The Education Network
Information Sheet 6
November 2014

e-Security

Managing and maintaining e-security/cyber-security in schools

The Education Network
Information Sheet 6
November 2014
http://www.nen.gov.uk

e-Security

Managing and maintaining e-security/cyber-security in schools

Introduction

From guidance published by CESG, the information security arm of Government Communications Headquarters (GCHQ):

> "In GCHQ we continue to see real threats to the UK on a daily basis, and the scale and rate of these attacks shows little sign of abating. The good news is that, despite the increase in sophistication and volume, there is much you can do to protect your organisation by adopting basic cyber security procedures."

Schools, just like any other commercial or public sector institutions, are now reliant upon the internet and broadband services for day-to-day operations and activities. These technologies bring a huge range of opportunities and benefits, offering news ways to support teaching and learning and streamlining operational and administrative processes. But they also bring a range of risks if not managed and maintained appropriately: these risks include the loss of sensitive, confidential personal data and potentially, where network services deteriorate or fail as a result of a security incident, reduced or lost capability to deliver timetabled events and scheduled teaching and learning.

Broadband and internet access are now 'mission critical' for schools, just as they are for businesses and the wider public sector. As such all schools need to put appropriate mechanisms in place to maintain the integrity and availability of their network services and resources. CESG estimate that about 80 per cent of known attacks would be defeated by embedding basic e-security practices for people, processes and technology. All the evidence shows that attacks are increasing, in terms of both numbers and complexity, necessitating a dynamic, strategic approach to their mitigation and prevention. In addition it is important to remember that security threats and incidents do not just come from outside the institution: internal users can pose a threat too, whether through accidents, carelessness, ignorance of their responsibilities or malicious intent.

This document, intended for school network managers and technicians, provides an overview of how schools should manage network security, often referred to as cyber-security or e-security. This is distinct from managing e-safety and data security in schools, which present related but different sets of issues and risks. It is intended to support schools in drawing up a policy setting out their approach for the ongoing management of e-security risks, issues and incidents. This policy should in turn inform schools' acceptable use polices (AUPs) which all users of school network services should be aware of and abide by.

Two accompanying documents set out 10 steps to protect your school's network for school leaders and a detailed e-security checklist for school senior leaders and network managers (see sources of further advice on page 12). The potential impact now necessitates that e-security issues, risks and mitigations are understood and embedded at a senior level within schools.

1. Understanding e-security requirements and the threat landscape

School systems are threatened by a growing array of risks and dangers that require informed and effective mitigation to avoid the potential loss and damage that can result. In summary, threats can include:

- **Malicious technical attacks** - these include external attempts to compromise systems through methods such as Distributed Denial of Service (DDoS) attacks, malware propagation (such as Trojan horses) or physical hacking attempts. Typically these attacks seek to gain access to school data and systems, to use school systems to mount further attacks on other systems, or use school systems for illegal or unauthorised purposes, leading to reputational damage. For example, unpatched school web sites could be used to host malicious content. Unpatched and unguarded PCs could be harnessed for use in botnets[1] which could again be traced back to the school. The PCs in the school could be used in parallel processing activities contrary to the Computer Misuse Act for password cracking or bitcoin mining which again could be unbeknown to the school. Also some automated attacks could affect schools with untreated vulnerabilities – improperly protected school networks are just as susceptible to these kinds of attacks as any other network.
- **Accidental attacks** - issues can also arise that may not be malicious or deliberate (for example, attacks created as a result of programming errors, bugs in software or user entry), but can be equally problematic.
- **Internal attacks** - these include the introduction of infected devices or storage facilities (like USB flash drives) into networks, and malicious or accidental actions by users. For example, keystroke loggers[2] can capture private, confidential keyboard inputs such as usernames and passwords. AUPs should expressly forbid such attacks with proper enforcement and clear sanctions for any such kind of malicious activity.
- **Social engineering** - these typically result from exposure of an internal weakness, such as poor password use (or passwords being written down and left visible), or emails or websites designed to capture credentials from unsuspecting users (typically referred to as 'phishing'). Many security experts believe that the biggest risk to any system continues to be an ignorant or careless user.

Service providers also continue to develop their protections. The number of malicious attacks directed towards service providers is continuing to increase, and the industry in general considers the number and complexity of attacks to be a major problem.

It is also important to understand whether any particular security requirements have already been set out, that certain types of organisation are expected to comply with. Where more than one

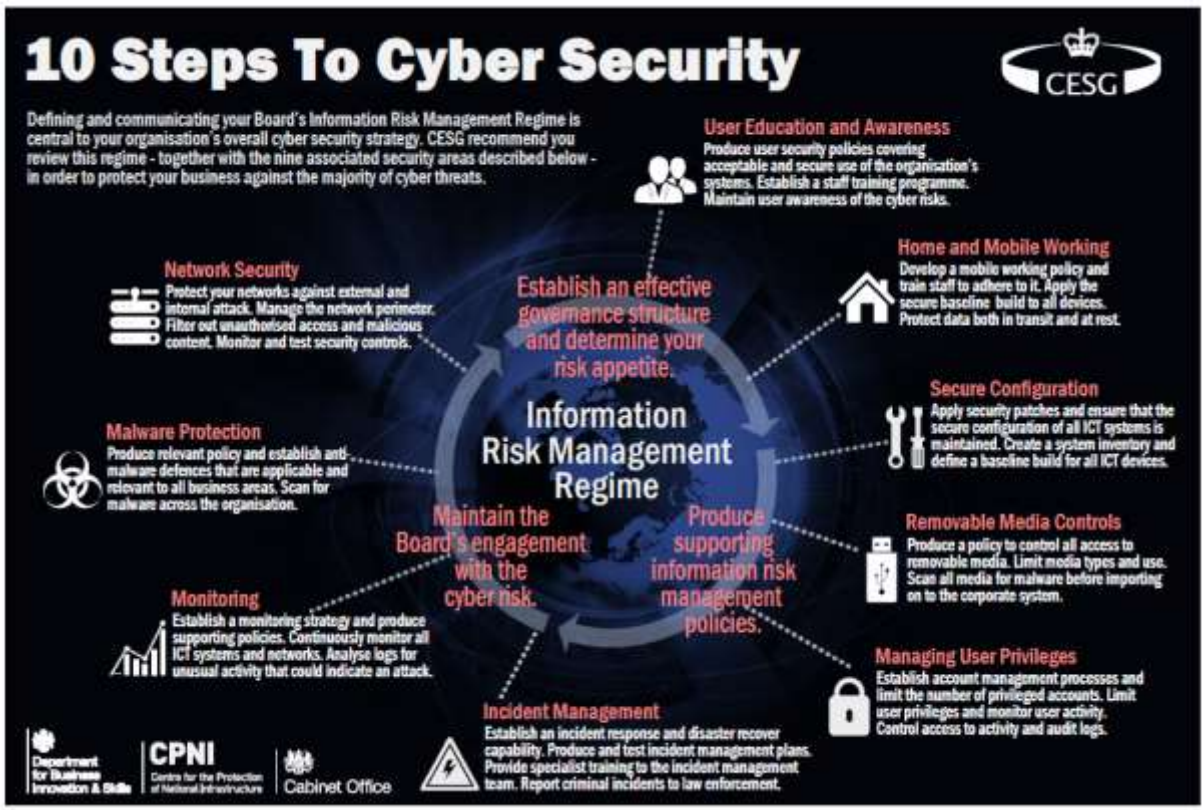
[1] http://en.wikipedia.org/wiki/Botnet
[2] http://en.wikipedia.org/wiki/Keystroke_logging

'agency' uses a single network and security infrastructure, it may be necessary to consider additional security undertakings. As an example, a school that also hosts a council, health or emergency service unit within their premises will need to consider the security requirements of each agency using the network. It is essential to segregate the traffic of each agency to maintain the security levels required.

2. Ten steps for managing e-security

The scale and scope of e-security issues and risks today necessitates a holistic approach that encompasses a range of technical measures alongside organisational policy approaches.

CESG has set out ten related actions and measures[3] to help organisations implement, manage and maintain e-security effectively:



[3] https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

These actions and measures provide a helpful framework for implementing an e-security strategy and are as applicable to schools as to any organisation that needs to keep its network services, data and users secure. To interpret the above in a school context:

1. **Information risk management regime** – this involves recognising and taking ownership of and responsibility for e-security at a senior level and ensuring that all staff and pupils are aware of, understand and abide by all their obligations and responsibilities. Schools should establish and maintain via regular review an e-security policy which sets out the approach for managing risks, issues and incidents. The e-security policy should inform the school's acceptable use policy (AUP) for IT; this key document should set out everything that end users need to know in an accessible way.

2. **Secure configuration** – this involves keeping an inventory of all school IT hardware and software and making sure that policies and procedures are place to ensure all changes are authorised, documented and implemented appropriately. It also involves establishing processes for monitoring and the timely updating of systems as required; for example, when new versions of software (including operating systems, web browsers and plugins) are released, when security patches become available or when hardware or software goes 'end of life'. This is when suppliers end their support for outdated or superseded products and services, such as when Microsoft ended its support for Windows XP after 12 years in April 2014[4]. Any security issues subsequently identified in unsupported products and services will not be rectified by suppliers, potentially creating security vulnerabilities if they are not replaced. Another aspect of securing IT configuration involves locking down hardware, operating systems and software to prevent access to facilities which could be used to compromise network security, either maliciously or accidentally. Heartbleed and Shellshock[5] are two recent examples of high-profile security risks that underline the importance of secure configuration procedures and policies to keep hardware and software up to date and protected. Inventories must include all school hardware and software, for example school-provided staff mobile phones need to be included and kept secure through locking and password policies.

3. **Network security** – school, local authority and regional broadband networks provide access to the internet and other networks that could be the source of attacks, for example though the distribution of malware or distributed denial of service (DDoS) attacks. These are increasing in number and are becoming increasingly easy to initiate. It is important to remember that a security vulnerability or incident in one school could potentially impact on many other schools and organisations as well. For example, a successful denial of service attack may flood a local authority or regional network with traffic, preventing all schools

[4] http://windows.microsoft.com/en-gb/windows/end-support-help

[5] http://www.bbc.co.uk/news/technology-26969629 & http://www.bbc.co.uk/news/technology-29375636

from using the network even though only one school has been targeted. Schools therefore not only have responsibilities in relation to their own users but to any other schools and institutions they share network services and infrastructure with. It is therefore essential to ensure the perimeter of the school's network is policed appropriately. Technical measures to assist here include firewalls (of which more detail later in this document), filtering of websites for malicious as well as inappropriate content, antivirus and malware checking, monitoring and establishing appropriate internal network security configurations, for example through the segregation of network assets. Wireless network security is an important consideration here too, to prevent access from unauthorised users and devices. Antivirus and other malware tools need to be updated regularly to keep pace with new and changing threats.

4. **Managing user privileges** – this involves controlling what individual users can and cannot do on the network. User privileges need to be differentiated and set appropriately so that all users can access the facilities they require while minimising the potential for deliberate or accidental misuse of the network. Processes should be set up for creating, managing and deleting user accounts when they are no longer needed. Automated user provisioning systems can provide a way to manage these risks including automatically deleting the accounts of users that have left the school, something which is often overlooked. Password management processes and policies can ensure both that passwords are strong (i.e. not easy to guess either manually or via a dictionary attack[6], for example requiring upper and lower case letters as well as numbers and/or symbols) and that they are changed regularly. Monitoring user activity is also important here; it is advisable to inform all users that their usage of the network may be monitored if this is the case. The key document for doing this is the school's IT acceptable use policy (AUP). It is essential that all users are aware of and understand the school's AUP which should be reviewed regularly and updated as necessary.

5. **User education and awareness** – all users need to understand their e-security obligations and responsibilities and user education and training are essential if this is to be achieved. As stated above, schools should develop a user security policy and embed this within their IT acceptable use policy (AUP). Training and induction processes should be available for all new users (staff and pupils); new threats emerge all the time so AUPs need to be reviewed and refreshed regularly. Key aspects for end users include password policies, use of removable media/personal devices in school and remote access to school network facilities (for example, remote access for staff to the school management information system). All users should be made aware of and understand any disciplinary processes and sanctions for misuse in the event of malicious e-security incidents. Schools should ideally encourage a strong culture of e-security in order to keep the use of disciplinary procedures and sanctions

[6] http://en.wikipedia.org/wiki/Dictionary_attack

to a minimum. The key here is ensuring that everyone understands e-security risks and their own responsibilities in relation to them

6. **Incident management** – the nature and range of issues and threats means all schools will experience an e-security incident at some point. Having plans and procedures in place in advance for logging, reporting on, monitoring and dealing with e-security incidents will help ensure that any damage is minimised, that services can return to normal as soon as possible and that lessons can be learned to prevent similar incidents from occurring again. These lessons may need to be applied in a range of areas. For example, it may be necessary to update a firewall's configuration after an incident. This may in turn lead to a review of configuration and patch management processes. Similarly, it might be necessary to update the school's AUP, which then leads to a review and update of e-security awareness training for pupils and staff.

7. **Malware prevention** – malware is any malicious code or content which could damage the confidentiality, integrity and availability of a school's network and IT services. Malware can proliferate in many ways, for example via email attachments, social media, malicious websites or removable media such as USB flash drives. Key ways to mitigate the risks from malware include antivirus and malware scanning, web filtering to block access to known malicious websites and also encouraging appropriate user behaviours in relation to aspects such as web browsing, accessing email and using removable media in school. Again, user education and training in relation to the school's AUP for its IT services are key here.

8. **Monitoring** – monitoring systems, network traffic and user activity allows attacks and other e-security incidents to be detected quickly, allowing a rapid and effective response in keeping with defined incident management processes. It is also important to preserve event logs as potential evidence in dealing with an as yet undiscovered misdemeanour. It is important that key individuals are tasked with reviewing the outputs from monitoring systems and responding to alarms and alerts. Reports, logs and alarms are all useless if no one is responsible for or has the time to look at or respond to them. Means for storing and accessing data from monitoring also need to be considered, as monitoring systems can rapidly generate large amounts of data. User activity monitoring processes need to be able to spot unauthorised, accidental or malicious usage and should be able to identify the user, the activity that prompted the alert and the information or service the user was attempting to access.

9. **Removable media controls** – it is important to control what can enter and leave the organisation via removable media and personal IT devices, especially as such devices become more widely available and used in schools. Further information on this area is available in NEN Information Sheet 5, *Using consumer IT devices in schools: Options,*

opportunities and issues[7]. Key risks in relation to removable media include information leakage and theft and the potential for the introduction of malware into the school. Protections in this areas include limiting what data can be stored on which type of media/device together with strategies for encrypting[8] removable media and or secure remote access to centrally held data. Holding date centrally negates the need for multiple copies to be created and transferred via removable media.

10. **Home and mobile working** – pupils and staff need to be able to access school systems from home and elsewhere from a range of devices, in order to extend learning opportunities and support administrative functions. A key development in this area is "bring your own device" (BYOD) where users wish to connect their own personal devices to school wireless networks[9]. Risks include the possible loss or theft of staff laptops and the potential for access to and leakage of sensitive information from devices with limited security features. User education is paramount in this area; technical strategies may include encrypting school-owned devices to prevent unauthorised access and use. Schools should include consideration of remote and mobile working in their overall security policy, particularly in relation to securing teacher laptops that are used in school, at home and potentially other locations as well. Another consideration is how to ensure security across multi-site schools that share a single network; whilst collaboration between such sites is important this must be implemented in such a way that does not compromise overall network security.

3. How to get started

The 10 CESG processes described above tie in with the top 20 critical controls for effective cyber defence, as endorsed by the Centre for the Protection of National Infrastructure (CPNI)[10]. These 20 controls (and sub-controls) focus on various technical measures and activities, with the primary goal of helping organisations prioritise their efforts to defend against the current most common and damaging computer and network attacks.

Implementing an effective e-security policy from scratch is a complex task so schools need to develop a plan for assessment, implementation, and process management based on their particular circumstances. The 20 critical controls document suggests five quick wins, highlighting five controls that have the most immediate impact on preventing attacks and incidents:

[7] http://www.nen.gov.uk/using-consumer-it-devices-in-schools-options-opportunities-and-issues/
[8] http://ico.org.uk/news/current_topics/Our_approach_to_encryption
[9] NEN advice on BYOD is available at http://www.nen.gov.uk/using-consumer-it-devices-in-schools-options-opportunities-and-issues/
[10] http://www.cpni.gov.uk/advice/cyber/Critical-controls/

1. **Application whitelisting** (found in Critical Security Control 2, *Inventory of Authorized and Unauthorized Software*) – This technology allows software to be run only if it is included on the whitelist of authorised software tools, preventing all other software from being run. It is important that the whitelist includes all the software that users need to be able to run in the school.

2. **Use of standard, secure system configurations** (found in CSC 3, *Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers*) – Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. Hardening typically includes: removal of unnecessary accounts (including service accounts), disabling or removal of unnecessary services, configuring non-executable stacks and heaps, applying patches, closing open and unused network ports, implementing intrusion detection systems and/or intrusion prevention systems, and use of host-based firewalls. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

3. **Patch application software within 48 hours** (found in CSC 4, *Continuous Vulnerability Assessment and Remediation*) – Implement automated patching tools and processes for both applications and for operating system software. When outdated systems can no longer be patched, update to the latest version of application software or operating systems. Remove outdated, older, and unused software from the system.

4. **Patch system software within 48 hours** (also found in CSC 4); and

5. **Reduce the number of users with administrative privileges** (also found in CSC 3 and CSC 12, *Controlled Use of Administrative Privileges*) – Limit administrative privileges to very few users who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system. This will help prevent installation of unauthorized software and other abuses of administrator privileges.

Whilst these five offer a helpful starting point it is important that a school's e-security policy encompasses all of the CESG's 10 steps described in Section 2 of this document. The top 20 critical controls document offers more technical detail for school network managers on how the principles and processes set out in the CESG's 10 steps can be implemented.

4. Managing and maintaining firewalls in schools

As described under network security in the previous section, every establishment with a broadband connection requires a firewall in order to prevent unauthorised external access to its data and systems.

Firewalls can be complex systems, and require good management in order to deliver the appropriate level of security and protection from external threats. They can also require frequent configuration changes to allow access to new services and applications required by the school; schools need to ensure that any such configuration changes do not compromise overall network security. Any such changes should only be considered as part of the secure configuration function described in the previous section.

Typically, firewalls can be deployed in one of two key ways:

- a **centralised deployment**, in which the firewall is located within a data centre or other major network location to which the school's broadband service connects; or
- a **localised deployment**, in which the firewall is located on an appliance or system within school premises, either as a discrete technology or as a component of another system (such as a filtering solution)

A key consideration in either case is the configuration and ongoing management of the firewall, more so even than the specification of the firewall itself. The quality, consistency and methodology of firewall and security service configuration, change and maintenance is the most significant factor in ensuring the firewall continues to protect the establishment and its users.

If your firewall is managed on your behalf by a third party rather than in-house, what aspects of the firewall management service should you investigate and understand?

- the **service level agreement (SLA)** provided by the organisation undertaking the management of the firewall. Changes and updates to firewall configuration should be logged by authorised users within the establishment, and undertaken quickly enough by the provider to maintain operational effectiveness within the school. Patches and fixes should be applied within a short period of time to ensure vulnerabilities are not exposed.
- the **expertise and experience** of the team providing the management service. Suitably qualified engineers should be supported by a robust change management methodology and a rigorous policy and management environment to ensure changes are not made to the firewall configuration without an appropriate level of assessment, testing, and documentation.

Schools may like to consider enabling or installing software firewalls on their servers in addition to the service provided by the third party to provide an additional layer of protection.

So, should schools manage their own firewalls? The answer very much depends on whether the expertise is available in-house to enable the school to do so (if this is the responsibility of one key individual what happens if he or she leaves?), and the level of confidence the school has in its capability to protect itself against security threats and deal with incidents.

5. Email security

Over 70% of email across the globe appears to be spam, and this is increasing year on year. Email continues to be a common medium for transmitting threats, as for a potential attacker it is very cheap and very widely used.

Mail security technology can be employed to detect and block malware transmitted by email, as well as spam and other messages designed to try to exploit users. These technological solutions need to be kept up to date in order to maintain accurate details of the sources, signatures and techniques used by spammers and prevent the spread of malware by email.

If a site or email address is identified as source of spam and/or other malware, it may be added to the email blacklists used by providers to block unwanted emails. It is important to ensure that appropriate measures are in place to ensure that this does not happen to your school. You should also check that your service provider has the correct measures in place to reduce the risk to the global community.

Ensuring that users do not apply simple passwords is also an important way of protecting email systems from threats; 'brute force' attacks are used by attackers to attempt to access email accounts using a list of thousands of common passwords, so setting more complex passwords, or passphrases, helps to keep accounts secure.

6. Additional e-security measures

While firewalls are essential in order to protect today's networks from attack, there are a range of further measures that can be taken to provide a more complete and in-depth security provision. Such measures may include:

- Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS)
- Heuristic Threat Analysis (HTA)
- Penetration Testing

The extent to which these types of solution is required depends on the security requirements of the school and its users, but the same philosophy applies: these systems and services only really deliver value when they are well configured and well managed.

Schools may also need to consider the provisioning of wireless network access for guests. Typically users of this type of service should be prevented from accessing a number of internal resources (such as printers, shared storage areas, and applications) and this is often achieved by separating such wireless networks from the other wireless networks available in the school. For example, virtual local area networks (VLANS) can be employed to group and manage wireless access points and users appropriately.

Conclusion

Regardless of whether they procure and manage their own broadband services or subscribe to services provided by a local authority or regional broadband consortium (RBC), all schools need to ensure they have an appropriate and up to date strategy in place to ensure the security and integrity of their networks and systems are maintained.

All schools should draw up a policy for how e-security is managed, maintained and reviewed in the light of new and emerging issues and risks. E-security is not something that can be 'fixed' on a one-off basis; the changing nature of the threat landscape means that e-security policies and strategies require regular review and update if they are to remain effective. This brief overview document suggests a framework to assist schools in doing so, outlining the key processes, procedures and responsibilities schools should have in place to protect their networks, data and users.

Key to managing e-security is understanding where the responsibilities for different aspects reside. Schools' e-security responsibilities will differ depending on the nature of their broadband service. For example, some schools may rely upon in-house expertise to maintain their firewalls locally while others may choose to subscribe to a managed firewall service provided by a third party. Local authorities and RBCs provide e-security protections as part of the services they provide to schools. It is essential that schools understand how their network is protected and by whom (including what the school is responsible for and what service providers and other third parties are responsible for) if security incidents are to be understood and dealt with effectively.

The increasing number of security threats and schools' increasing reliance on broadband networks and applications as 'mission critical' services mean this is now more important than ever.

Sources of further advice

NEN: 10 steps to protect your school's network: a guide for school leaders
http://www.nen.gov.uk/10-steps-to-protect-your-schools-network-a-guide-for-school-leaders/

NEN: school e-security checklist
http://www.nen.gov.uk/school-e-security-checklist/

CESG: Cyber security guidance for business
https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

HM Government – 'Responsible for Information' – a free e-learning course aimed at staff in micro, small and medium-sized enterprises (SMEs)
http://www.nationalarchives.gov.uk/sme/

HM Government – Keeping the UK safe in cyber space
https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/providing-cyber-security-advice-for-businesses-and-the-public

HM Government - Small businesses: What you need to know about cyber security
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/197177/bis-13-780-small-business-cyber-security-guidance.pdf

Ofcom – Safer smartphones – keeping your device secure
http://consumers.ofcom.org.uk/files/2013/10/mobile-guideV8.pdf

Get Safe Online – Businesses
https://www.getsafeonline.org/businesses/

Get Safe Online – The Rough Guide to Online Safety
https://www.getsafeonline.org/themes/site_themes/getsafeonline/pdf/GetSafeOnline_RoughGuide.pdf

Council on Cyber Security – Critical Security Controls
http://www.counciloncybersecurity.org/critical-controls/

Computing at School (CAS) Whitepaper: School ICT Infrastructure Requirements for Teaching Computing
http://www.computingatschool.org.uk/data/uploads/CASInfrastructure.pdf

Federal Communications Commission – Small Biz Cyber Planner
http://www.fcc.gov/cyberplanner & http://transition.fcc.gov/cyber/cyberplanner.pdf

Hong Kong Education Bureau: IT security in schools
http://www.edb.gov.hk/attachment/en/edu-system/primary-secondary/applicable-to-primary-secondary/it-in-edu/it%20security%20in%20schools.pdf

NB: the above links are provided for information and illustration only; the inclusion of a link in this list does not imply any endorsement by the NEN, nor does exclusion imply the reverse.