | Oct 2020 (1)



Top 6 targeted industry sectors by NSNs delivered (July 2019–June 2020)

32% Non-governmental organisations

31% Professional services

13% Government organisations

10% International organisations

7% Information technology firms

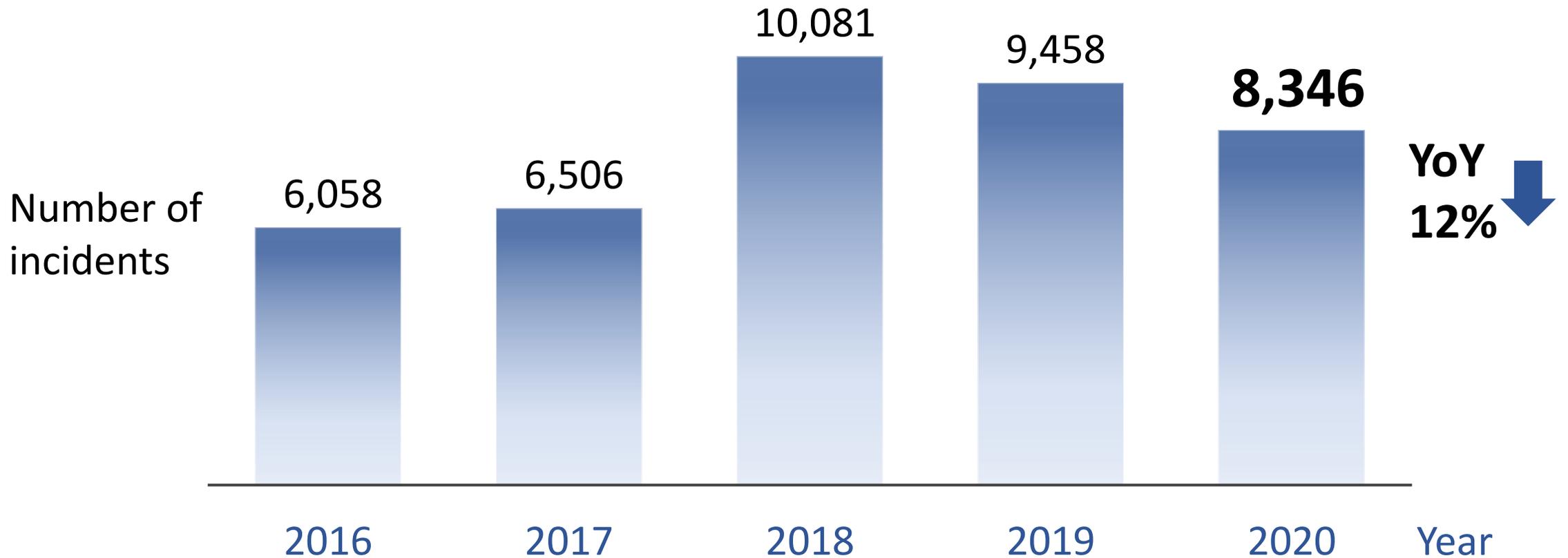
7% Higher education

NGOs targeted: advocacy groups, human rights organizations, nonprofit organizations, and think tanks focused on public policy, international affairs.



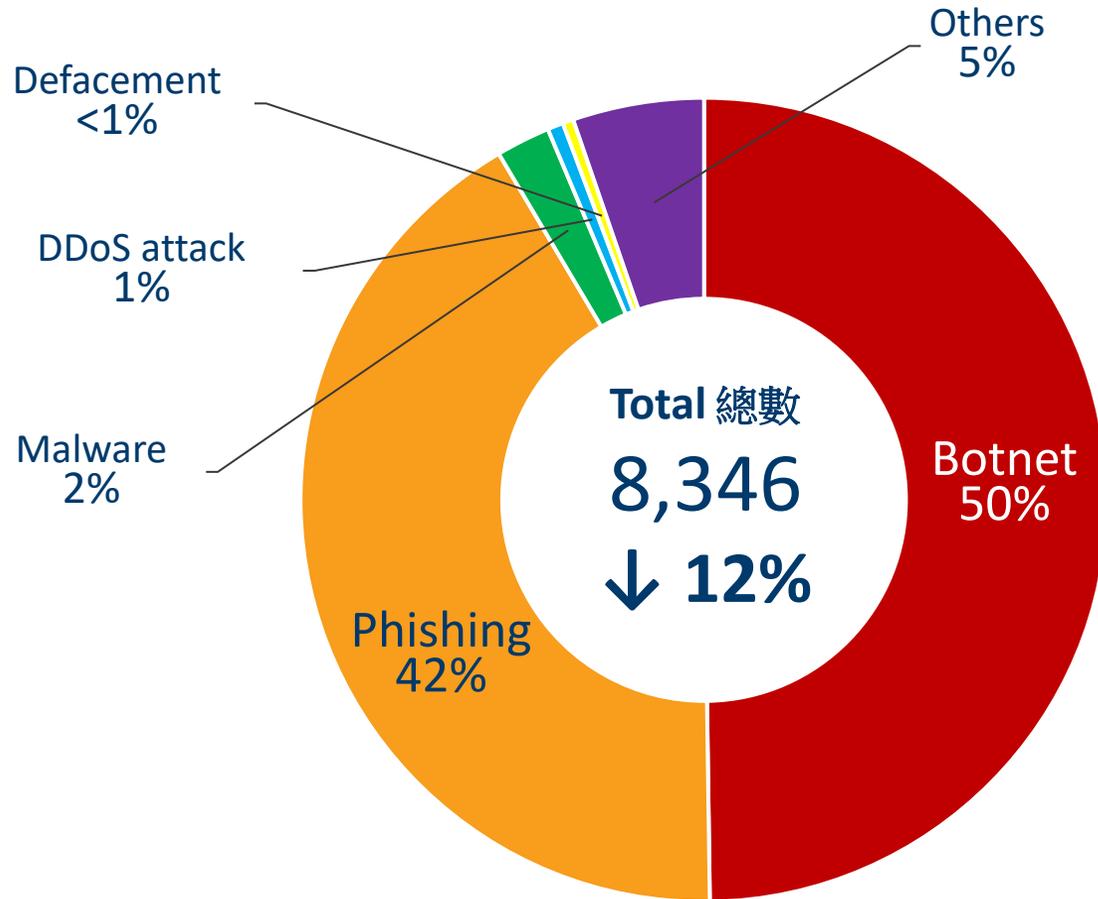
Cybersecurity Threats & Trends

HKCERT Security Incident Reports Handled



Source: HKCERT

HKCERT Security Incident Reports

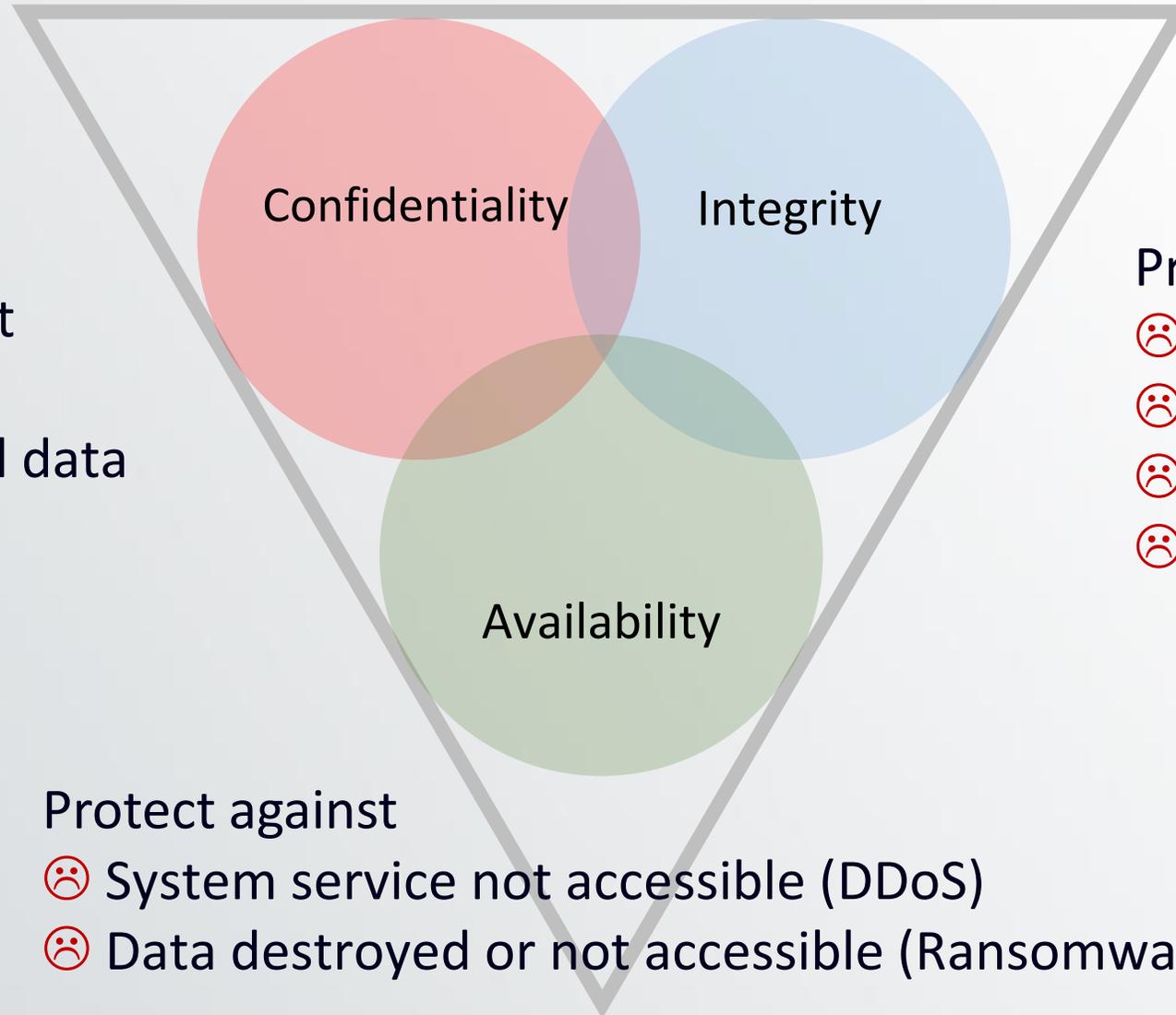


Major Security Incidents

	2019	2020	Change 變化
Botnet	4,922	4,154	↓ 16%
Phishing	2,587	3,483	↑ 35%
Malware	1,219	181	↓ 85%

Ransomware mainly targets the enterprises, causing a drop of personal malware cases

CIA Triad of Cyber Security



Protect against
☹️ Leaking
confidential data

Protect against

- ☹️ Data contaminated
- ☹️ Forged transaction
- ☹️ System compromised
- ☹️ Identity spoofed

Protect against

- ☹️ System service not accessible (DDoS)
- ☹️ Data destroyed or not accessible (Ransomware)

Security 101

威脅

Threats

漏洞

Vulnerabilities

攻擊

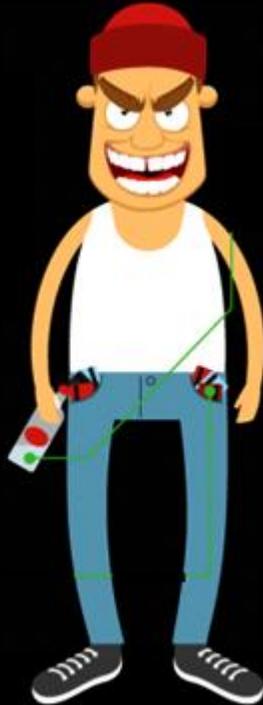
Attacks

風險

Risks

Threat Actors | *Modern Attackers*

Cyber
Criminal



Hacktivist

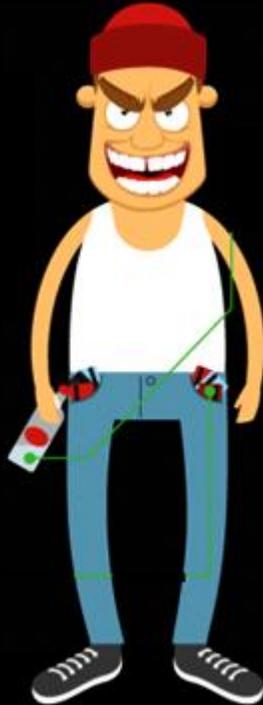


Nation
State



Threat Actors | *Modern Attackers*

Cyber
Criminal

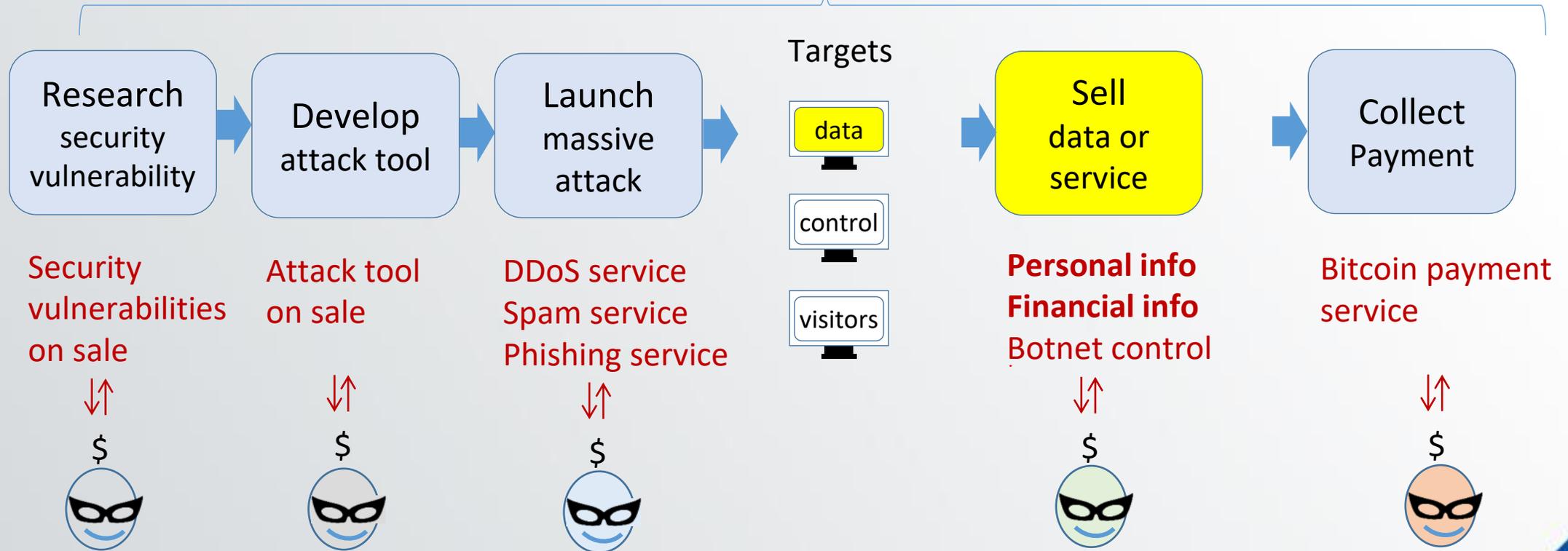


- Motive: \$\$\$
 - ✓ Underground Economy
 - ✓ Crime-as-a-Service
- Botnet infrastructure
- Advanced (banking) Trojan
- Moving to mobile and cloud

Crime-as-a-Service



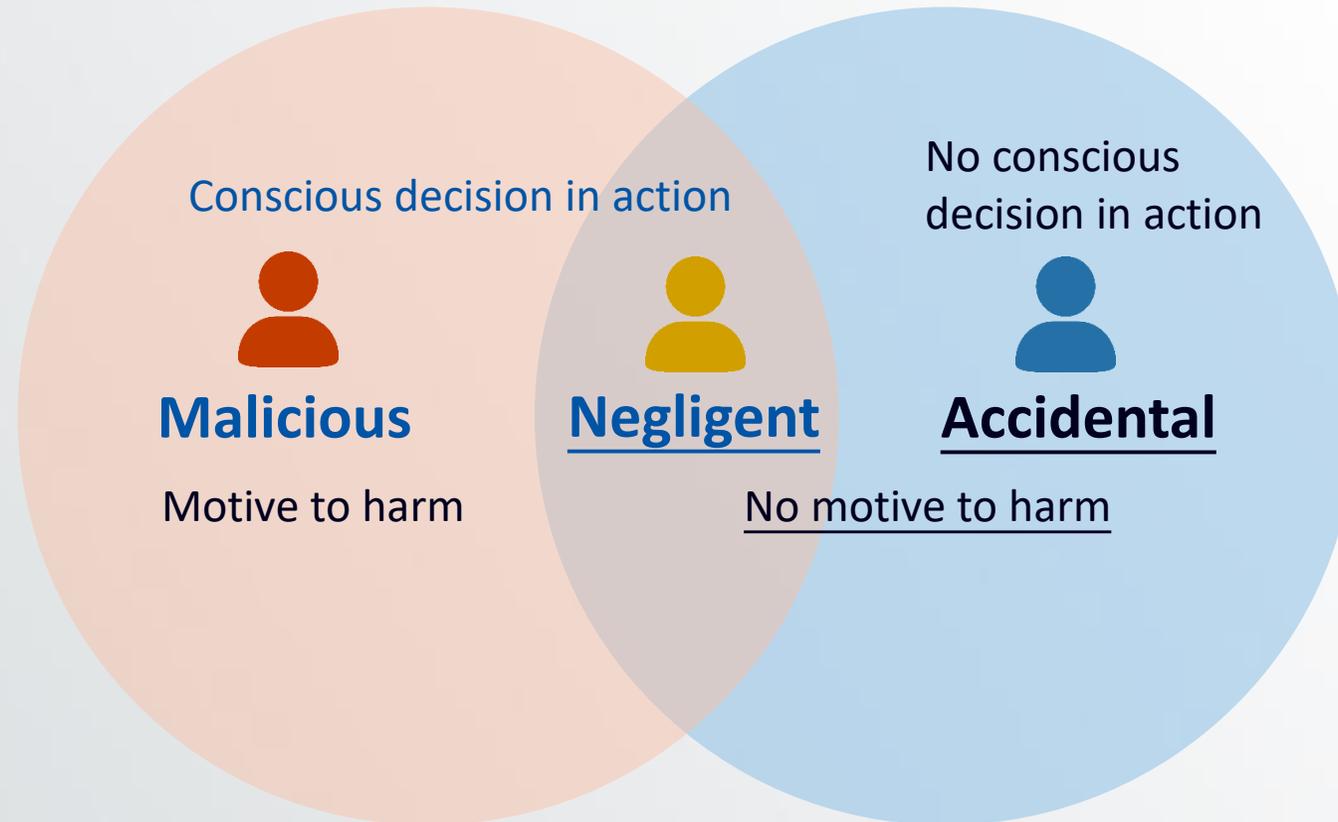
DIY → Service Provision
→ Sharing of Profit



Values in the Underground Market

Rank	Item	Percentage	Range of Prices
1	Credit cards	28%	\$1 - \$30
2	Bank accounts	24%	\$10 - \$125
3	Email accounts	8%	\$5 - \$12
4	Email addresses	5%	\$5 - \$10 per MB
5	Credit card dumps	4%	No specified prices
6	R57 & C99 shells	3%	\$2 - \$5
7	Full identity	3%	\$3 - \$20
8	Mailers	3%	\$1 - \$5
9	Attack toolkits	3%	\$5 - \$20 or \$120 per month
10	Cash-out services	2%	\$200 - 100 or 50% - 70%

Insider Threat



- Insiders pass through the physical wall and network firewall
- They have access to organisation assets
- Impact of insider threat is usually large



A SANS Survey

Written by Dr. Eric Cole

April 2015

*Sponsored by
Veriato*

Insider Threat has great impact

SANS Survey 2015 (772 respondents)

- 33% experienced an insider attack
- 74% most concerned about negligent or malicious insider threats
- Financial impact is significant - potential loss:
 - 19% valued at over US\$ 5M
 - 15% valued at US\$ 1M - 5M



Impacts of Cyber Attacks

Service Disruption

Data Breach or Loss

Financial Loss

Damage to Reputation

Legal Liability



Security Risk & Risk Management

What is Risk?

$$\text{Risk} = \text{Likelihood of exposure} \times \text{Impact of exposure}$$

Security Risk Assessment





Risk

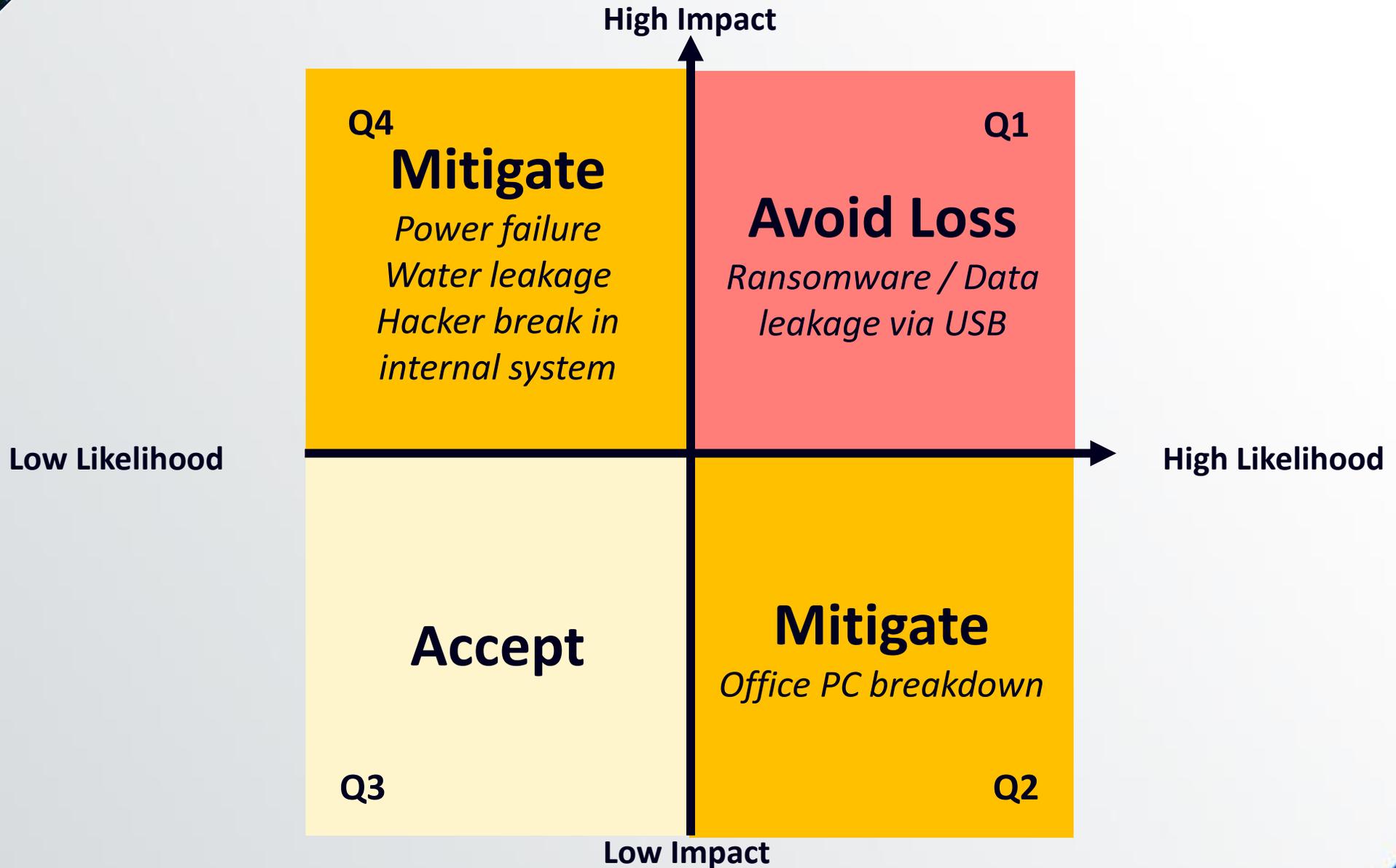
Transfer

Accept

Avoid

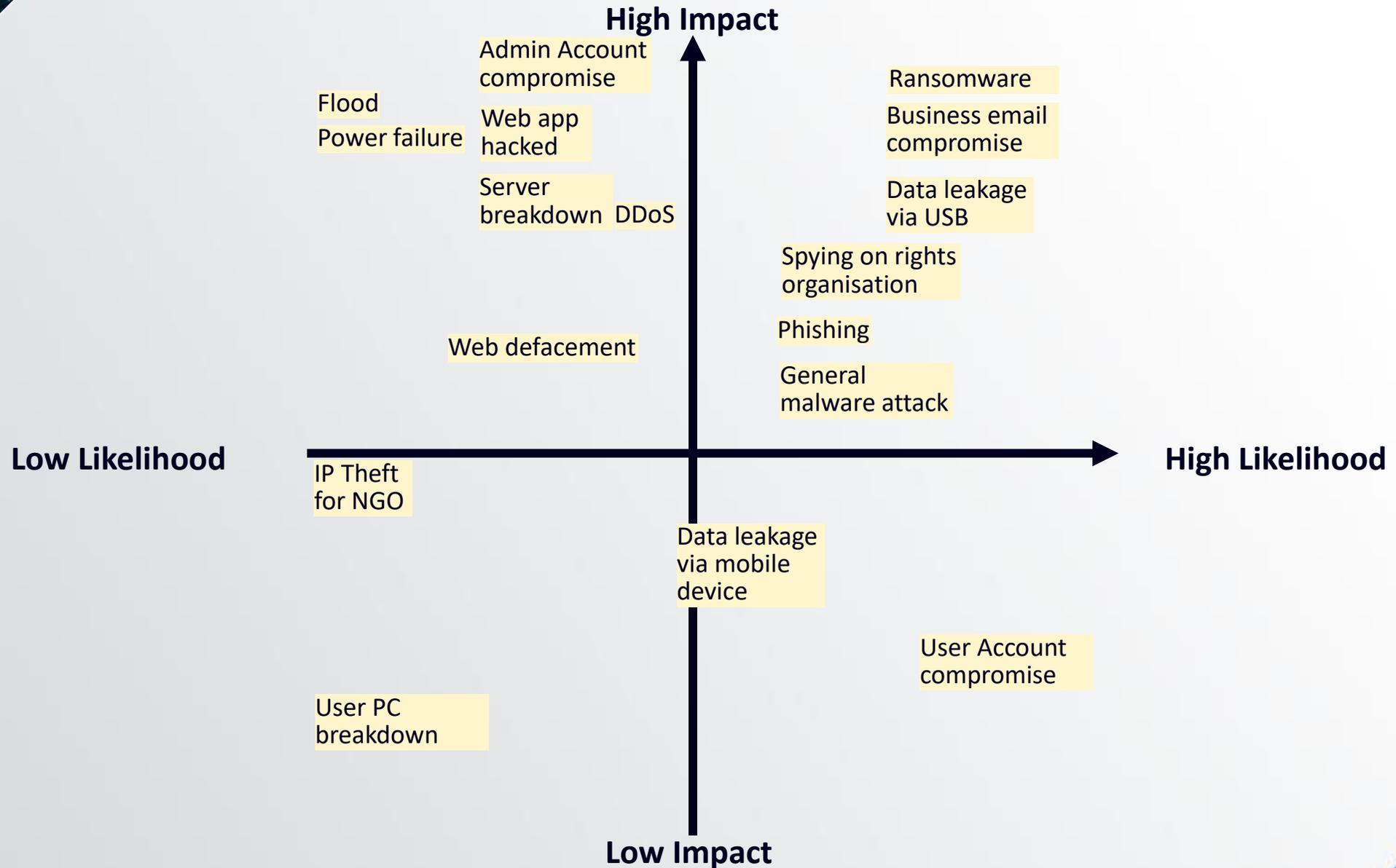
Mitigate

Risk Control Matrix (2x2)



Build your own Risk Control Matrix

(for reference only)





Cyber Security Investments

- Cyber security investment is for **mitigating potential loss** of security breach (vs. traditional concept of ROI), and is
 - **Prioritised according to Risk** (likelihood x impact)
 - **Lower than the expected loss** due to security breach
- Cyber security investment should include these costs
 - IDENTIFY - Regular security **assessment and monitoring**
 - PROTECT - **Technology** (hardware/software/services) and **Maintenance** service
 - EDUCATE - **Training** (technical and user awareness)

TRENDING: Virtual Cybersecurity & Fraud Summit London - 20 October • Live Webinar 10/21 | Simplify Sensitive Data Security Using a

Crypto-Lock and Tell: Ransomware Gangs Double Down on Leaks

Dedicated Leak Sites Are Likely Driving More Victims to Pay, Security Experts Warn

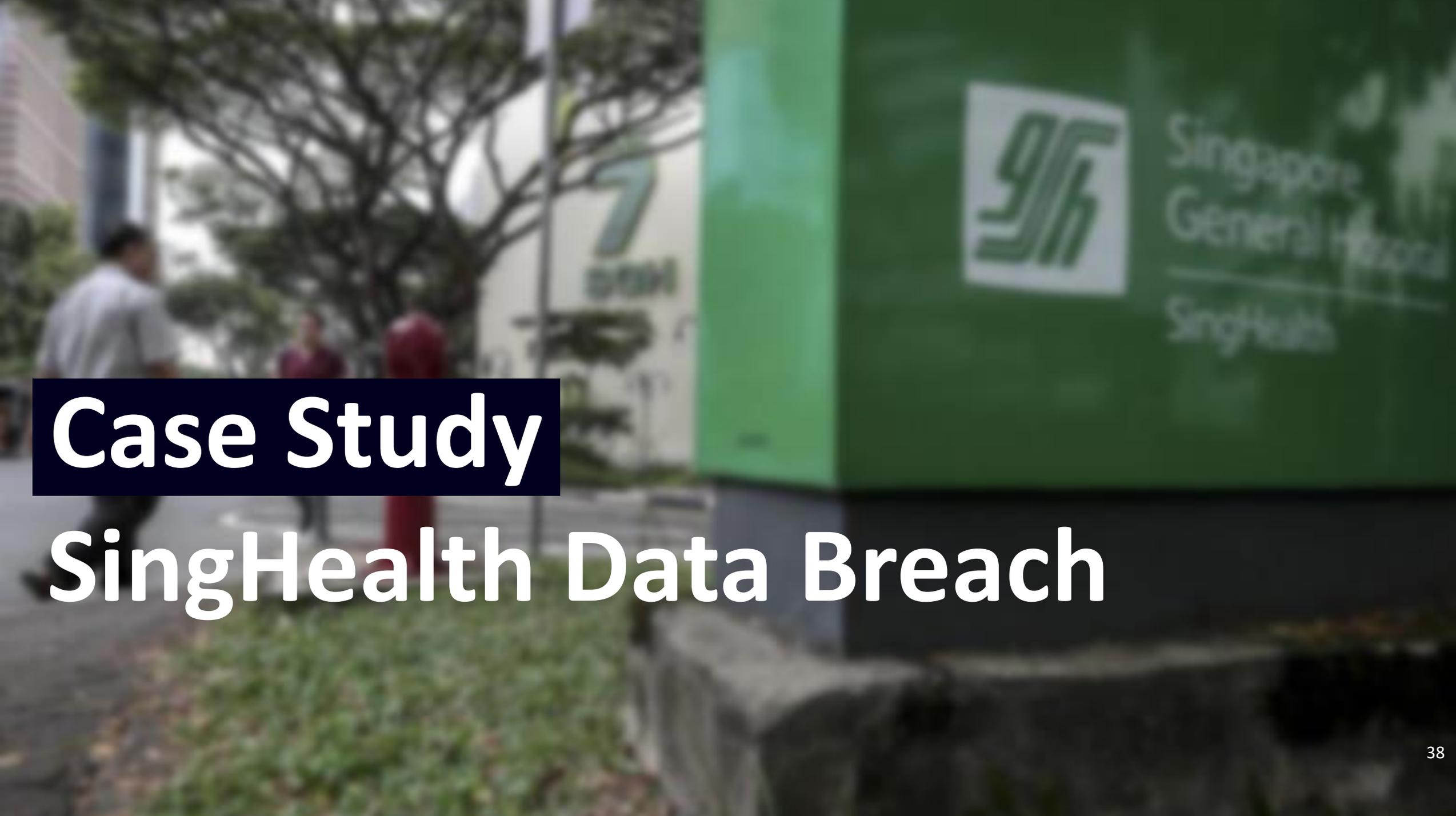
Mathew J. Schwartz ( euroinfosec) · May 15, 2020 



- Hacker will disclose the leaked data to threaten the victim to pay ransom



- Backup of data isn't enough anymore, increase the awareness of employee is crucial



Case Study

SingHealth Data Breach

SingHealth hacking incident 2018

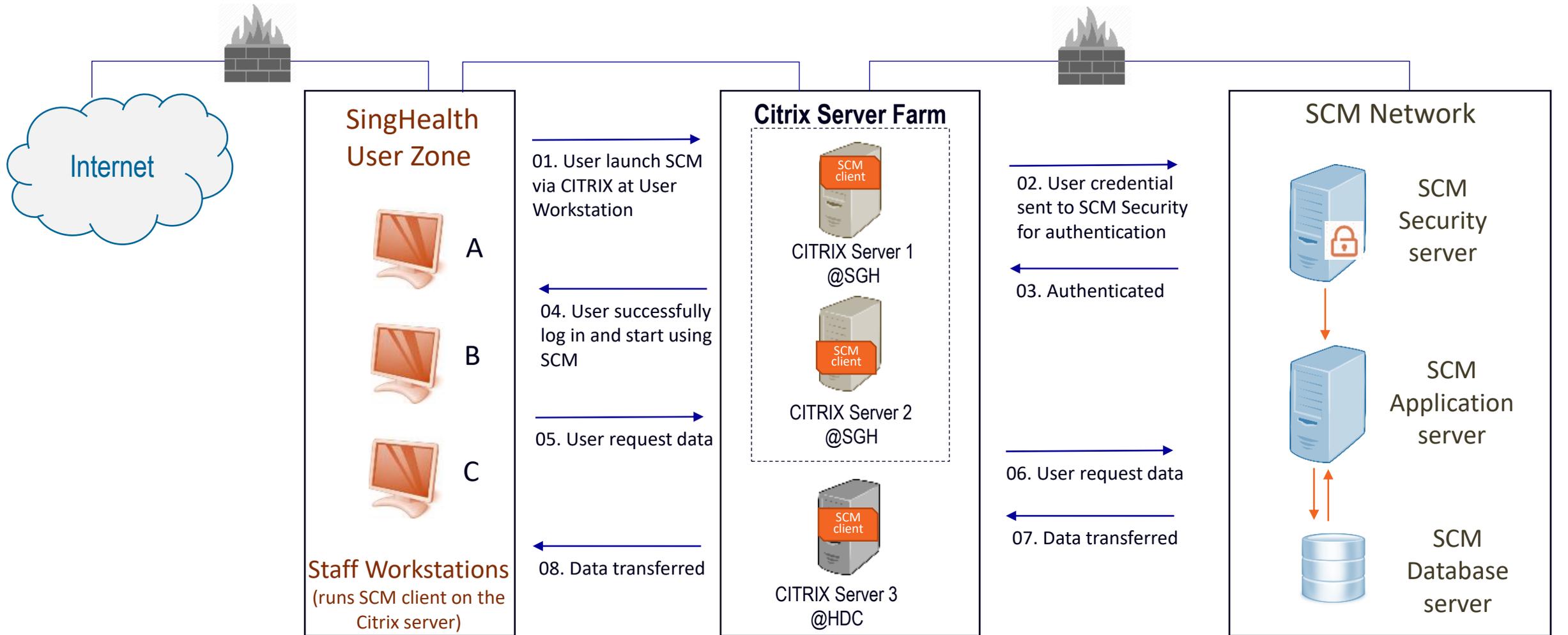


20 July 2018 | SingHealth and CSA announced a SingHealth hacking case

- 1.5M non-medical patient data illegally accessed and copied (including **Prime Minister Lee Hsien Loong**)
- Attack started with a user workstation
- Planned and Organised Attack – **Advanced Persistent Threat (APT)**
- Data copied but not contaminated

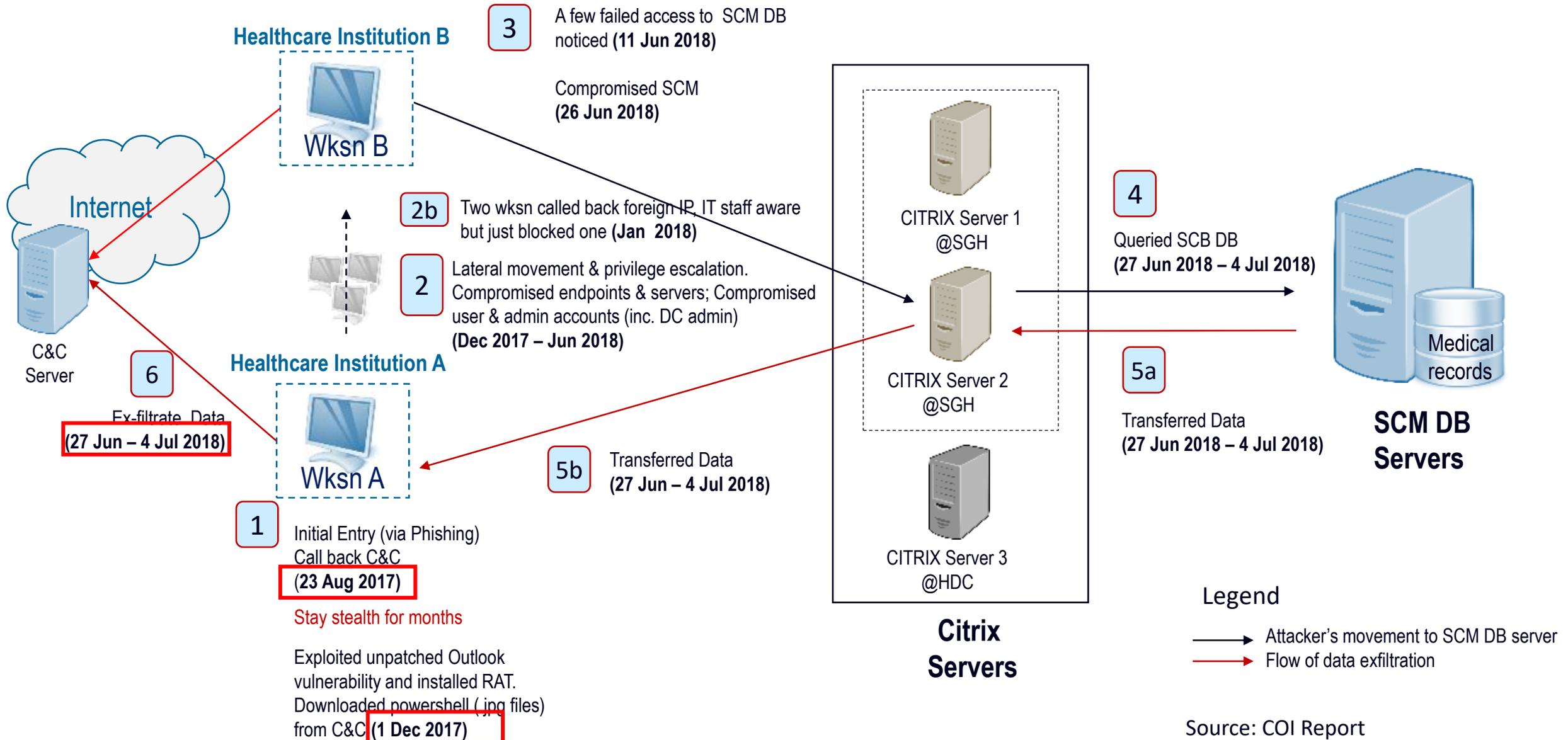
10 Jan 2019 | Full Report of Committee of Inquiry (COI) published

SingHealth Sunrise Clinic Manager (SCM) System



Administered by Integrated Health Information Systems (IHIS)

Anatomy of SingHealth Attack



Lesson Learnt

- **Cyber attack starts with anybody (may be you) in the office**
 - Opportunity for attackers: phishing, weak password (no 2FA), late patching
- **It is not a matter to get in but STAY IN**
 - Attacker stay stealthy for months
- **Lateral movement is key feature of Advanced Persistent Threat**
 - Key targets: Domain controller, remote access, entry points to critical services
- **Early opportunity to discover attacks**
 - Detecting of bulk query, large traffic volume
 - Experience of IT personnel to handle incidents
- **Intelligence sharing is very important for the industry to pre-empt attacks**



明報新聞網

2020年9月18日星期五

向晴軒失USB 涉121理大生求助資料

【明報專訊】明愛向晴軒一名社工本月初遺失USB裝置，內有為理工大學學生提供情緒支援熱線服務「為理在線」的資料，共121名學生受影響。理大表示當中數個檔案未加密，明愛則稱所有資料均有加密處理。接獲求助的油尖旺區議員李傲然表示，有事主哭訴非常擔心個人資料被不法使用，他批評向晴軒處事嚴重失當；對於明愛與理大就加密的說法有矛盾，他要求明愛從速全面交代真相，及對所有求助人提出補償方案。

- Personal information has been leaked (e.g. Name, ID number and conversation record)

Lesson Learnt

- Restrict use of **removable storage**
 - USB, Smart Phone, etc
- Sensitive information should always be **encrypted**, in any scenarios
 - At rest, in use, and in transit)
- Security policy should be **extended outside of organisation**
if remote access is involved
 - Work from home





Cyber Security Oversight: The Role of Board & Senior Management

A man with grey hair, a beard, and glasses is shown in profile, looking out a large window. The window shows a blurred city skyline at dusk or dawn, with some lights visible. The text is overlaid on the right side of the image.

Cyber Security Oversight | The Role of Board & Senior Management

Embed Cyber Security in Business Operation

- **Executive Level Awareness and Commitment**
- **Governance and Ownership (from top to bottom)**
- **Security Policy**
 - Apply **Security-by-Design** Principle to Products & Services
 - Apply **Security-by-Default** Principle to System Deployment
 - Embed Cyber Security in **Project Management**
 - Embed Cyber Security in **Third Party Management**
 - Build a **Cyber Security Culture** within Organisation



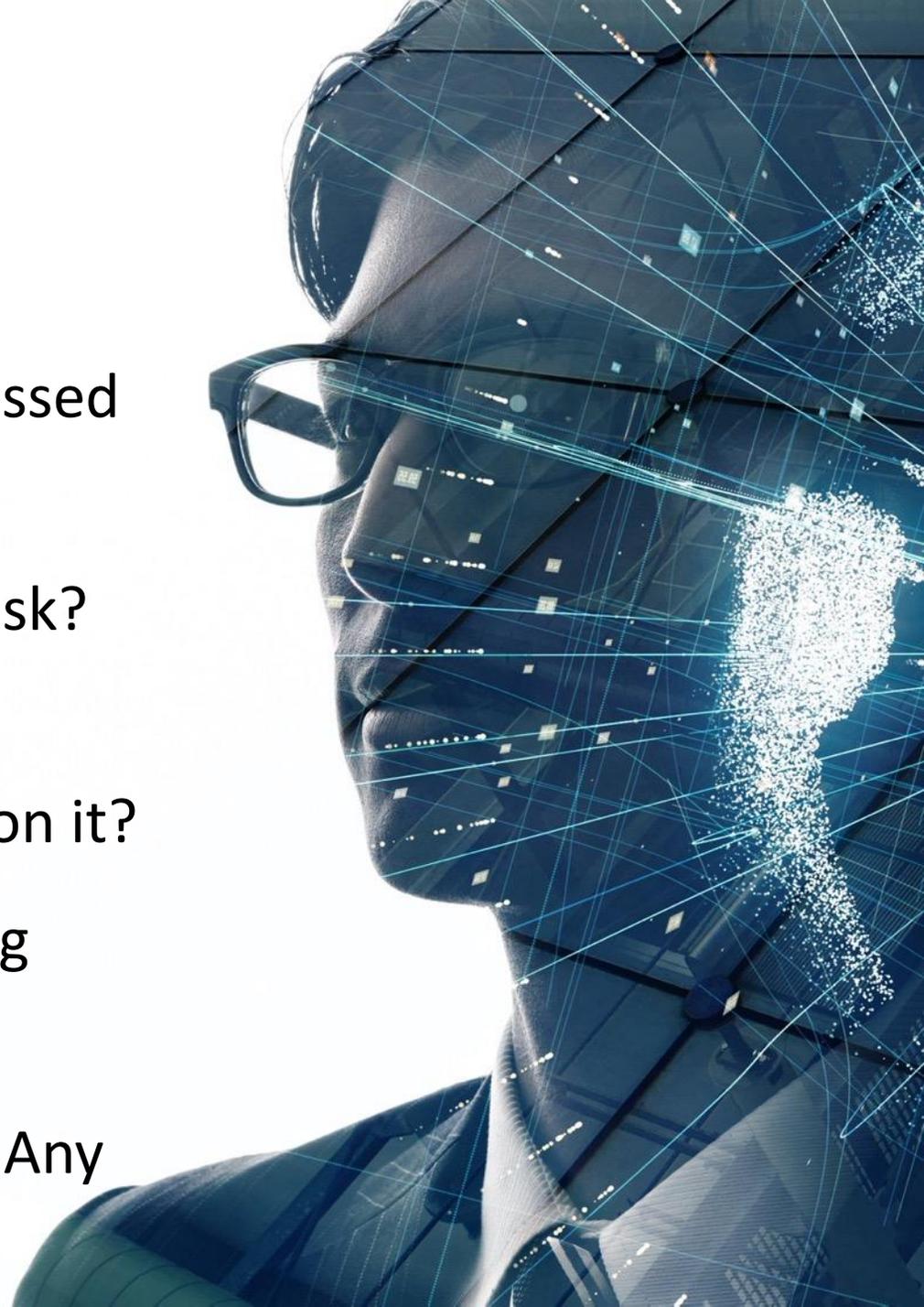


Situation Awareness of Board/Executive Level

- Is Cyber Security on the Executive's Agenda?
- Is there an annual Cyber Security Briefing by industry expert to the Board/Executive?
- Is there a cyber security framework like NIST?
- Does the Board/Executive get report from the Management on the strategy in managing cyber security?

Governance

- Who are **accountable** for cyber security?
- Who are your likely **adversaries**? Have you assessed the **insider threat**?
- Has the Company **assessed** its Cyber Security Risk? What are they?
- Has the Management got a **management plan** on it?
- Is the management plan **updated** of the ongoing progress?
- How is cyber security performance measured? Any **metrics**?





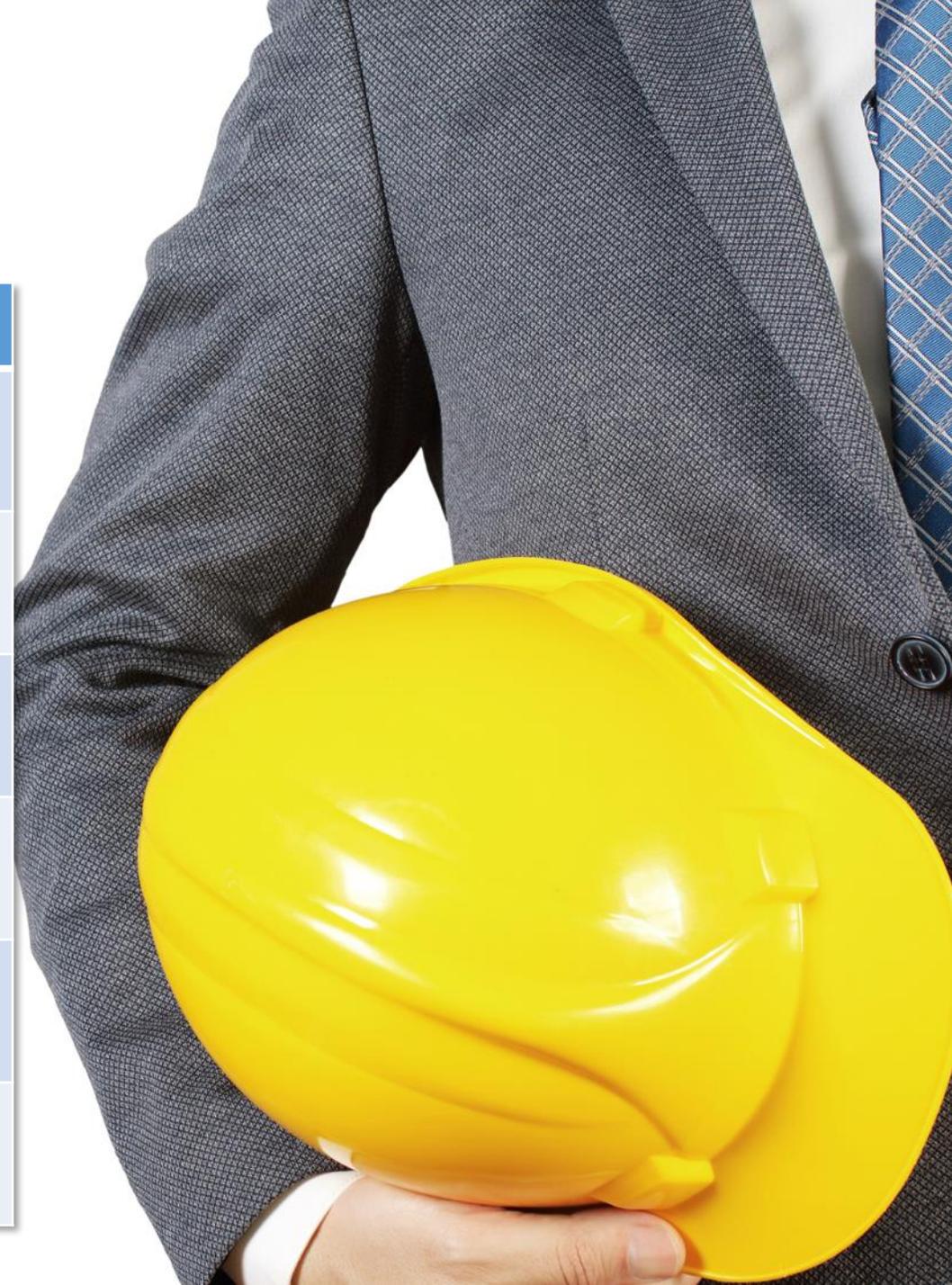
Business Ownership of Cyber Security

- **Identify Critical business data / services**
 - Classify data according to sensitivity
- **Assess Risks from the Corporate Perspective**
- **Apply Security Measures**
 - Process : approve access level to different roles
 - Technology : apply as advised and provided by IT
- **Incident Response**
 - Identify abuse
 - Post-event review for improvement
 - Business Unit involved in compiling report
 - Staff appraisal affected by cyber security performance

Embed Cyber Security in Project Risk Management

Business Risk Assessment for Project Management

Financial Risk – risk with financial structure?	✓
Schedule Risk – can deliver on time?	✓
Capability Risk – have the technology and skill?	✓
Compliance Risk – need to comply to regulation?	✓
Cyber Security Risk - system and data resilient to cyber attacks?	✓
Other risk – site safety, etc.?	✓



Integrate Cyber Security into PM Methodology

Task name
<input type="checkbox"/> IT Project - Security Milestones
<input type="checkbox"/> Initiating
<input type="checkbox"/> Develop project charter.
Security impact assessment completed.
<input type="checkbox"/> Planning
<input type="checkbox"/> Develop project management plan.
Secure communications plan completed.
<input type="checkbox"/> Collect requirements.
Security requirements collected.
<input type="checkbox"/> Executing
<input type="checkbox"/> Develop project team.
Security training completed.
<input type="checkbox"/> Operational Handoff
Security responsibility transferred.
<input type="checkbox"/> Closing
Security Lessons Learned recorded.



Manage 3rd Party Security Risk

Tackling Supply Chain Attacks



Cyber Security Implication of Supply Chain Attacks

Software update mechanism for attacking enterprise



Supply Chain Attack | **Software Update Contamination**



Dec 2020 | Solarwinds Orion backdoor

- Contaminated network monitoring software affecting global enterprises and US government
- Trojanised update had authentic signature



Nov 2018 | Operation ShadowHammer

- Millions of Asus computers installed a backdoor
- Trojanised update had authentic signature



Aug 2017 | Avast's CCleaner Backdoor

- 2.3M contaminated copies downloaded
- Attacker targeted 20+ companies with more malware



Manage Supply Chain (Third Party) Risks

1. Put third party security management in place

- Put third party security into security policy and security risk assessment
- Purchase only from authorized suppliers; check supplier reputation
- Put in place controls in contracts, e.g. right to audit for third parties
- Employ network separation and restrict partner access to enterprise network
- Test third party software and updates before deployment

2. Require service providers to implement security measures in service provision

- Provide transparency to client of their security controls including access control and annual security audit
- Provide proof of authenticity and integrity to delivered software and patches
- Give timely notification of the cyber incidents and the critical vulnerability of their products and services
- Provide security awareness education to staff

3. Involve partners and contractors in company-side security awareness programme

Build Human Firewall

- **Organize Cyber Security Awareness Training**
- **Build a Strong Culture of Security**
 - Business units take accountability
 - Staff used to use alternative communication channel to verify transaction requests
 - Staff stay vigilant to unsolicited email and website
- **Develop Metrics on Security Awareness**
 - Regular cyber security drill exercise



FREE Security Awareness Training Video



<https://www.youtube.com/watch?v=FH7zWAb4-GQ>

HKCERT Cyber Security Initiatives 2021

1. “Hack me if you can” animation series (Jan – Apr) <https://www.youtube.com/user/hkcert>



(1) 遙距工作及視像會議安全攻略



(2) 雲端保安要做足 確保資料無漏出



(3) 釣魚攻擊要小心 不明電郵咪亂開

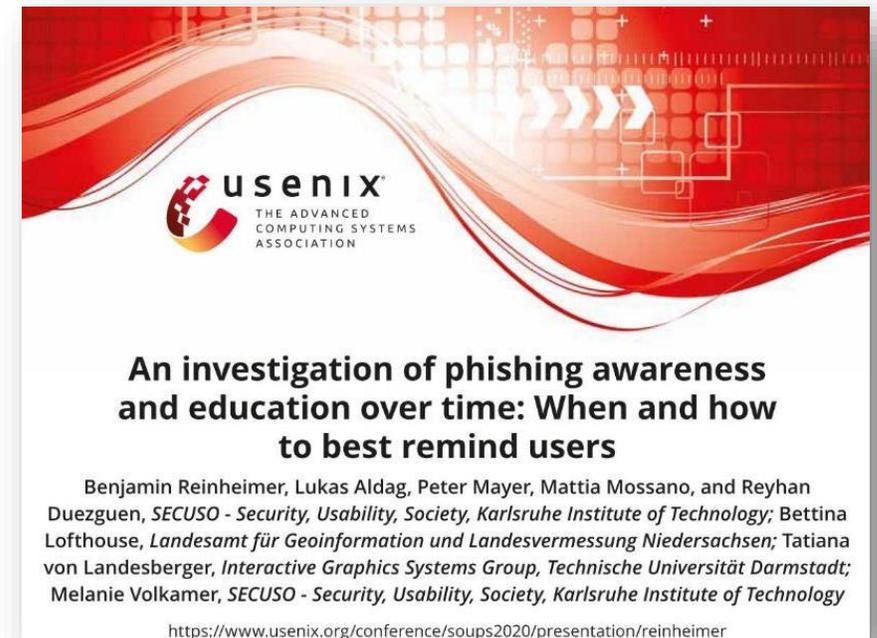


(4) 5G和物聯網保安

Awareness Building – Effectiveness and Retention

1. **Video** and the **interactive examples** performed **best**
2. Respondents **correctly identified** phishing emails even **after four months**
3. Awareness training **forgotten over time**
→ need to retrain **after six months**

Survey on Phishing Drill Effectiveness



Changing Role of CISO



Pre-2000

2000-2004

2004-2008

2008-2016

2016-2020

Future

**Limited
Security**

**Regulatory
Compliance**

**Risk-
oriented**

**Social-Mobile-
Cloud Enable
Threat aware**

**Privacy and
Data Aware**

What is it?



Steps to Cyber Security for Social Welfare Sector

International Reference

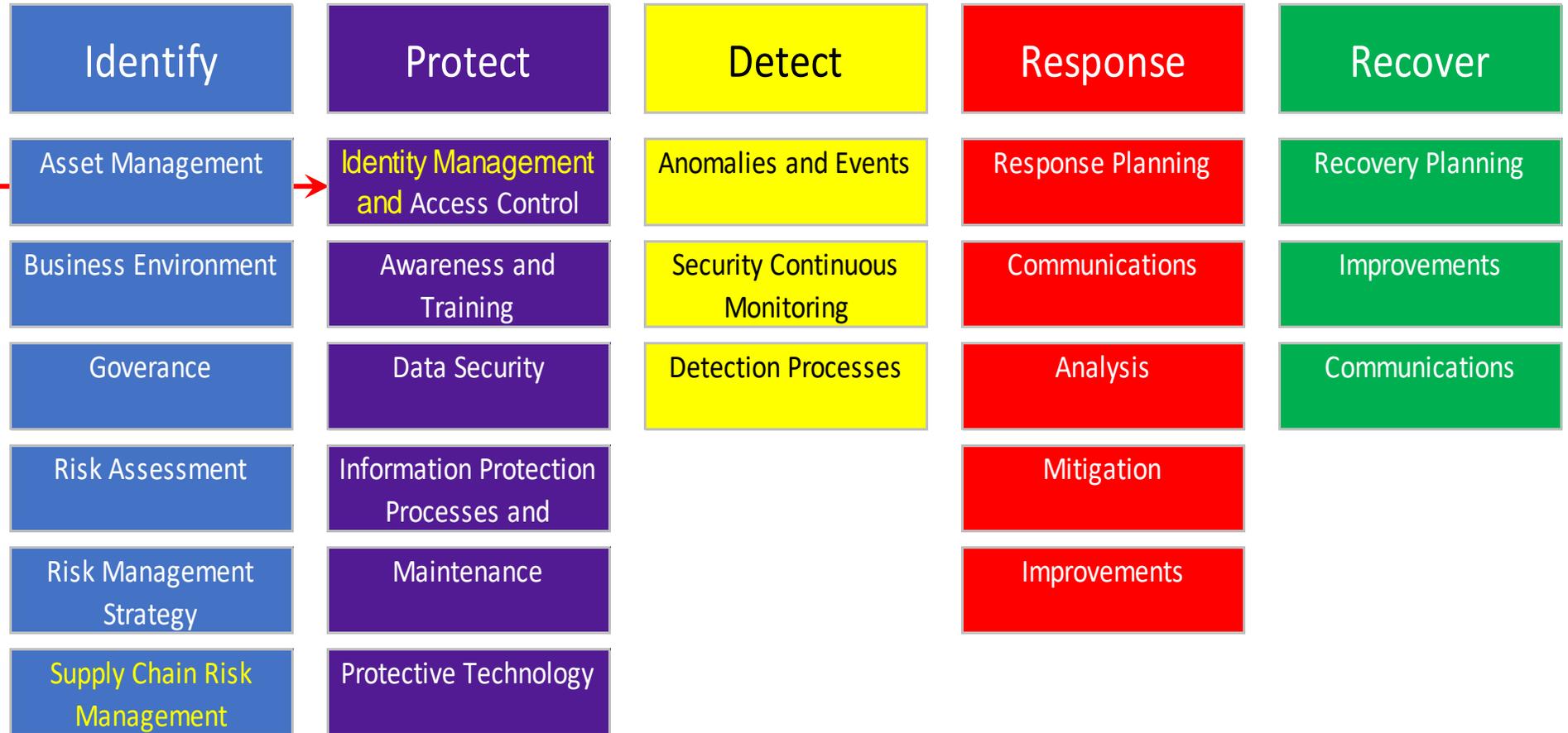
NIST Cyber Security Framework



- U.S. best practices, standards, and recommendations that help a **private** organization **identify, assess and improve** its cyber security measures.
- Risk-based approach – self-assessment and improvement
- Voluntary for critical infrastructure; widely adopted in US and overseas
- Five Core Functions: Identify, Protect, Detect, Respond and Recover

NIST CSF 1.1 Changes

- CSF 1.0 (2014)
- CSF 1.1 (2018) added **Identity Management** and **Supply Chain Risk Management**





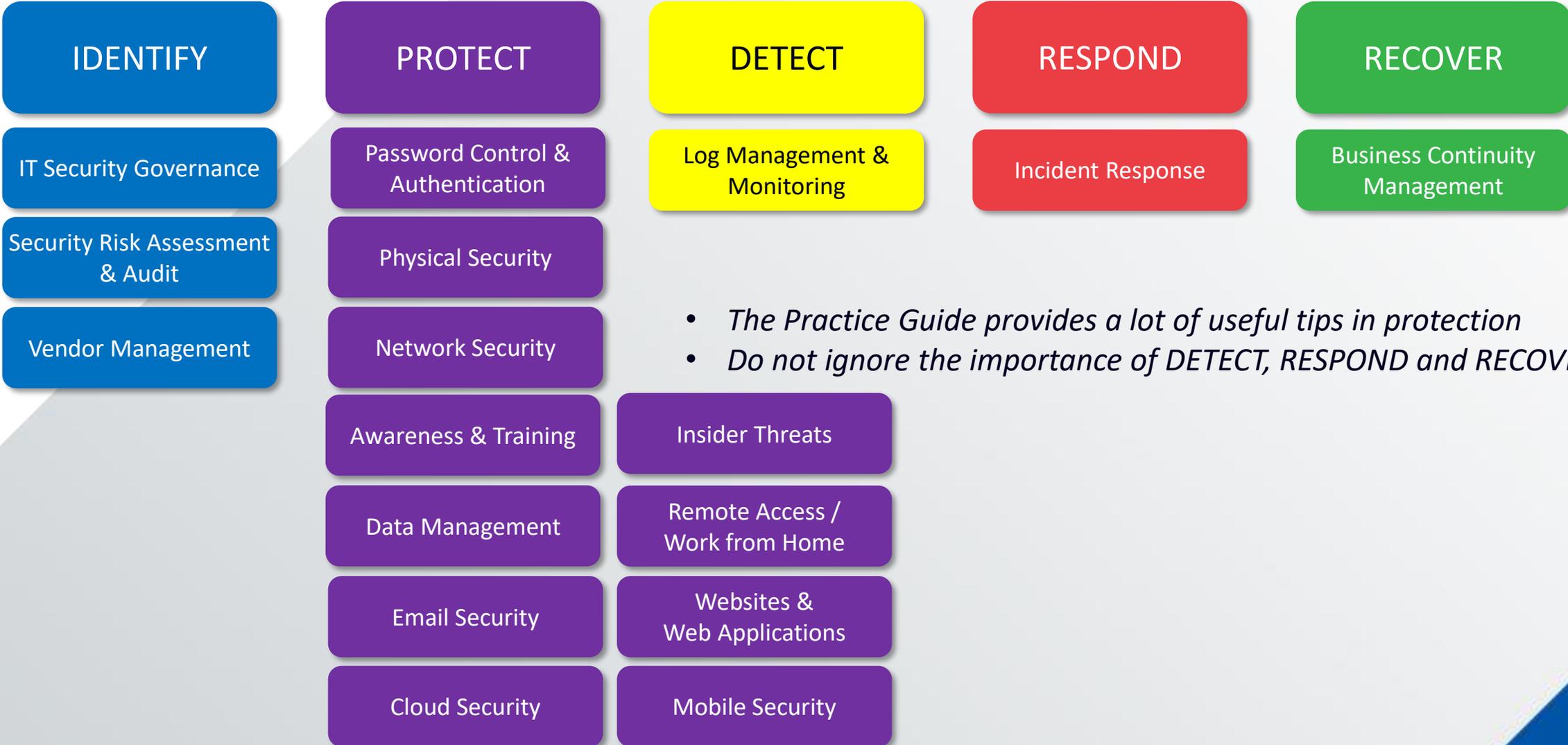
IT Security Practice Guide for the Social Welfare Sector

*Covered 17
Security Domains*

- 1) IT Security Governance
- 2) Password Control and Authentication
- 3) Websites and Web Applications
- 4) Data Management
- 5) Computer Networks Security
- 6) Email Security
- 7) Cloud Computing Security**
- 8) Physical Security
- 9) Mobile Security
- 10) Remote Access/Work from Home**
- 11) Security Risk Assessment and Audit
- 12) Insider Threats
- 13) Vendor Management**
- 14) Awareness and Training
- 15) Incident Response
- 16) Business Continuity Management
- 17) Log Management and Monitoring

- Mapping domains in IT Security Practice Guide to NIST CSF

NIST CYBER SECURITY FRAMEWORK



- The Practice Guide provides a lot of useful tips in protection*
- Do not ignore the importance of DETECT, RESPOND and RECOVER*

Mapping Domains in IT Security Policy to ISO/IEC 27001-2013

Awareness & Training
Insider Threats

IT Security Governance

Password & Authent.

Data Management

Physical Security

Remote Access / WFH

Email Security

Cloud Security

Websites & Web App

Mobile Security

Network Security

Vendor Management

Incident Response

Business Cont Mgmt

Sec Risk Assess & Audit

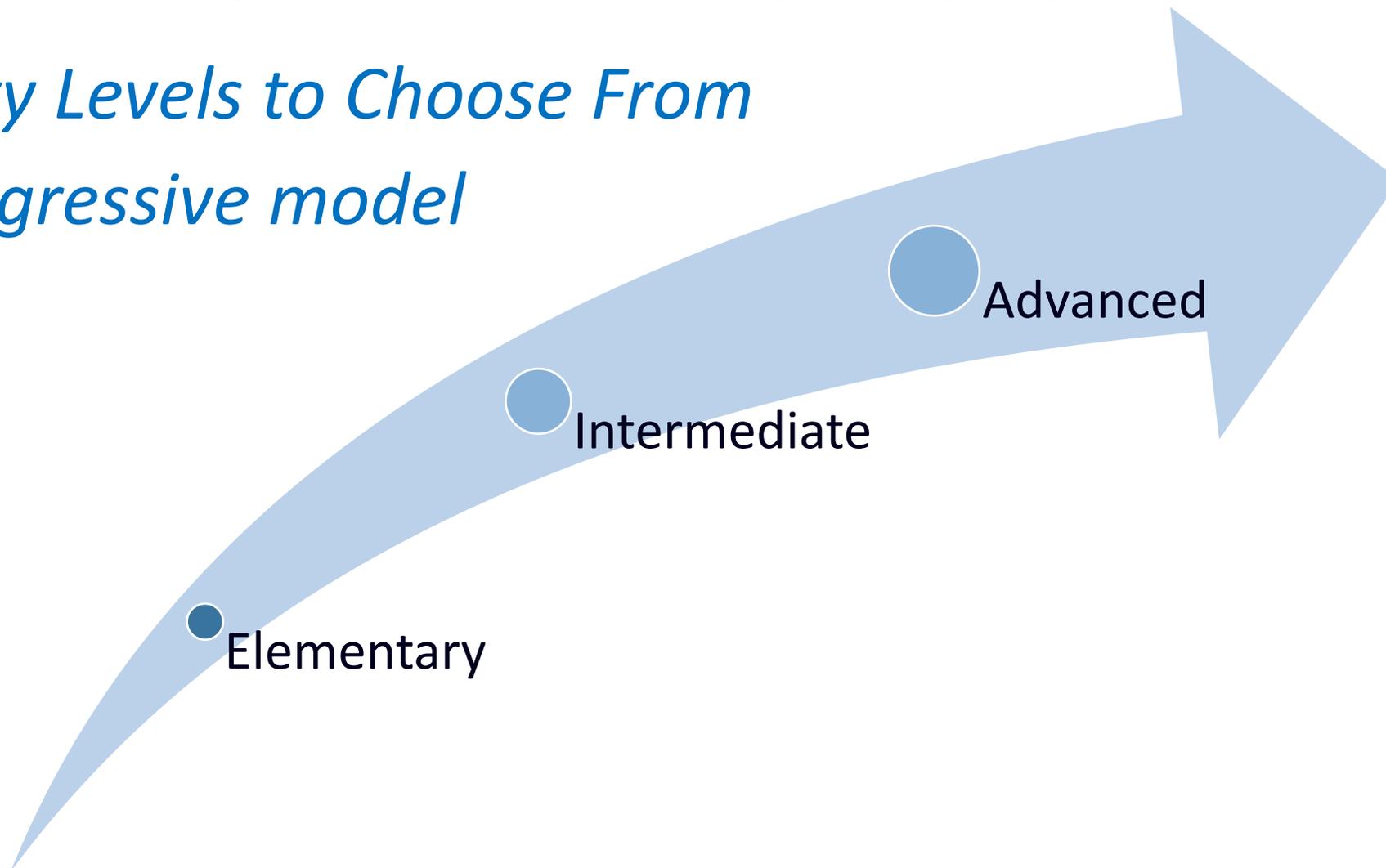
Log Mgmt & Monitoring

- A.5 Information Security Policy
- A.7 Human Resources Security
- A.9 Access Control ... network access control, password management
- A.10 Cryptography
- A.11 Physical and environmental security
- A.13 Network security ... information transfer
- A.14 System acquisition
- A.15 Supplier relationships
- A.16 Incident management
- A.17 Business Continuity
- A.18 Compliance

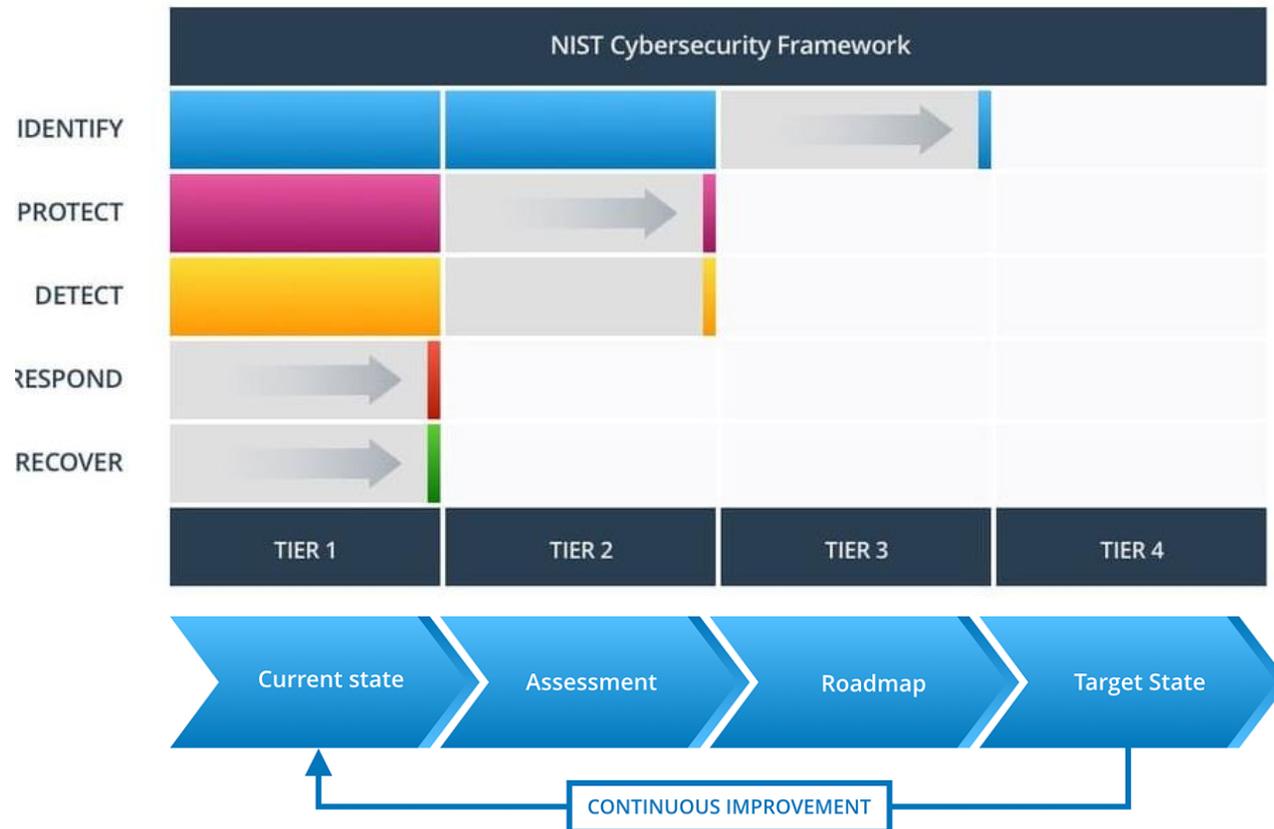
IT Security Practice Guide for the Social Welfare Sector

3 Security Levels to Choose From

- *A progressive model*



NIST CSF Emphasises Improvement



- Tier denotes maturity of each core function
- CSF Profile (“Profile”) is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization
- Continuous Improvement
 - Define the Current State and Target State
 - Assess the Gap to Fill
 - Define the Roadmap of Improvement

Image credit: www.praetorian.com

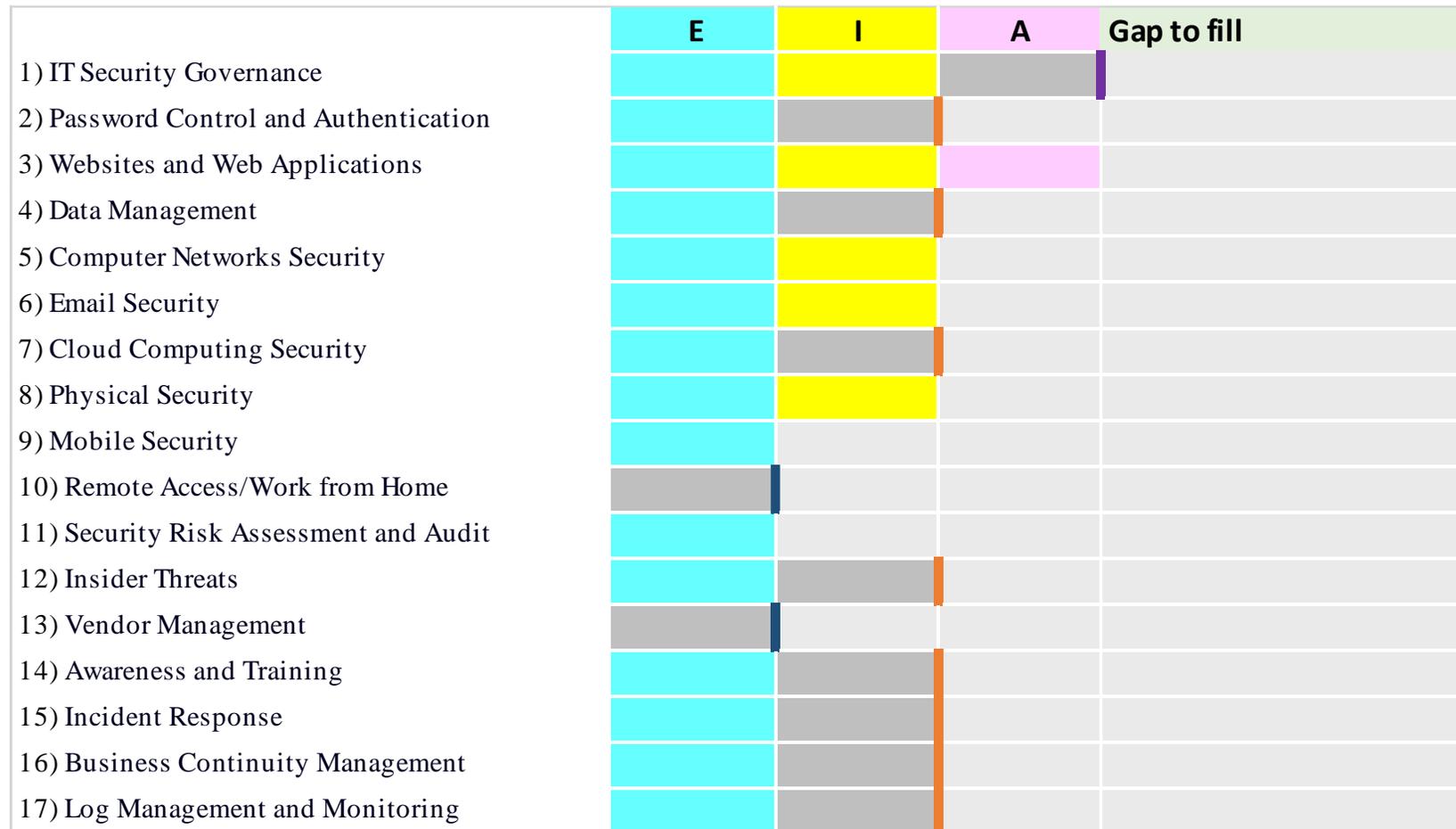
IT Security Practice Guide for the Social Welfare Sector

Current State

	E	I	A	
1) IT Security Governance				
2) Password Control and Authentication				
3) Websites and Web Applications				
4) Data Management				
5) Computer Networks Security				
6) Email Security				
7) Cloud Computing Security				
8) Physical Security				
9) Mobile Security				
10) Remote Access/Work from Home				
11) Security Risk Assessment and Audit				
12) Insider Threats				
13) Vendor Management				
14) Awareness and Training				
15) Incident Response				
16) Business Continuity Management				
17) Log Management and Monitoring				

IT Security Practice Guide for the Social Welfare Sector

Current State → Target State



IT Security Practice Guide for the Social Welfare Sector

Security Checklists & Templates



- 1) IT Asset Valuation List Template
- 2) Security Incident Response Form
- 3) Security Incident Response Records
- 4) Vendor Risk Assessment Checklist
- 5) Security Audit Checklist Template
- 6) Seven Habits of Cyber Security
- 7) Security Risk Assessment Guidelines

IT Security Practice Guide for the Social Welfare Sector

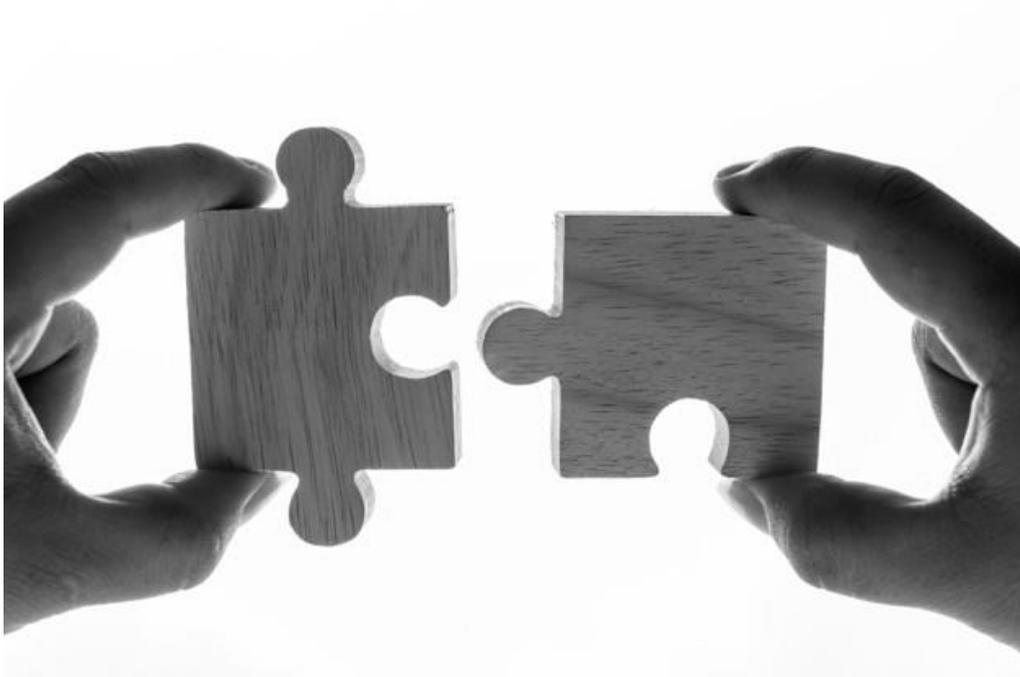
Security Risk Assessment Tools



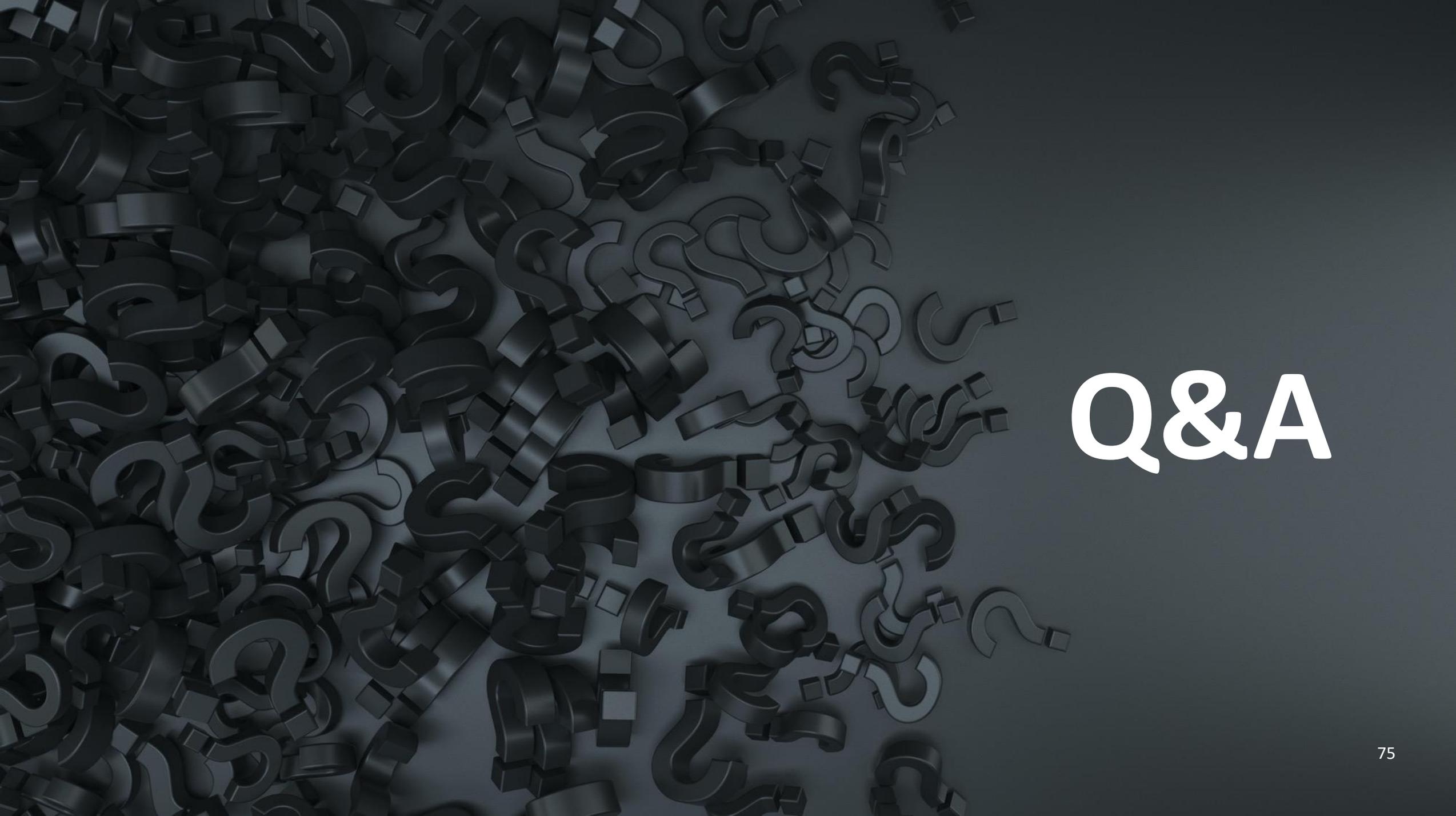
- 1) Windows Asset Audit Tool – Windows
- 2) NMap/Zenmap Security Scanner
- 3) Nessus Network & Host Vulnerability Scanner
- 4) OWASP Zed Attack Proxy (ZAP)
- 5) Kali Linux – Professional Security Assessment Distribution
- 6) Logging Made Easy (LME)
- 7) VeraCrypt

IT Security Practice Guide for the Social Welfare Sector

CONCLUSION



- 1) No “**One-Size-Fit-All**” Approach
- 2) Prepare for Now, **Plan for Future.**
Progressive Improvement
- 3) Serve as a **Security Guideline**
- 4) Plan Based on **Priority & Resources**

The background of the slide is a dark grey, almost black, field filled with a dense, chaotic arrangement of 3D question marks. The question marks are rendered in a dark charcoal color with a slight metallic or glossy sheen, giving them a three-dimensional appearance. They are scattered across the entire frame, with some appearing larger and more prominent than others, creating a sense of depth and texture. On the right side of the slide, the text 'Q&A' is displayed in a clean, white, sans-serif font. The 'Q' is significantly larger than the '&' and 'A', making the entire text stand out prominently against the dark, textured background.

Q&A

**Share Your
Experience &
Challenges with us**





Hong Kong Productivity Council
香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 6168 www.hkpc.org