Pilot Project of IT Security Audit for NGOs of the Welfare Sector in Hong Kong

(20 January 2022)

Information Technology Resource Centre

The Hong Kong Council of Social Service

資訊科技資源中心
Information Technology Resource Centre

Agenda

1

Project Background

2

Deliverables

3

Focus Areas

1 Project Background

IT Security Model – CIA Triad

Availability means that the authorized users should be able to access data whenever required

Integrity helps maintain the trustworthiness of data by having it in the correct state and immune to any improper modifications

Confidentiality makes sure that only authorized personnel are given access or permission to modify data

Cyber Attacks could lead to serious consequences

1 Website Defacement / Distributed Denial-of-Service (DDoS) / Cryptojacking

2 Ransomware

3 Spyware / SQL Injection

IT Security Incidents and Threats

Weekly cyberattacks jumped by 50% in 2021, with a peak in December due largely to the Log4J exploit

by **Lance Whitney** in **Security**
on January 10, 2022, 8:47 AM PST

Check Point Research said Africa had the highest amount with an average of 1,582 per week per organization. Here's how to combat the latest surge in attacks.

WHITE PAPERS, WEBCASTS

Mimecast Connect
White Papers from Mim
REGISTER NOW

Get started with Co
free
Tools & Templates from
REGISTER NOW

Master your server
informative resourc
Research from TechRep
DOWNLOAD NOW

Make sense of com
with these glossarie
Research from TechRep
DOWNLOAD NOW

【網絡保安】香港銀行學會遭勒索軟件攻擊　承認會員資料有被洩露風險、部分電子服務暫停

股市 18:46 2022/01/10 讚好 0

關注文章 儲存文章 分享:

About the Pilot Project of IT Security Audit

OBJECTIVES

1. Raise IT Security Awareness and Knowledge
2. Enhance IT Security of Developed Applications
3. Formulate an IT Security Baseline for the Social Welfare Sector

DELIVERABLES

IT Security Training

- Management
- General staff
- IT staff

IT Security Portal Website

- IT Security News
- IT Security Practice Guide and Toolkit

IT Security Audit & Scanning

- Pre-scanning
- General Patching
- Assistance for fixing the identified vulnerabilities
- Compliance Check (i.e. Post-scanning)

IT Security Practice Guide

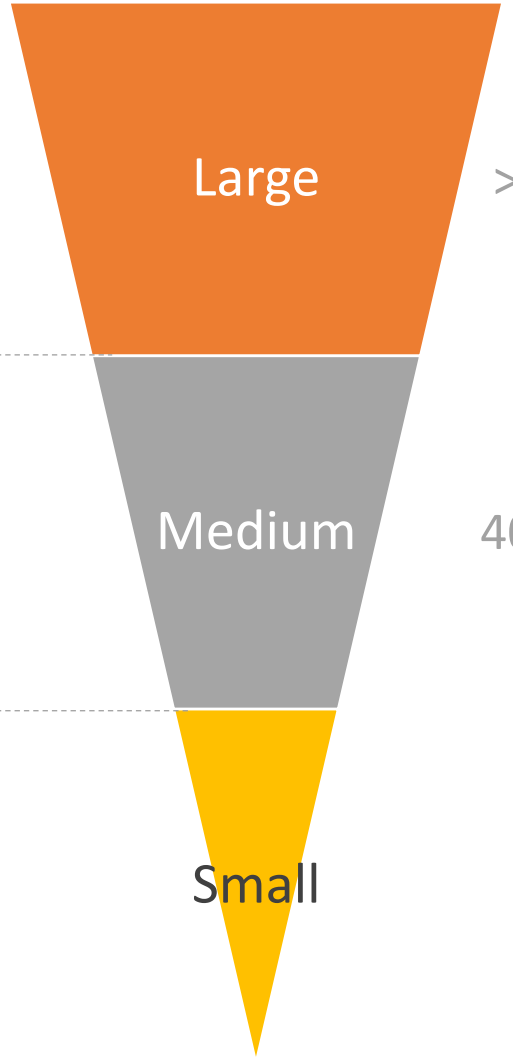
- Guidelines for NGOs in the Social Welfare Sector
- Toolkit with templates and IT security scanning software

The Participating NGOs

22

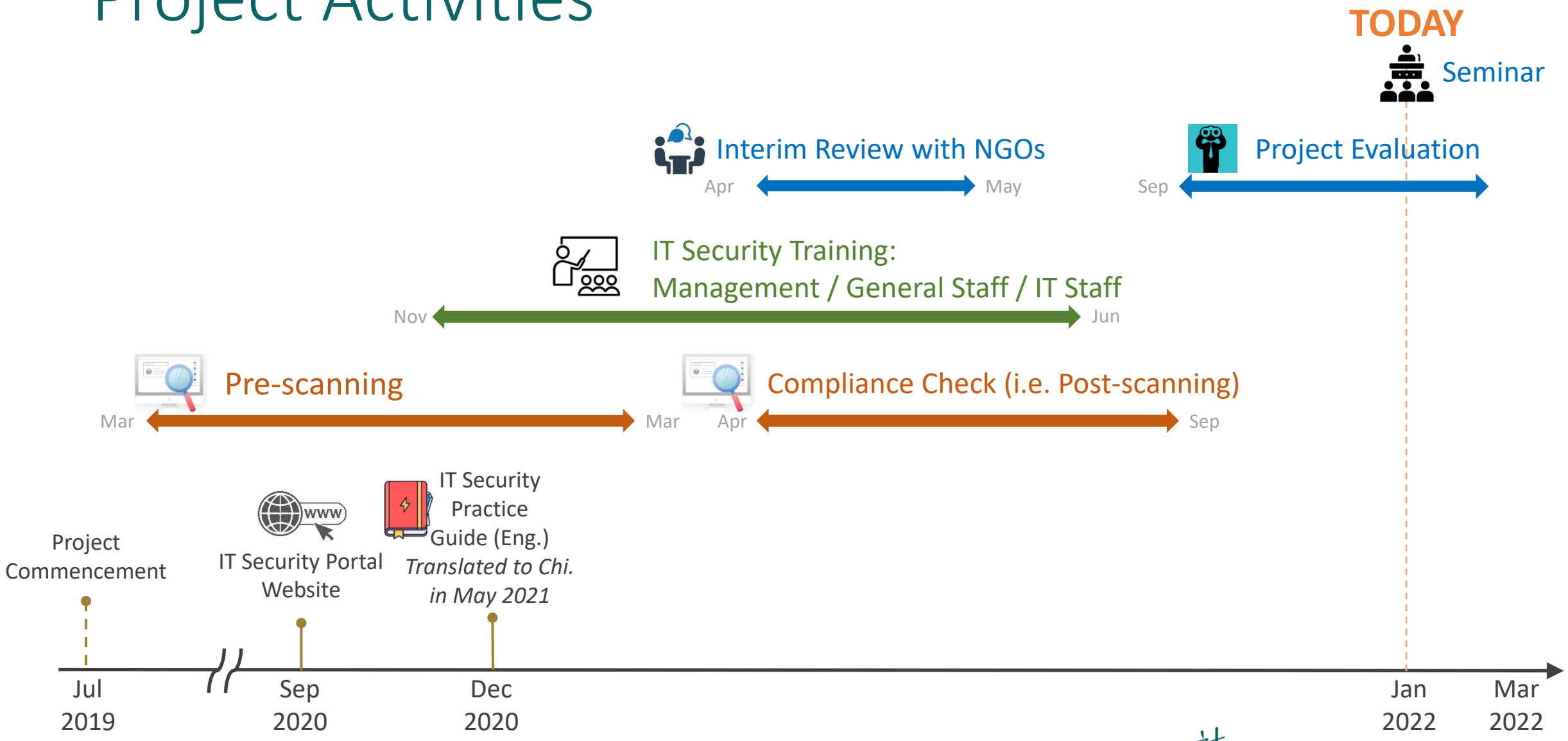
Total

Staff Size:



8	Large	>= 1,000
6	Medium	400 – 999
8	Small	< 400

Project Activities



2 Project Deliverables

Project Deliverable 1 - IT Security Practice Guide

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

6

Attributes

Impact	Threat	Likelihood
Asset Value Info. Classification	Security Risk Assessment Security Patches	Resilience Accessed By

3

Security Levels

Elementary → **Intermediate** → **Advanced** →

Project Deliverable 1 – Toolkit

Templates and Checklists

- IT Asset Valuation
- Security Incident Reporting Form
- Information security incident reporting
- Vendor Risk Assessment Management Record
- NGO IT Audit Checklist
- Seven Habits of Cyber Security

IT Security Scanning Tools

- WinAudit
- VeraCrypt
- OWASP Zed Attack Proxy (ZAP)
- Nessus Essentials
- Nmap Zenmap Security Scanner
- Logging Made Easy
- Kali Linux

Project Deliverable 2 - IT Security Audit & Scanning (w/ Penetration Testing)

11

Security Domains assessed

1. Security program
2. Security policy
3. Training and awareness
4. Personal security
5. Physical security
6. Network security
7. Logical access
8. Operation management
9. Incident management
10. Business continuity management
11. Asset management

Network-Level

Automatic vulnerability scanning tools (such as Nessus Professional 8) were used to identify the running services of relevant servers, and vulnerabilities of each identified running services.

Host-Level

System information and security configuration, such as password policy, were extracted from the servers for analysis.

System / Application

System/application scanning covered the web system and application via the Hyper Text Transfer Protocol (HTTP), including HTTP Secure (HTTPS). It was performed to exploit common web application vulnerabilities, such as SQL injection and Cross-Site Scripting (XSS), Weak password, SSL 2.0 deprecated protocol, etc.

Risk Assessment

Risk Rating

		Likelihood			
		Very Low 1	Low 2	Medium 3	High 4
Impact	Critical 5	Low 5x1 = 5	Medium 5x2 = 10	High 5x3 = 15	Critical 5x4 = 20
	High 4	Low 4x1 = 4	Low 4x2 = 8	Medium 4x3 = 12	High 4x4 = 16
	Medium 3	OFI 3x1 = 3	Low 3x2 = 6	Medium 3x3 = 9	Medium 3x4 = 12
	Low 2	OFI 2x1 = 2	Low 2x2 = 4	Low 2x3 = 6	Low 2x4 = 8
	Very Low 1	OFI 1x1 = 1	OFI 1x2 = 2	OFI 1x3 = 3	Low 1x4 = 4

Implication and Recommendation

Risk level	Implication and recommendation
Critical	Critical impact and improvements should be done immediately
High	High impact and improvements should be done as soon as possible (approx. within 1 month)
Medium	Moderate impact and improvements should be done within a short time (approx. within 3 months)
Low	Low impact and improvements should be done within a reasonable time (approx. within 6 months)
Opportunity for Improvement (OFI)	Does not impose immediate threats but implementation of such items will improve the environment. These enhancements should implement when resources are available.

Project Deliverable 3 - IT Security Training

Management Training

~400

No. of Participants

22 courses

(3 Hours each session)

General Staff Training

1,111

No. of Participants

17 courses

(3 Hours each session)

IT Staff Training

48

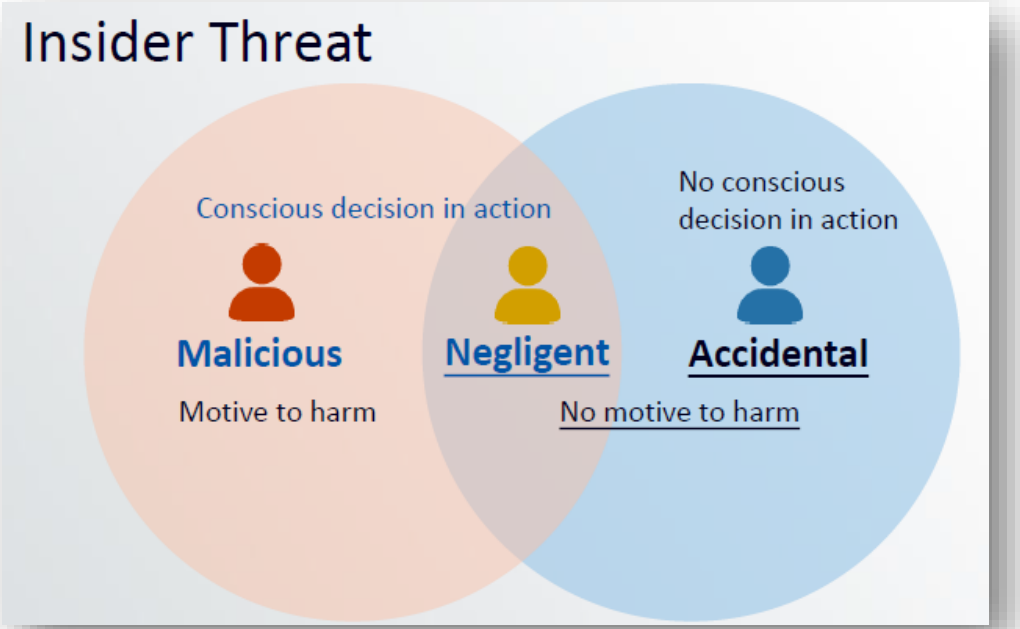
No. of Participants

3 courses

(1 Day each session)

IT Security Training (Management training)

Theory

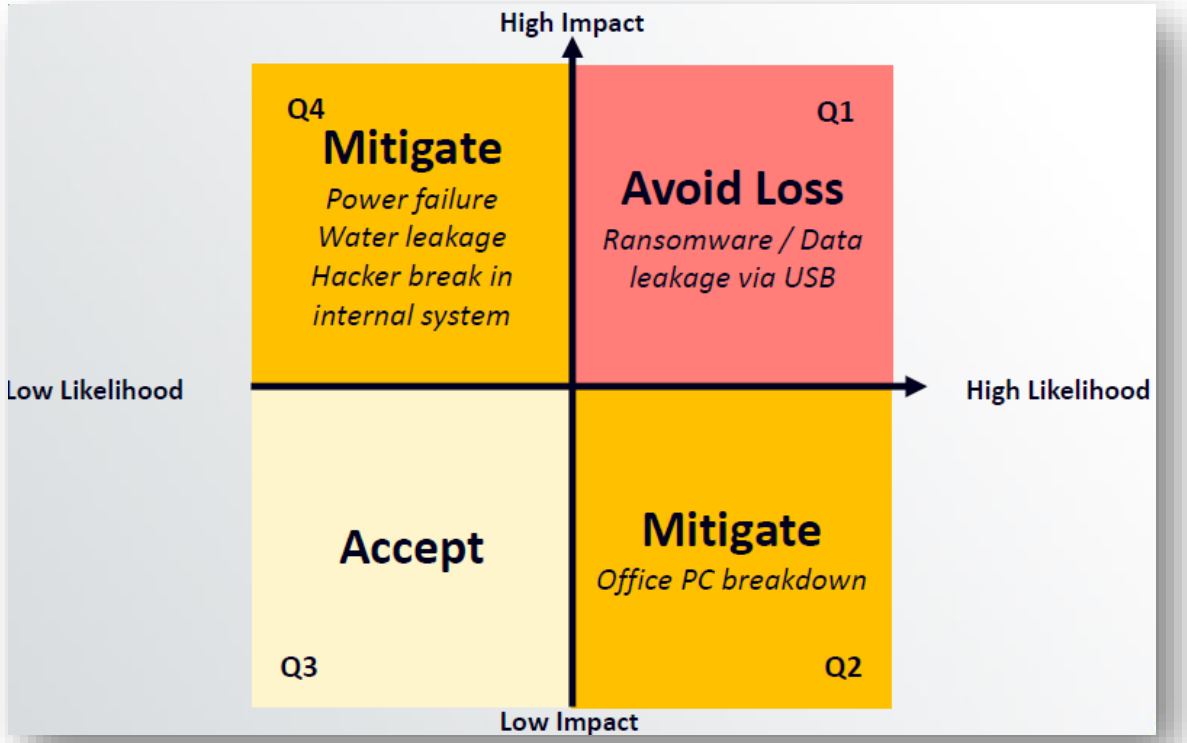


Case Sharing

新加坡醫療保健集團（SingHealth）

IT Security Training (Management training)

Risk Management Strategy



Example for Elaboration

IT Security Training (General Staff)

How To Recognize and Avoid Phishing Scams

Phishing Attacks

Phishing attackers pretend to be a **trusted institution** or **individual** in an attempt to persuade victims to expose personal data and other valuables.

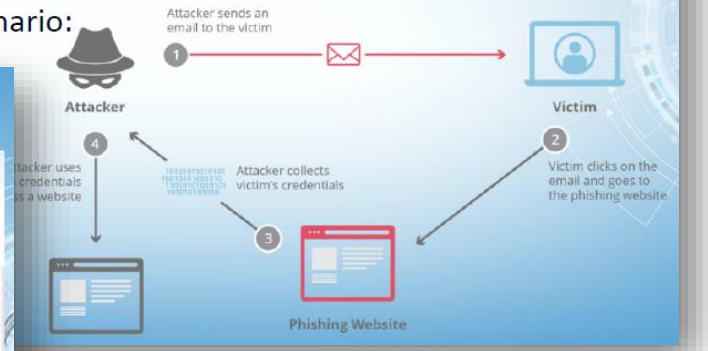
Phishing ways:

- **Spam** phishing
- **Spear** phishing

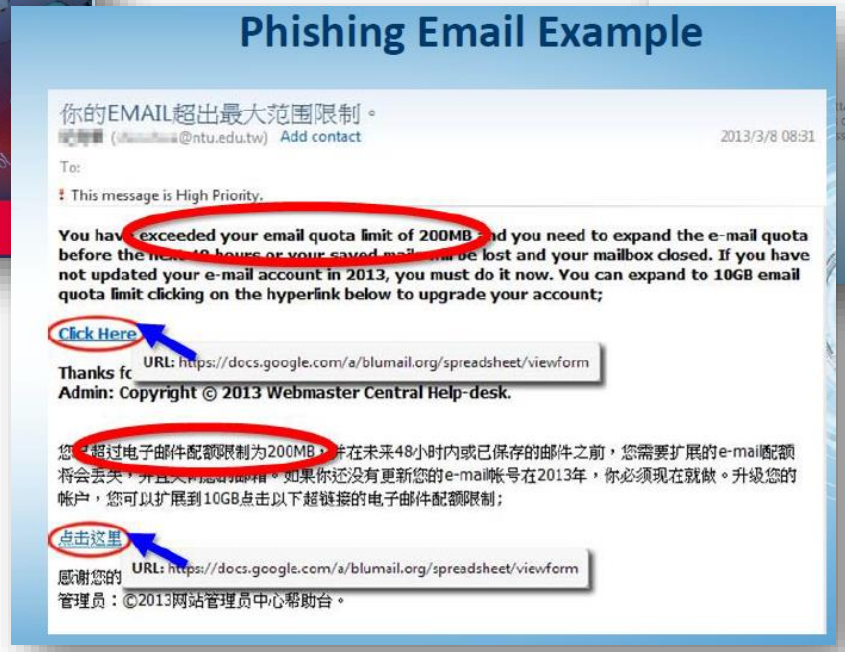
Email Phishing

Email phishing is the most traditional means of phishing, using an email urging you to reply or follow-up by other means. Web links, phone numbers, or malware attachments can be used.

Typical scenario:



Phishing Email Example



你的EMAIL超出最大范围限制。

(@ntu.edu.tw) Add contact 2013/3/8 08:31

To:

This message is High Priority.

You have exceeded your email quota limit of 200MB and you need to expand the e-mail quota before the next 48 hours or your saved mail will be lost and your mailbox closed. If you have not updated your e-mail account in 2013, you must do it now. You can expand to 10GB email quota limit clicking on the hyperlink below to upgrade your account;

Click Here URL: https://docs.google.com/a/blumail.org/spreadsheet/viewform

Thanks fo

Admin: Copyright © 2013 Webmaster Central Help-desk.

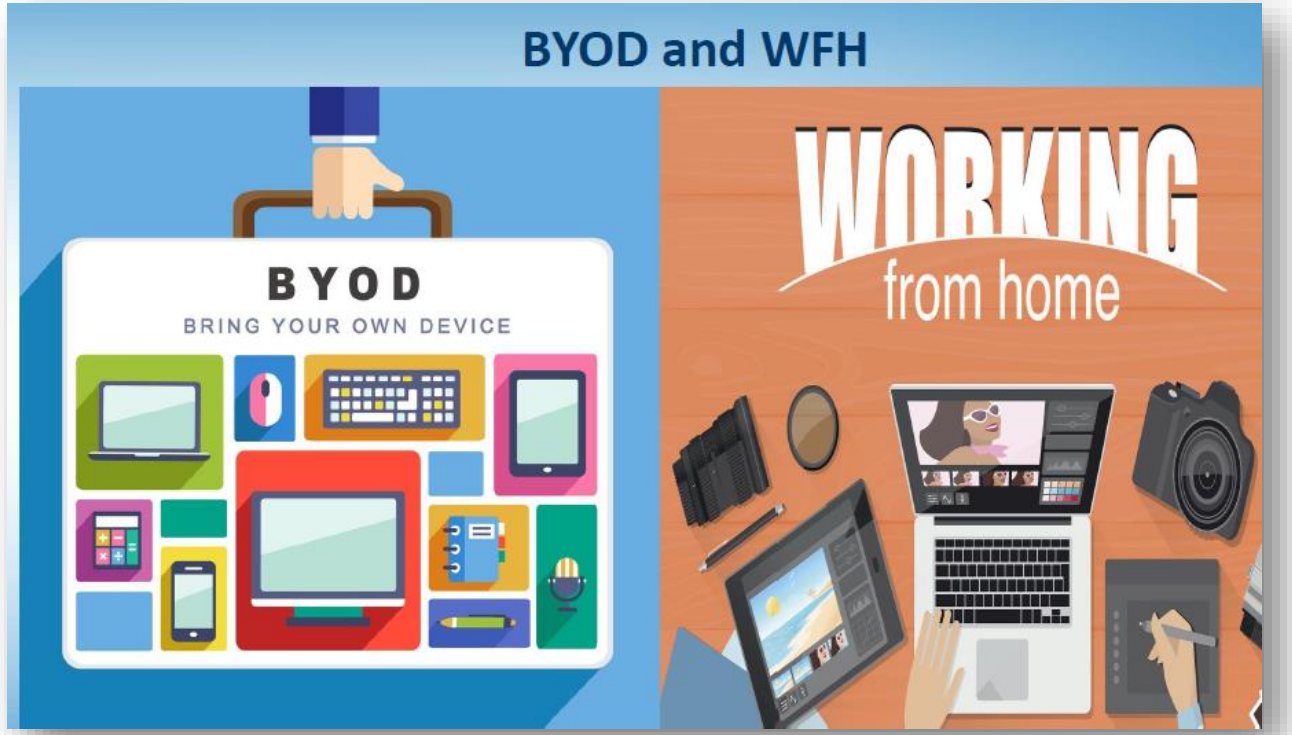
您超过电子邮件配额限制为200MB，并在未来48小时内或已保存的邮件之前，您需要扩展的e-mail配额将会丢失，并且关闭邮箱。如果你还没有更新您的e-mail帐号在2013年，你必须现在就做。升级您的帐户，您可以扩展到10GB点击以下超链接的电子邮件配额限制；

点击这里 URL: https://docs.google.com/a/blumail.org/spreadsheet/viewform

感谢您的

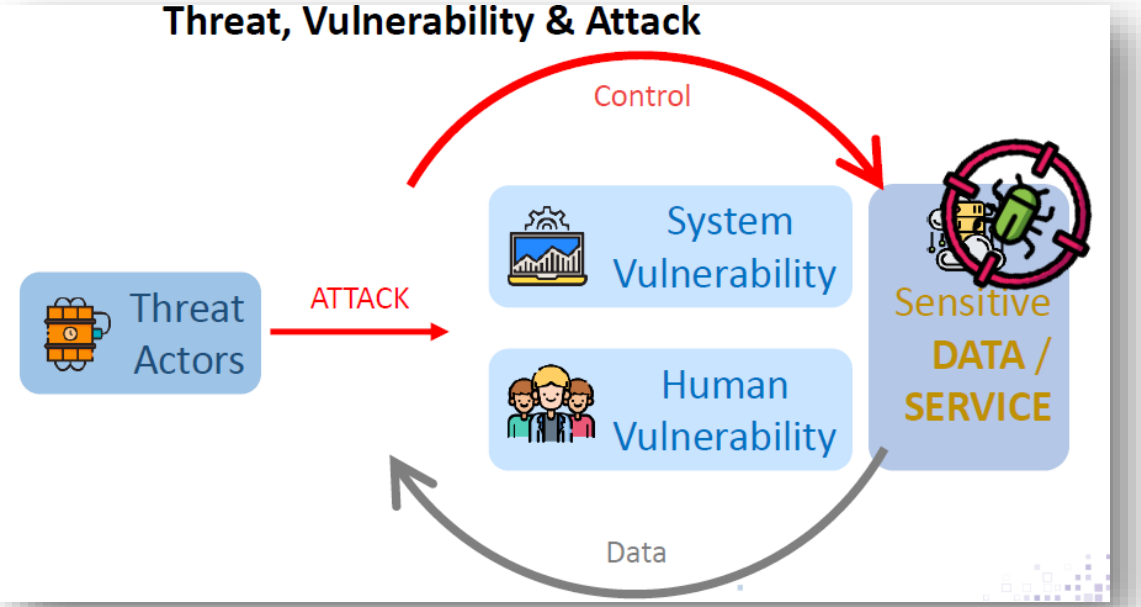
管理员：©2013网站管理员中心帮助台。

IT Security Training (General Staff)

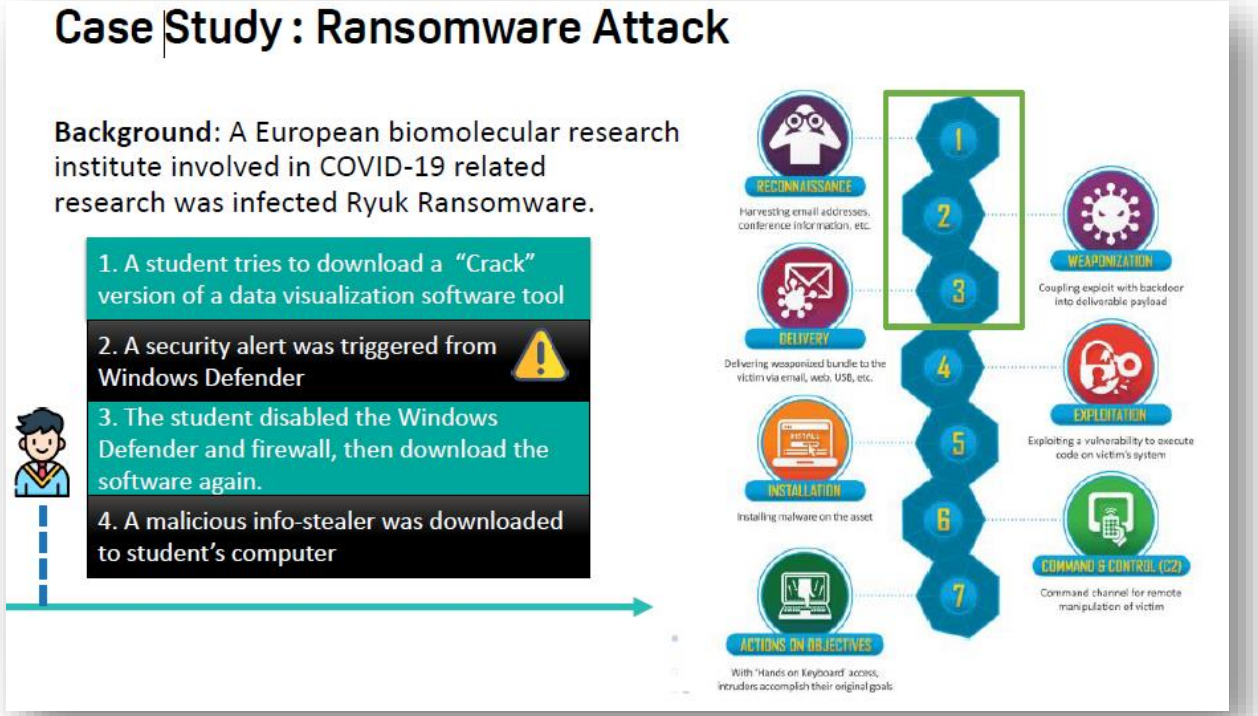


IT Security Training (IT staff)

Theory



Case Study



IT Security Training (IT staff)

Hands-on Exercises

Exercise 1: Using OWASP ZAP

(Open Web Application Security Project)

1. Launch XAMPP
2. Start Apache and MySQL
3. Launch ZAP
4. Open Browser with ZAP Proxy
5. Go to testing web site (http://127.0.0.1:5080/test)

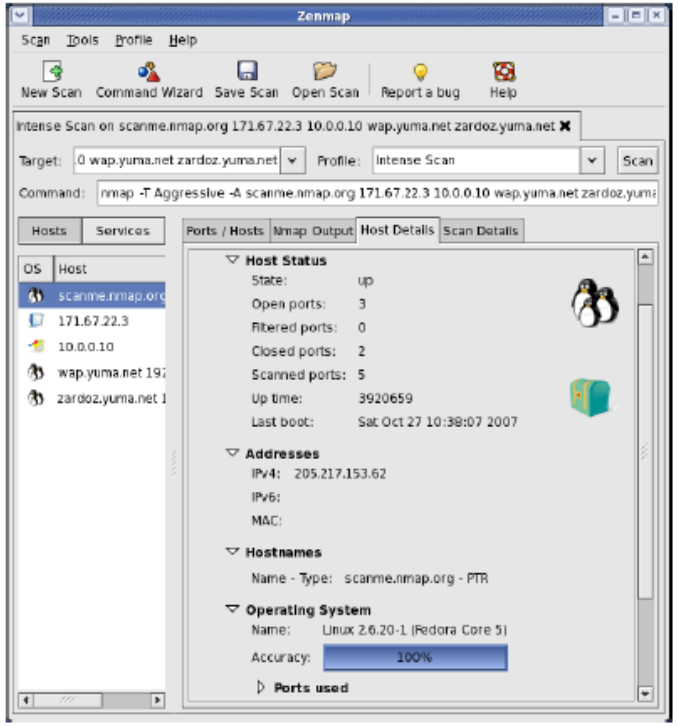
How many findings identified? (HINTS: Alerts)

Exercise 1: My First Scan

1. Launch Nessus Web Client
2. Login Nessus (admin, IT$taff2021)
3. New Scan
4. Click Advanced Scan
5. Type “Exercise1” in Name
6. Type 127.0.0.1 in Targets

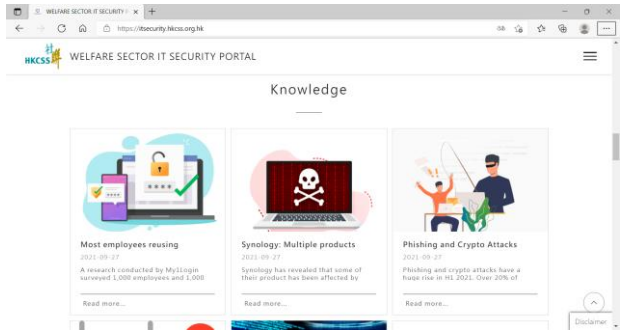
Introduction to Tools

Nmap / Zenmap

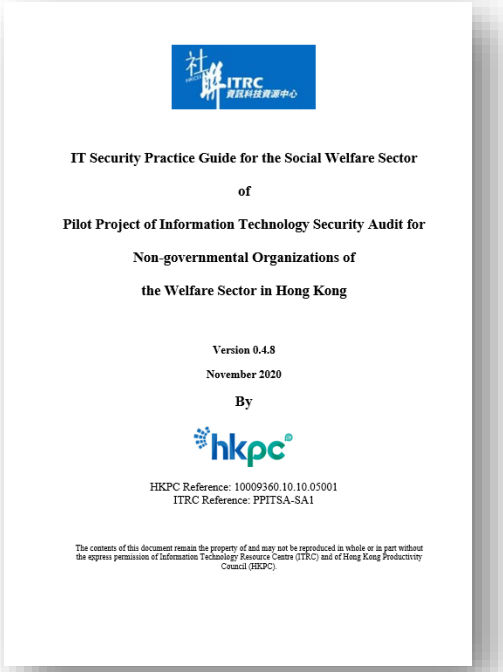


Project Deliverable 4 - IT Security Portal Website for Knowledge Sharing

https://itsecurity.hkcss.org.hk



IT Security News and Tips



IT Security Practice Guide for the Social Welfare Sector

of

Pilot Project of Information Technology Security Audit for

Non-governmental Organizations of

the Welfare Sector in Hong Kong

Version 0.4.8

November 2020

By

HKPC Reference: 10009360.10.10.05001
ITRC Reference: PPITSA-SA1

The contents of this document remain the property of and may not be reproduced in whole or in part without the express permission of Information Technology Resource Centre (ITRC) and of Hong Kong Productivity Council (HKPC).

IT Security Practice Guide & Toolkit

IT Security Training Materials

Opened to all the 169 subvented NGOs in late October 2021

Total No. of Visits: 150,052

Total No. of Visitors: 25,476

Total No. of Downloads: 346

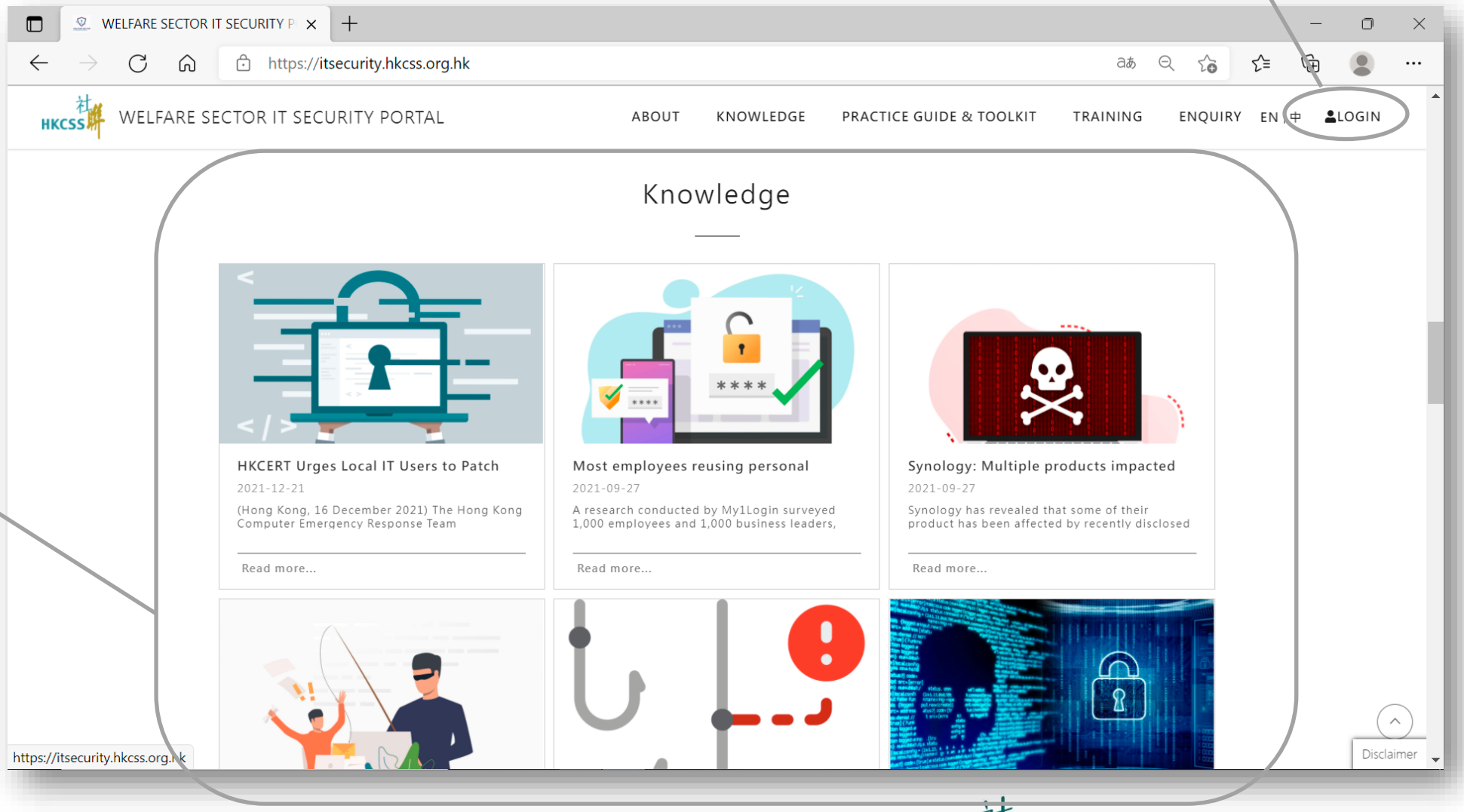
(September 2020 - December 2021)

資訊科技資源中心
Information Technology Resource Centre

IT Security Portal Website

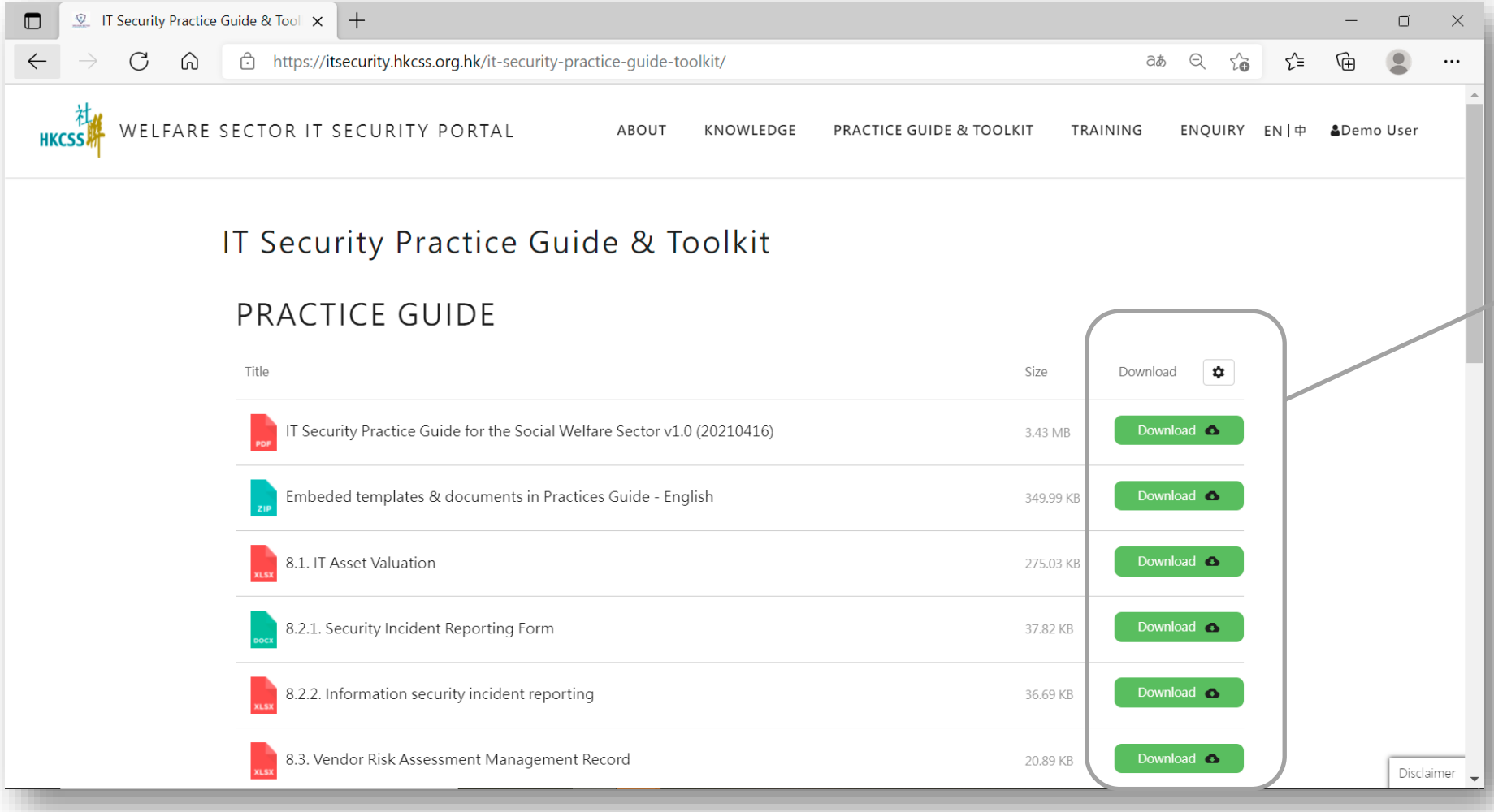
NGO Zone

IT Security News and Knowledge



IT Security Portal Website

IT Security Practice Guide and Toolkit



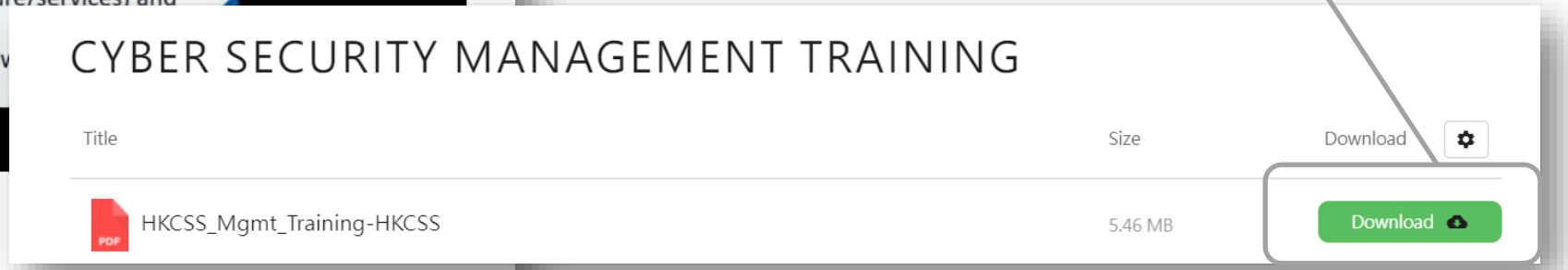
Click to Download

IT Security Portal Website

IT Security Training Recordings and Materials

Click to Play

Click to Download



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

Additional sharing with other NGOs for the Pilot Project

6th August 2021

81 Participants
50 NGOs

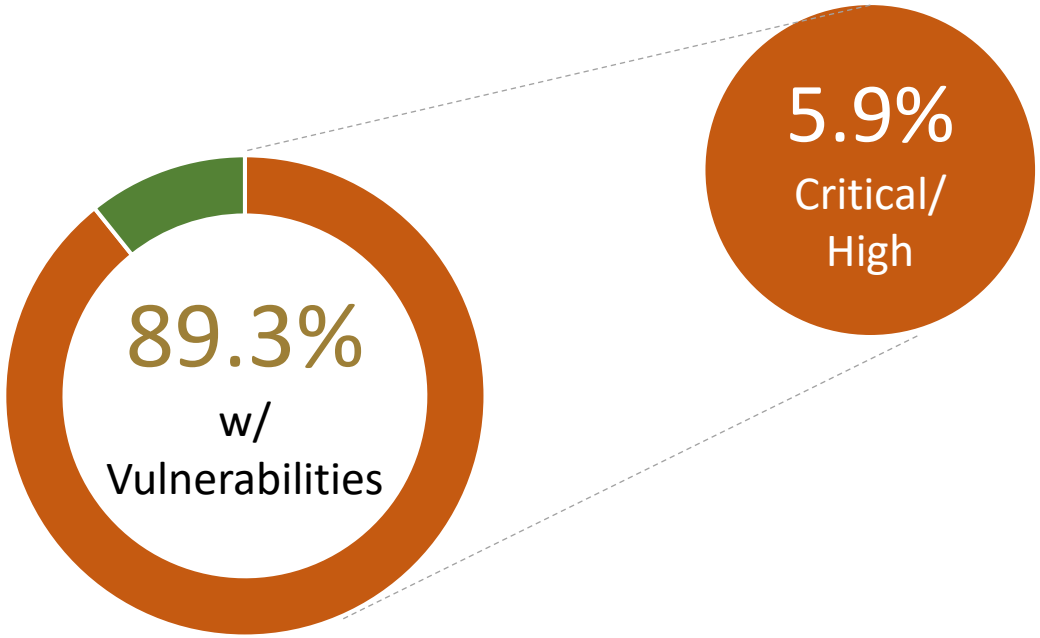
- IT Security Practice Guide, portal website and other resources of the Pilot Project were promoted to NGOs
- Experience sharing of IT security
  by Kwun Tong Methodist Social Service (循道衛理觀塘社會服務處)
- Feedback of IT Security Pilot Project
  by Hong Kong Sheng Kung Hui Welfare Council Limited
  (香港聖公會福利協會有限公司)
- Sharing on Security Operation Center (SOC)

3 Focus Areas

Most of the IT applications scanned were at risk.
The IT security scanning enabled the NGOs to mitigate risk.

~400

Hosts/ URLs scanned



HIGH Likelihood

x

HIGH Impact

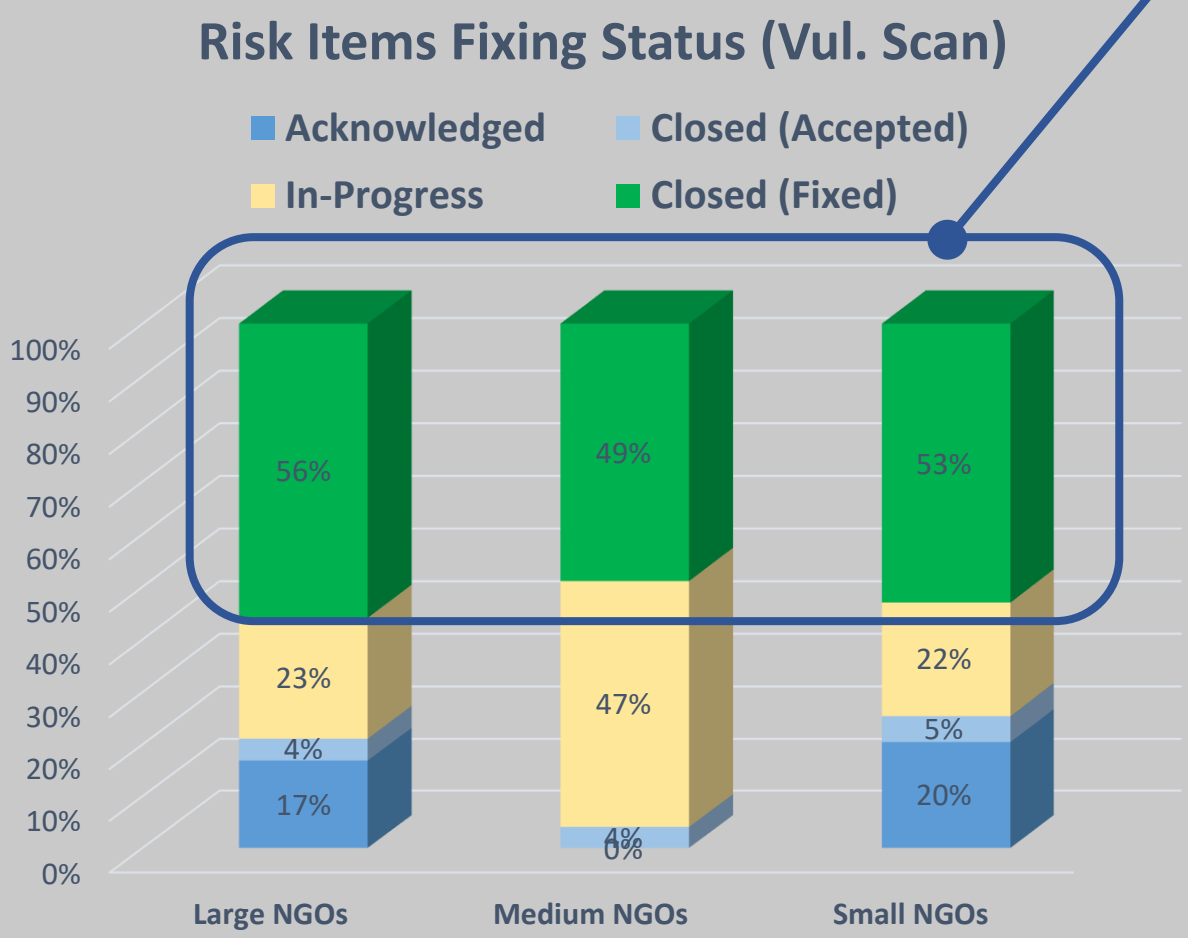
Possible impacts:

- Leakage of confidential information
- Data corruption/ encryption
- System suspension
- Website defacing

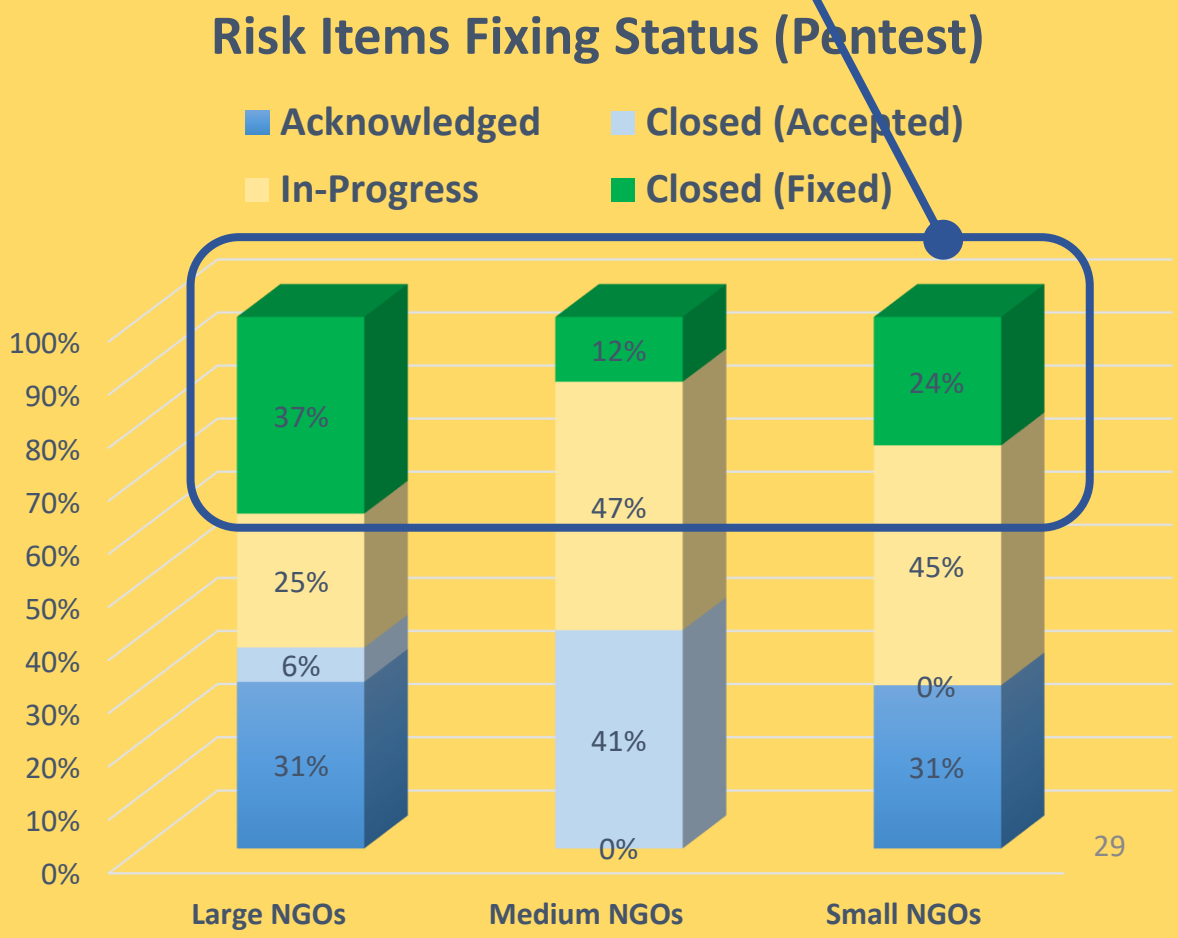
Results of Post-scanning (i.e. Compliance Check)

Only less than half of the identified vulnerabilities fixed

Vulnerability Scanning

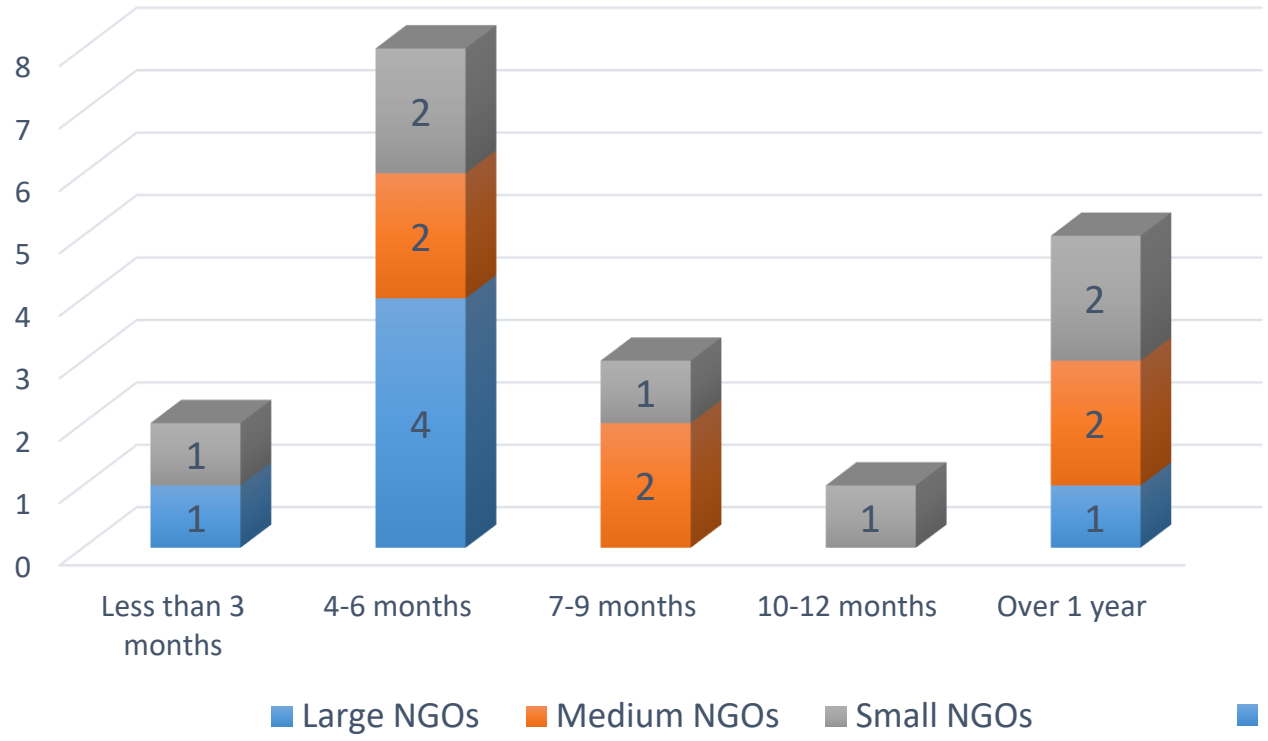


Penetration Testing

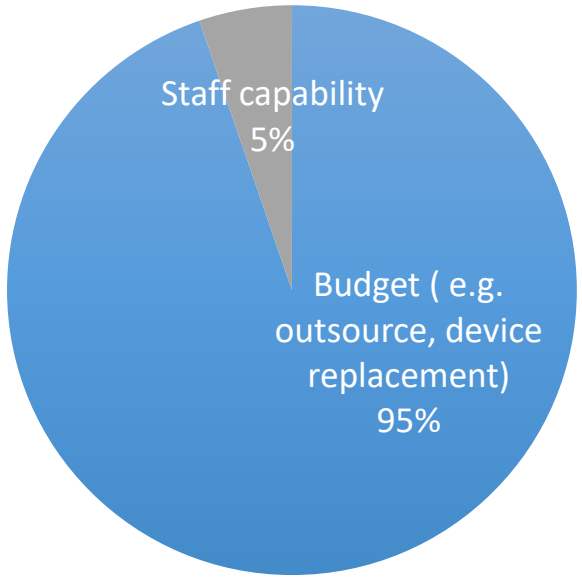


More time and funding resources required for fixing the identified vulnerabilities

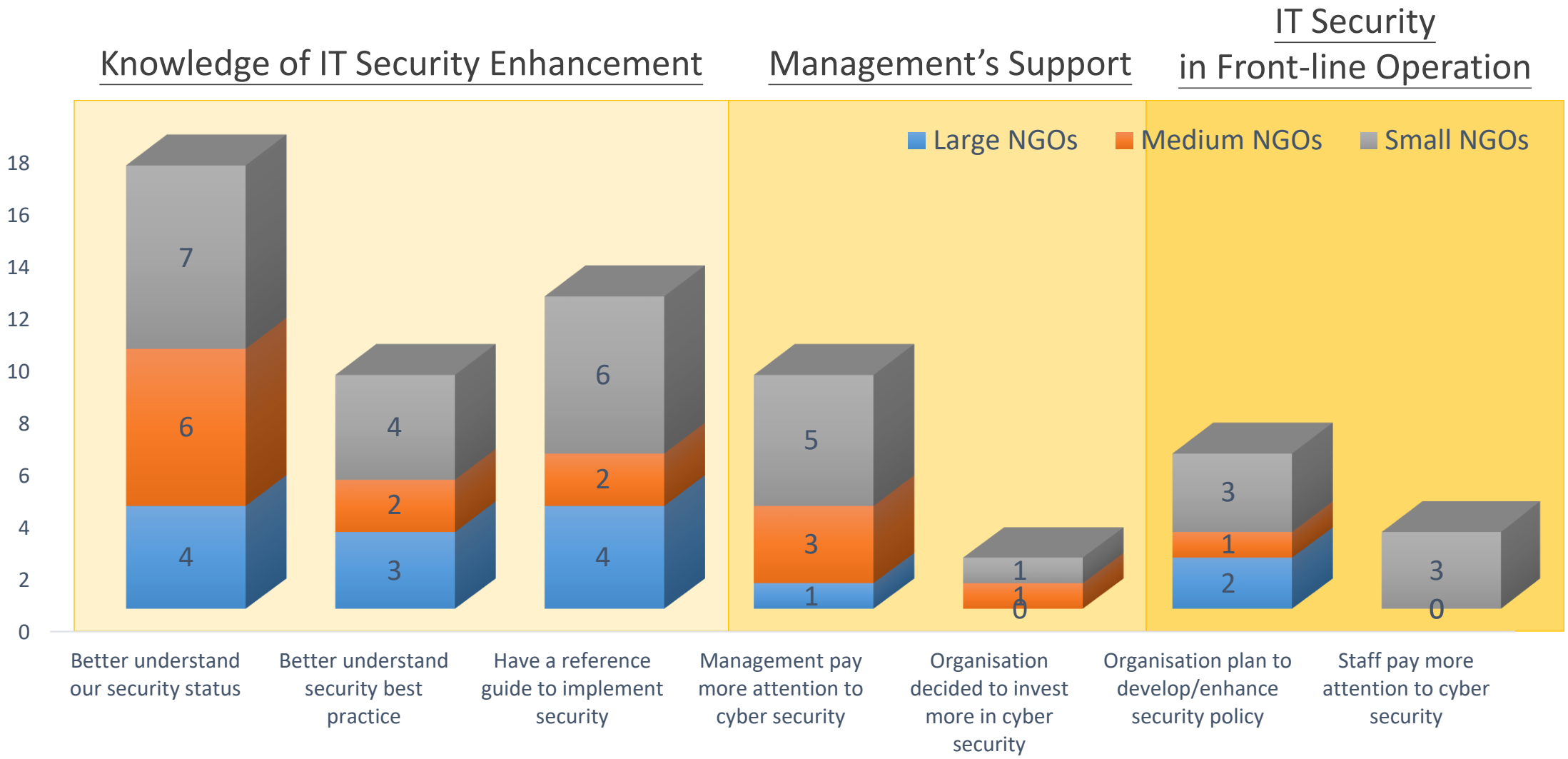
The Time Required for Vulnerability Fixing in General



The Most Important Hurdle to Fix the Risk Items



Changes made in the NGOs after the Pilot Project

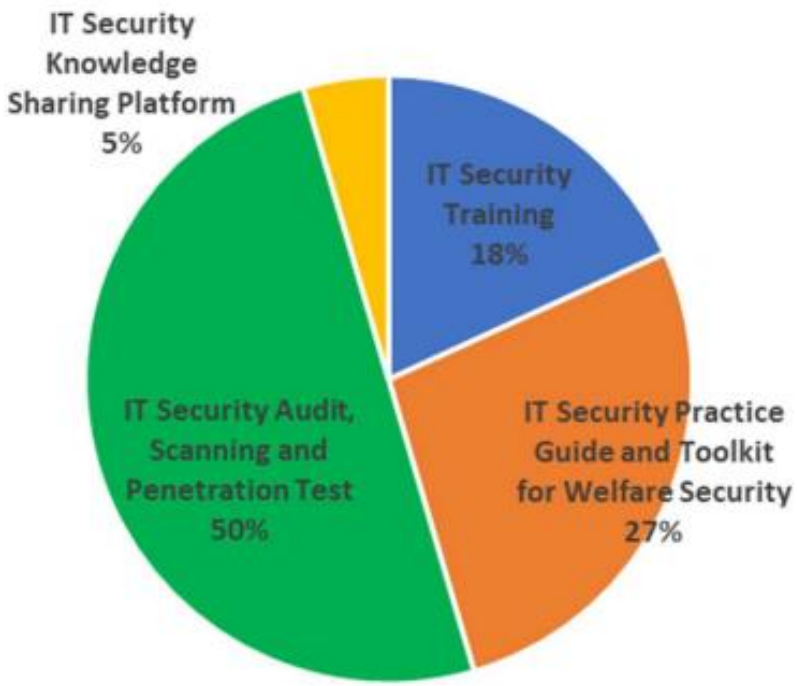


The NGOs appreciate IT Security Scanning and Practice Guide most

Overall Satisfaction Score

4.1/5

The Services the NGOs appreciate most



NIST Cyber Security Framework

1. Identify

What processes and assets need protection?
a. Security Risk Assessment and Audit (SRAA)
b. Asset management

2. Protect

Implement appropriate safeguards to ensure protection of the enterprise's assets
a. Vulnerability fixing
b. IT security training
c. IT security policies and guidelines
d. IT security solutions, such as firewall, Web Application Firewall (WAF), anti-virus, anti-ransomware, etc.

3. Detect

Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents
a. Security Operation Centre (SOC)
b. Cyber security monitoring

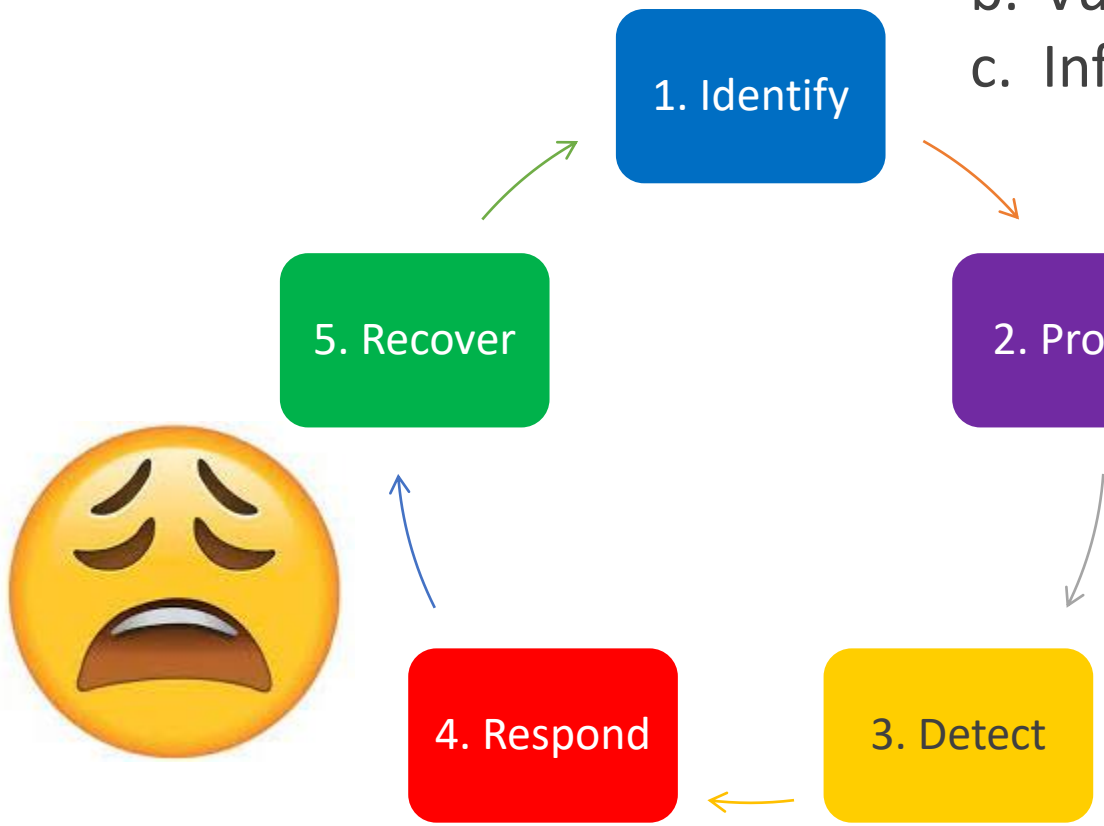
4. Respond

Develop techniques to contain the impacts of cybersecurity events
a. Isolation
b. Stakeholder management

5. Recover

Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events
a. System recovery
b. Digital forensics

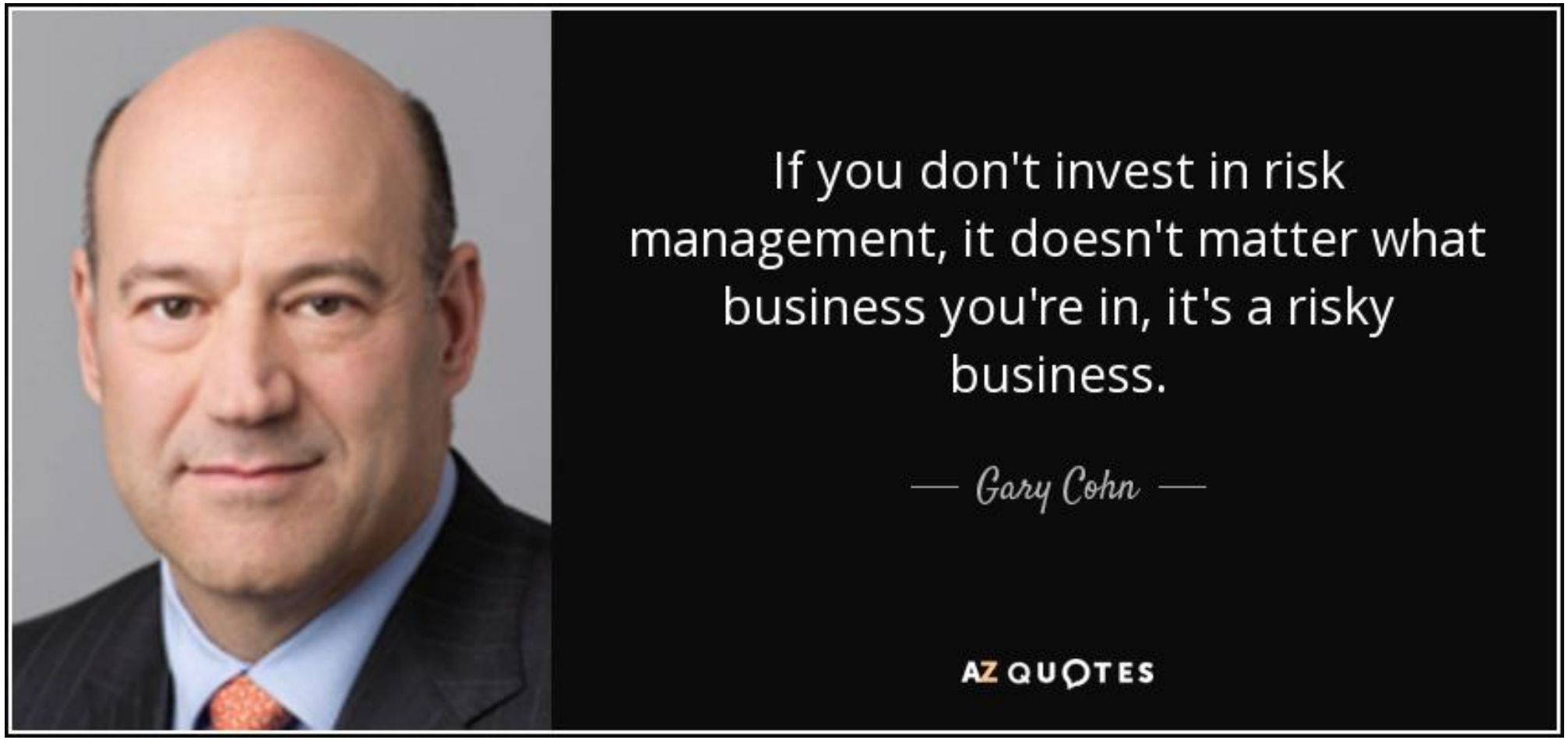
Common Weaknesses



a. Asset management
b. Vulnerability assessment
c. Information classification

d. Operation management
e. Network security
f. Change management

g. Security Monitoring



Gary Cohn - the former President and COO of Goldman Sachs and director of the National Economic Council


Thank
you