



Use of Deliverables of the Pilot Project of IT Security Audit for NGOs

6 September 2022

Information Technology Resource Centre

The Hong Kong Council of Social Service



1

Project Background



2

Project Deliverables

Agenda



1

Project Background

Project Background

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 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



IT Security Portal Website

- IT Security News
- IT Security Practice Guide and Toolkit

Participated NGOs

Pilot Project
22 NGOs

8 Large NGOs
6 Medium NGOs
8 Small NGOs



2

Project Deliverables

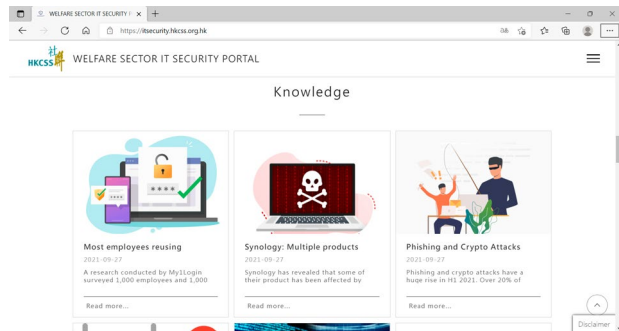
Project Deliverable 1 – IT Security Portal Website



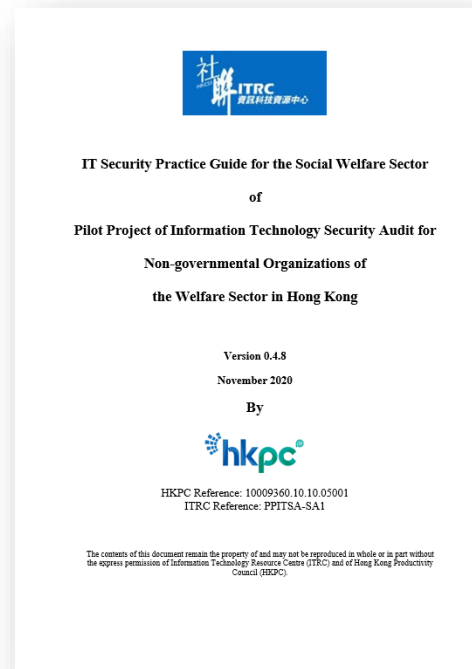
<https://itsecurity.hkcss.org.hk>



IT Security Portal Website for Knowledge Sharing



IT Security News and Tips



IT Security Practice Guide & Toolkit



IT Security Training Materials

Opened to all the **170** subvented NGOs
in late October 2021

 Total No. of Visits: **267,904**

 Total No. of Visitors: **41,742**

 Total No. of Downloads: **1558**

(September 2020 - July 2022)

Knowledge



HKCERT Urges Local IT Users to Patch Apache "Log4j" Vulnerability ASAP

(Hong Kong, 16 December 2021) The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) of the Hong Kong Productivity ...



Most employees reusing personal passwords to protect corporate data

A research conducted by My1Login surveyed 1,000 employees and 1,000 business leaders, found that 85% of employees are reusing passwords ...



Synology: Multiple products impacted by OpenSSL RCE vulnerability

Synology has revealed that some of their product has been affected by recently disclosed remote code execution and denial of ...





1


Login

2

Please login before accessing the IT Security Practice Guide/ Toolkit and attaining IT security training online

Username or E-mail

Password

 Keep me signed in

Login

The login information had been sent to the official e-mail address of each NGO in late October 2021

Project Deliverable 2 – IT Security Practice Guide/ Toolkit

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

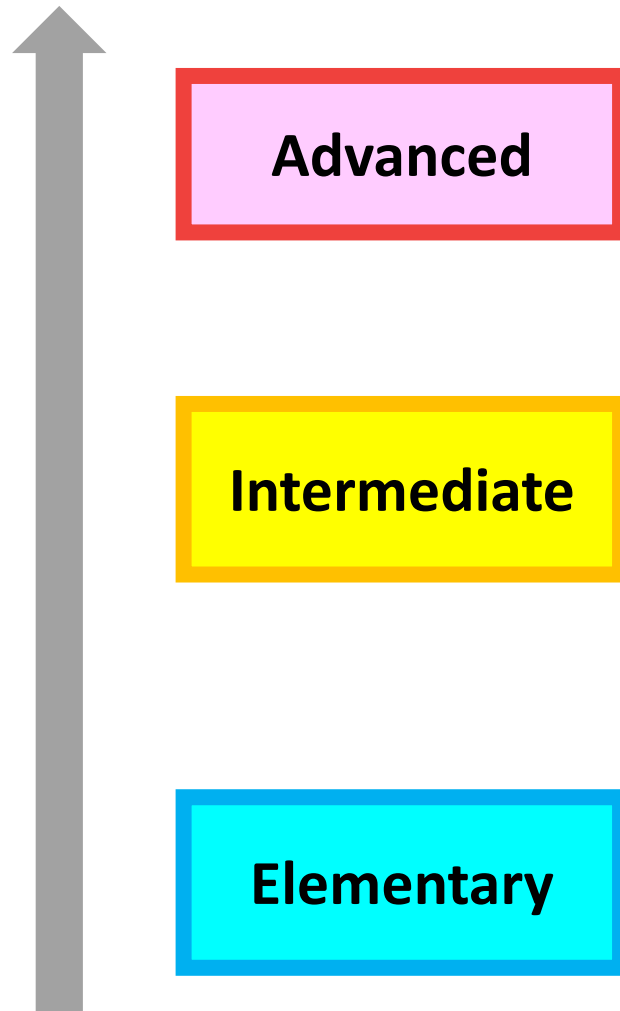
3

Security Levels



IT Security Practice Guide

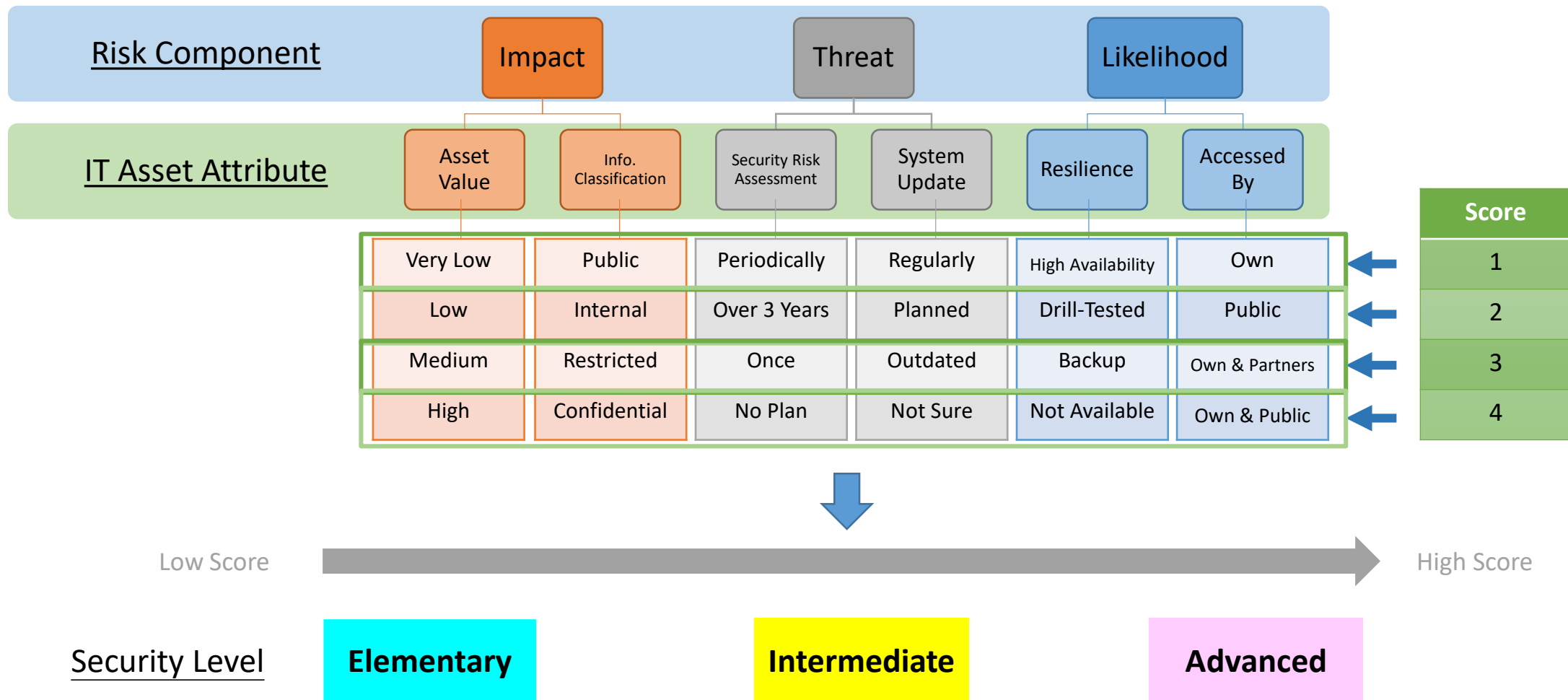
Different Security Levels would be recommended for various IT assets in different natures



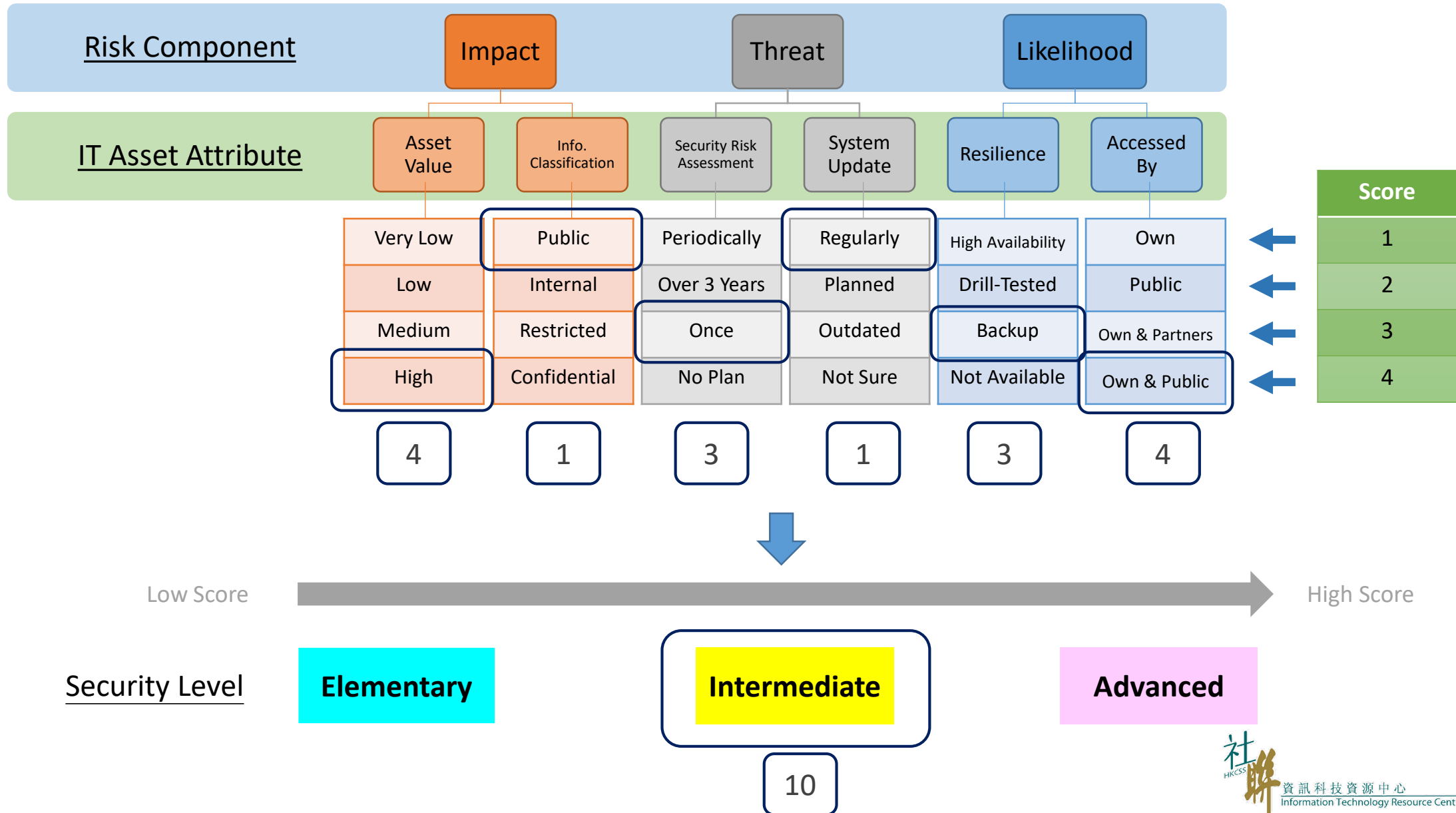
Remote Access/Work from Home				
Security Level: E = Elementary, I = Intermediate, A = Advanced		E	I	A
1	Access to your home computer's desktop and mobile devices should at least be password protected, and the password should be strong one.	✓	✓	✓
2	Update your personal devices antivirus solution with an updated signature and update your software and operating systems.		✓	✓
3	Encrypt devices and other media that contain sensitive personal information. Includes laptops, tablets, smartphones, removable drives, and cloud storage solutions. Disk encryption or folder encryption also helps protect information on stolen or compromised computers.			✓

IT Security Practice Guide

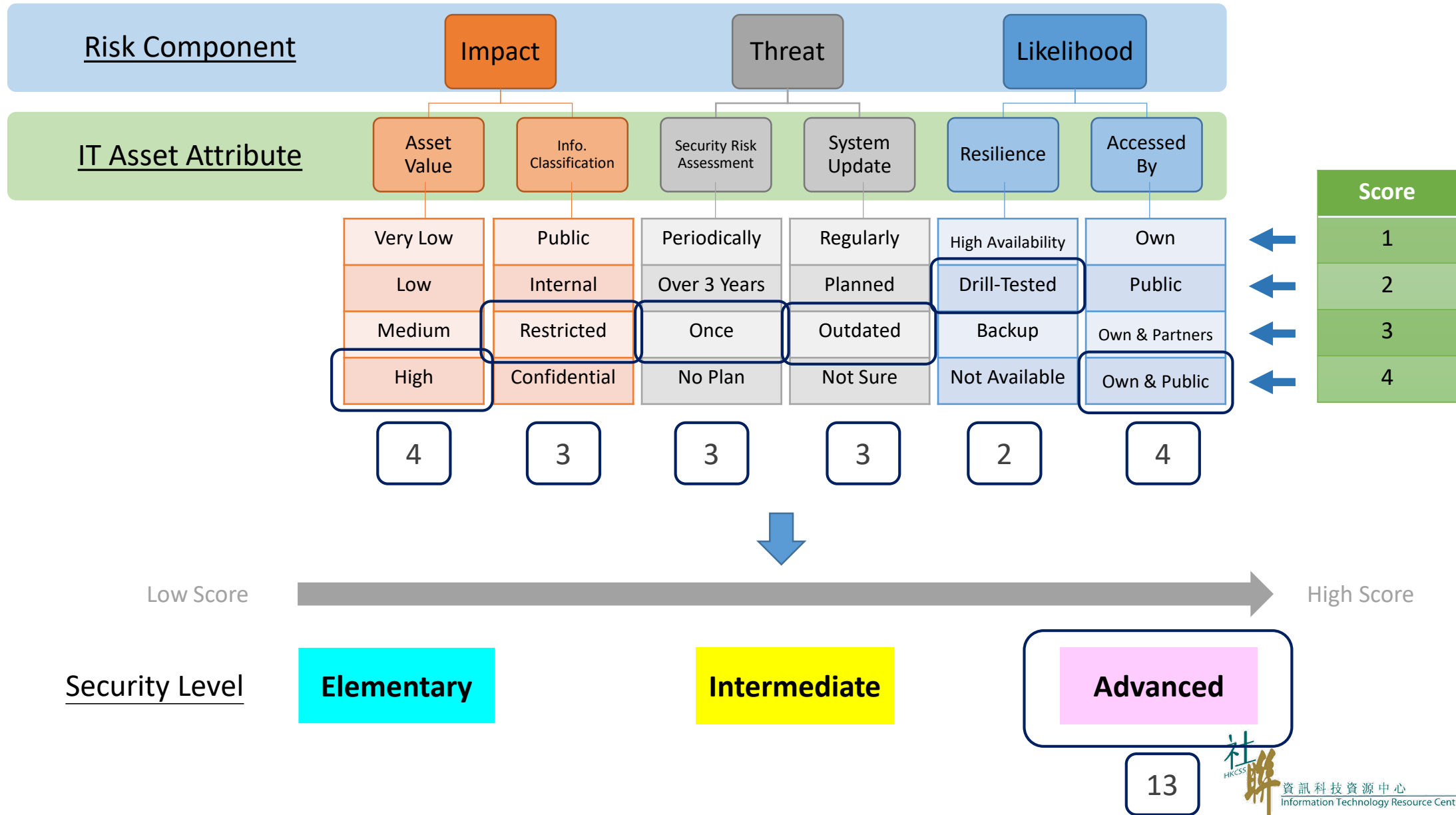
Determination of Security Level based on IT Asset's attributes



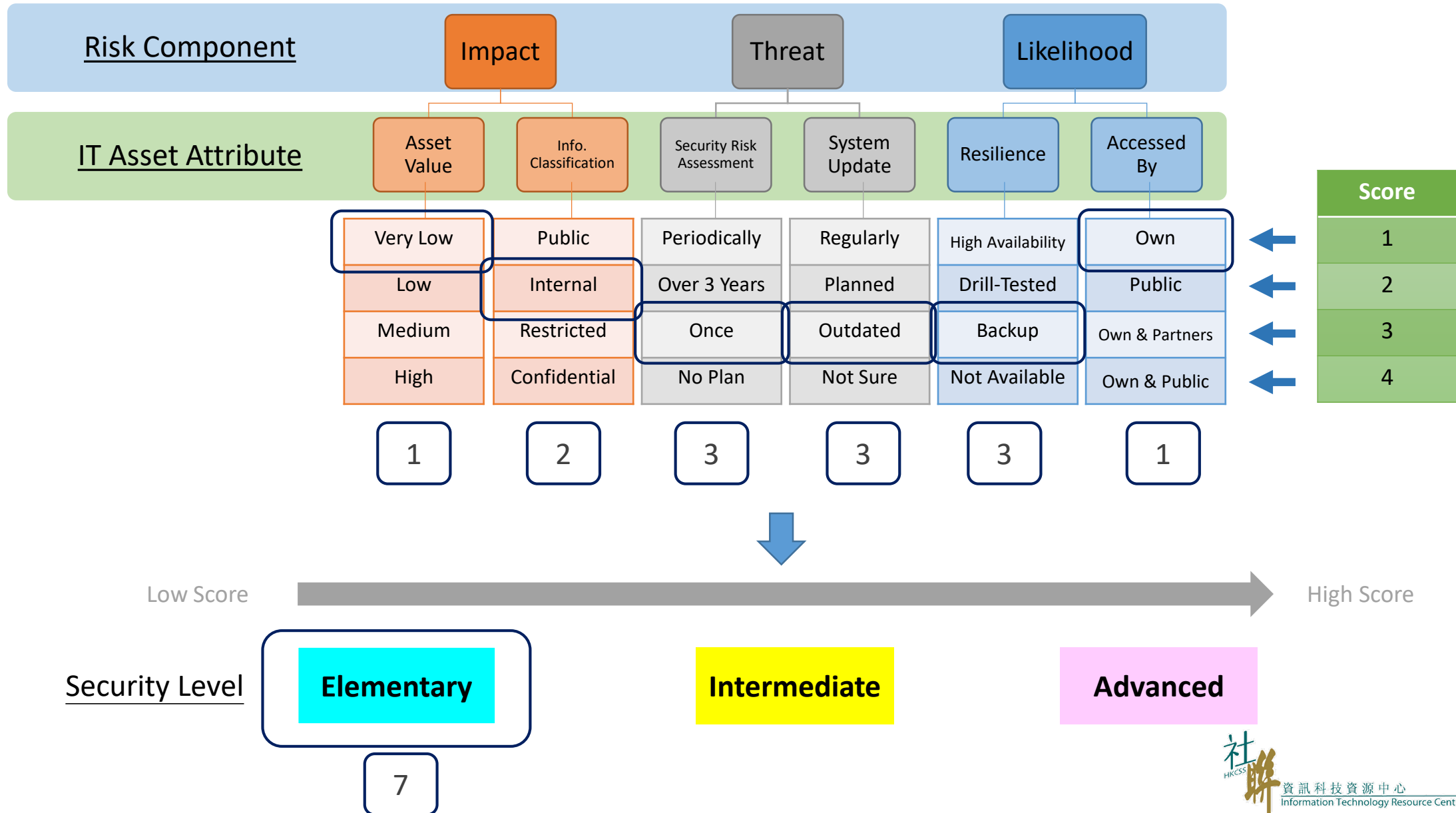
Case Study – Organization Website



Case Study – Event Management System (Online Enrollment)



Case Study – Fixed Asset Management System (Internal, Stand-alone PC)



IT Asset Valuation Calculator

	B	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	Asset Information	Asset Value	Info. Classification (Confidentiality)	Security Risk Assessment	Sys. Update (Integrity)	Resilience (Availability)	Accessed By	Consequence (Impact)	Vulnerabilities (Threat)	Probability (Likelihood)	Security Score	Elementary (3 - 7)	Intermediate (8 - 11)	Advanced (12 - 15)
2	Organization Website	High	Public	Once	Regularly	Backup	Own & Public	Medium	Low	Very High	10		10	
3	Event Management System	High	Restricted	Once	Outdated	Drill Tested	Own & Public	Very High	High	High	13			13
4	Fixed Asset Management System	Very Low	Internal	Once	Outdated	Backup	Own	Very Low	High	Low	7	7		

Asset Information
Organization Website
Event Management System
Fixed Asset Management System

Security Score	Elementary (3 - 7)	Intermediate (8 - 11)	Advanced (12 - 15)
10		10	
13			13
7	7		

Download IT Security Practice Guide/ IT Asset Valuation

WELFARE SECTOR IT SECURITY PORTAL

ABOUT KNOWLEDGE **PRACTICE GUIDE & TOOLKIT** TRAINING ENQUIRY EN | 中 Demo User

IT Security Practice Guide & Toolkit

2 IT Security Practice Guide

IT Security Practice Guide & Toolkit

PRACTICE GUIDE

Title	Size	Download
 IT Security Practice Guide for the Social Welfare Sector v1.0 (20210416)	3	Download
 Embedded templates & documents in Practices Guide - English	349.99 KB	Download
 8.1. IT Asset Valuation	3	Download
 8.2.1. Security Incident Reporting Form	37.82 KB	Download

IT Security Toolkit

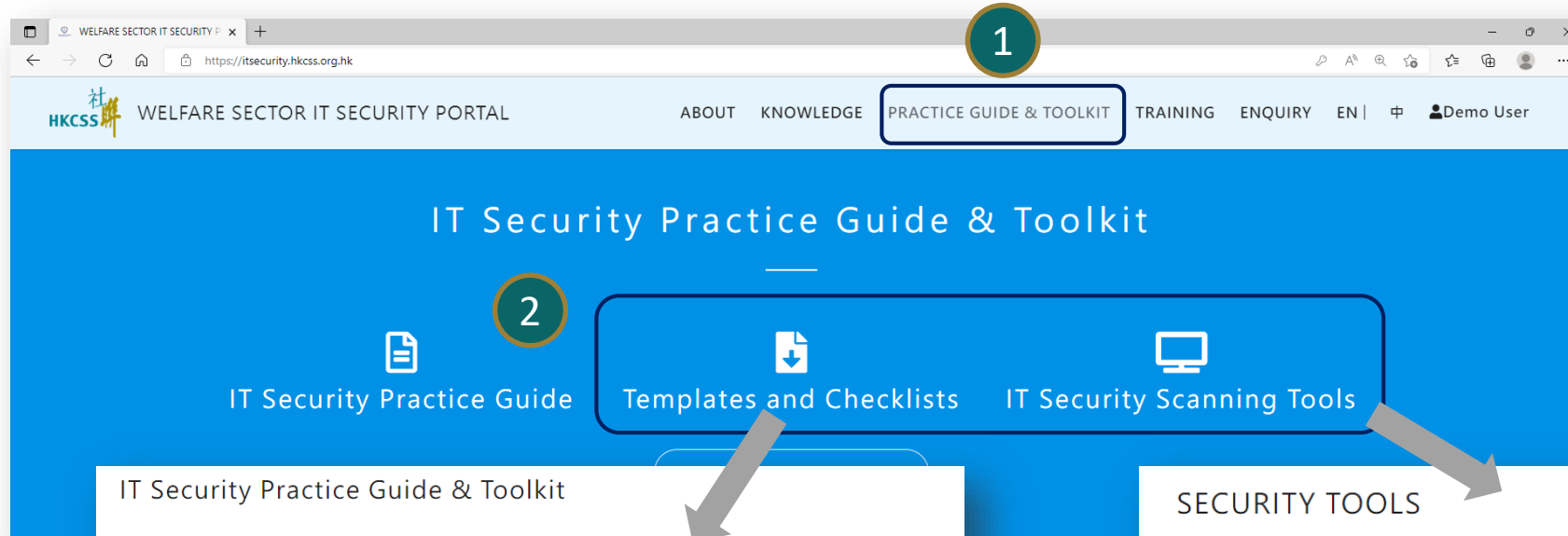
Templates and Checklists

- 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
- Security Risk Assessment Guidelines

IT Security Scanning Tools

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

Download IT Security Templates/ Checklists



The screenshot shows the 'PRACTICE GUIDE' section. It features a table with columns for 'Title', 'Size', and 'Download'. A circled '3' is placed to the left of the table. The table lists several documents, each with a download button.

Title	Size	Download
IT Security Practice Guide for the Social Welfare Sector v1.0 (20210416)	3.43 MB	Download
Embedded templates & documents in Practices Guide - English	349.99 KB	Download
8.1. IT Asset Valuation	275.03 KB	Download
8.2.1. Security Incident Reporting Form	37.82 KB	Download
8.2.2. Information security incident reporting	36.69 KB	Download
8.3. Vendor Risk Assessment Management Record	20.89 KB	Download
8.4. NGO IT Audit Checklist	16.86 KB	Download
8.5. Seven Habits of Cyber Security	28.36 KB	Download
8.6. Security Risk Assessment Guidelines	31.94 KB	Download

The screenshot shows the 'SECURITY TOOLS' section. It features a table with columns for 'Title', 'Size', and 'Download'. A circled '3' is placed to the left of the table. The table lists several tools, each with a download button.

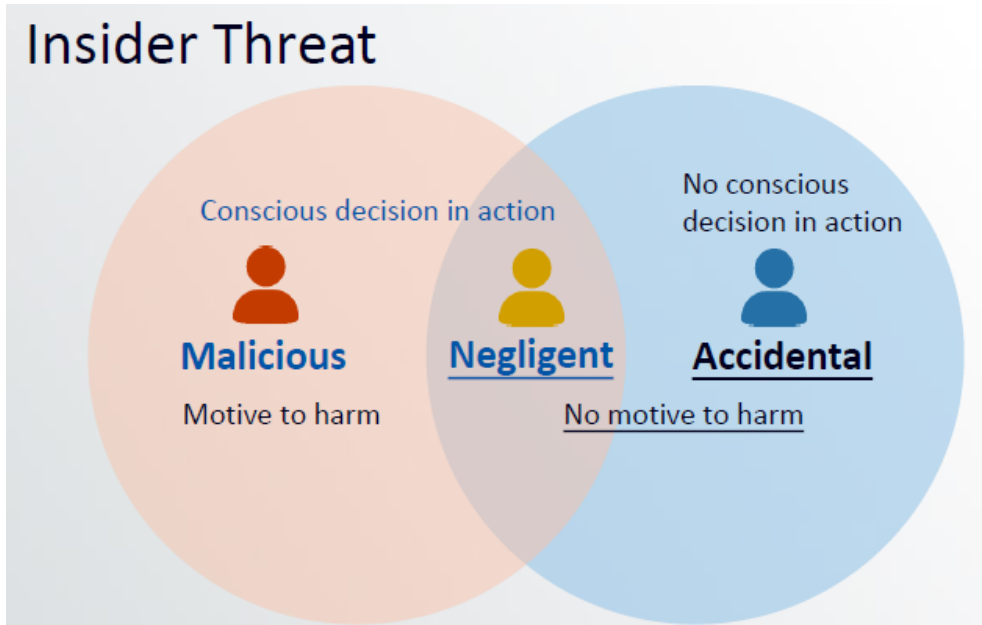
Title	Size	Download
WinAudit	290.75 KB	Download
VeraCrypt	61.29 KB	Download
OWASP Zed Attack Proxy (ZAP)	159.75 KB	Download
Nessus Essentials	128.83 KB	Download
NMap Zenmap Security Scanner	77.44 KB	Download
Logging Made Easy	176.49 KB	Download
Kali Linux	117.14 KB	Download

Project Deliverable 3 – IT Security Training

IT Security Training - Management

- 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

IT Security Training - Management



SingHealth hacking incident 2018

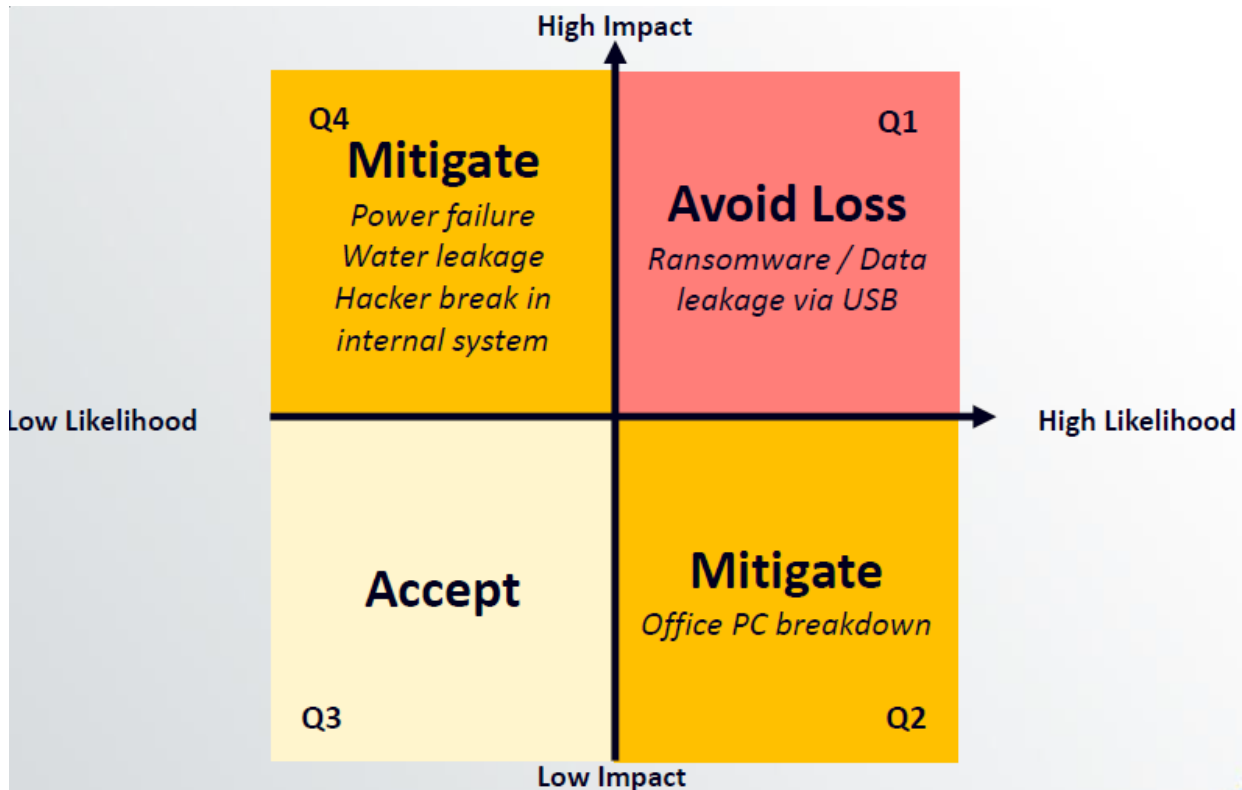


20 July 2018 | SingHealth and CSA announced a SingHealth hacking case

- 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

新加坡醫療保健集團 (SingHealth)

IT Security Training - Management



IT Security Training – General Staff

- To learn Cyber Security basic concept
- To share Cyber Security status and recent incidents
- To learn external cyber threat analysis and security advice such as social engineering scams, malware, browser and mobile security issues
- To learn internal cyber threat analysis and security advice such as data leakage, BYOD and WFH risks

IT Security Training - General Staff

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



Phishing Email Example

你的EMAIL超出最大范围限制。
[Redacted] (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 for
Admin: Copyright © 2013 Webmaster Central Help-desk.

您已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，并且关闭您的邮箱。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。

Email Phishing

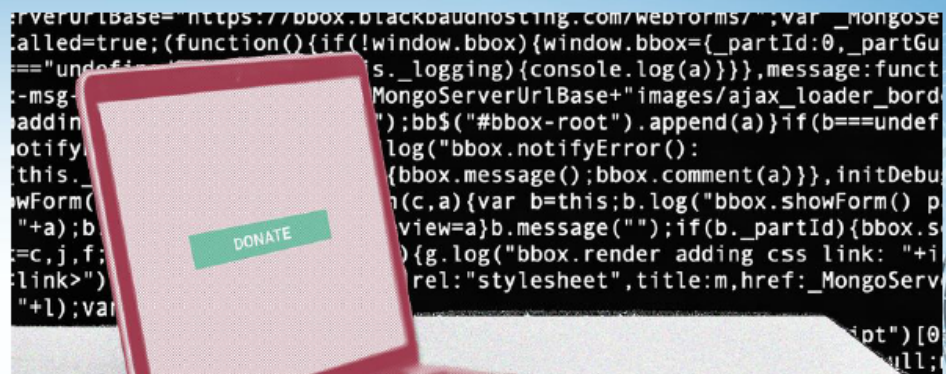
Email phishing is the most traditional means of phishing, using an email urging you to reply or follow-up by other means. Web links, phone numbers, or malware attachments can be used.

Typical scenario:



IT Security Training - General Staff

Ransomware Attacks on NGOs



A major ransomware attack has affected dozens of international NGOs and their records of private donations, but details of the hit on a US fundraising platform are scarce, and two weeks after being warned some aid groups are yet to notify their donors or the public.

BYOD and WFH

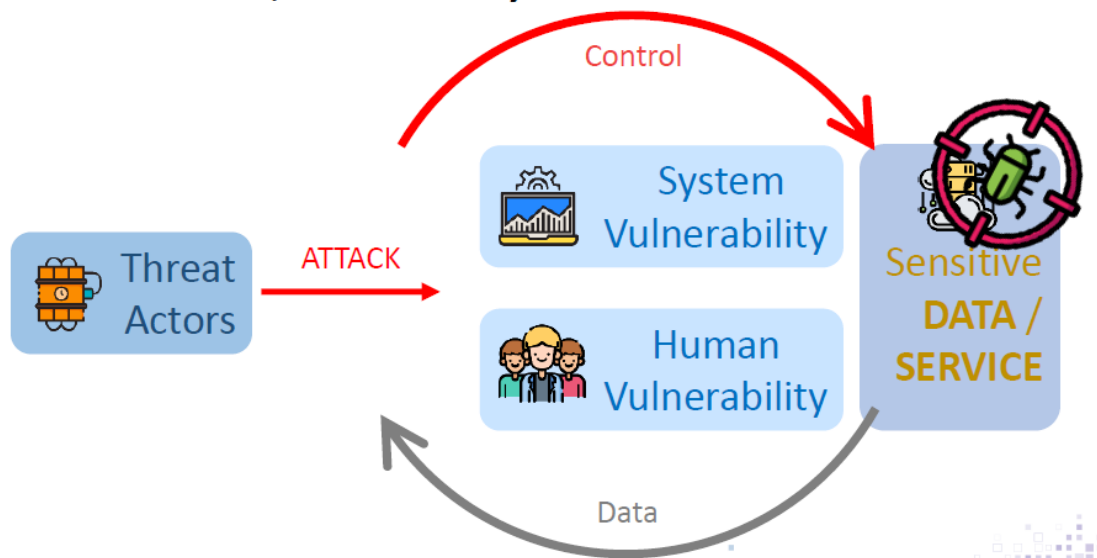


IT Security Training – IT Staff

- To learn how to control and manage information security
- To learn the routine housekeeping work and monitoring required
- To learn the techniques of detecting vulnerabilities/ security breach, and how to respond when there is a security incident
- To learn up-to-date IT security technology
- To understand resource/ cost impact on IT security measures


IT Security Training - IT Staff

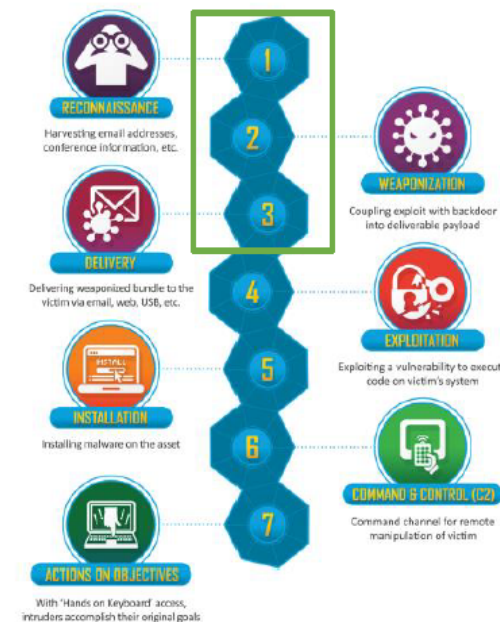
Threat, Vulnerability & Attack



Case Study : Ransomware Attack

Background: A European biomolecular research institute involved in COVID-19 related research was infected Ryuk Ransomware.

1. A student tries to download a "Crack" version of a data visualization software tool
2. A security alert was triggered from Windows Defender 
3. The student disabled the Windows Defender and firewall, then download the software again.
4. A malicious info-stealer was downloaded to student's computer



IT Security Training - IT Staff

Exercise 1: Using OWASP ZAP

(Open Web Application Security Project)

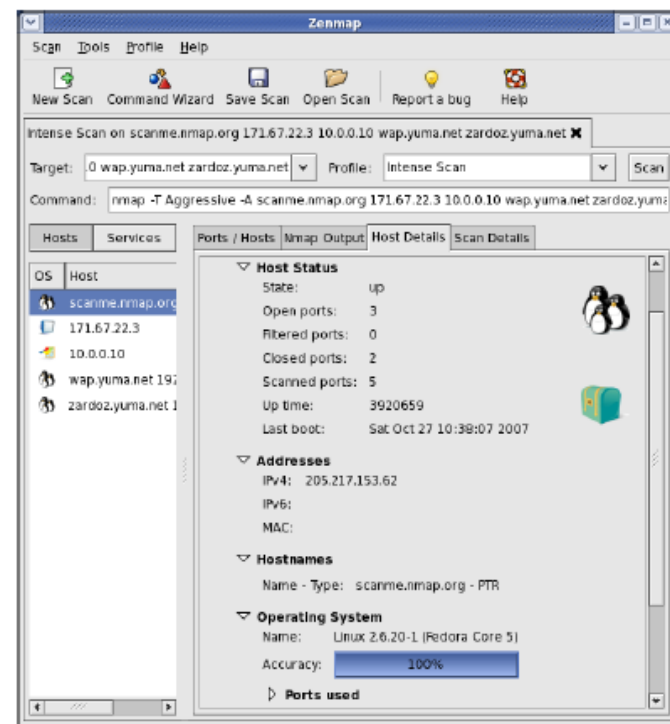
1. Launch XAMPP
2. Start Apache and MySQL
3. Launch ZAP
4. Open Browser with ZAP Proxy
5. Go to testing web site (<http://127.0.0.1:5080/test>)

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

Nmap / Zenmap



Online Training

Training – WELFARE SECTOR IT S x +

https://itsecurity.hkcss.org.hk/training/

HKCSS 社 聯 WELFARE SECTOR IT SECURITY PORTAL ABOUT KNOWLEDGE PRACTICE GUIDE & TOOLKIT **TRAINING** ENQUIRY EN | 中 Demo User




CYBER SECURITY MANAGEMENT TRAINING VIDEO

1 Cyber Security Management Training for Welfare Sector Part1

稍後觀看 分享

2 Click to watch training video

CYBER SECURITY MANAGEMENT TRAINING

Title	Size	Download
 HKCSS_Mgmt_Training-HKCSS	5.46 MB	 

3 Click to download presentation file

Recommendations

- 1 Strengthen IT governance and formulate IT security policy
- 2 Incorporate IT security as an integral part of digitalization of social services
e.g. performing Security Risk Assessment and Audit (SRAA) regularly, planning and budgeting for vulnerability fixing/ system updating, protection of IT assets, detection of cybersecurity incidents
- 3 Build the mind-set and awareness of IT security in the organization
e.g. by training, phishing e-mail drill
- 4 Get prepared for emergency response
e.g. system recovery, maintaining public relationship, stakeholder management

ITRC contact point

Ricky Fung

Deputy General Manager

T: 2922 9268

E: ricky.fung@hkcss.org.hk

Eric Tang

Manager, Project Management

T: 2922 9263

E: eric.tang@hkcss.org.hk

Peter Cheung

Analyst Programmer

T: 2922 9264

E: peter.cheung@hkcss.org.hk

*Thank
you*

