Information Security in Schools

Sierra Lam
IT in Education Section
Education Bureau
28-29 Nov 2017
Six Actions of ITE4

1. Infrastructure
2. e-Learning resources
3. Curriculum & pedagogy
4. Capacity building
5. Involving stakeholders
6. Research & evaluation

Development of ITE4
Relevance to information security

• Vendors
  – Infrastructure under WiFi100 and WiFi900
• Schools
  – Grants
• TSS / end users
  – Information Security in Schools – Recommended Practices
• Students
  – Information Literacy (IL) in curriculum
Infrastructure: WiFi100 & WiFi900

Terms and conditions in the specifications relevant to:

- Preventive measures
- Detective measures
- Responsive measures
- Recovery measures
Preventive measures

Design a secure network…

- Existing Network Facilities – not rely on any existing network facilities and cabling of the School, nor interfere with the existing WiFi network of the School. The Wi-Fi network shall be physically separated from the school network.

- The firewall policy should be applied to control network traffic such that public users should be prohibited to access the internal network segments of the School.
Preventive measures

Enforce Network Security Policy…

➢ The configuration settings of the appliance shall support blocking specific network ports, including ports of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Blocking denial of service (DoS) attacks and malformed packet attacks shall also be configured.
Preventive measures

Apply Access Control …

- Authentication Method – use 802.1x standard based authentication and Hong Kong Education City single sign-on services.

- The WLAN system shall allow single or multiple devices per user account to be authenticated using 802.1x and Hong Kong Education City single sign-on service.

- The WLAN system shall suspend the session of the user once the session control is expired and the suspension time shall be configured by the school.
Detective measures

A proactive monitoring system is important…

- Managed Service – operate the WiFi network using managed service model, provide end-to-end service with single point of contact including configuration, provisioning of service, proactive monitoring, maintenance and regular reporting.
Responsive / Recovery measures

Define a response mechanism...

- Service Level Agreement – ensure at least 99.7% availability of the WiFi service, support four-hour response time and four-hour service recovery with active monitoring, helpdesk support with support hours from Mon to Sat 8:00 am to 6:00 pm, and provide monthly monitoring reports for the School.
Overview of ITE Grants

Recurrent

CITG

$197,929 – 680,748 ($397,000 on average)
• IT-related consumables
• Digital resource materials
• Internet fee
• Employment/hire of TSS
• Opening for school's IT facilities
• Maintenance, upgrading and replacement of IT facilities

Funding for ITE4

$48,530 to $121,340 ($70,000 on average)
• WiFi subscription
• Maintenance/replacement of mobile devices

ITSSG

$300,000
• Employment/hire of TSS
• Additional technical support services such as data migration and cloud management

One-off

ITE4 ($100,000)
• Mobile device

OITG ($200,000)
• Mobile device
• Employment/hire of additional TSS
• E-resource/platform
Support for TSS / End Users: Information Security in Schools – Recommended Practice

Information Security in Schools

Security measures

- Preventive measures
- Detective measures
- Responsive measures
- Recovery measures

Suggestions to Schools

Security Incident Handling

- Establish school-based IT Security Incident Response Team
- Setup proper reporting procedures:
  - Report to the school’s IT Security Incident Response Team
  - School decision to report to
  - HKCERT? HKPF?

Part 3, Page 11, “Information Security to Schools – Recommended Practice”
Information Security Website

Information Security in Schools

(14/11/2017) Special Attention on Ransomware Attacks Leveraging Remote Desktop Services (RDP) for Infection

We notice that there have been reports of Crysis/Dharma ransomware attacks through RDP recently in Hong Kong, resulting in data being encrypted and inaccessible. TSS are advised to review and take the following preventive measures to protect the computers of your school from ransomware attacks:

(a) Block RDP protocol access from the Internet. If remote access from the Internet is unavoidable, additional protection (such as VPN and multiple-factor authentication for the access) should be applied;
(b) Restrict the use of RDP in computers;
(c) Apply the least privilege principle to the account(s) that can remotely access the computer. Do not grant the administrator right unless necessary;
(d) Use strong passwords and change password frequently;
(e) Implement account lockout policy to lock out account after a set number of failed login attempts;
(f) Restrict only specific IP(s) to access the RDP;
(g) Limit the time period allowed for remote connection.

Reference:
Secure the Remote Desktop Services (RDP) for https://www.hkcert.org.hk/en/blog/771509
Crysis/Dharma variant. arena Ransomware

(28/06/2017) Beware of Petya Ransomware spreading

Please take note to the message from Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT):

A new variant of ransomware known as Petwrap / Petya / Nyetya is spreading quickly. It encrypted victims’ data file and demand for ransom. Some overseas countries were hit. The different names of the ransomware indicate that there is a debate among security experts on where this ransomware is directly related to another known ransomware Petya.

The ransomware can be spread via phishing email or via local network.

An infected computer uses two methods to attack computers on local network. It uses the EternalBlue exploit previously employed by the WannaCry ransomware to attack computers that have not applied the SMB patch (MS17-010). It also tries to force computers in the local network that it has administrative rights to install the malware.

H K CERT likes to alert organizations to take measures to prevent your network from infection and data loss. The centre had issued security alert on the ransomware. Please refer to this URL: https://www.hkcert.org.hk/en/alert/17062801

Malware Prevention
Training and Education for End Users

- Avoid opening suspicious electronic messages, and do not follow URL links from untrusted sources to avoid being redirected to malicious websites.
- Check attachments and downloads against malware before use.
- Perform regularly data backup and keep them offline.
- Prevent to use remote access software to connect to a school server or user workstation directly. Use secured channels (e.g. VPN gateway) with two-factor authentication for better protection.
- Use strong passwords and change password frequently.
Handling Malware

Some of the ransomware infections and outbreaks in 2017 …
Crysis/Dharma, Bad Rabbit, Petwrap / NotPetya, WannaCry ransomware attacks

In case a computer is infected, users should take the following IMMEDIATE actions.

a) **DISCONNECT** the network cable of the computer to avoid affecting network drives and other computers;

b) **POWER OFF** the computer to stop the ransomware encrypting more files;

c) **JOT DOWN** what have been accessed (such as programs, files, emails and websites) before discovering the issue; and

d) **REPORT** the case to relevant personnel/ organisation, such as ICT coordinator in school, HKCERT, HK Police Force, etc.
Information Literacy for Hong Kong Students

Introduction

Information technology (IT) is a powerful tool to unleash the learning capability of students. With the advancement of technology and its application through innovative pedagogies in all KLA, students' capability in information literacy (IL), self-directed learning and other 21st century skills such as creativity, problem solving skills, collaboration skills and computational thinking skills are enhanced. Strategies on IT in Education are formulated at various stages to enable students to learn and excel through realising the potential of IT in enhancing interactive learning and teaching experiences.

As an important competency, IT helps students identify the need for information; locate, evaluate, extract, organise and present information; create new ideas; cope with the dynamics in our information world; use information ethically as well as refrain from immoral practices such as cyber bullying and infringing intellectual property rights. IL could be developed through the application of the generic skills (see Section 2.3.1 and Appendix 1 of this booklet) in the context of handling information in different media in our information world. This also involves various knowledge contexts and has close linkage with the KLA.

Schools can make reference to the “Information Literacy for Hong Kong Students” for suggestions on how to develop students' knowledge, skills and attitudes to use information and information technology ethically and effectively as responsible citizens and lifelong learners. Incorporation of IL in the whole-school curriculum will provide authentic contexts for students to apply the skills and benefit their learning in relevant KLA.
Promotion of Infographics, Posters and Leaflets
The Way Forward

Professional Development Programmes for Senior Management and Principal IT coordinators / IT team members

Migrate to Cloud Services

Update the “Information Security in Schools – Recommended Practice”

What are the needs of schools? Any suggestions?
THANK YOU!

Enquiry
Use of Funds : (852) 3698 3606
Professional Development Programmes : (852) 3698 3610
Technical Advisory Services : (852) 3698 4148 / 3698 3566