CYBER-SECURITY CHECKLIST

Introduction

This National Education Network (NEN) Cybersecurity checklist is divided into two sections - **Personnel** and **Technical** with an Appendix giving a very brief outline of some of the more common Cybersecurity threats and where they may originate. For more details please read NEN's Cyber Security Guidance for Schools notes and the associated What If document.

Ultimate responsibility for the school's cybersecurity rests with the Senior Management Team but they will likely delegate the technical and day-to-day aspects to particular staff. In general, we would expect one of the SMT to take overall responsibility for the personnel aspects (staff training, policy development, ensuring documentation is completed, etc) while the Systems Manager would take responsibility for designing overall security policies and processes, and manage their implementation.

Completing the checklist will help define and formalise the responsibilities of each part of the school community from SMT to teaching staff and pupils. Clearly defining who is responsible for different aspects of Cyber Security will provide a basis for the development of a Cyber Incident Response Plan which will set out the actions to take in the event of an incident: who will take the technical lead, who is to inform other stakeholders and when, for example.

How to use the checklist.

This checklist can be downloaded and used in either paper or electronic form. The responsible person for each section should use the form to guide them through the required actions. Once an item has been reviewed and any actions taken, the reviewer should date and initial the item and add a date for the next review. There are two blank pages after each section for notes, comments, references to other school policies, etc.

This checklist should be regularly reviewed by the SMT to ensure that all the items are covered and none left unreviewed for too long.

It is important to note that both parts of this checklist are equally important. However stringent the technical security is, human error can allow it to be compromised by accident or design. Similarly, however careful and aware staff are of the threats around them, poor network security will make a cyber incident more likely.

Finally, an ethos of openness and “no-blame” must be cultivated amongst all staff and students to ensure than any incidents that do arise are reported swiftly and treated quickly.

SCHOOL DETAILS

School Name:	
Address:	
Telephone:	
Web Address:	
Head	
Name:	
e-mail:	
Phone:	

PERSONNEL

Contact details of the persons responsible for completing each section of this checklist:

Personnel		Technical	
Name:		Name:	
Title:		Title:	
e-mail address:		e-mail address:	
Phone:		Phone:	
Mobile:		Mobile:	

Item No.	*Description*	*Date*	*ReviewDate*	*Initials*
GENERAL STAFFING				
1.1	What is the agreed password policy? All users should have strong passwords. The **definition** of strong may vary for different users (i.e. between teaching and SMT) but there must be a policy in place that ensures users have a password appropriate to their privileges.			
1.2	What is the agreed policy on access rights? All users should should be able to access only their own files and any specifically shared with them or a group of which they are a member. Privacy, confidentiality and security must be enforced by these controls.			
1.3	What is the two-factor authentication policy for key staff/software (e.g. SMT, MIS, accounting)? Is it still relevant and up-to-date?			
	CPD:			
1.4	General cyber hygiene training: have all staff received training on general cyber security? This should include awareness of new threats, how to deal with them, the school reporting policy and school AUP. Where is this recorded?			
1.5	Phishing: has awareness training been provided to all staff?			
1.6	Passwords: to reinforce the importance of password strength and security (i.e. how are passwords being created and managed), Password management software, 3-word system, changing, etc.			
1.7	GDPR: Have all staff had GDPR training? (*What is it and how does it affect the use of data in school? e.g. parental records, student data, data-storage and copying, home working, etc.*). Where is staff training recorded?			
1.8	Where is staff training CPD recorded?			

SENIOR MANAGEMENT TEAM				
2.1	What is the policy on reporting cyber incidents? This should specifically state that those reporting will not be disciplined unless there was a clear, intentional breach of the school's cyber policy: "no blame" culture. Are cyber incidents being reported to the appropriate staff and where are they recorded? Are staff aware of this policy and is it easily available via, for example, the school web-site?			
2.2	What is the agreed process for validating and signing off invoices that are received both electronically and on paper to prevent fraud?			
2.3	What is the agreed process for any financial changes (e.g. change of bank details) to be confirmed in writing by the SMT?			
2.4	What is the policy on ensuring that the accounts of staff leaving the schools are immediately deactivated, their files either archived or deleted, and the changes documented? This policy should include details of how often SMT should audit this documentation.			
2.5	What is the management structure defining how IT staff are managed and who is responsible to whom? For example, what is the structure from technician to SMT? Is the network IT team managed by, or distinct from, the teaching IT staff?			
2.6	What is the policy on the SMT's use of mobile devices when working way from school? For example, do the SMT use personal phones for school use? Are they allowed to connect to the school network? Does the policy advice against connecting to public WiFi networks? Does it mandate anti-virus protection?			
2.7	Is the list of key IT service suppliers complete and their contact details accurate?			

IT TEAM				
3.1	What is the process to ensure leaving staff accounts are closed in a timely manner (e.g who is to inform the IT Dept. of personnel changes)?			
3.2	What agreed and documented processes are in place to ensure that the IT department works closely with the SMT and suppliers? To ensure, for example, that contract terms are agreed with SMT, and suppliers managed effectively.			
	Responsibilities			
3.3	Maintain a complete and accurate list of the contact details of key suppliers.			
3.4	Enforce the password policy on all users accounts including resetting passwords on request.			
3.5	Manage updates to antivirus software on devices and servers - including any mobile devices used off site.			
3.6	Management of firewalls including managing any change requests - i.e. implementing any valid requests in a secure manner.			
3.7	Design and enforce the cyber security policy on any BYOD/USB devices attached to the network.			

TEACHING STAFF				
4.1	Check policy on the use of personal mobile phones on the school network. In particular the use of anti-virus software and recommendations re connecting to public WiFi networks.			
4.2	Check scheme of works to teach AUP/cyber-security/e-safety to students.			
4.3	Check/update appropriate cyber awareness courses for students.			
	Responsibilities			
4.4	To understand and adhere to the school AUP, etc.			
4.5	To report any suspected cyber incident. (see 2.1)			

OTHER STAFF				
	Responsibilities			
5.1	To understand and adhere to the school AUP, etc.			
5.1	To report any suspected cyber incident. (see 2.1)			

STUDENTS				
6.1	To understand and adhere to the school AUP, etc.			
6.2	To report any suspected cyber incident. (see 2.1)			

NOTES

NOTES (cont...)

NOTES (cont...)

TECHNICAL CHECKLIST

Item No.	*Description*	*Date*	*ReviewDate*	*Initials*
NETWORK				
7.1	Network monitoring: what systems are there in place to monitor the network, send alerts in case of unusual activity, and generate logs?			
7.2	Has intrusion detection/prevention software been installed and tested?			
7.3	Has the network been penetration tested? If so have any recommendations been acted upon?			

GENERAL SYSTEM CONFIGURATION				
8.1	Is the Password Policy up-to-date? How is it being enforced?			
8.2	Are all systems (servers and clients) running on secure settings (o/s and applications). e.g. can software only be installed with administration rights which are strictly controlled. Where are the setting documented and/or backed-up in the event that a full reinstall is required.			
8.3	Are all systems appropriately physically secured? In particular, are servers and network devices (switches, routers, etc.) in secure rooms or cabinets with controlled access, laptops/pads in locked cabinets when not in use, etc.?			
8.4	Office Admin systems: check hardware, software and physical security of all office administration clients. These systems will be a prime target for hackers and scammers so require the highest level of security.			
8.5	Staff systems: check hardware, software and physical security of all clients which are used primarily or exclusively by staff.			
8.6	Student systems: check hardware, software and physical security of student clients.			
8.7	Guest systems: what is a policy for any guest systems which connect to the school network (BYOD)?			
8.8	How is the BYOD policy enforced (e.g. management software)?			

FIREWALL/ROUTER				
9.1	Analyse firewall rules. Are they accurate? Default should be to DENY all inbound and outbound traffic unless specifically ALLOWed. When were they last audited. How often is the configuration backed up and to where?			
9.2	Log analysis: are logs regularly or automatically analysed for suspicious activity and alerts sent?			

WEB-FILTER				
10.1	Are web-filter logs regularly checked for unusual activity?			
10.2	Are false positives/negatives managed in a timely manner?			

BACKUP REGIME				
11.1	Are critical servers (admin/MIS/Email/File-servers) being backed up regularly (daily/hourly/etc)?			
11.2	Are non-critical clients (e.g. desktops, laptops, pads) being backed up?			
11.3	Are there off-site backups? (e.g. backup data moved to Cloud)			
11.4	Has the backup of any cloud based files (e.g. Dropbox, or similar services) been assessed for security and robustness?			
11.5	Has the impact of a Cloud based service being discontinued been assessed and mitigated?			
11.6	What are the backup and restore policies for each type of device (e.g. key servers, staff desktops, student computers, etc)? Have the backups been tested within the last 3 months? Tests should include checking that the backups are being completed and are valid (e.g. test partial and full restore where possible).			
11.7	Which staff been identified and trained in performing both full and partial restore from backup?			

WEB SERVERS				
	For both internally and externally hosted websites check the following:			
12.1	What is the policy regarding administrative access to web servers (e.g. who has root access, is password access available or are ssh-keys demanded, etc)?			
12.2	What user access controls to Web software (e.g. admin, editor rôles, etc. in Wordpress) are in place?			
12.3	Antivirus software installed and up-to-date.			
12.4	Operating system software fully patched and up-to-date version.			
12.5	Web server software (e.g Apache) fully patched and up-to-date version.			
12.6	Web software (e.g. Wordpress) full patched and up-to-date version.			

EMAIL SERVERS				
	For both internally and externally hosted email severs check the following where appropriate:			
13.1	What is the policy regarding administrative access to email servers (e.g. who has root access, is password access available or are ssh-keys demanded, etc)?			
13.2	Is Two-factor Authentication being used for all administrative and “high-value” users (e.g. SMT, Accounts)?			
13.3	Administrative access controls to Email software (e.g. Zimbra).			
13.4	Antivirus/spam software installed and up-to-date.			
13.5	Operating system & email server software fully patched and up-to-date version.			
13.6	Mailbox backup and restore process tested.			
13.7	User Account Policy: (e.g. mailbox quota, allowed attachment types and max size, etc). What is the current policy and is it still appropriate?			

13.8	What is the change control policy inc. account creation and removal?			

MIS SERVERS (Management Information Systems)				
	For both internally and externally hosted MIS severs check the following where appropriate:			
14.1	What is the policy regarding administrative access to MIS servers (e.g. who has root access, is password access available or are ssh-keys demanded, etc)?			
14.2	Administrative access controls to MIS software (e.g. SIMS).			
14.3	Is Two-factor Authentication being used for all MIS users?			
14.4	Antivirus software installed and up-to-date.			
14.5	Operating system & MIS server software fully patched and up-to-date version.			
14.6	Backup regime tested.			

NON-CRITICAL SYSTEMS (inc Student and Guest systems)				
	Check the following where appropriate:			
15.1	Antivirus software installed and up-to-date.			
15.2	Administrative and User access controls are enforced and appropriate.			
15.3	Operating system & installed software fully patched and up-to-date versions.			
15.4	Backup regime appropriate and tested.			

REMOVABLE MEDIA				
16.1	What is the policy for the use of USB drives by students and staff. Where possible they should not be allowed at all. If this is not possible then we recommend only allowing after virus scanning on a dedicated, isolated computer.			

WIFI SECURITY				
17.1	Is the local WiFi secure? Consider network security (e.g. MAC address validation), separate sub-net, encryption, guest access, etc.			

GENERAL USERS				
	The following are covered above but are repeated here for completeness:			
18.1	Passwords: to reinforce the importance of password strength and security (i.e. how are passwords being created and managed), Password management software, 3-word system, changing, etc. (1.1)			
18.2	Access rights: Check all users have appropriate access rights. Users should be able to access only their own and common files. Privacy, confidentiality and security must be enforced by these controls. (1.2)			
18.3	Account maintenance policy. (2.4, 3.1			

NOTES

NOTES (cont...)

NOTES (cont...)

What threats am I protecting my school against and where do they come from?

Glossary of possible cyber threats:

The following are some of the types of cyber incident that could affect your school. It is not an exhaustive list but covers the most likely ones you should be aware of so you can protect yourself against them. More information on Cyber Security can be found in the companion NEN guidance note.

Port scanning

Port scanning is the systematic probing of an IP address for open ports. The IP probed may be your network firewall/router, a public facing server or, if the network has been compromised, an individual host. If a port responds to the probe information can then be gathered on the device from a range of other tools. So, while port scanning is not, in itself, a cyber incident such port scanning and associated information gathering can be the precursor to one.

Ransomware

WannaCry is one of the most familiar pieces of ransomware due to the recent, highly publicised incident experienced by the NHS. Schools have also been the victim of such attacks. See here.

Ransomware is a worm that once installed (typically by opening an email or running an attachment) encrypts all the files on the host and installs itself on other connected computers. Users are then instructed to pay a ransom (often in BitCoin) to have the files decrypted. Only if you have comprehensive, uninfected, backups can the files be retrieved.

Malware

The term Malware covers a whole range of software that is intended to do damage to either the hardware itself or the files on it. This Wikipedia article on Malware goes into more detail about the range of software covered by the term, some of the techniques used to get a user to install it, and its effects. For example, both “virus” and “trojan horse” are well known terms - both are malware but they differ in how they become active.

DoS/DDoS

A (Distributed) Denial of Service Attack is a general term for any attack designed to overwhelm a service (or host) with so many requests that other users cannot use it. For example, a typical DoS attack is one where a huge number of requests are targeted at a particular website so that its performance is very degraded or is crashed altogether. The Wikipedia article above goes into more details of the various methods of attack.

If you are the victim of a DoS attack always consider the possibility that it could be being used as a diversionary tactic to hide the real target of the attack. After such an attack the network should be thoroughly checked to see whether or not other breaches have occurred.

Data theft

An external incident may target information (typically school finance including supplier details and parental banking details in the case of private schools). It is also important to secure data from internal users who may have access to it: for example, staff may require access to student and parent records but their level of access should not, generally, include banking details nor the right to copy the database to a file.

Where are the threats likely to come from?

As well as appreciating the types of incident outlined above it is important to know the basic routes an attack may take to compromise your network - the "attack vectors".

The Internet

This is the most direct route - someone on another internet connected computer is trying to break into your system. In this case the firewall is your first line of defence. Only allow external access on required ports (e.g. 80/443 for internal web-servers) and hosts (e.g. traffic on port 80 should ONLY be allowed in to a dedicated web server or reverse proxy and blocked to all other hosts). Your firewall should be set up to control all inbound and outbound traffic with the default rule set to DENY.

Unauthorised access

Any unauthorised access should be taken very seriously. If the user is coming from an unexpected IP address, then this could indicate an external breach of the network and, potentially, a very serious cyber incident. In this case, you need to secure the network to block subsequent access and attempt to trace what actions have been taken, what servers/users have been compromised and take appropriate actions to secure them.

Internal users may also get unauthorised access either on purpose (i.e. they are making a concerted attempt to gain unauthorised access to a server) or by accident. In the latter case, the user or file permissions may need adjusting so that users can only access areas of the network that they are authorised to and that root (administrator) access is strictly limited to those users that require it and only on the devices they need it for.

Insider Breach

As noted above (*Unauthorised access*) not all cyber incidents are instigated by outsiders - there is always the possibility that local users may either (a) deliberately try to "hack" into the system to gain unauthorised access or introduce malware or, (b) do so my mistake.

Deliberate attempts can be mitigated by making sure user permissions are at the minimum level actually required for each user, password policies are in place and observed, and network security is generally sound including anti-virus software.

External/Removable Media

Although the rise of leaning platforms, remote access, and the increased use of cloud-based storage systems has reduced the needs for removable media there are still schools that use USB sticks to transfer files between school and home.

Removable media (primarily USB sticks or Drives but also CDs) are easily infected at home where there will be many fewer barriers (e.g. virus-infected web sites that are filtered in school will probably be accessible at home). A single infected file on a USB drive brought from home to school may compromise the entire school network. The use of these devices should be very strictly controlled. This should apply to staff as well as students.

They should certainly not be used to move personal data from school to home: access to personal data must be restricted and kept "on-site". If staff require access at home, then this should be made available via secure, remote access.

Web

Web-sites are another key vector - just browsing a site which contains malicious code can be enough to instigate a cyber incident as, for example, a java-script can be run as soon as the page is displayed in the browser which may install spyware or other malware.

Pupils (and staff?) like playing online games which makes them a particularly good way of enticing users into running a program which may contain malware.

This is where good filtering and anti-virus software is crucial for protecting the network.

Email

Perhaps the best known vector. It is very easy to click on an attachment from what appears to be a legitimate site or even a known contact. It is crucial, especially for administrative staff, to know how easy it is for the visible email address to be spoofed so any unknown or unexpected email attachment should be treated with care.

Anti-spam software running on the mail server will protect the user from much of the spam email but it cannot be 100% accurate so care must still be exercised.

Loss/theft of equipment

If hardware is lost or stolen any data on it (unless it has a fully encrypted hard-drive) may be vulnerable to abuse. For example, a contact list can be used to send spam email directed at, or masquerading as, a current email address.

Improper Usage

Any improper usage may also be used, either on purpose or inadvertently, to instigate an attack. For example, while USB access may be disabled for ordinary users, gaining administrator access may allow a memory stick to be read and an infected file uploaded.

Attrition

This refers to any attack that uses brute force methods to compromise or degrade the target system - typical examples being a DoS attack or probing for username/password pairs.