Cyber Security Guidance for Schools

Management Summary

Schools are very reliant on a wide range of internet based services for day-to-day operations and activities but such reliance brings with it certain risks.

This Guidance provides Senior Managers and Governors with (1) a broad overview of the range of online threats that an internet connection exposes their schools to, and (2) directs them to tools which can be used to develop a robust cybersecurity policy to avoid or mitigate these risks.

Critically, it is essential that schools understand how their network is protected, and by whom, if security incidents are to be understood and dealt with effectively.

Drawing heavily on two particular organisations - the National Cyber Security Centre (NCSC, part of GCHQ) and Centre for Internet Security (CIS) - this guidance provides the education context for the detailed, generally business oriented, advice available online.

A quote from the NCSC that is well worth bearing in mind in all discussions about cybersecurity is:

> *All organisations have something of value that is worth something to others. If you openly demonstrate weaknesses in your approach to cybersecurity by failing to do the basics, you will experience some form of cyber incident.*

Whether you run a school, university, SME or multinational you have something of value which may provide the incentive for an attack. And everyone is likely to experience an cybersecurity incident at some point: good cybersecurity will make an attack less likely to succeed and will mitigate the impact of any cyber related incident.

Two specific sets of documents are referred to in this Guidance (10 Steps to Cyber Security and 20 Controls) which cover all facets of a comprehensive approach to cybersecurity. This may take the form of a dedicated policy document or embedding it into other documents as appropriate (e.g. the Acceptable Use Policy).

While 10-steps offers a very readable overview, the 20-controls are aimed at the IT professionals charged with implementing cybersecurity and provide fine-grained, detailed,

advice. We have, in addition, provided extra details in two specific areas - firewalls and email - which we feel have their own particular issues within schools.

Being aware of the range of cybersecurity threats will enable senior managers to ask appropriate questions of the staff responsible for these areas, be they in-house or third party providers, and to ensure they have a robust cybersecurity strategy in place.

The thread landscape is outlined with reference to the NCSC's detailed paper - Common Cyber Attacks - where they note the different skills sets of attackers and define targeted and un-targeted attacks. The reported rise in cybercrime against Academy Trusts, in particular, and schools more generally is also noted.

A high percentage of attempted attacks can be avoided by basic cybersecurity measures: the NCSC's Cyber Essentials website provides advice on these basic measures and a certification process for organisations to demonstrated their good practice. This certification also provides a benchmark when looking to engage third party IT service providers.

There then follows an outline of the NCSC's "10 Steps". Each of the steps is briefly explained with some education context and a link to the full documentation. Addressing each of these areas in a school will go a long way to reducing the possibility of suffering a cyber incident and, at the very least, mitigating its effect.

Once an approach to cybersecurity has been agreed there is still the challenge of implementing it. This could take the form of a dedicated cybersecurity policy document, or by embedding statements, as appropriate, in other policy documents - such as the Acceptable Use Policy, for example.

A cybersecurity policy (however documented) cannot be static: it must be managed, maintained and reviewed in the light of new and emerging issues and risks. Depending on the skills available this management may be undertaken by in-house staff or, for example, by a third party as part of the school's general IT support.

An appreciation of the wider network - e.g. the fact that many other schools are likely to be connected to the same local authority or RBC - emphasises the need to protect not just your own school but the others on the same, wider, network. A virus introduced into your network could, for example, then go on to infect all schools connected through the same provider.

In addition to the technical aspects of implementing a cybersecurity policy, the importance of encouraging a cybersecurity "mindset" in staff and students through engagement and training is also emphasised.

The NCSC has assisted in the review of this guidance.

Cyber Security Guidance for Schools

Introduction

Schools, just like other commercial and public sector institutions, are reliant upon both their local IT systems and networked services delivered over their broadband connection for day-to-day operations and activities. While these technologies bring a huge range of opportunities and benefits, they also bring risks.

The most common are shown in this infographic from the National Cyber Security Centre (NCSC) site and covered in more detail in their Common cyber attacks: reducing the impact paper (2016) where they note that every organisation is a potential victim - and schools are no exception:

> *All organisations have something of value that is worth something to others. If you openly demonstrate weaknesses in your approach to cybersecurity by failing to do the basics, you will experience some form of cyber attack. (p5)*

In addition, the NCSC have recently (June, 2019) produced two new sets of guidance for small and medium sized organisations, which would include schools and Academy Trusts. These cover Cyber Security in general and, if you are unfortunate enough to suffer an incident, how best to respond and recover.

To avoid becoming a victim - or at least reduce the chances and mitigate the impact of an attack - schools need to put appropriate mechanisms in place to maintain the integrity and availability of their network services and resources. The evidence is that attacks are increasing in both number and complexity.

And it is very easy to become the victim of an attack.

For example, recently (March, 2019) GCSE coursework was lost in a cyber attack on a school in Bridport and the government, also in March 2019, sent a reminder to all Academy Trusts about the risk of fraud as there has been a "…significant increase in incidents of cybercrime against academy trusts in the past year…".

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, intentionally or otherwise.

This document, intended for school leaders, provides an overview of how schools should

manage their cybersecurity in a “big-picture” sense. Being aware of the issues, the range of threats, and the techniques used to protect the network should enable them to ask appropriate questions of the staff responsible for these areas be they in-house or third party providers. Links to other information are embedded in the document and a list of useful links is provided at the end.

It should also allow them to appreciate, and be sympathetic to, requests from their network staff for increased security measures. For example, staff may, if unaware of the security benefits, perceive two factor authentication as merely an inconvenience.

It is essential that schools understand how their network is protected, and by whom, if incidents are to be understood and dealt with effectively.

Structure and Purpose

The aim of this guidance document is twofold:

- to provide senior managers with a broad overview of the range of cyber threats, which any organisation is open to when they use networked services over a broadband connection and

- to direct senior managers to tools which can be used to develop and document an approach to cybersecurity which protects themselves, their school, and their users. This may take the form of a dedicated cybersecurity policy document, or by embedding statements, as appropriate, in other policy documents - such as the Acceptable Use Policy, for example. Further references to a cybersecurity policy should be taken to cover both these possible formats.

We do not intend to repeat the often excellent, detailed advice already available from various organisation but to bring some of it together in an accessible form. All online advice is, by definition, general advice and unlikely to be a perfect fit for any particular school. It is important, therefore, that schools take care to consider their own environment when deciding what advice to act upon.

This guidance draws heavily on two particular organisations: the National Cyber Security Centre (NCSC) and the Centre for Internet Security (CIS).

The NCSC is part of the Government Communications Headquarters (universally known as GCHQ) which "*…is part of the team which protects the UK, along with law enforcement and the other intelligence agencies. Working with HMG and industry, we defend Government systems from cyber threat, provide support to the Armed Forces and strive to keep the public safe, in real life and online.*" [What we do]

The Centre for Internet security (CIS) is an international, non profit organisation which developed and maintains the CIS Controls - the global standard and recognised best practice for securing IT systems and data against the cyber attacks. These proven guidelines are continuously refined and verified by a global, volunteer community of experienced IT professionals.

In particular we refer to the NCSC's The 10 Steps to Cyber Security and the CIS Controls. Both these tools, while couched in business terminology is just as appropriate for any managed IT environment which, of course, includes schools and others in Education.

The 10-steps documentation provides a high level overview of what general areas need to be considered in putting together a cybersecurity policy. This is complemented by the CIS Controls which give much finer grained, specific advice and recommendations for IT the professionals charged with implementing cybersecurity under each of the twenty areas they define.

By highlighting how particular elements of these tools apply in the school/education context, this guidance will assist schools develop an appropriate and effective security policy combining the key elements of pro-active preventative actions; a reliable, tested backup regime; and user education. While such a policy will not guarantee a school will not suffer an attack it will mitigate the damage if one does occur.

The Threat Landscape

The NCSC's Common cyber attacks: reducing the impact paper (2018)[download the full pdf] and their more recently produced (March 2019) Board Tookit both provide useful information on various types of threat. In particular, they make the distinction between those based on well known and understood techniques which can be guarded against and the highly sophisticated attacks using advanced methods to access well defended networks which are very much rarer. Schools are unlikely to be the target of such an attach which requires considerable, sustained effort to undertake.

It is important to appreciate this point: the majority of attacks can be prevented by the proper implementation of the basic cybersecurity principles outlined in The 10 Steps to Cyber Security and the Cyber Essentials (also provided by the NCSC) website.

A further distinction is made between Targeted and Un-targeted attacks. Un-targeted attacked are where the attack is indiscriminate and has no particular target in mind. So, for example, sending phishing emails to a large number of people asking for sensitive information or scanning large numbers of random devices looking for vulnerabilities.

Targeted attacks, on the other hand, are against a specific individual or organisation: perhaps the attackers have a particular interest in your school or are being paid to attack it. This is, probably, less likely in the schools' context but not impossible. See, for example, this story quoted in the TES (Jan, 2018). Similarly, the reported rise in cybercrime against Academy Trusts are likely to be mainly targeted attacks which could have severe consequences for the Trust.

The most common forms of targeted attacks are DDoS (Distributed Denial of Service), targeted phishing emails, "spear-phishing", and social engineering (for example, telephone calls purporting to come from an official source requesting information then used in a cyber attack). Schools should ensure that all administration staff are aware of this type of fraud, and that parents are also advised to be vigilant and to scrutinise requests to amend payment procedures.

Cyber Essentials

One of the services offered by the NCSC is their Cyber Essentials website which provides both basic, simple to follow advice on cyber security and a path to certification. As part of GCHQ the Cyber Essential Certification is Government backed scheme and designed to help organisations, of whatever size, protect themselves against a whole range of the most common cyber attacks.

Cyber attacks come in many shapes and sizes, but the vast majority are quite straightforward in nature and carried out by relatively unskilled individuals: the digital equivalent of a thief trying your front door to see if it is unlocked.

Their advice is designed to prevent these attacks and explains in more detail five fundamental steps to making your organisation more secure:

1) Use a firewall to secure your internet connection

2) Choose the most secure settings for your devices and software

3) Control who has access to your data and services

4) Protect yourself from viruses and other malware

5) Keep your devices and software up to date.

A Conclusion and Checklist that you can use to check your current understanding is also provided. The explanations under each of the five headings includes reference to what is required to gain the Cyber Essentials Certification.

By working towards the Cyber Essentials Certification you show your stakeholders that you take cybersecurity seriously, and provide yourself with some reassurance that you are making your organisation more secure. You can also use their Directory to check whether third party suppliers are themselves certified.

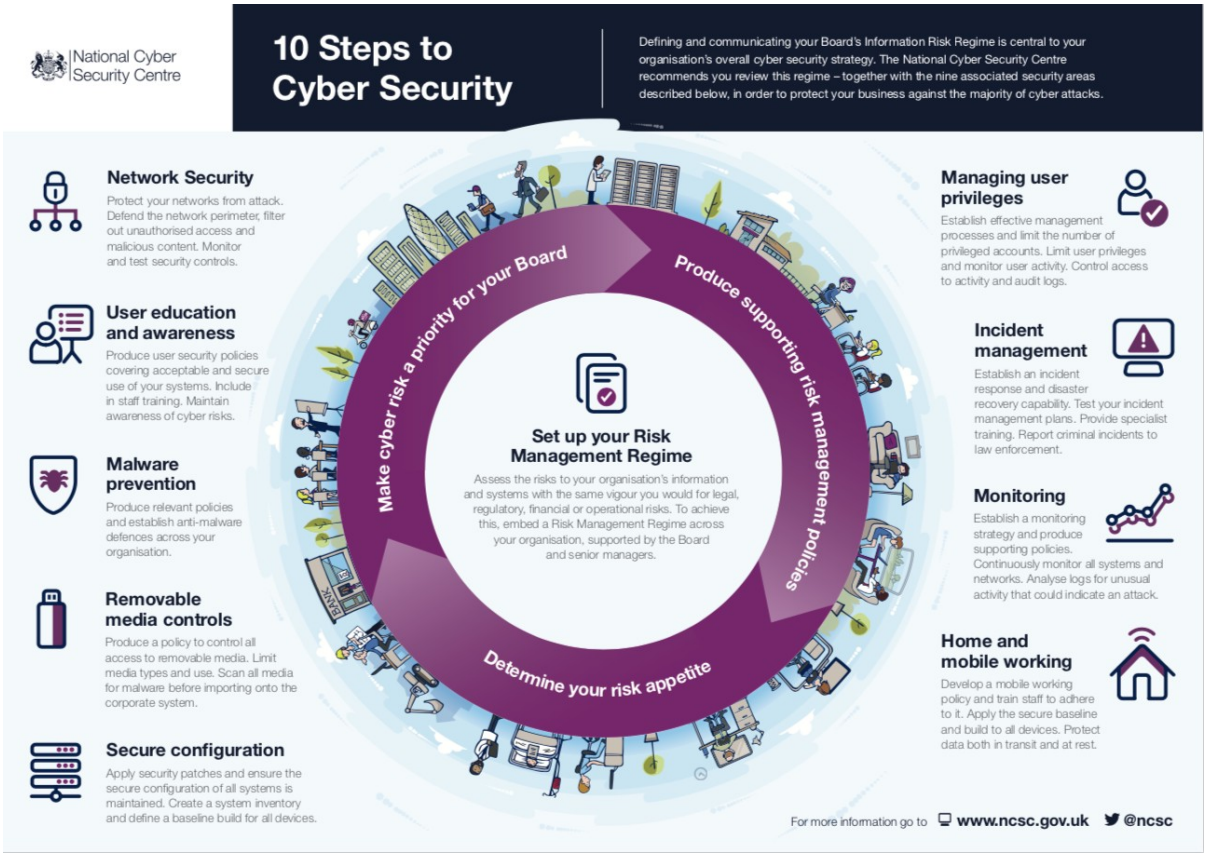
Certification can either by via a self assessment questionnaire or, for Cyber Essentials Plus, the mitigations in place will be validated by an independent certification body.

Ten steps for managing cybersecurity

While the Cyber Essentials advice and certification process offers basic advice a more detailed and comprehensive cyber security strategy is provided by the NCSC in their collection of webpages under the heading 10 Steps to Cyber Security.

There is an Executive Summary which provides a quick overview of the 10 steps and more detailed technical advice sheets covering each step. Each sheet is written in relatively accessible language and in "high level" terms for business managers rather than being deeply technical. However, they cover each step in very generic terms which may be difficult to interpret in the school context with its wide variety of interested parties - students, parents, administrators, teaching staff, governors, and range of third party providers from technical support to examination boards.

That being said, these 10-steps do provide a helpful framework for implementing a cybersecurity policy and are just as relevant to schools as to other organisation that need to keep their network services, data and users secure.



Source:https://s3.eu-west-1.amazonaws.com/ncsc-content/files/NCSC%2010%20Steps%20To%20Cyber%20Security%20NCSC.pdf

The following provides links to each of the advice webpages together with some school-related context.

1. Information risk management regime

This involves recognising that senior management and governors are responsible for settings the overall approach to cybersecurity. They must ensure it is implemented and documented appropriately, and that all users (both staff and student) understand and adhere to it.

This cybersecurity policy should sets out the approach for managing risks, issues and incidents and be regularly reviewed. It should also inform, or be part of, the school's IT acceptable use policy (AUP); this is a key document which should set out everything end users need to know in an accessible way.

2. Secure configuration

This means, for example, keeping an inventory of all school IT hardware and software, and making sure that policies and procedures are in place to ensure all changes (e.g. configuration changes, new software installations, etc) are authorised, documented and implemented appropriately. These inventories should include all school hardware and software, including school-provided mobile phones which need to be kept secure through locking and password policies and regularly updated to the latest operating system.

Processes should be established for monitoring and updating 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".

All hardware, operating systems and software should be "locked down" to prevent user access to settings or facilities which could compromise network security, either maliciously or accidentally - e.g. system network settings.

3. Home and mobile working

Pupils and staff need to be able to access school systems remotely from a range of devices, in order to extend learning opportunities or support administrative functions. The use of staff laptops at home brings with it the risk of unauthorised access to, and loss of, sensitive information when used off the school network. This may be through access to data stored directly on the laptop or, via the remote access client, to data stored on the school network itself.

Staff may also use their own laptops or mobile phones which may be less secure in terms of passwords, multiple users, etc. If these are to be allowed to remotely access the school's data then special consideration will need to be given to how best to achieve this in a secure manner.

User education is paramount in this area; technical strategies should include encrypting

school-owned devices to prevent unauthorised access and use. Schools must 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.

4. Incident management

The nature and range of issues and threats suggests that all schools will experience a cybersecurity incident at some point. Having plans and procedures in place for logging, reporting, monitoring and dealing with incidents will minimise any damage or disruption. While it is good to have a plan, it is difficult to test or realistically practice it. The NCSC's free Exercise in a Box can help by providing a range of exercises you can take in your own time and in a safe environment to test your school's response to a cyber incident. It offers table-top exercises as well as simulated exercises for more technical staff.

Mitigation of risk can take many forms including, among others, specialist training, data backup and recovery testing, etc. Each of these will incur some level of expense and individual schools will need to weigh up the cost against the potential benefit of any action they consider in their particular circumstances.

After an incident has been dealt with there should be a recognised process for discovering what happened, how, and what damage was done so that lessons can be a learned. This may lead to, for example, device configuration changes, software upgrades, and/or security process changes.

The process for the internal management of any incident is important for reducing its impact and learning lessons but the wider community must also be considered. For anything but the most trivial of incidents the process must include reporting outside the school: the local authority or Academy Trust, for example. Incidents involving data theft or compromise may need to reported to the ICO (Information Commissioner's Office). More serious incidents, particularly those incurring a financial cost, should be reported to the police at Action Fraud.

5. 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. It can proliferate in many ways, for example, via email attachments, cloud based storage, social media platforms, malicious websites or removable media.

The risks from malware can be mitigated by, for example, using antivirus and malware scanning software, web filtering to block access to known malicious websites and encouraging appropriate user behaviours in accordance with the AUP.

This video "Top Tips for Staff" from the NCSC may be a useful resource for staff cyber awareness training and is free to pull into local learning management systems.

6. Managing user privileges

Controlling what individual users can and cannot do is crucial to keeping the network secure. User privileges need to be differentiated (e.g. IT staff, teaching staff and students clearly have divergent needs for access) and set appropriately so that all users can access the data and facilities they do require but not those they do not need.

There should be procedures for creating, managing and deleting user accounts. Automated user provisioning systems can provide a way to manage user accounts, including automatically deleting the accounts of users that have left the school.

Password management processes and policies can ensure that passwords are strong. There is the NCSC's advice on password administration including a guide to password managers (1Password, is just one example) which may be considered for both staff and pupils to manage multiple passwords. Most also provide the facility to generate strong passwords. The "three-random-word" technique can often prove a popular, 'user-friendly' way to generate a secure password: many password managers can suggest these.

Monitoring user activity is also important. It is advisable to inform all users that their network usage may be monitored: the key document for this is the school's IT acceptable use policy (AUP). It is essential that all users are aware of, and understand, the AUP which should be regularly reviewed and updated.

7. Monitoring

Monitoring systems, network traffic and user activity allows attacks and other cybersecurity incidents to be quickly detected and responded to. It is important to preserve event logs as potential evidence in dealing with any, as yet undiscovered, breach.

It is essential that key individuals are tasked with reviewing the output of any monitoring systems and responding to alarms and alerts. Reports, logs and alarms are all useless if no one is responsible, or has the time, to look at or respond to them. For example, repeated failed remote log-in attempts to a server may indicate a 'brute force' attack is underway. If an alert is generated and acted upon at this point the threat can be averted.

8. Network security

A school's broadband connection(s) to the internet (provided by the local authority, regional broadband consortium, or commercial ISP) can be the route of an attack. Cloud services and mobile/remote working provide external access to the local network which could be utilised for an attack. Policies and technologies should be implemented to reduce the likelihood of

such an external attack.

Both external and internal attacks must be considered with security controls in place to protect against both by:

(a) managing the network perimeter through the use of firewalls to prevent intrusion and other software/hardware (e.g. anti-malware, anti-virus, web-content filtering, email-filtering, etc.) to prevent malicious content being imported into the network.

(b) protecting the internal network by monitoring activity, dividing the network (especially separating and securing wi-fi access for internal users and guests), secure administration practices (e.g. reviewing access logs, deleting the accounts of former staff and pupils), etc.

It is important to remember that a security incident in one school could have an impact on many other schools and organisations. For example, a successful denial of service attack against one school may flood a local authority or regional network with traffic, affecting many schools although only one was targeted. Schools, therefore, not only have responsibilities in relation to their own users but to other schools and institutions they share network services and infrastructure with. It is thus doubly important that all security software and devices are maintained regularly with an agreed procedure to ensure the most up-to-date patches/upgrades/updates are applied in a timely manner. Many applications and operating systems provide for automated updates so little intervention is required other than its initial configuration.

How to ensure security across multi-site schools that share a single network also needs to be considered. Whilst collaboration between such sites is important it must be implemented in a way that does not compromise overall network security.

Similarly, schools will need to consider how to provision wireless network access for guests. Typically, users of this type of service should be prevented from accessing certain internal resources (shared storage areas, for example). This is often achieved by separating such "open" wireless networks from the rest of the network: both wireless and wired. For example, virtual local area networks (VLANs) can be employed to group and manage wireless access points and users appropriately.

9. Removable media controls

Removable media (USB drives, for example) provide a common route for the introduction of inappropriate content into the network (including pornographic images and malware) and the accidental or deliberate export of sensitive data.

It is very important to control what can enter and leave the school via removable media and personal devices, so schools should be clear about any business/educational need to use removable media and apply appropriate security controls.

In addition to sensible limits on the general use of removable media there should be restrictions set on sensitive data itself being copied onto **any** other device. Holding such data centrally negates the need for it to be copied or moved. As such a central store will be an absolutely critical resource for the school access to it, both remotely and locally, will need to be provided in a very secure manner.

10. User education and awareness

Educating and training is essential so that all users understand their cybersecurity obligations and responsibilities but in the context of a "no blame" culture (See A positive security culture). All users, whether staff or pupils, should feel secure in the knowledge that being open when things go wrong will not result in sanctions but be used to improve the network's security. Sanctions should only be considered where there was intent to cause harm - but this is rarely the case.

All new users (whether staff or pupils) should have some induction training as soon as possible.

While specifically about primary schools the Shipton Report Improving e-safety in primary schools (2011) provides useful advice applicable to all schools on both staff training and on getting the message across to students and parents (pp8-12).

As well as teaching students about cybersecurity as a "consumer" it is also useful to provide technical security training material which reinforces the message that computer systems can be compromised and you need to protect yourself. Such training can also encourage those students interested in IT to see cybersecurity as a possible career path. Cyber Security Challenge UK provides training material, events, and competitions at school, FE and HE level with sponsorship from both government and industry.

Cyberfirst is a scheme run by GCHQ and NCSC, launched in 2016 originally for university students and 11-19 year olds to explore their passion for tech by introducing them to the world of cyber security. The net is wider now with opportunities for older adults as well!

As stated above, (4), schools should have a user security policy embedded within their AUP. As new threats continue to emerge, these 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 the school network (staff remote access to the school management information system, for example).

Schools should, as noted above, encourage a positive, just cybersecurity culture: the key is ensuring that everyone understands the risks, their own responsibilities in relation to them and feels comfortable sharing any concerns they may have with those in authority.

How to get started

The Centre for Internet Security (CIS) produces a set of 20 Controls (Version 7 at the time of writing) that, to quote from the introduction,

> *… are a prioritised set of actions that collectively form a defence-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defence, and others.*

The CIS Controls are divided into three broad categories - Basic ("Cyber Hygiene"), Foundational, and Organisational. Where the 10 steps provide a relatively broad brush approach to understanding the tasks and processes required to implement a Cybersecurity strategy the 20 CIS Controls provide a much more detailed and, with the supporting documentation, technical breakdown of each element.

The complexity of developing a full, effective, cybersecurity strategy can easily overwhelm the limited resources (both technical and managerial) available to schools. Taken together the 10 Steps and CIS Controls documents can help break the problem down into manageable chucks which can be implemented over time.

The first six of the CIS Controls (Basic) provide a good starting point:

> "*CIS Controls 1 through 6 are essential to success and should be considered among the very first things to be done. We refer to these as "Cyber Hygiene" – the basic things that you must do to create a strong foundation for your defence.*" [CIS controls]

1. **Inventory and Control of Hardware Assets**: Actively manage all hardware devices on the network so that only authorised devices are given access, and unauthorised and unmanaged devices are discovered and prevented from gaining access.

   Staff or pupils using their own devices need special consideration in that they can be authorised (by registering a MAC address with the network, for example) but are not directly managed. However, some specific requirements (e.g. insisting on the installation of approved anti-virus software) can be set before the device is authorised. "Guest" devices can be given limited access (e.g. to a separate, dedicated Wi-Fi network with internet access only).
2. **Inventory and Control of Software Assets**: Actively manage all software on the network so that only authorised software is installed and can execute, and that unauthorised software is found and prevented from installation or execution.

3. **Continuous Vulnerability Management**: Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimise the window of opportunity for attackers: for example, patch systems and software as soon as possible and use automatic updating where possible. When outdated systems can no longer be patched any benefit from using the legacy software must be carefully weighed again the risk of compromise.
4. **Controlled use of Administrative Privileges**: The misuse of administrative privileges (e.g. using the 'root' user to perform mundane tasks) is a primary method for attackers to spread inside a network. The more extensively administrative rights are distributed among users and used to carry out tasks which do not require such a high level of access, the greater the likelihood the privilege will be compromised at some point.
5. **Secure Configuration for Hardware and Software on all devices**: Establish, implement, and actively manage the security configuration of all devices which connect to the network using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. For example, network settings (IP address, gateway, web proxy, etc) should be set automatically and not modifiable by a user.
6. **Maintenance, Monitoring and Analysis of Audit Logs**: Collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack.

Whilst these Basic controls offer a helpful starting point it is important that a school's cybersecurity policy encompasses all of the 10 steps described previously. The CIS 20 Controls document offers more technical detail for school network managers on how the principles and processes set out in the 10 steps can be implemented.

Managing and maintaining firewalls in schools

Every establishment with a broadband connection to the internet requires a firewall in order to prevent unauthorised external access to its data and systems.

There may be some debate as to whether an individual school requires a dedicated, local firewall **if their broadband connection is to a trusted network** (their Local Authority or Regional Broadband Consortium, for example) which connects to the internet and provides a robust firewall service. In these case, it may be argued, the school's local network is adequately protected and does not need its own firewall. While this may be appropriate for small schools without dedicated IT staff it is unlikely to be satisfactory for larger ones where what data going in and out of their network should be understood.

If the broadband connection is via a commercial ISP then a well managed local firewall will be essential.

Typically, firewalls are either deployed as:

- **a centralised service**, in which the firewall is on the network that the school's broadband service connects to (e.g. Local Authority, or Regional Broadband Consortium); or

- **locally**, where the firewall is on the school's own premises as either a dedicated network device or part of another service (e.g gateway or filtering server).

Firewalls are complex systems that require management in order to deliver the appropriate level of security and protection from external threats. They may also require 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 and are documented through an approval process.

If your firewall is managed on your behalf by a third party then you need to reassure yourself that:

- the service level agreement (SLA) provided by the organisation documents that changes and updates to the firewall's configuration will be logged by authorised users within the establishment, and undertaken quickly enough to maintain operational effectiveness within the school. Additionally, it should provide for patches and fixes to be applied within a short period of time to ensure that new vulnerabilities are not exposed;

- the expertise and experience of the engineering team providing the service are suitably supported by a robust change management methodology to ensure changes are not made without an appropriate level of assessment, testing, and documentation.

Schools may also consider enabling or installing software firewalls on individual servers to provide an additional layer of protection.

Additional cybersecurity 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. Any of these measures will incur costs to a greater or lesser degree which must be considered when assessing their potential usefulness.

Such measures may include:

- Intrusion Detection/Prevention Systems
- Heuristic Threat Analysis
- Penetration Testing

The extent to which any of them are considered will depend 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.

Email security

There is a range of estimates for the percentage of emails which are spam - for example, Talos Intelligence estimate 85% of emails sent in January 2019 were spam, whereas Symantec's 2018 Internet Security Threat Report (pdf) puts the figure at 54.6% - but, whichever percentage you agree with, there is no doubt that the ubiquity of email and its extremely low cost, continue to make it a common medium for transmitting threats.

A variety of threats use email as their delivery mechanism including: malware, ransomware, and phishing. While mail security technology can be employed to detect and block the majority messages designed to try to exploit users it only takes one to bypass these systems for a potentially damaging incident to take place (see this BBC report, for example). It is essential that any technological solutions are kept up to date in order to maintain accurate details of the sources, signatures and techniques used by spammers and minimise the probability of their success.

As noted above (Secure Configuration) the risk of malware being installed on purpose or by accident can be reduced by ensuring systems are "locked down" so that non-administrative users cannot install **any** software. Similarly, the auto-running of specific files types should be prevented either at the browser level or, if accessing email via a web-browser, by blocking the files themselves through a web-filter.

While dedicated email clients are still used (MS Outlook, for example) many users now access their email via a web browser. This being the case, it is essential that only the most recent browser versions are deployed within the school and are regularly patched and updated.

Most popular browsers employ a database of phishing and/or malware sites to protect against the most common threats. These filters should be enabled by default and locked so users cannot turn them off.

Similarly popup blockers should be turned on (specific, trusted sites can be made exceptions, as required) because popups are not only annoying, they can also host embedded malware directly or lure users into clicking on something using social engineering tricks. DNS filtering services can also block attempts to access these websites at the network level.

Email represents one of the most interactive ways humans work with computers - which makes it an ideal method of attack - so encouraging the right behaviour is just as important as the technical settings. However, as phishing emails become more sophisticated ordinary users cannot be expected to be able to identify every one: so software must be employed to block these emails before they even reach email server and the users' mailboxes.

Microsoft's Office365 web-based email system has become a target for email scams as it is the system most widely used by both teaching and administrative staff in the UK's schools.

Others do exist and suffer similar problems. There have been instances of user passwords being compromised resulting in, for example, email forwarding rules being added to mailboxes which target emails containing financial details and forward them to the hackers.

Another result of a cybersecurity breach may be to compromise the mail server or its clients so that they become generators of spam emails: if a site or email address is identified as a 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 that appropriate measures are in place to ensure that this does not happen to your school. For example, email should only be allowed out of the network from a dedicated mail server, and monitoring outgoing traffic so that sudden spikes in can be identified and blocked. You should also check that your service provider has the correct measures in place to reduce the risk to the global community.

Educating users about passwords (as noted above) is not only important for local network security but also for email accounts. Ensuring users do not apply simple passwords is an important way of protecting email systems from threats; “brute force” attacks are used by attackers attempting to access email accounts using a list of thousands of common passwords, so setting more complex passwords, three random words, or pass-phrases, helps to keep accounts secure.

In relation to phishing JISC offer simulated phishing and awareness training via KHIPU who also offer other cybersecurity related services in partnership with JISC.

CIS Control 7 is specifically about Email and Web Browser protection and the full, downloadable documentation provides extensive details on the preventative steps that may be taken.

Conclusion

All schools need to ensure they have an appropriate cybersecurity strategy in place to ensure the integrity of their data, networks and systems: regardless of whether they procure and manage their own broadband services or subscribe to those provided by a Local Authority or Regional Broadband Consortium (RBC).

The approach a school takes to cybersecurity issues and how it is documented is not static. As threats and personnel change over time so the approach must change: it must be managed, maintained and reviewed in the light of new and emerging issues and risks.

Key to managing cybersecurity is understanding where the responsibilities for different aspects reside. To some extent, who is responsible for controlling them will differ depending upon the school's circumstances and level of in-house expertise. Of course, the ultimate responsibility will always reside with the Senior Management Team but small schools may choose, or need, to delegate these responsibilities to others: for example, a local firewall managed by a trusted third party.

Local authorities and RBCs provide cybersecurity protection as part of the services they provide to schools.

Finally, as noted in the introduction, it is essential that schools understand how their network is protected, and by whom, if incidents are to be understood and dealt with effectively.

The NCSC has assisted in the review of this guidance.

Sources of further advice

(1) Nation Cyber Security Centre
https://www.ncsc.gov.uk
Annual Review 2017 [pdf]
Information for small to medium-sized organisations
Recent Incidents Report (changes regularly)
Response and Recovery Guide
Exercise in a Box
10-steps to cyber Security
TopTips for Staff

(2) GCHQ
https://www.gchq.gov.uk/
CyberFirst

(3) Common cyber attacks: reducing the impact (pdf)

(4) Cyber Essentials Website
https://www.cyberessentials.ncsc.gov.uk/

(5) Centre for Internet Security (CIS Controls v7)
https://www.cisecurity.org/controls/

(6) Symantec 2018 Internet Security Report (pdf)
https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

(7) Phishing Statistics
https://blog.barkly.com/phishing-statistics-2018

(8) JISC simulated Phishing and Awareness Training
https://www.khipu-networks.com/news/jisc-framework-simulated-phishing-associated-awareness-training-services/

(9) Action Fraud
https://www.actionfraud.police.uk/

(10) Get Safe Online
https://www.getsafeonline.org/

(11) Cyber Streetwise
https://www.cyberstreetwise.com

(12) National Crime Agency
http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime

(13) Home Office:
https://www.cyberaware.gov.uk/

(14) Information Commissioner's Office
https://ico.org.uk/for-organisations/report-a-breach/