

# 香港中、小學資訊保安調查報告

---

主辦團體:



專業資訊保安協會



香港電腦教育學會



資訊科技教育領袖協會

# 香港中、小學資訊保安調查報告

## 第一節：背景、目的及方法

---



資訊科技教育領袖協會主席

趙錦華先生講解

## 香港中、小學資訊保安調查報告

---

### 背景:



政府於98年開始在本港所有中、小學推行五年 (1998/99-2002/03) 資訊科技教育計畫。

## 香港中、小學資訊保安調查報告

---

### 背景:



現在，所有學校大致上已完成有關基建項目及已接上互聯網。

## 香港中、小學資訊保安調查報告

---

### 調查目的:

1. 學校資訊保安現況?
2. 除教統局指定的基本設施外，學校還增加了什麼資訊設施?



## 香港中、小學資訊保安調查報告

---

### 調查目的:

3. 學校執行資訊保安時所遇到的困難?



## 香港中、小學資訊保安調查報告

---

### 調查目的:

4. 提供適當的建議和跟進，使現存資訊保安有所改善。



## 香港中、小學資訊保安調查報告

---

### 方法:

1. 使用問卷調查方式。
2. 於2002年6月寄出問卷至各中、小學校共1200份。
3. 於2002年7月尾回收問卷共181份，回收率15.1%。



# 香港中、小學資訊保安調查報告

## 第二節：分析及結果

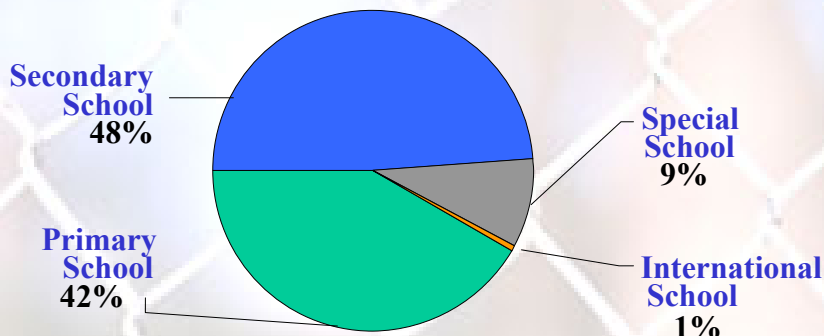


專業資訊保安協會代表

連奕茂先生講解

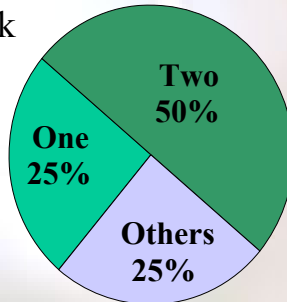
## Response & Distribution

- Total 181 questionnaires received (15.1%)
  - Response Distribution agrees with actual distribution



## Work Load of Technical Staff

- About 100 sets of computers (desktop & notebook) were to be managed by every school
- Number of full time technical staff to support the school network



## Common IT Services in School

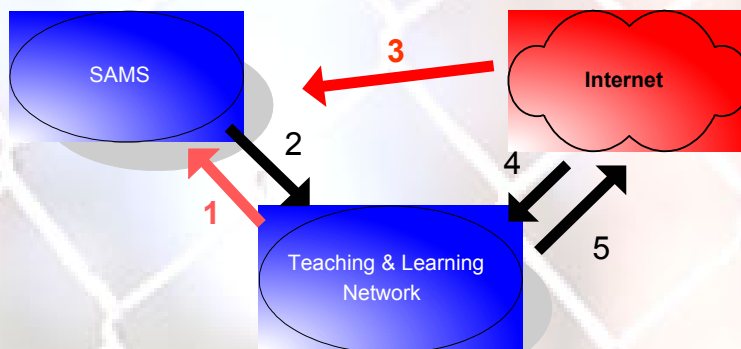
- Common IT Services in School
  - Web servers (62%), FTP servers (49%), database servers (42%), mail servers (30%)
- Not included in the core IT services
- Not sufficient configuration guidelines issued by ED
- **High Risk: Internet servers are common hacking target**

## Wireless LANs

- 1/3 of schools – already installed in school
- 1/3 of schools – planned to implement before 2004
- The rest –no plan to implement by 2002 June
- WLAN again not included in core IT services
- **High Risk: open internal network to next door attackers**

## SAMS Network

- 21% of schools had incoming traffic to the SAMS network from the ITED (**Arrow 1 – High Risk**)
- 16% of schools had incoming traffic to the SAMS network from the Internet (**Arrow 3 – Very High Risk**)



## Remote Access

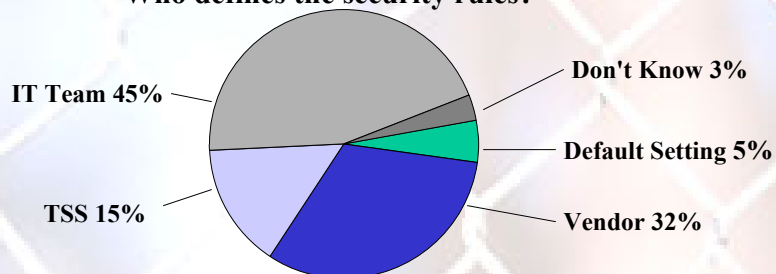
- 37% schools – provide remote access to staff & students
  - **Only 18% – VPN in remote access**
  - 15% – dialup without a call back
  - 63% – using FTP
  - 26% – using Telnet
  - 30% - using Remote NT Logon
- **VERY HIGH RISK – Insecure Remote Access to the heart of school network where sensitive data reside.**

## Firewall

Note: Firewall is a basic defense on the perimeter against Internet

- 50% of schools – No Firewall implemented

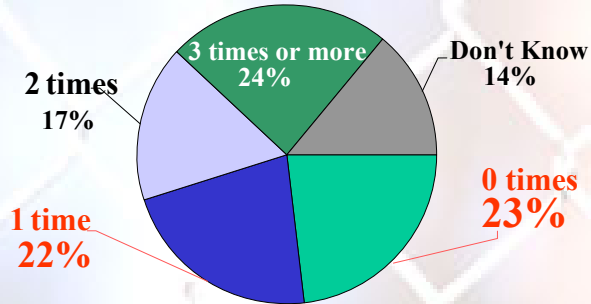
Who defines the security rules?



- **Only 30% of schools have properly configured firewall**

## Firewall

How often are these rules reviewed in the past 12 months ?



- **Now: 23% WITHOUT firewall rules review**

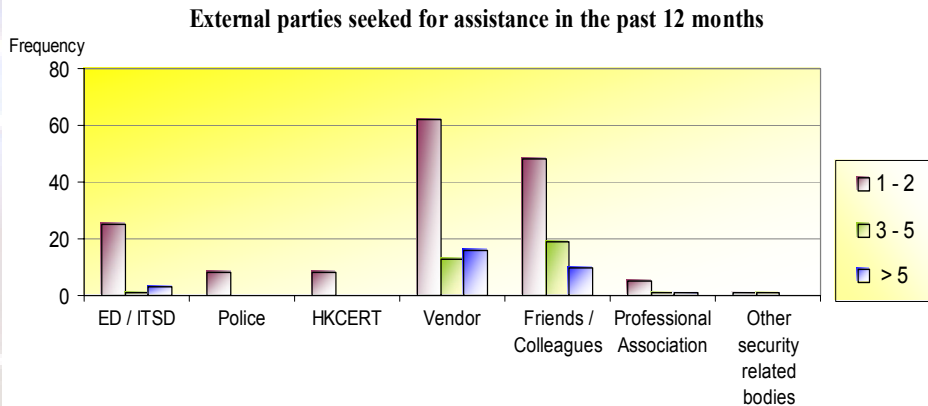
Good Practice: rules reviewed when there is a change or 2 time per year.

## Backup Practice

- 93% schools – data backup practice
- 14% schools – performed the periodical recovery test of backup data
- Purpose of backup:  
Isn't it for recovery when necessary?

## Incident Handling

Ever sought assistance from the following **external parties** to deal with security incidents in your school in the past 12 months?



- **Schools do not know proper channel to report Incident**

## Security Policy

- 64% schools – no written security policy
- Security Policy
  - It defines the direction of security, the roles and responsibilities of staff and the requirements to comply with.
  - **No policy → these definitions are not clear**

## Summary (1)

- ED is out of sync. of some common IT services in school and has not issued sufficient guidelines
- Web, FTP, Wireless LAN and Remote Access are very common IT services in schools. Unsecured WLAN & Remote Access are especially regarded as **HIGH RISK**.
- Connection from the Internet to SAMS – **VERY HIGH RISK**

## Summary (2)

- Improper firewall management (update patch, review security rules..) – **HIGH RISK**
- Schools – don't know the proper channel to report Incident
- Schools – not enough knowledge to handle and aware IT security

# 香港中、小學資訊保安調查報告

---

## 第三節：建議及跟進



香港電腦教育學會主席

伍學齡先生講解

### 取捨的考慮

- 教育需要與保安需要
- 校本決策與中央指引



## 建議一：學校應分等級處理不同的保安需要

- 學校網絡中儲存了不少數據，如試卷、個人資料、考試成績、學生作業、老師教材等，應按數據的**敏感度分等級**：
- 權衡服務的**需要程度**及**保安考慮**分成等級：如必需、支援性、增潤、可有可無
- 把學校網絡按其敏感度及保安需要**分成不同區域**

## 建議二：學校應有成文的資訊保安措施

- 定期對系統進行保安**檢查**
- 防病毒軟件、Firewall等均需定期**更新**其中的關鍵數據，始能發揮防禦的作用
- 清晰界定有關人員的**權責**及工作程序
- 明確出事時的**處理程序**
- 建議由教統局制定一份標準樣本，學校再按實際情況加以增刪

### 建議三：學校宜把部份易受外界入侵的服務交由供應商負責

- 例如網頁及電郵服務等
- 減輕學校處理保安問題的壓力
- 可借助供應商的專門知識處理保安問題
- 學校可聯合向供應商爭取較佳的條款，例如網頁過濾、阻止垃圾電郵等
- 若寧可自行在校內設立有關服務，學校有關人員宜清楚瞭解其利弊，並有適當的保安措施，方可進行

### 建議四：教統局應就教育科技的迅速發展作出敏捷的反應

- 學校不時會對新科技感到興趣，並積極引進以改善教學果效
- 教統局宜及時找專家對新科技進行評估，並對潛在的危險作出警告及指引

## 建議五：定期由獨立機構 評核學校的資訊保安水平

- 讓教統局及時瞭解問題所在及作出補救措施
- 一定程度發揮監管的作用，學校可安心把日常保安措施交由技術支援人員負責，減輕負責老師的工作及心理壓力

## 建議六：普及資訊保安知識 及加強有關人員培訓

- 校長、資訊科技小組、一般老師、技術支援人員均應對這問題有一定的認識
- 學校應有受過相當訓練的專人負責資訊保安，並賦予其適當的權力
- 明確發生問題時的報告及處理機制，善用現有的相關資源

## 調查後的跟進工作

- 合辦一系列培訓課程
- AiTLE網頁刊登資訊保安常見問題及解答
- PISA制作自我檢查套件
- 向學校推介「香港電腦保安事故協調中心」(HKCERT)的服務

## 香港中、小學資訊保安調查報告

---

### 第四節：答問時間



三個團體代表