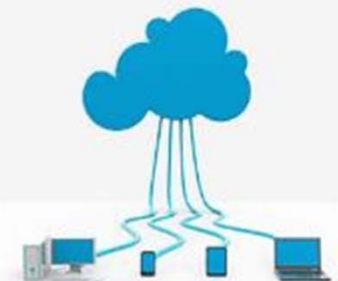


Setting up school-based information and incident handling procedures as well as roles and responsibility of stakeholders



KAM WAI MING, KAN KA HEI
Hong Kong Association for Computer Education
香港電腦教育學會 (HKACE)

Security VS Convenience



Students sue Miami-Dade school district after Social Security numbers posted online

BY KYRA GURNEY

KGURNEY@MIAMIHERALD.COM

JUNE 21, 2017 12:31 PM, UPDATED JUNE 21, 2017 12:34 PM

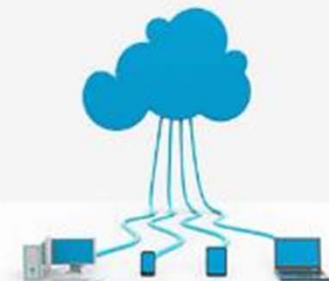


The Miami-Dade School Board has been sued by two students who say their Social Security numbers were posted on a district website.

Two former Miami-Dade students are suing the School Board after they found their Social Security numbers and test scores online along with the personal information of hundreds of other students.

The plaintiffs did a basic online search of their names and discovered that the information was posted on the Miami-Dade school district's website, according to the lawsuit.

"The carelessness with how the district manages students' private information needs to be addressed," lawyer Stephanie Langer said in a statement. The students are asking for both monetary damages and an "overhaul" of school district policies on the protection of student information.



1,446 views | May 22, 2018, 11:00am

School Hackers Changed Grades And Tried To Get A Free Lunch



Lee Mathews Contributor ⓘ

Security

Observing, pondering, and writing about tech. Generally in that order.

f

🐦

in

School districts around the U.S. are busy wrapping up their academic years. Some are also wrapping up other business, like criminal investigations into breaches of the school's computer systems.



Screen capture: Lee Mathews/Forbes LEE MATHEWS/FORBES





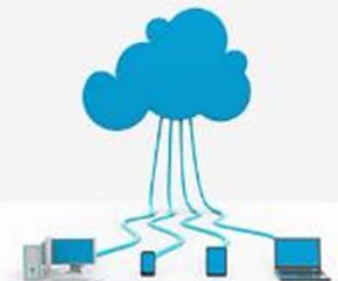
Building a Cyber-Secure Culture

- Mindset
 - Given the prevalence of cyber attacks, we need to stay alert and prepared.
- Leadership
 - Set overall direction, establish priorities, maintain influence, and mitigate risks
 - School IT Team should model good personal security habits based on guidelines
- Training and Awareness
 - Awareness training programs build an understanding of risks and provide specific steps for mitigating them.



Managing and Maintaining Cyber-security in School

- Policies and Procedures
- Infrastructure and Technology
- Education and Training
- Standards and Inspection



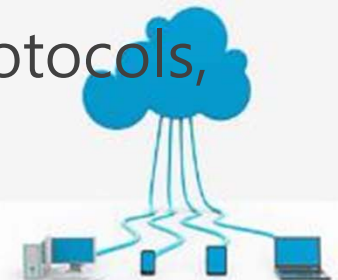
Policies and Procedures

- Include cyber risks in the school risk management process
- Nominate right person responsible for cyber security issues
- Systematic and regular review of cyber security policies, at least on an annual basis
- Ensure policies and procedures that incorporate cyber security concerns are in place
- Establish a routine reporting process for cyber risks within the school
- Maintenance, Monitoring, and Analysis of audit logs
- Record cyber security incidents and actions taken



Infrastructure and Technology

- Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers
- Ensure that appropriate filtering and monitoring is in place.
- Inventory of Authorized and Unauthorized Devices
- Managing user privileges
- Malware prevention
- Patch system software and application software
- Data Recovery Capability
- Limitation and Control of Network Ports, Protocols, and Services
- Data Protection



Tools for Encryption



AxCrypt

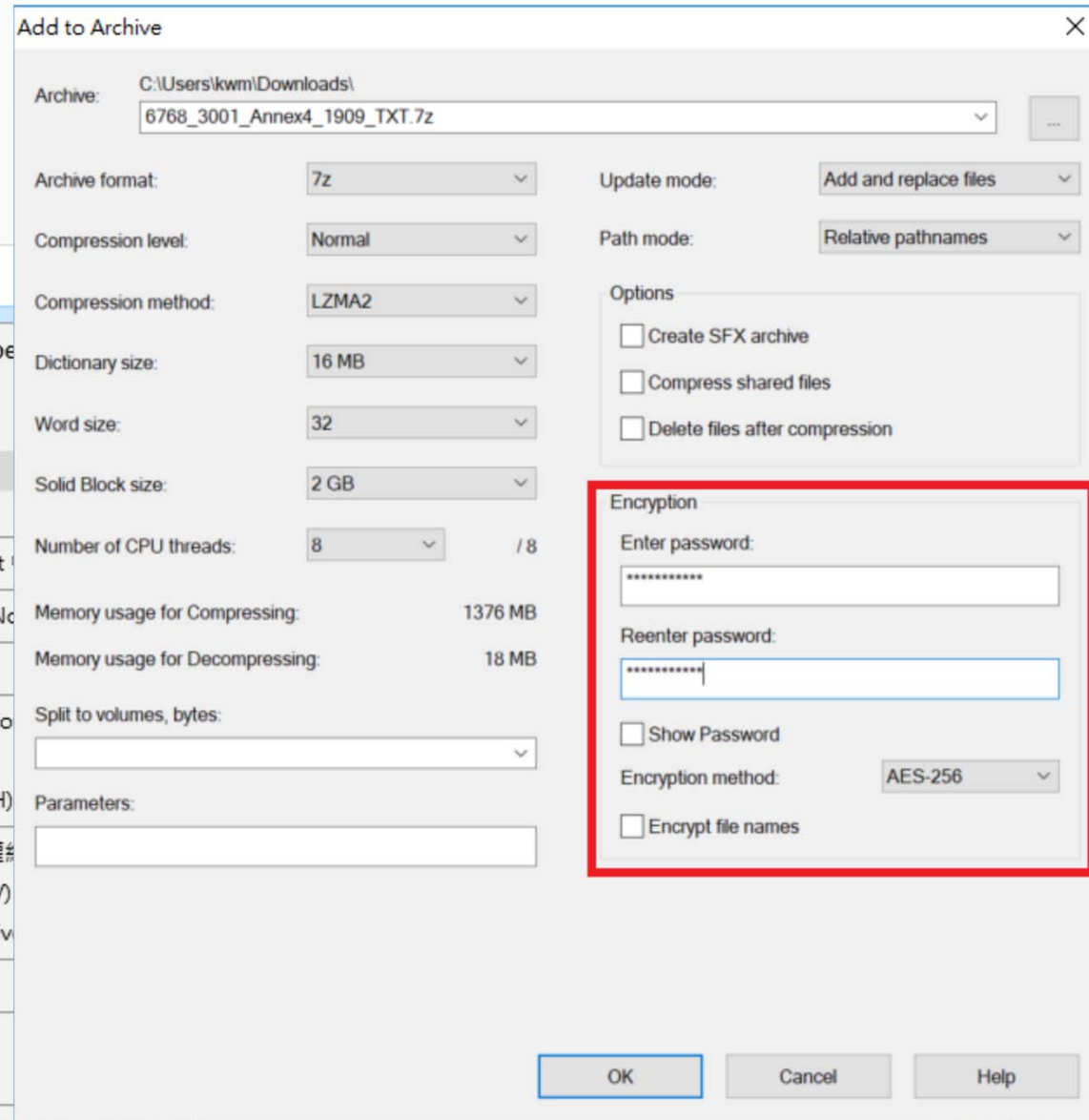
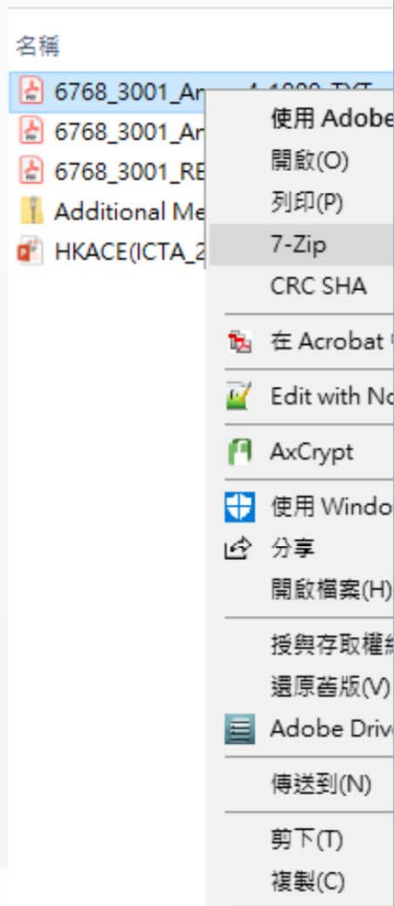
File security for you and your team

File Name	Modified	Size
Nomination Form	1/4/2019 13:00	309 KB
Programme Aims and Objectives	13/3/2019 12:10	51,254 KB
Invoice -Times Publishing HK	25/2/2019 14:32	295 KB
香港電腦教育學會	22/4/2019 11:00	63 KB

- 開啟(O)
- 編輯(E)
- 新增(N)
- 列印(P)
- 7-Zip
- CRC SHA
- 轉換為 Adobe PDF(B)
- 轉換為 Adobe PDF 並由電子郵件發出(E)
- 在 Acrobat 中合併支援的檔案...
- Edit with Notepad++
- AxCrypt**
- 使用 Windows Defender 掃描...
- 分享
- 開啟檔案(H)...
- 授與存取權給(G)
- 還原舊版(V)

- Encrypt
- Advanced
- Secure Delete
- Sign Out
- About

Tools for Encryption



3:48
3:48
3:48
3:47

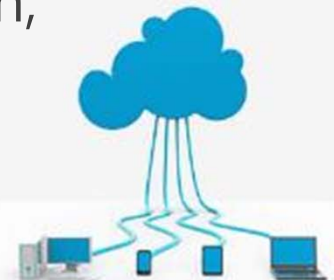
Mobile device management Device Enrollment Program (IOS) / Zero Touch Enrollment (Android)

- Force the device to enroll with SimpleMDM
- Select which SimpleMDM group devices should initially join
- Disable users ability to un-enroll from SimpleMDM manually
- Place device in supervised mode
 - Skip passcode setup, location services, restoring from backup, signing in to Apple ID and iCloud, Apple Pay setup



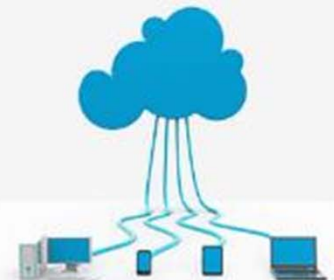
Education and Training

- Ensure the whole school community is aware of what is appropriate online behaviour and understand the sanctions for misuse.
- For teachers :
Implement regular training for all members of staff
- For TSS :
Refresh knowledge and skill at regular intervals to enable them to keep up-to-date with current research, legislation and trends



Education and Training

- For students :
 - Ensure that appropriate cyber security education is embedded throughout the curriculum; promoting the responsible use of technology and empowering students to keep themselves and others safe online
 - Actively engage with events to promote positive online behavior
- For parents :
 - Ensure that online safety is promoted to parents through a variety of channels and approaches



HKACE 舉辦學生獎勵計劃

<https://www.hkace.org.hk/>



HKACE 支持活動：新媒體素養

<http://media>



保

互動教材



《肥明裂傳》、工

10 分鐘

5 分鐘



香港青年
the hongkong

主頁 關於我們



PROJECT NET
新媒體素養提升計劃

主辦機構



香港青年協會
the hongkong federation of youth groups

贊助



優質教育基金
Quality Education Fund

協理機構

香港浸會大學
傳理學院新聞系

香港翻譯教學協會



香港科學教育學會
The Hong Kong Association
for Science Education

媒體夥伴



HKACE 支持活動：網絡安全比賽

主辦機構



網絡安全中心
CyberSecurity
Centre



香港專業教育學院(柴灣)
資訊科技系

支持機構

香港電腦教育學會 (HKACE)
香港奪旗賽協會 (HKCTF)
專業資訊保安協會 (PISA)

< 網絡安全比賽 / >

2019

比賽目的 / 比賽背景

- 提倡和推動網絡安全教育，提高青少年對網絡安全的興趣，培育21世紀所需要的網絡安全人才。
- 鼓勵及嘉許積極推動網絡安全教育的學校、老師及學生團體。

參賽資格

全港中學中四至中六、青年學院(YC)及香港專業教育學院(IVE)基礎課程文憑課程(DFS)的學生

比賽形式

- 比賽以隊制方式進行，每隊上限人數為2人
- 比賽採用網絡攻防形式進行，參賽者將按照題目指示以不同技巧找出目標電腦系統的保安漏洞，例如：枚舉(Enumeration)、掃描(Scanning)和提權(Gaining Access)

比賽日期

2019年12月7日(六) | 10:00 - 13:00
香港專業教育學院(柴灣)教學樓3樓316室 網絡安全中心

評判委員/評判團

網絡安全業界人士
資訊科技系網絡安全課程導師

獎項

金、銀、銅獎及優異獎，各得獎座一個及現金書卷
(每位參賽者均可獲發參賽證書)

賽前培訓

2019年11月23日(六)及29日(五) | 16:00 - 18:30
香港專業教育學院(柴灣)教學樓3樓316室 網絡安全中心

截止報名日期

2019年10月31日(四)

網上報名表格

<http://bit.ly/2ZugJy8>



比賽目的：

- 提倡和推動網絡安全教育，提高青少年對網絡安全的興趣，培育21世紀所需要的網絡安全人才。
- 鼓勵及嘉許積極推動網絡安全教育的學校、老師及學生團體。

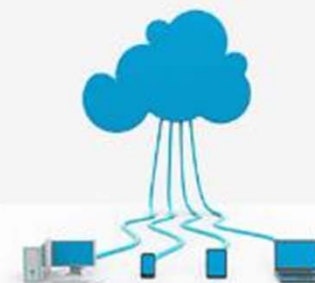
比賽形式：

比賽採用網絡攻防形式進行，參賽者將按照題目指示以不同技巧找出目標電腦系統的保安漏洞，例如：枚舉(Enumeration)、掃描(Scanning)和提權(Gaining Access)

賽前培訓：2020年2月15日 及 2020年2月22日

比賽日期：2020年2月29日(六) 10:00 - 13:00

地點：IVE(柴灣) 教學樓3樓316室 網絡安全中心



共建安全網絡2019

網絡攻擊花樣多 保護數據靠你我

研討會 暨 海報設計比賽頒獎典禮

http://www.cybersecurity.hk/campaign.php

2019年9月20日（星期五）

上午9時至下午5時30分

九龍塘達之路78號
生產力大樓四樓會議廳

詳情及報名方法：
www.cybersecurity.hk/campaign.php
 2788 5617 event@hkcert.org

主辦機構



CyberCERT.HK
網絡安全中心網絡支援中心



協辦機構

香港網絡安全中心
香港網絡安全中心

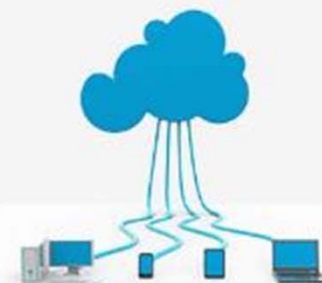
支持機構

教育局
Education Bureau



Hong Kong Customs &
Border Protection
香港海關及邊境保護處

Deloitte





<https://zh.surveymonkey.com/r/GSN32HN>

HKIRC網絡安全研討會 2019: 網站安全技術講座

HKIRC Cybersecurity Seminar 2019:
Web Security Technical Seminar

HKIRC 網絡安全研討會 2019：網站安全技術講座

HKIRC將聯同香港電腦保安事故協調中心 (HKCERT)、香港社會服務聯會(HKCSS)及生產力促進局 (HKPC)的資訊保安專家舉行網絡安全研討會，與參加者分享及交流OWASP十大網路應用系統安全、網絡安全的最新趨勢及最佳實踐。活動詳情如下：

日期：2019年12月13日

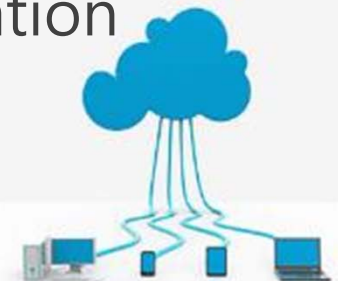
時間：14:30-17:00

地點：香港金鐘道95號統一中心22樓演講廳 A (金鐘港鐵站 D 出口)

語言：廣東話

Standards and Inspection

- Evaluate the delivery and impact of the settings security policy and practice
- Review any reported online safety incidents to inform and improve future areas of teaching, training and policy development
- Regular Vulnerability Assessment and Remediation





Hong Kong Internet
Registration Corporation Limited
香港互聯網註冊管理有限公司




免費學校網站 驗身服務

根據調查顯示，網上每39秒便會有一次黑客攻擊。沒有人可以負擔黑客攻擊，因此保持警惕及加強網站安全是網絡安全重要的一環。作為.hk的一份子，我們明白網絡安全對貴校至關重要。因此，我們現在向持有.hk域名的學校提供**免費的網站安全掃描**。

本項目的目標

- ✓ 協助學校識別網絡安全問題並實施緩解方案
- ✓ 提高學校對網絡安全重要性的安全意識
- ✓ 分享網絡安全的最佳措施



資訊科技保安風險評估 - 學校篇

自第四個資訊科技教育策略推出至今，學校的無線網絡基建已基本完成，以自攜裝置（BYOD）進行電子學習的學校亦逐漸增加。在推行電子學習的同時亦要提高學校對保護學校、學生和家長的資料及資訊科技資產的警覺。根據教育局的《學校資訊保安建議措施》所述，學校有責任採取適當的資訊科技保安措施，以保護學校的資訊科技系統和數據。

資訊科技保安風險評估跟體檢大致相同，藉著定期檢查希望能夠發現一些隱藏的病毒或潛在的風險。透過重複評估與使用資訊科技相關之保安風險的程序，過程中把收集到的數據進行評估和分析，呈報已發現的保安漏洞，並作出評估及提出相關安全性的建議。

資訊科技保安風險評估

在眾多的資訊科技系統中，學校最多使用而又連接到互聯網的便是學校的網站。要使有關網站的數位服務系統和應用系統的安全，良好的設計和開發過程是必須重視的。有見及此，我們顛拍了專業網絡安全管理專家 **UDomain** 為學校進行保安風險評估，以網站弱點性測試及滲透測試*為學校網站分析和測試數位服務的安全性。這樣的安全測試工作，應當作是學校專案中要持續進行的活動，不應當作是最後或有需要時才執行的一項檢查。

網站弱點測試 (Vulnerability Test) –

- 找出網站漏洞
- 進行系統掃描
- 有助系統達致符合保安及審查的標準

免費評估 名額 10 個
(由專業網絡安全管理專家
UDomain 提供)

Further resources

School e-Security Checklist –

- 20 e-security controls

<https://www.tripwire.com/state-of-security/security-data-protection/20-critical-security-controls-control-1-inventory-of-authorized-and-unauthorized-devices/>

- 10 steps to protect your school's network

<http://www.nen.gov.uk/advice/10-steps-to-protect-your-school-s-network-a-guide-for-school-leaders>





香港電腦教育學會
The Hong Kong Association
for Computer Education

Whatsapp Groups :

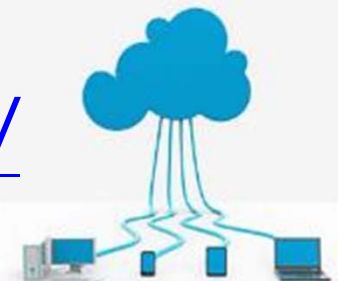
<http://tiny.cc/nekqgz>

WEBSITE :

<https://www.hkace.org.hk/>

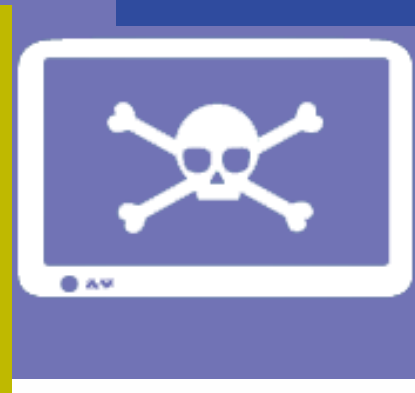
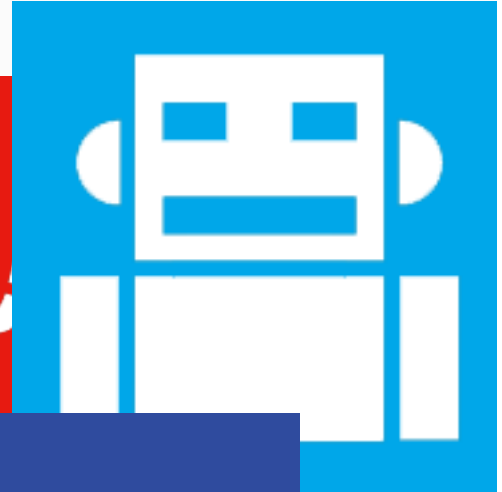
FACEBOOK :

<https://www.facebook.com/hkace.org/>



Common threats to be aware of

- Hacking
- **Malware**
- **Pharming**
- **Phishing**
- Spam
- **Ransomware**
- **Spyware**
- **Trojan Horses**
- **Viruses**
- **Worms**
- **DDoS**
- **Botnets**



Cyber Security Framework

School Case 1: Ransomware

Threat : Ransomware **Critical**

Vulnerability : Email Attachment **Critical**

Asset : Data Files on share drive **Critical**

Impact : Files will be encrypt **Critical**

Likelihood : **Critical**

Risk : Permanent loss of data **Critical**

Control Recommendations :

- (1) Regularly Backup on offline drive
- (2) Update latest patch of OS
- (3) Education (Phishing...)



Cyber Security Framework

School Case 2: DDOS Attack

Threat : DDOS Attack **High**

Vulnerability : Firewall is configured **Low**

Asset : Website **Medium**

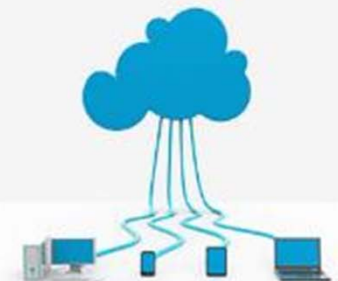
Impact : Website resources will be unavailable.
Medium

Likelihood : **Medium**

Risk : **Medium**

Control Recommendations :

- (1) Monitor the firewall
- (2) update patch of web server.



Cyber Security Framework

School Case 3: Privacy leakage

Threat : Privacy leakage **critical**

Vulnerability : Human Negligence **Critical**

Asset : Student / Staff Privacy Information **Critical**

Impact : School Reputation / legal Consequence **Critical**

Likelihood : **High**

Risk : **Critical**

Control Recommendations :

- (1) Define the privacy information.
- (2) The policy of handling privacy information is necessary. (e.g. password protection, send the document and password in different way.)
- (3) Education / Training



Cyber Security Framework

School Case 4: Files Deleted

Threat : Accidental Files Delete low

Vulnerability : Users can modify on Public drive low

Asset : Public Drive low

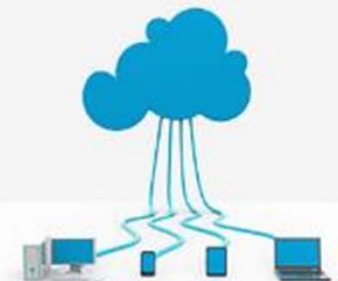
Impact : low

Likelihood : Medium

Risk : recover in few minutes low

Control Recommendations :

- (1) Regular backup with versioning function
- (2) Backup policy listed in teacher's handbook
- (3) Education (Promote the use of cloud drive)



Cyber Security Framework

School Case 5: software license lost

Threat : software license lost medium

Vulnerability : Only have a hard copy Document of License low

Asset : Software (Photoshop, Unity) medium

Impact : Can not be used in license medium

Likelihood : TSS resign Medium

Risk : Buy a new one.... Medium

Control Recommendations :

- (1) Proper Asset register
- (2) Centralize the software license document



Cyber Security Framework

School Case 6: Password leakage

Threat : Password leakage **High**

Vulnerability Human Negligence / System vulnerabilities **Medium**

Asset : Websams, eclass, Window password **medium**

Impact : Depend on system **low- Critical**

Likelihood : **Medium**

Risk : Depend on system **low- Critical**

Control Recommendations :

- (1) Password policy
- (2) Education



Cyber Security Framework

School Case : Conclusion

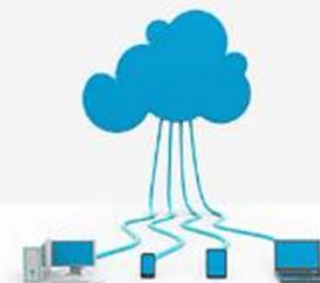
- (1) Identify (辯識)
- (2) Protect (保護)
- (3) Detect (偵測)
- (4) Response (回應)
- (5) Recover (復原)



Cyber Security Framework

(1) Identify (辨識)

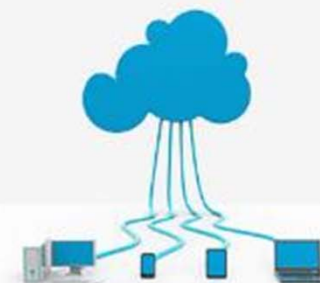
- Asset Management 資產管理
- Risk Assessment 風險評估
- Risk Management Strategy 風險管理策略
- Governance 治理
- Business Environment 營運環境



Cyber Security Framework

(2) Protect (保護)

- Access Control 存取控制
- Awareness and Training 意識與教育訓練
- Data Security 資料安全
- Maintenance 維護
- Protective Technology 防護技術
- Info Protection and Procedures 資訊保護與程序



Cyber Security Framework

(3) Detect (偵測)

- Security Continuous Monitoring
持續性的安全監測
- Anomalies and Events 異常事件
- Detection Processes 檢測流程



Cyber Security Framework

(4) Respond 回應

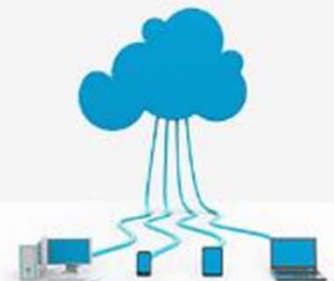
- Response Planning 回應計劃
- Mitigation 緩解
- Analysis 分析



Cyber Security Framework

(5) Recover (復原)

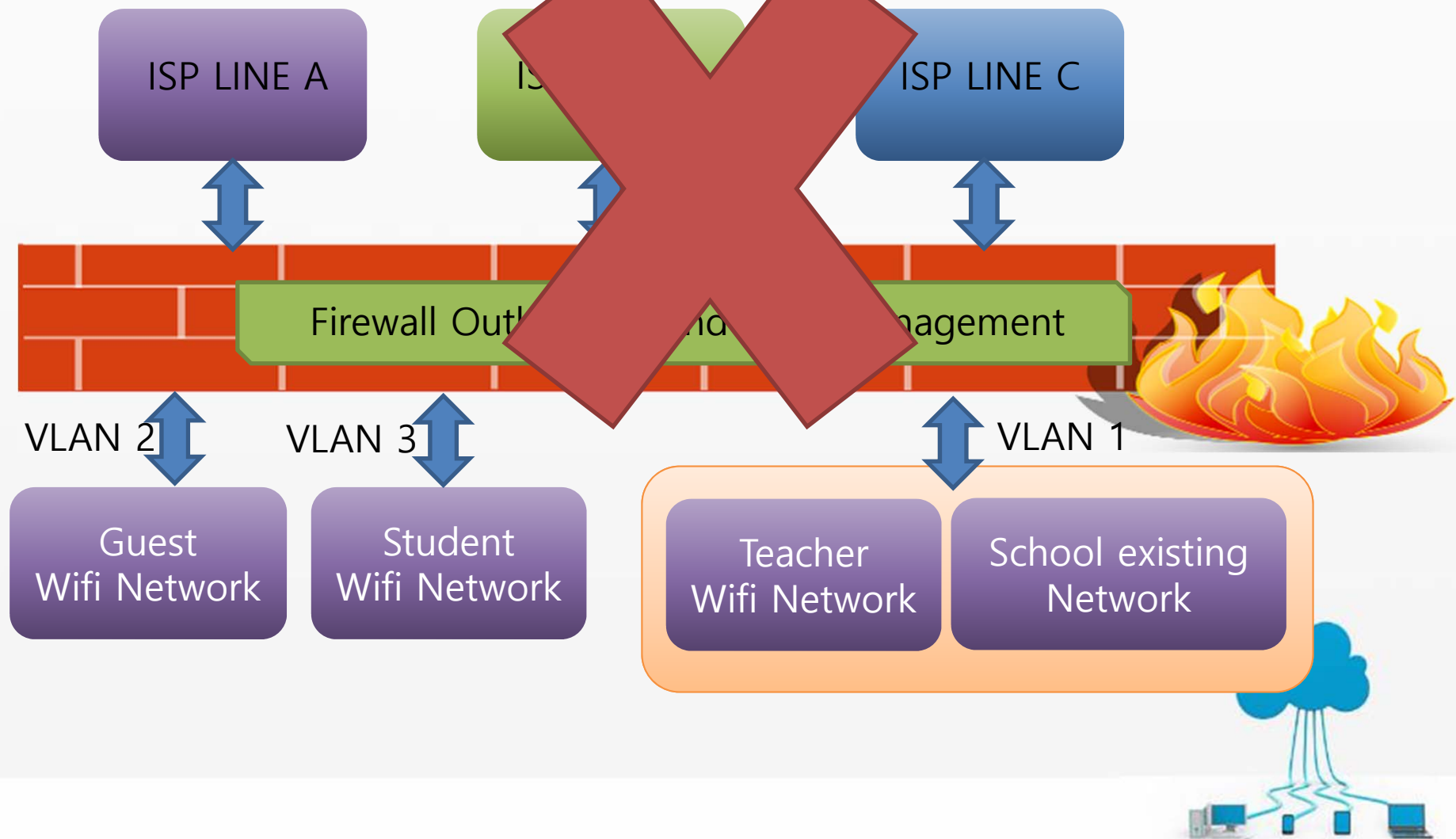
- Recovery Planning (復原計劃)
- Communications (溝通)
- Improvements (改善)



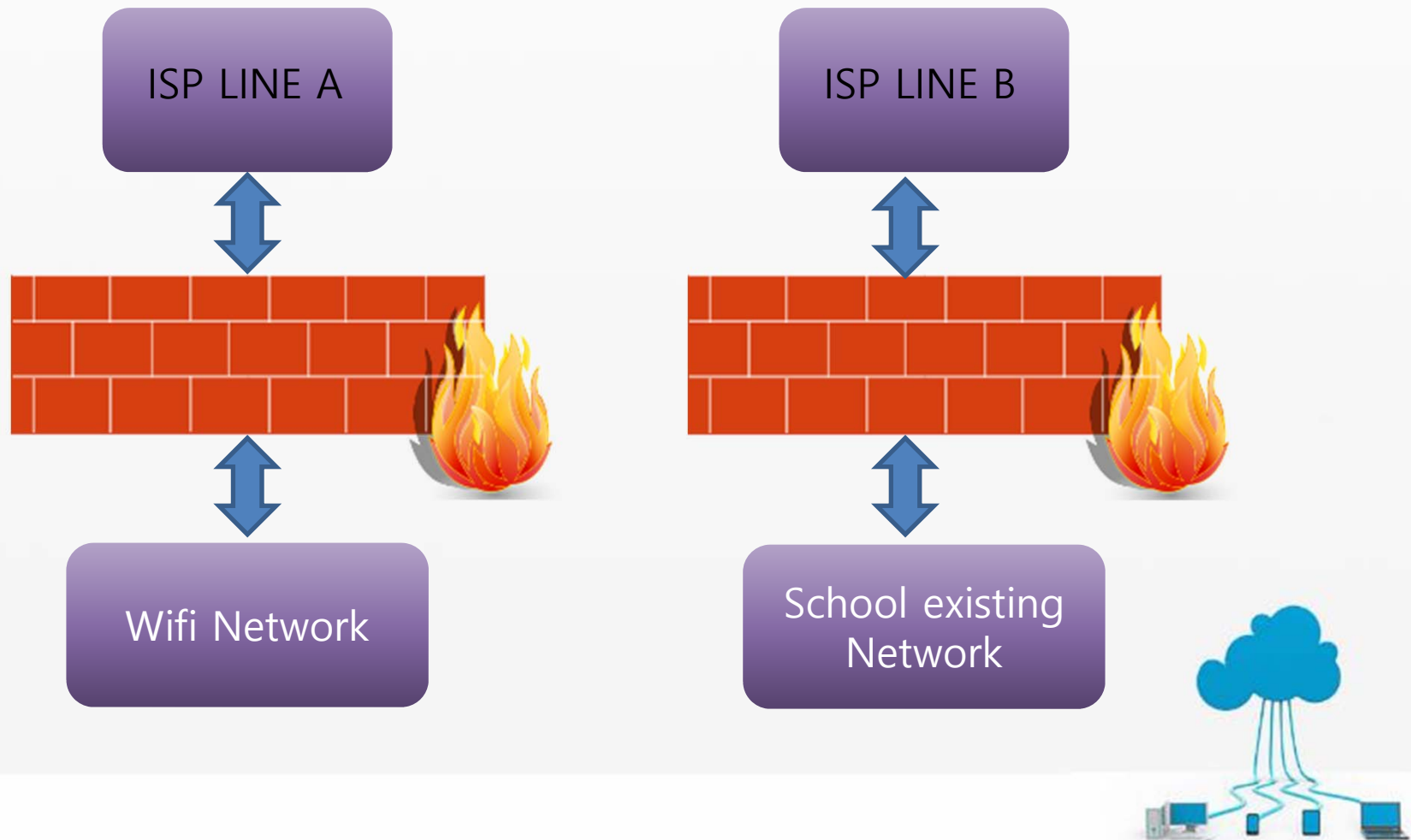
THANK YOU



Wi-Fi Network and Existing School Network (Model 1)



Wi-Fi Network and Existing School Network (Model 2)



Wi-Fi Network and Existing School Network (Model 3)

