

# ***Report of Information Security Survey on Education Sector***

January 2003

## *Organizers of the Survey*

Professional Information Security Association (專業資訊保安協會)

Association of I.T. Leaders in Education (資訊科技教育領袖協會)

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



## **Aims and Motives**

In his first Policy Address in 1997, Mr. TUNG Chee Hwa, the Chief Executive of HK SAR, proposed to make Hong Kong “a leader, not a follower, in the information world of tomorrow”. The Education and Manpower Bureau therefore in 1998 issued the document “Information Technology for Learning in a New Era: Five-Year Strategy 1998/1999 to 2002/2003” as the blueprint for the development of IT in Education (ITEd). Subsequently, a series of ITEd initiatives were carried out. Under these ITEd initiatives, schools were provisioned with various computers and networking systems. Most computers in schools were Internet-ready. After four years of implementation, the building of infrastructures in local schools is coming to completion. Some schools went one step further by adding extra facilities to their existing systems. Non-standard services such as hosting web servers in schools are quite common. What is the current situation with regard to hardware and networking systems within schools? Are the school network systems strong and secure enough to resist internal & external hackers’ attack? These are the main points we wish to find out in the current study. With these preliminary aims in mind, three organizations, the Professional Information Security Association (PISA), the Association of I.T. Leaders in Education (AiTLE) and the Hong Kong Association for Computer Education (HKACE) jointly carried out a survey project (**Appendix A**) on this issue. A survey in the form of a questionnaire was carried out in all primary and secondary schools in Hong Kong in June 2002. Based on the data collected in the questionnaire survey, this report was written.

## **Method of Survey**

Questionnaires were sent to the headmaster/principal of 1200 Primary and Secondary schools in Hong Kong by mail in June 2002. The number of questionnaires sent out was about 1200. Schools were asked to answer the questions and mail back the questionnaires by the end of July 2002.

## **Summary of Findings**

A total of 181 questionnaires were received. Among them, there were 75 primary schools, 88 secondary schools, 16 special schools and 1 international school. The data were analyzed. Details of the response to each question can be found in **Appendix B**. Here is a summary of the findings.

1. About 100 sets of computers (desktop & notebook) were to be managed by every school. About 25% of the schools replied that they had only one full time technical staff, and about 50% of the schools replied that they had two full time technical staff to support the school network.
2. About 50% of the schools replied that they did not have firewall protection to their school network from the Internet.

3. From the school replies, Web, FTP, database and mail servers were found to be the common services. As a point of note, such services were not supposed to be the core IT services in schools. In addition, the proper configurations of these infrastructure components were not highlighted and were not even mentioned in the current guidelines issued by the Education and Manpower Bureau, EMB (formerly by the Education Department, ED).
4. Wireless LANs (WLANs) were installed in about one-third of the schools replied. In the coming two years, another one-third of the schools replied planned to implement WLAN. WLAN, if only configured as factory defaults, would be very insecure and would create a backdoor for the school internal network. However, it was a common practice that most administrators of WLAN only adopted the factory defaults in their network security. For the firewall security rules, only 24% of the schools replied that they were defined by the school's IT Team and had them reviewed regularly.
5. According to the ED / EMB Guideline, the SAMS network, which contained the personal information of students and staff, as well as the important information of the schools, should be prohibited from the access of the ITED network (the main network for teachers and students) and the Internet. However, the survey showed that about 21% of schools replied that they had incoming traffic to the SAMS network from the ITED network and 16% had incoming traffic from the Internet too. There had been a great exposure to information leakage and hacking.
6. 93% schools replied that they had data backup practice, but only 14% of them had performed the periodical recovery test of the backup data.
7. There was a general phenomenon that schools lacked information security management know-how. Though they had got the budget to implement the security infrastructure, they did not know how to manage and to maintain them properly, thus rendering the question of investment cost-effectiveness of the fund.

## **Basic Concept on Information Security**

### ***Confidentiality, Integrity, Availability***

Confidentiality, integrity, and availability represent three fundamental principles of information security. All of the information security controls, threats, vulnerability, etc. are subject to these three principles.

- Confidentiality aims to prevent intentional or unintentional unauthorized disclosure of information.
- Integrity aims to ensure that unauthorized modifications are not made to data, and if they are made, such modifications can be detected.
- Availability aims to make sure the reliable and timely access to data, resources, or services by the authorized personnel.

### ***Assets, Threats, Risk***

Many risk analysis methodologies start with identification and classification of the assets which need protection because they are vulnerable to threats.

- Typical information assets include information and data, services, hardware and software, etc.
- Threats will cause loss or damage to the assets
- Risk is the potential that a given threat will exploit vulnerabilities of an asset to cause loss or damage to the asset

### ***Security Controls***

Security Controls are the policies, practices, and organizational structure to reduce the undesirable effects imposed by security threats on assets.

### **Guiding Principles**

The major objectives of a school are to provide quality education and fruitful learning experiences to students. The IT infrastructure of a school helps to enhance the students' learning experiences and provide a platform for cost-effective school administration. There are several characteristics of the school IT infrastructure when considering the security issues:

- Most of the expertise in schools is centered around education, it is not encouraged to put too much technical burden on teaching staff. On the other hand, the education business does not generate direct revenue. Given the heavy workload of teachers, cost-effectiveness will refer to provide more room for teachers to facilitate students' learning, and to transfer those technical workload to technical expertise.
- Disparity in the philosophy of information security is found in school situations. Many teachers / schools try to expand the infrastructure and to provide more non-standard services. The purpose is to provide more opportunities for the students to explore the information world and to support the diverse learning and teaching activities in schools as a result of curriculum reform. However, in information security point of view, most of these services are of higher risk and therefore not recommended. It is quite difficult to give a suggestion applicable to all primary and secondary schools in Hong Kong. Schools have to consider carefully the gain in educational value and the risk in security, and try to minimize the risk if the services are really necessary.

It would be quite difficult and time-consuming for every school to design its own information security strategy. Although each school may have its own need and school-based development, all the schools share more or less homogeneous IT infrastructure and similar problems. Furthermore, all Hong Kong schools are adopting management guidelines from ED / EMB. Thus there arises a need to have ED / EMB to play a more active role to develop guidelines on those "non-standard" services. Schools may then make further modifications if and only if they have the appropriate expertise.

## Recommendations

### 1. Adopt a simple IT security framework in schools

Other than TSS staff, the manpower of full-time-equivalent technical staff to support the IT infrastructure in most schools is limited. The following chart shows the survey result on percentage of number of extra-manpower of full-time-equivalent technical staff: -

Numbers of full-time-equivalent technical staff (other than TSS)	Percentage
0	26%
0.5	7%
1	53%
1.5	3%
2	11%

Such a small team of TSS and technical staff barely suffice to handle a wide spectrum of security tasks and issues in a complicated IT environment. Schools should adopt a simple IT security framework that is manageable by the IT team.

#### 1.1 Security Framework

We propose a simple framework that aims to protect two types of assets: information and IT services. It includes the following components:

##### (a) *Classifying information*

Information should be classified so that appropriate security controls are applied to ensure their confidentiality, integrity, and availability. For example, the following classification terms are commonly used in private sector:

- Public

Unclassified information, e.g. school announcement. Such type of information should be protected from unauthorized modification.

- Sensitive

Information that should be protected from loss of confidentiality and/or integrity, e.g. student assignments.

- Private

Information that is personal in nature, e.g. student particulars.

- Confidential

Very sensitive information, e.g. examination paper.

We shall adopt this classification system in the subsequent discussion.

**(b) Classifying IT services**

In a school environment, IT services should directly or indirectly facilitate teaching and learning functions. It is recommended to classify these services in order to balance between the educational need and the possible security risk. Compared with information, security controls on these IT services is more focused on availability.

- Core IT services

These services are directly related to teaching and learning functions, e.g. Internet access for web-based learning, internal real-time chatting, internal website, internal email, multi-media learning materials accessible in school, etc.

- Supporting IT services

These refer to those services that are not directly related to teaching and learning but are mainly used to produce the teaching and learning deliverables or materials, or record the corresponding results. For example, a database used to record the examination results. It is noted that private and confidential information are normally handled by supporting IT services.

- Add-on IT services

These services are considered neither core nor supporting to the teaching and learning functions. However, they provide some added features or values which enhance the core or supporting IT services. The values of these services may vary from school to school and are very much depended on the learning and teaching methods the school adopts. Sometimes these features or values are indispensable. For example, an Internet website, Internet email, etc.

- Optional IT services

These services may have certain value to the teaching and learning functions. However, the associated risks may be disproportionately high or appropriate security controls are difficult to implement, and there may be some alternatives that are more secure. For example, ICQ, Telnet services, etc.

**(c) Defining IT Security zones**

The figure in Q19 in the questionnaire depicts the various logical security zones for schools. Different zones require different security levels.

- SAMS

It was originally isolated from other zones. For better resources sharing and utilization, users of SAMS might be allowed access to the public Internet and the Teaching and Learning School Network. This is the most restricted zone and the security level is high.

- ITED  
All core services are located in this zone. The security level in this zone is medium.
- Internet  
Practically this zone lies outside the Security perimeter of schools. Schools have no control at all on this zone. The security level in this zone is low.

**(d) Classifying threats**

We adopt a simple approach to classify threats in our discussion context:

- Internal threats  
These are threats originated from internal users in a security zone.
- External threats  
These are threats that come from users outside a security zone. External threats include those fired by internal malicious programs, e.g. Trojan Horse implanted by external attackers.

## 1.2 Suggested Measures

With this IT Security framework, the following are proposed in order to make the security controls simple and effective. The bottom line is to minimize the interaction among the security zones and the security controls at the zone perimeter play major roles to protect the internal zone, namely, SAMS and ITED.

- (a) Only access initiated from higher security zone to lower security zone is allowed but not vice versa. Moreover, the access should be on a necessity basis. Below is an example:
- SAMS & ITED to Internet: http, https
  - SAMS & ITED to pre-assigned servers: ftp, pop3, smtp
- (b) The access from other directions should be strictly prohibited. Any exception to this policy must be scrutinized with respect to the needs and the risks by the school management in advance. One possible exception is Virtual Private Network (VPN). Only 9% of the schools replied implements VPN at the moment.
- (c) At the moment, 21% of the schools replied allow access to SAMS from ITED and 16% from the Internet. 40% of schools replied allow access to ITED from the Internet. Moreover, the survey found that quite a number of these schools do not have firewall in place to protect the internal network. Here's the breakdown:
- Internet to SAMS only: 3%
  - Internet to ITED only: 12%

- Internet to both SAMS & ITED: 5%

We strongly recommend to eliminate such access from the Internet to the internal network and to set up the firewall immediately.

- (d) SAMS is the most restricted and secure zone. Threats from internal users should be low in this zone. We recommend to store confidential and private information and to host supporting IT services in this zone.
- (e) ITED is a less secure zone. Threats from internal users should be low in primary schools while higher in secondary schools in view of the levels of IT competency of the students. In this zone, core IT services for teaching and learning purposes should be set up whenever possible, e.g. real time chatting, websites, multimedia, etc. This is to ensure that the students can explore the information world freely. To minimize the risks, however, these IT services should be confined within ITED. Sensitive information, e.g. student assignments, may be stored in this zone.
- (f) Add-on IT services (e.g. Internet website, Internet mail) and public information (e.g. school brochure) should be located outside the perimeters of SAMS and ITED. Either a Demilitarized Zone (DMZ) or a Service Provider premise can serve this purpose. However, we recommend the add-on IT services to be hosted by external Service Providers. The purposes are:
  - To concentrate the limited resources of the IT team to the core and supporting IT services without bothering them with the add-on IT services
  - To use the expertise from external Service Provider to handle the wide spectrum of security threats originated from the Internet
- (g) Optional IT services are those accompanied with disproportionately high risks or have no simple security controls. Before implementing any optional IT services, school management should carefully evaluate the benefits against the risks. Or the school should only consider implementing these services after simple and satisfactory security controls are available in the market.

## 2. Outsourcing Add-on IT services to Service Providers

To facilitate schools to outsource add-on IT services to external Service Providers, we recommend the following measures:

- (a) Different schools should join force to bargain for better terms and conditions with the external Service Providers.
- (b) *A well-defined Service Level Agreement (SLA) is the prime prerequisite for outsourcing to be successful.* We suggest ED / EMB to issue a SLA template for schools. Schools should use this

template as a baseline to negotiate with the external Service Providers.

- (c) The SLA must include terms on security and privacy. The external Service Providers must have well developed security and privacy policies and processes in place. These policies and processes should be subjected to external auditing regularly and schools should have the rights to view and comment on the audit report.
- (d) *Releasing School IT Team from unnecessary burden is one of the directions.* If the school IT team (1) has better guidelines to follow; (2) has some secure infrastructure outsourced; and (3) has a standard vulnerability assessment and proposal for enhancement, they can focus on providing IT services for the school and not on chasing after skill levels that an average IT team could hardly attain.

### 3. ED / EMB to take charge of the ever-changing technology

The technological change is fast for schools to keep up with. If the ED / EMB is not responsive to the ever-changing technology trend and provides guidance to schools promptly, the burdens will be eventually laid on the IT Teams of schools, where their primary duty is to support the use of IT in teaching and learning. School IT Teams are facing a security challenge that is beyond their capability to cope with. The school is composed of a very large population of users including, students, administration staff, teachers, parents, and alumni. The IT team has to take care of service requirements of a large user population which is continuously growing in size and complexity.

Here is a list of outpaced technologies in schools

#### 3.1 Non-core IT services like Web, FTP, and Database Server

In Q15, services regarded as “non-standard” or “non-core” such as Web Server (62%), FTP Server (49%) and Database Server (42%) are widely used in schools now. In the coming 2 years, the adoption ratio in Web Server (89%), FTP Server (71%) and Database Server (66%) are even higher. The IT team now could just marginally manage such IT matters. Security seems to be an unreachable goal in terms of resources and technical know-how.

#### 3.2 Wireless LAN

Wireless network has been widely implemented in school environment. ED / EMB should provide appropriate guidelines and recommendations for implementing wireless network in schools.

In Q14, it was noted that, 33% of school replied have already installed Wireless LAN and in the coming 2 years, another 33% of schools are planning to have it installed. WLAN, if only configured as factory defaults, is very insecure and will create a backdoor to the school internal network. However, it is a common practice that most administrators of WLAN only adopt the factory defaults in their network securities.

Wireless network has many benefits in the school environment. Therefore, we anticipate that many schools will install Wireless LAN in the future regardless of the high security risk of this new technology. Thus, the following security measures are proposed to minimize the risk and protect the Information:

- Do not set up Wireless network in SAMS zone
- Wi-Fi Alliance ([www.weca.net](http://www.weca.net)) has announced Wi-Fi Protected Access (WPA) on October 31, 2002. WPA aims to fix some critical security vulnerabilities in Wireless LAN products. Wi-Fi Alliance will start to certify WPA products in February 2003. Schools should delay Wireless LAN equipment procurement until then or only procure WPA ready products at the moment.

### 3.3 A Remote Access Control Security Policy is definitely required

In Q16, it was noted that 37% of the schools replied (66 out of 178) provided remote access to their staff or students. In Q17, the survey showed that only 12 out of the 49 schools replied (i.e. 24%) used VPN in remote access. Many of them (27 out of 49) just use simple dial-up without a call-back. The security level of the remote access control is very low.

In Q17, when looking at the accessed service from Remote Access, most of them used FTP (42 out of 67), probably for website maintenance. There were also a substantial number of school replied using Telnet (17 out of 67) and Remote NT Logon (20 out of 67). These two services could allow logged-in users to perform privileged activities like changing security profiles, modifying or deleting system files. Coupled with the lax remote access security control, it implied a high risk of these vulnerabilities that can be exploited by hackers to break in the school system and compromise the confidentiality, integrity and the availability of the infrastructure.

The criteria for justifying the need for remote access in school environment, the security implications and the management procedure for remote access in schools had not been fully understood. It should be put at a top priority of the enhancement of the proposed IT security policy to be drafted by ED/ EMB

With the simple security framework proposed in the above recommendation (recommendation point 1), the need for remote access by teaching staffs or students should be at minimal or prohibited. A dedicated FTP site standing outside the SAMS and ITED perimeters should be sufficient to meet the upload requirements of teaching staffs and students. Security controls to such FTP site are simple, effective, and proven.

Opening up remote access to vendors is not advisable and must be evaluated carefully. If it is necessary, appropriate security measures must be in place, including but not limited to access logging, activity logging, on-demand access, etc.

#### 4. Developing a General Security Policy for Schools

According to the survey results, 64% of the schools replied do not have any written security policy. The ED / EMB should setup and highlight guidelines on security policy for schools to follow. Such guidelines might include, for example, strong password and account sharing policy. IT teams in school should formulate their own security policy based on these guidelines.

In Q25, more than 64% of the schools replied have no security policy and in Q26, only half of the schools replied have security management measures.

*From the above data, it indicates that there has a wide gap between available policy and the service requirements of schools nowadays. Security Policy regarding popular services used in schools like Remote Access, Web server, FTP server and Database server are absent. This is potentially a serious security loophole. Policy must be developed for the whole education sector to minimize the security loopholes and make the security risks manageable.*

The following is an example of Security Policy Guideline in School: -

1. *Classification of Information*
  - *Public*
  - *Sensitive*
  - *Private*
  - *Confidential*
2. *Password Policy*
  - *Who can own the administrator account?*
  - *How often are the users required to change their passwords?*
  - *Any minimum requirement about the password length?*
3. *Backup Policy*
4. ..
5. ..

#### 5. Introducing an Outsourced Security Assessment

A security assessment could be conducted annually so as to get the overview of security level of school. This assessment should be carried out by expertise other than the TSS or the IT Team, therefore outsourced service is recommended. The ED / EMB can use this information to plan the overall security policy and school can also use this assessment result to design the information security policy within school.

In Q26, about 50% of the schools replied have no security management measures and another 20% were not updated. This indicates that the security awareness is far from enough among schools.

*ED / EMB should introduce Security Vulnerability Assessment to provide control information to improve ongoing security of schools.* The issues of non-compliance to guidelines of ED / EMB (e.g. in Q19, significant number of the schools replied made SAMS network accessible from ITED network or from Internet.) This non-compliance to the guidelines of ED / EMB and the modifications on school IT services could never be tracked if there is no review and audit. A standard review process across schools provided by ED / EMB could improve the compliance and allow ED / EMB to arrange remedial measures to these threats. It also helps schools to focus and prioritize on critical security problems.

## **6. Strengthen the Incident Response Capabilities of Schools**

ED / EMB, education sector and HKCERT/CC can have more collaboration to raise the awareness of schools towards information security and timely response to security incidents. HKCERT/CC needs to promote herself more in the education sector so that schools can benefit from the free security early warning service and the incident response services provided by HKCERT. Public seminars could also promote the security awareness of schools.

In Q21, it was noted that most of the schools replied sought assistance from vendors (52%) and friends (47%), while the percentage of seeking help from public service like HKCERT/CC (4.7%) and HK Police Force (4.7%) was comparatively low. Security threats usually need a timely response. Seek assistance from vendors because the vendors were usually the most familiar party on their technical configuration. Seeking assistance from friends merely indicated that they might have no known source for help but to find a last resort from friends. The figure showed that this situation happened to about half of the school replied. It indicates that the free security advisory services of HKCERT/CC is not within their handful touch or they do not know the availability of such a service.

## **7. Allocate more resources on education and awareness training**

Besides simplifying the school IT infrastructure and outsourcing non-core IT services, the ED / EMB should allocate resources to promote the awareness of information security in schools.

From the result of Q27, the greatest obstacles for schools to address the information security issues are:

- Budget (69%),
- Technical Competence (52%),
- Human resources (43%) and
- Awareness of employee (37%).

From the result of Q28, the most needed solution to improve the current situation are :

Increase budget (68%)

Provide more information security training to IT team (64%)

Provide more information security awareness training to employee (58%)

ED issues more clear technical and management guideline (57%)

Perform periodic security assessment to school system and network (43%)

As from Question 12, only 8% of the school replied considered their school IT infrastructure as secure or highly secure. A clear direction from ED / EMB and commitment of resources is required to improve the information security of schools.

### **Conclusion:**

1. The complexity of school network implementation in various schools at present has gone far beyond the initial proposal from the ED / EMB. On the other hand, all school IT Coordinators (ITC) are teachers who received professional training on the science of teaching and learning, but not on technical support. It is neither their duty nor their strength to maintain the complexity of security of school network.
2. The roles of the ITC specified under the Information Technology Co-ordinator Scheme (ITC) does not call for making decision on security policies and security controls enforcement in their schools. So there is a need to develop a clear guideline on who, the ITC or the Principal or both, to take up such important and decision role.
3. According to the ITed documents, "IT Security In Schools" and "Technical Guidelines for School LAN Administration under the IT in Education project – Summary of the guideline", guidelines were given based on the assumptions "...to suit the Basic IT security knowledge and concepts which are applicable to the school environment..." and "...on the assumption that hardware and software items built under the standard provision of bulk tender for ED (Tender Ref.pt/83/98)...". In reality, schools have been diverted from these limitations and had built many extra web and internet services to suit their own needs. The current guidelines have proved to be outdated and inadequate to serve the current needs.
4. So far there was not a clear school security policy within the schools. Some schools placed their trust on the TSS for security controls, some on the vendors.

5. From the result of the survey, many of the schools replied were quite aware of the importance of Information Security, but often the IT Teams are facing problems in technical competency and lack of clear policy. We proposed an option for schools to outsource part of the security services to external expertise in a bi-annual contract. ED / EMB should help to make a bulk bargain and issues guidelines on selection of external suppliers.
6. There is a need for ED / EMB to organize more Information Security awareness programs to schools. More in-depth trainings to school IT Team are also worthy.

**We (PISA, AiTLE, HKACE) have proposed and planned to hold the following activities to support the implementation of information security in schools:**

- (a) Maintenance of an IT and Security FAQ forum for sharing of information and experiences among school IT teams.
- (b) Seminars and guidelines on Security Self-Assessment for schools
- (c) Seminars and guidelines on Perimeter Defense (firewall, etc.) for schools
- (d) Seminars and guidelines on System hardening for school internet services
- (e) Workshops and guidelines on Wireless LAN security
- (f) Seminars on other hot topics found in the survey.

**Appendix A*****Information Security Survey on Education Sector Project Team***

<i>Name</i>	<i>Organization</i>
Mr. Ng Hok Ling	Hong Kong Association for Computer Education
Mr. Yu Chi Wing	Hong Kong Association for Computer Education
Mr. Matthew Lai Man Yau	Hong Kong Association for Computer Education / Association of I.T. Leaders in Education
Mr. Chiu Kam Wa	Association of I.T. Leaders in Education
Mr. Albert Wong Kin Wai	Association of I.T. Leaders in Education
Mr. Reeve Lin	Professional Information Security Association
Mr. Jim Shek	Professional Information Security Association
Mr. Denis Li	Professional Information Security Association
Mr. Peter Cheung	Professional Information Security Association
Mr. S.C. Leung	Professional Information Security Association

## **Appendix B**

### ***Questionnaire and results***

1. What is your post in school?
 

[1] Principal / Vice Principal    [150] IT Team Leader / Coordinator    [24] IT Team Member

[ ] Others : Clerk, ITA, CM Teacher, APSM, TSS
2. What is the type of your school?
 

[75] Primary                    [88] Secondary                    [16] Special                    [1] Other : International
3. What is your school funding source?
 

[15] Government    [153] Subsidized                    [5] DSS                    [4] Private
4. How many students are there in your school?
 

[37] < 500                    [68] 500-1000                    [70] 1000 –1500                    [3] Above 1500
5. How many desktop computers are there in your school?
 

[35] < 50                    [54] 50-100                    [63] 100 –200                    [27] Above 200
6. How many notebook computers are there in your school
 

[89] 20 or less    [19] 21-40                    [21] 41-60                    [30] 61-80                    [20] More than 90
7. Other than TSS staff, how many technical staff members (full-time-equivalent) are supporting the IT infrastructure?
 

[46] 0.0                    [12] 0.5                    [95] 1.0                    [5] 1.5                    [20] 2.0
8. Account sharing
 

(a) Student:

[70] Personal account for each student    [54] One shared account by each class    [42] One shared account by all students

[ ] Other : No [3] , Not Applicable, [5] a/c for all students, [2] students shared one a/c, [1] shared a/c with each form [3] , one share account by one computer [2] , [1] shared a/c by each, project based,

(b) Teaching staff:

[171] Personal account for each teaching staff    [7] One shared account by all teacher staff

[ ] Other : [1] shared a/c for most teachers, [2] shared a/c by all teacher staff,
9. What is the total bandwidth of the school Internet access?
 

[0] No Internet access                    [2] Modem                    [50] 1 – 2 Mbps

[58] 3 – 9 Mbps                    [68] 10 Mbps or more

10. Have you heard of these security facilities and are they being used in your school? (May check more than one option)

Security Facilities	Heard	Now using in school	Incomplete
a) Anti-virus 病毒防禦	[82]	[177]	[0]
b) Firewall 防火牆	[115]	[95]	[5]
c) Intrusion Detection System 入侵偵測系統	[114]	[17]	[52]
d) Access Control List of Router 路由器的存取控制表	[88]	[75]	[43]
e) Web Content Filter 網頁內容過濾	[91]	[142]	[4]
f) File Encryption 檔案加密	[143]	[33]	[14]
g) Email Encryption (e.g. PGP) 電子郵件加密	[144]	[9]	[27]
h) Virtual Private Network 虛擬私人網絡	[134]	[16]	[34]
i) Data Backup 數據備份	[83]	[169]	[2]
j) Disaster Recovery 災難復原	[113]	[77]	[15]
k) CCTV (Closed Circuit TV) 閉路電視	[140]	[28]	[20]
l) Motion Detection Sensor 活動感測器	[97]	[94]	[26]
m) Infrared Temperature Detection Sensor 紅外線溫度感測器	[118]	[67]	[19]

11. From what channel(s) do you usually learn about the latest security related news? (May check more than one option)

[83] Education Department      [97] Vendor      [124] Newspaper

[87] Colleague / Friend      [3] Student

[21] HKCERT (香港電腦保安事故協調中心)

[ ] Others : newsletter, magazine [9], Cisco networking academy, internet [15], ITSD, mass media, KENFIL,

12. How do you rate the level of information security in your school?

[2] Very Low    [48] Low    [113] Medium    [13] High    [2] Very High    [2] No Idea

13. Who is responsible for information security in your school?

[3] Principal      [126] IT Team      [44] TSS

[ ] Others : no reason, me & a.v.p., ITC, computer panel chairman, ITA, IT I/C

14. (a) Is there any computer in your school network that does not have "User ID / Password" access control?

[54] Yes      [122] No. (skip to question 15)      [4] Don't know (Skip to question 15)

(b) If yes, what function(s) is/are provided by the computer(s)? (May check more than one option)

[19] Email                      [30] Web-browsing              [13] FTP                      [ ] VPN

[ ] Others: clerical work, Desktop application, fax, no reason, standalone pc for student's study, convert VCD & video tape info, general usage, office [4], teachers' personal use, presentation, document, library, login, students playing games, technicians computer.

15. Types of service currently in use or planned to implement?

Types of Service	Now In Use	Planned to implement		Incomplete
		In 2002	In 2003-2005	
a) Web Server 網頁伺服器	[112]	[30]	[18]	[20]
b) FTP Server 檔案傳輸伺服器	[88]	[21]	[18]	[53]
c) Database Server 資料庫伺服器	[75]	[22]	[22]	[61]
d) Mail Server 電郵伺服器	[54]	[25]	[27]	[74]
e) News Server 新聞伺服器	[11]	[10]	[31]	[128]
f) Telnet Server Telnet 伺服器	[31]	[6]	[22]	[121]
g) Instant Messaging Services (e.g. ICQ, MSN) 即時通訊服務	[20]	[10]	[16]	[134]
h) Wireless Network 無線網絡	[59]	[21]	[31]	[69]
i) VPN 虛擬私人網絡	[17]	[19]	[26]	[118]
j) Video Conferencing 視像會議	[14]	[27]	[38]	[101]
k) VOD Server 實時視訊傳輸伺服器	[68]	[13]	[31]	[68]

16. Who can access your school's internal network from outside your school network? (Not including the web services)

[112] No one (*skip to question 18*)

[35] IT Team only

[19] IT Team and teaching staff

[12] IT Team and teaching staff and students

[1] Don't know (*skip to question 18*)

17. For the remote access,

(a) which access method is being used?

[27] simple dial-up              [10] dial-up with callback              [12] VPN

[ ] Others: Internet [2], no reason, None [2], FTP [3], VNC, Broadband, school , telnet [2], VCN, web, SSH, remote

(b) what services can be invoked by remote access? (May check more than one option)

- [15] Email                      [17] Telnet to web server                      [9] Telnet to network equipment
- [42] FTP                      [20] Remote logon to NT Domain
- [ ] Others : Full Control, web [2] , Netstorage, SSH only,

18. Is there any Firewall in place to protect your school network?

- [92] Yes                      [81] No                      [3] Don't know

If the answer is "Yes", answer the following sub-questions:

(a) Who defines the security rules of the Firewall initially?

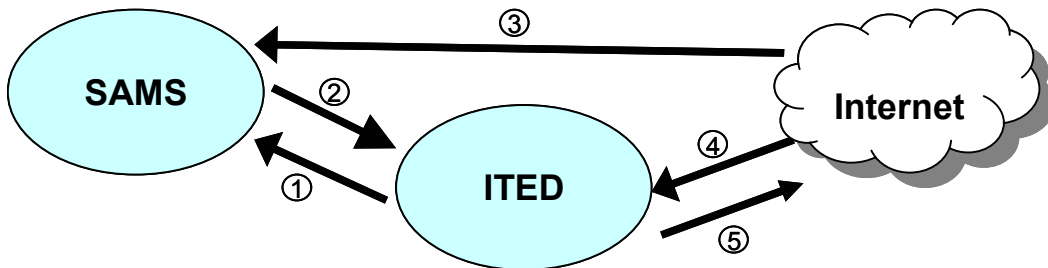
- [5] Use Default Settings                      [29] Vendor                      [14] TSS
- [41] IT Team                      [3] Don't know

[ ] Others : me, Sponsoring Organization, vendor & IT Team, no firewall,

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

- [21] 0 times                      [20] 1 time                      [16] 2 times
- [22] 3 times or more                      [15] Don't know                      [86] Incomplete

19. Below is the school network architecture. An arrow indicates "can access from the direction indicated". For example, "arrow 5" indicates that the ITED network can access the Internet.



Please indicate the connection(s) that exist. (May check more than one option)

- [38] connection 1                      [102] connection 2                      [29] connection 3                      [73] connection 4
- connection 5 (example)

20. During the past 12 months, how many cases of information security incidents were reported in your school?

Information Security Incidents Reported	No. of Cases reported			
	0	1-5	6-10	10 or more
a) Server being <b>infected</b> by virus (not detected by anti-virus software) 電腦病毒避過防毒軟件，感染伺服器	[91]	[76]	[0]	[8]
b) PC workstation <b>infected</b> by virus (not detected by anti-virus software) 電腦病毒避過防毒軟件，感染 PC 工作站	[61]	[84]	[17]	[16]
c) Server having been hacked 駭客侵入伺服器	[134]	[39]	[1]	[2]
d) PC workstation having been hacked 駭客侵入 PC 工作站	[158]	[14]	[0]	[0]

Information Security Incidents Reported	No. of Cases reported			
	0	1-5	6-10	10 or more
e) Data loss due to hardware or software failure 硬件或軟件失效而引致數據流失	[86]	[80]	[6]	[4]
f) Leakage of school record information 學校記錄資料外洩	[174]	[2]	[0]	[0]
g) Capacity (e.g. disk space or Internet bandwidth) overflow due to misuse of computer 濫用電腦而導致容量(例如磁碟空間或互聯網頻寬)滿溢	[88]	[59]	[13]	[17]
h) Denial of Service attack 拒絕服務攻擊	[160]	[10]	[1]	[3]
i) Email Spamming by external party 由外面湧進的不速電郵	[137]	[23]	[5]	[12]
j) Student browsing malicious and pornographic web contents 學生瀏覽有惡意或色情內容的網頁	[87]	[67]	[11]	[9]
k) Student misconduct : Spam or hack other people's computer and accounts 學生不端行為: 發出不速電郵或入侵他人的電腦和戶口	[139]	[29]	[2]	[4]
l) Harassment or Threats by email 接到騷擾或恐嚇電郵	[159]	[16]	[0]	[0]
m) Others (please specify)	[31]	[1]	[1]	[1]

21. In the past 12 months, have you ever sought assistance from the following external parties to deal with security incidents occurred in your school?

Seek assistance from external party	Frequency (times)				
	Never	1-2	3-5	> 5	Incomplete
a) ED 教育署 / ITSD 資訊科技署	[143]	[25]	[1]	[3]	[8]
b) Police	[165]	[8]	[0]	[0]	[10]
c) HKCERT 香港電腦保安事故協調中心	[164]	[8]	[0]	[0]	[8]
d) Vendor Support	[86]	[62]	[13]	[16]	[3]
e) Friends or Colleagues	[95]	[48]	[19]	[10]	[8]
f) Professional association	[134]	[5]	[1]	[1]	[39]
g) Other Security related bodies	[110]	[1]	[1]	[0]	[68]

22. If there is a virus infection report in the school, who will be informed in the subsequent incident handling? (May check more than one option)

[153] TSS staff

[158] IT Team Leader / Coordinator

[47] Principal or Vice Principal

[2] Form Master / Mistress

[4] ED 教育署 / ITSD 資訊科技署

[ ] Others : All staff [2], computer panel chairman, IT assistant [2],

23. How often are these tasks performed (either manually or automatically)?

Tasks	Frequency (in each month)					N.A.	Incomplete
	Never	< 1 times	1 - 2 times	3 - 6 times	> 6 times		
a) Check the log of servers (and firewall, etc.)	[2]	[15]	[61]	[28]	[68]	[4]	[2]
b) Patch (修補) the system security holes (保安漏洞)	[10]	[52]	[71]	[18]	[17]	[9]	[3]
c) Patch the PC/Notebook security holes	[23]	[59]	[61]	[12]	[11]	[9]	[5]
d) Patch the firewall security holes	[41]	[40]	[29]	[8]	[7]	[49]	[6]
e) Monitor newly published virus or security alert information	[7]	[22]	[71]	[20]	[53]	[1]	[6]
f) Make sure the virus signature is updated	[2]	[14]	[66]	[25]	[70]	[2]	[1]
g) Data Backup	[0]	[1]	[16]	[22]	[130]	[6]	[5]
h) Check the space usage of server hard disk	[2]	[21]	[54]	[36]	[62]	[3]	[2]
i) Others (please specify)	[5]	[0]	[1]	[0]	[0]	[10]	[164]

24. Do you perform Recovery Test for your system? (choose one only)

- [98] No
- Yes, and the frequency of the recovery test :
  - [52] is only once after the system is up, no periodic test plan
  - [26] follows a periodic test plan

25. Is there any written security policy in your school? (choose one only)

- [117] No
- Yes, and it is approved by the :
  - [45] IT Team Leader / Coordinator
  - [10] Principal / Vice Principal
  - [ ] School Management Committee

26. Is any of the following security management measures adopted in your school?

Security Management Measure	No	Yes, and		Incomplete
		it is not updated	it is updated	
a) Record of network and system configuration	[34]	[41]	[97]	[8]
b) Record of security incidents reported	[99]	[20]	[52]	[9]
c) Procedure of Incident Response and Reporting	[102]	[28]	[40]	[10]
d) Procedure of System Maintenance and Log Management	[86]	[20]	[65]	[9]
e) Procedure for Approval of Changes to the network, servers and other systems	[99]	[21]	[49]	[11]
f) Documentation of all changes to the network, servers and other	[76]	[38]	[57]	[9]

systems				
---------	--	--	--	--

27. What do you think is/are the **GREATEST** obstacle(s) for your school to address the information security issues? (May choose more than one, but not more than 3 options)

[8] No obstacle, everything is alright (if choosing this option do not check any others)

[125] Budget

[93] Technical competence

[29] Management commitment

[67] Awareness of employee

[77] Human resources

[0] Others (please specify): Technical training for all, not enough time, irresponsible, affecting the rate of access,

28. What do you think is(are) the **MOST** needed solution(s) to improve the current security situation of your school. (choose not more than 5 items)

[3] Everything is alright, no solution is needed (if choosing this option do not check any others)

[122] Increase budget

[41] Increase IT team head count

[102] ED issue more clear technical and management guidelines

[27] School management give more power to IT team

[115] Provide more information security training to IT team

[104] Provide more information security awareness training to employees

[53] Set up a web site to share technical FAQ (Frequently Asked Questions)

[77] Perform periodic security assessment to school system and network

[ ] Others (please specify) : Increase wages of IT coordinator, 免費提供過濾網頁服務, Hire expert to handle the issue, ED should supports us by budget, one man job

[4] Incomplete