Cyber Security Guidance for Schools

What if you have a Cyber Incident?

Introduction

This guidance document should be read in conjunction with the NEN's Cyber Security Guidance which outlines the online threats schools face and provides guidance on what can be done to reduce the risk of becoming a victim.

Here we chiefly discuss what to do if you find yourself caught up in a cyber incident.

Any school can fall victim to a cyber incident regardless of its size. Schools are perceived to be soft targets due to the low levels of cyber security some of them employ. They also hold sensitive personal data on staff, pupils and parents that can be valuable to attackers, and have financial assets and processes that can be exploited by criminals to steal money.

Their networks are also used by many different users and devices, including pupils who might wish to look for a readymade network to practice their cyber skills on.

A school may also suffer an incident where they are not the explicit target but are just caught up in a more generalised, non-targeted attack (e.g. DDoS or ransomware) or because they are using a particular piece of vulnerable technology.

The basic outline of this guidance is taken from the NCSC's Response and Recovery Small Business Guide, but written specifically for schools and Academies.

The five stages identified in the NSCS document are, however, just as relevant to schools as they are to small business.

1. Prepare for an incident so you know what to do if one happens.

2. Identify what is happening so you can work out the steps required to stop it.

3. Resolve - take the actions identified above to stop whatever is happening, repair any affected systems, and restore any affected data.

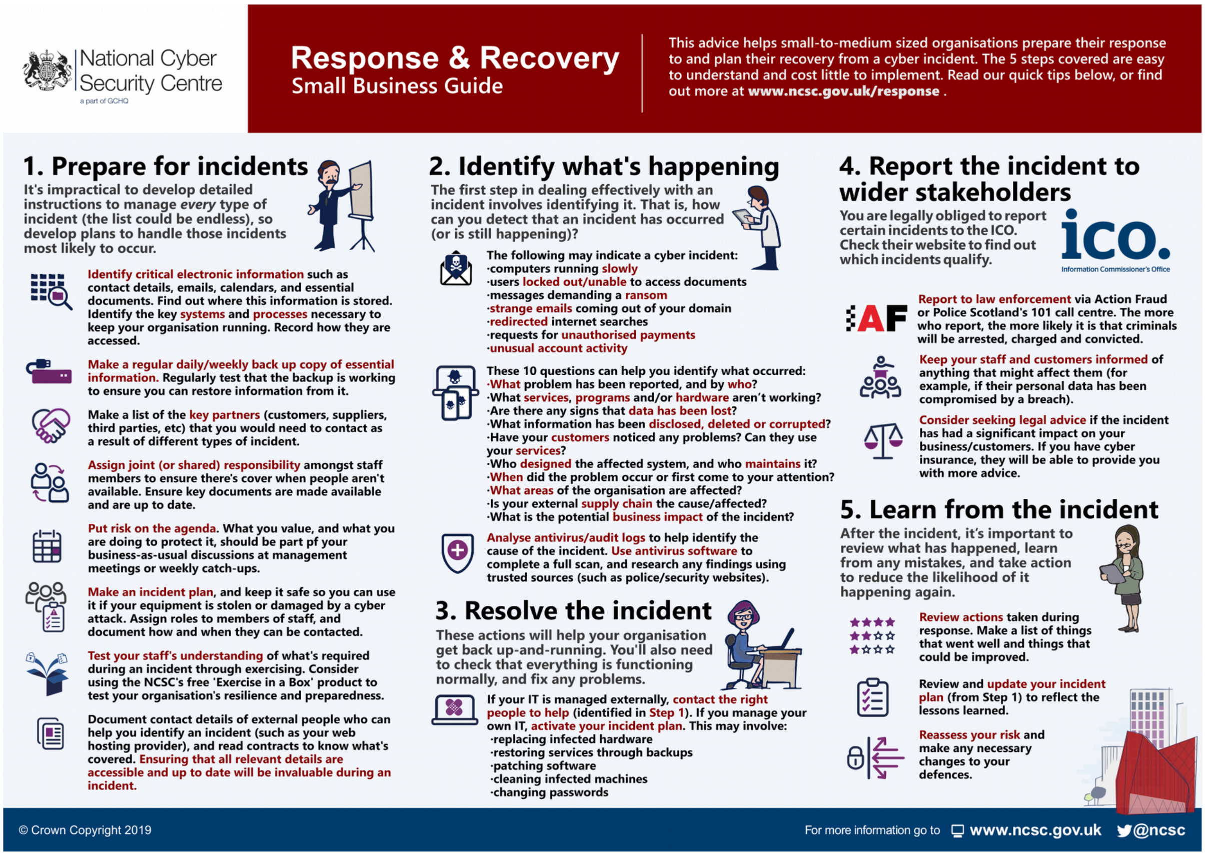
4. Report the incident to the appropriate stakeholders and authorities. A cyber attack is a crime and should be reported to the Police - usually, this is either to Action Fraud or, in Scotland, the Police Scotland call centre on 101.

5. Learn from the incident. What could have been done to prevent the incident from happening at all? Could the response have been better?

Each of these stages will be covered in more detail below.

Stages of an incident

The “life-cycle” of all cyber incidents is essentially the same and can be broken down into the five stages identified in the graphic below.



National Cyber Security Centre
a part of GCHQ

Response & Recovery
Small Business Guide

This advice helps small-to-medium sized organisations prepare their response to and plan their recovery from a cyber incident. The 5 steps covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/response** .

1. Prepare for incidents

It's impractical to develop detailed instructions to manage *every* type of incident (the list could be endless), so develop plans to handle those incidents most likely to occur.

Identify critical electronic information such as contact details, emails, calendars, and essential documents. Find out where this information is stored. Identify the key systems and processes necessary to keep your organisation running. Record how they are accessed.

Make a regular daily/weekly back up copy of essential information. Regularly test that the backup is working to ensure you can restore information from it.

Make a list of the key partners (customers, suppliers, third parties, etc) that you would need to contact as a result of different types of incident.

Assign joint (or shared) responsibility amongst staff members to ensure there's cover when people aren't available. Ensure key documents are made available and are up to date.

Put risk on the agenda. What you value, and what you are doing to protect it, should be part pf your business-as-usual discussions at management meetings or weekly catch-ups.

Make an incident plan, and keep it safe so you can use it if your equipment is stolen or damaged by a cyber attack. Assign roles to members of staff, and document how and when they can be contacted.

Test your staff's understanding of what's required during an incident through exercising. Consider using the NCSC's free 'Exercise in a Box' product to test your organisation's resilience and preparedness.

Document contact details of external people who can help you identify an incident (such as your web hosting provider), and read contracts to know what's covered. Ensuring that all relevant details are accessible and up to date will be invaluable during an incident.

2. Identify what's happening

The first step in dealing effectively with an incident involves identifying it. That is, how can you detect that an incident has occurred (or is still happening)?

The following may indicate a cyber incident:
·computers running slowly
·users locked out/unable to access documents
·messages demanding a ransom
·strange emails coming out of your domain
·redirected internet searches
·requests for unauthorised payments
·unusual account activity

These 10 questions can help you identify what occurred:
·What problem has been reported, and by who?
·What services, programs and/or hardware aren’t working?
·Are there any signs that data has been lost?
·What information has been disclosed, deleted or corrupted?
·Have your customers noticed any problems? Can they use your services?
·Who designed the affected system, and who maintains it?
·When did the problem occur or first come to your attention?
·What areas of the organisation are affected?
·Is your external supply chain the cause/affected?
·What is the potential business impact of the incident?

Analyse antivirus/audit logs to help identify the cause of the incident. Use antivirus software to complete a full scan, and research any findings using trusted sources (such as police/security websites).

3. Resolve the incident

These actions will help your organisation get back up-and-running. You'll also need to check that everything is functioning normally, and fix any problems.

If your IT is managed externally, contact the right people to help (identified in Step 1). If you manage your own IT, activate your incident plan. This may involve:
·replacing infected hardware
·restoring services through backups
·patching software
·cleaning infected machines
·changing passwords

4. Report the incident to wider stakeholders

You are legally obliged to report certain incidents to the ICO. Check their website to find out which incidents qualify.

ico.
Information Commissioner's Office

AF

Report to law enforcement via Action Fraud or Police Scotland's 101 call centre. The more who report, the more likely it is that criminals will be arrested, charged and convicted.

Keep your staff and customers informed of anything that might affect them (for example, if their personal data has been compromised by a breach).

Consider seeking legal advice if the incident has had a significant impact on your business/customers. If you have cyber insurance, they will be able to provide you with more advice.

5. Learn from the incident

After the incident, it’s important to review what has happened, learn from any mistakes, and take action to reduce the likelihood of it happening again.

Review actions taken during response. Make a list of things that went well and things that could be improved.

Review and update your incident plan (from Step 1) to reflect the lessons learned.

Reassess your risk and make any necessary changes to your defences.

© Crown Copyright 2019

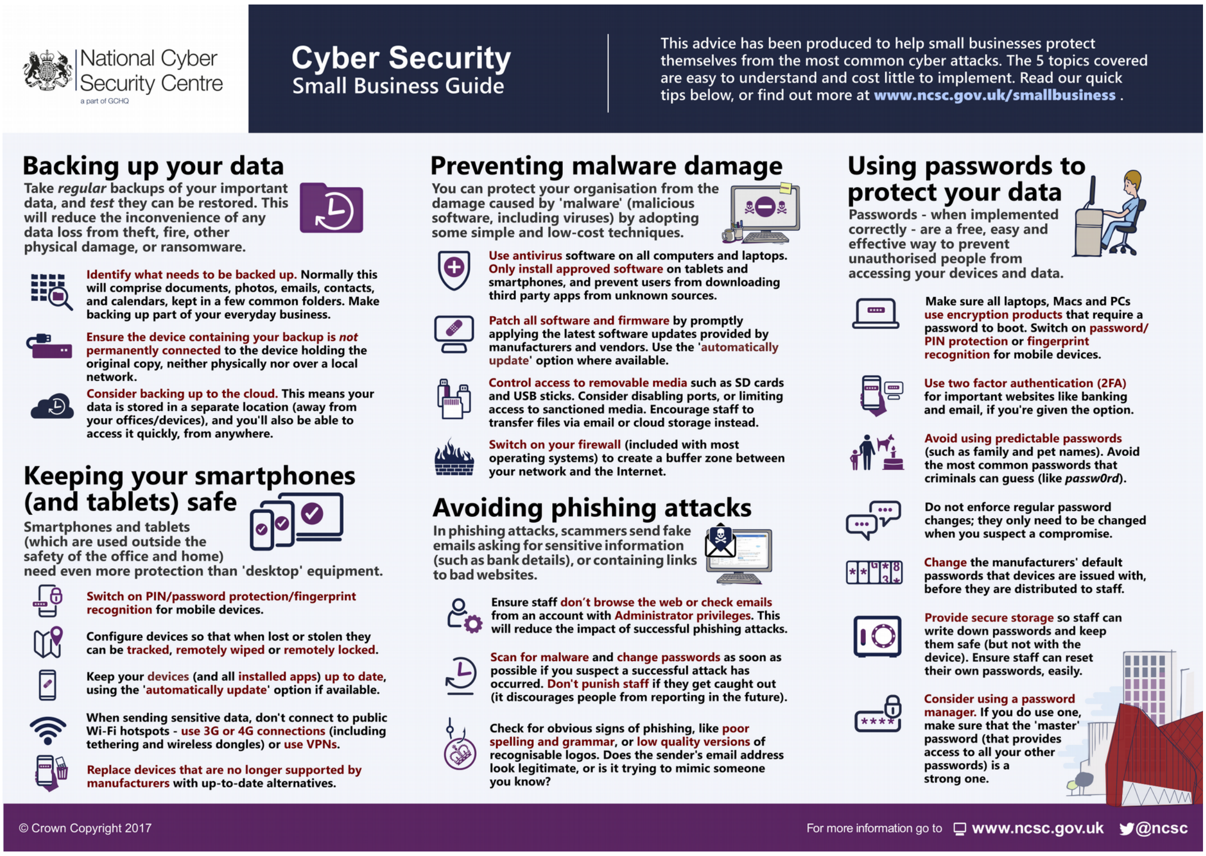
For more information go to www.ncsc.gov.uk @ncsc

source https://nbcc.police.uk/images/NCSC_response_infographic.png

This guidance helps schools plan ahead in the event that they become the victim of a cyber incident. Part of this preparation should include investigating what preventative steps can be taken to avoid becoming a victim in the first place. And implementing them. This is covered in more detail in our companion cyber security guidance.

The key actions that all schools, however large or small, should take are shown in this infographic from the NCSC.

If your school finds itself at the centre of a cyber incident, then having a well documented, thought-through response plan will be immensely helpful in tackling the immediate situation and subsequent clean-up.



National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/smallbusiness** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- Identify what needs to be backed up. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.
- Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.
- Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- Switch on PIN/password protection/fingerprint recognition for mobile devices.
- Configure devices so that when lost or stolen they can be tracked, remotely wiped or remotely locked.
- Keep your devices (and all installed apps) up to date, using the 'automatically update' option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots - use 3G or 4G connections (including tethering and wireless dongles) or use VPNs.
- Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- Use antivirus software on all computers and laptops. Only install approved software on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the 'automatically update' option where available.
- Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
- Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff don't browse the web or check emails from an account with Administrator privileges. This will reduce the impact of successful phishing attacks.
- Scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred. Don't punish staff if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like poor spelling and grammar, or low quality versions of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptops, Macs and PCs use encryption products that require a password to boot. Switch on password/PIN protection or fingerprint recognition for mobile devices.
- Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.
- Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).
- Do not enforce regular password changes; they only need to be changed when you suspect a compromise.
- Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.
- Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

For more information go to www.ncsc.gov.uk @ncsc

source: https://www.ncsc.gov.uk/static-assets/documents/Small%20Business%20Guide%201.2a%20Infographic.pdf

Prepare

Preparing for an incident is, perhaps, the most critical of all the stages. If an incident does occur then being well prepared will allow you to react quickly and efficiently to mitigate its effect.

It is not feasible to give detailed instructions for dealing with every possible type of cyber incident a school might experience. You can, however, prepare your school for the most common threats by developing plans to handle those incidents most likely to occur.

From a management perspective, developing and maintaining cyber security and incident response plans as living documents requires that cyber related risks are discussed regularly at a senior level so they become a part of normal practice.

Identify critical systems and assets

These are the systems and data that, if compromised, will have the most profound impact on the running of the school. Central to most schools is their MIS (Management Information System) which holds key information critical to the running of the school. MIS systems vary in their scale and the number of modules employed so you need to identify exactly what information it holds, and what information is held on other systems.

The various critical areas include, for example, finance, timetabling, calendar, staff records, email (staff and management), external examinations (e.g. entries), internal testing and student progress data, parent/student records, supplier records, etc.

The location of this data needs to be understood: some may be on systems physically located in the school, which will need special protection. Data may also be held in cloud-based systems which may require different mechanisms for backup and access control. In both cases, it is critical that data back-ups are properly segregated from the school's network to protect them from ransomware and malware attacks. Whatever backup system is used it must be easy to recover files and should be regularly tested.

As well as "business" data (i.e. data and systems required for the day-to-day running and management of the school) there may also be data which, while not critical for the running of the school itself, is critical for its owners: the pupils, staff and parents. Most schools, for example, have file servers which store both non-critical files and examination work which must be retained for external evaluation. Many schools also store work on cloud-based services, which require different approaches. Cloud based services are, if correctly configured, generally more secure than local storage as they will have their own sophisticated backup regimes in place.

Once the critical systems and assets have been identified the risks they present - i.e. what would be the impact on the school if they were to be compromised - can be evaluated. While it is important to understand the financial cost of an incident involving a critical system, the operational - loss of teaching time - and reputational risks also need to be recognised. For example, data theft of parental contact information (name, address, bank details) from the MIS server would be a major incident that, in addition to the clean-up costs, may incur penalties from the ICO under GDPR, a potential loss to affected parents and reputational damage to the school.

What needs to be considered then, is how best to protect each critical system. Are there adequate processes in place to ensure staff have appropriate cyber security training, to ensure all passwords are secure, and to ensure that critical software is updated in a timely manner?

For some data (e.g. parental contacts, supplier details, etc.) having a regular print-out may allow the school to function, at least temporarily, in an emergency.

Scam and phishing emails are, unfortunately, a fact of modern communications and some will get through any email filtering system. The risk that these represent can never be entirely eliminated, but it can be reduced with good staff training and robust financial processes.

The assessment of risk (whether cyber or more physical like fire or flooding) is not a one-time-only event: it should always be on the agenda of the SMT and Heads of Department. The introduction of a new technology, for example, will itself create a new risk to be considered and managed.

Planning and Mitigation

Once you have identified the most important services and data, a plan can be developed for their security and the steps to take if they are breached.

Firstly, overall security. The NEN cybersecurity document provides a wealth of more detailed information on how to protect your network and data, but some general pointers are outlined here for convenience.

Backups: it is important that regular backups are made (daily, weekly). These backups should be regularly tested to ensure that the backup process is working as expected. Regular testing will ensure that whoever has responsibility for restoring data remains familiar with the process. Backups should be segregated from the rest of the network to minimise the possibility of a virus attacking the backup copies of files as well as the originals.

Anti-virus software: make sure anti-virus software is installed on all devices used by the school community (including mobile phones), active and regularly updated.

Downloading dodgy apps: DON'T! Best practise is that all school-owned devices should be managed centrally and set up so that only administrative users can run or install software. Devices allowed onto the network which are not owned by the school pose are more difficult problem: your IT support need to put processes in place to protect the network.

Updating software: updates to both operating systems and applications should be done as soon as practicable on all devices. These will include servers, routers, switches, etc. as well as computers, tablets, and mobiles. Updating should, where possible, be an automated, overnight process.

Control USB (and other peripherals): do not, in general, allow users to introduce their own storage devices. If this is required it must be strictly controlled by, for example, using a non-network connected computer to scan the device for malware before being connected to a networked computer.

A firewall will allow you to better control what enters and leaves the local network increasing protection again malware and other Internet based threats.

Set up two-factor authentication for all accounts where it is available (e.g. Banking, MIS management, senior management email accounts, etc.). This gives some protection against unauthorised access if the other details are compromised (via a scam email, for example).

Password management security: there is varying advice online about how best to create secure passwords (random, 3-word, 4-word, etc) with their differences in memorability and strength. The NCSC's current advice is to use three random words. Using a password manager can help manage users' passwords and, for the most sensitive accounts, generate very strong passwords that the user does not have to remember. Passwords should not be shared between accounts: using a password managers makes this a realistic option.

Change default passwords: make sure any new device has its default password changed as soon as it is installed onto the network!

Accounts management - “least privilege”: users should be configured so that they have only the access they need to carry out their work. No more, no less! When staff leave or change roles, their account should immediately be updated accordingly. You don’t want disgruntled ex-staff accessing their old account!

Staff training: staff need to be trained to spot possible cyber incidents and to respond accordingly. A “no blame culture” should be encouraged. Then, if a user realises they have made a mistake (opened a malicious email attachment, for example), they will know they can inform their IT staff without fear of censure. This way the issue can be isolated and dealt with quickly, causing the least damage.

Mobile phones: these present some unique challenges if they are allowed to connect to the school network. As a minimum, password protection (or Face/Fingerprint ID) should be enabled and lost devices must be able to be tracked, locked and/or wiped remotely. As a matter of policy, local Wi-Fi sharing should be disabled and users should not connect to untrusted Wi-Fi hotspots. Of course, this is easy to enforce on school-owned mobiles but is more problematic for staff and students’ personal phones. But tools do exist to manage mobile devices. See here for some examples.

Documentation

As part of the planning process it is important that certain information is documented and stored in a safe place - for example, on a removable disk or CD - which can be held separate from the network in case of an incident. It would also be prudent to have paper copy versions of critical documents on file in case the whole IT infrastructure became unusable making even using a CD impossible!

This information should include, for example, the incident plan itself and the details of key external contacts (contractors, web-hosting supplier, ISP, local authority ICT support team, etc.).

The NEN Cyber Security Checklist can be used as a starting point to develop an Incident Response Plan which needs to be circulated to SMT, Governors and other parties who may have specific responsibilities detailed in the plan (e.g. Heads of Departments). The plan should contain important contact information, agreed ways of working to investigate and mitigate any incident, the agreed management and decision making structure, and who to contact when and how (phone, SMS, email).

This plan needs to be available online (preferably on both an internal server and a “cloud” service) as well as in paper form.

Identify what is happening

A cyber incident needs to be identified before it can be effectively dealt with, and not all incidents are obvious. A DoS (Denial of Service) attack which slows the broadband connection to a crawl or hits websites may be spotted early and investigated. But beware of jumping to conclusions: not every slowdown will be an attack.

The theft of sensitive data, however, may go unnoticed until much later. Ransomware may have been on the system for some time before being activated.

No network will stop every incident as we know from the high-profile cases that are reported every so often. Statistically, a school is unlikely to be the intended target: it is much more likely to be just one recipient of a more general attack. The most important thing is that, by being alert to the possibilities, the time between the start of the incident and its being noticed can be reduced.

So how can a school detect that an incident is happening or has already occurred?

The following are some things to look for as an indication that something is not right:

- computers running slowly
- users being locked out of accounts
- users being unable to access documents
- receiving messages demanding a ransom for the release of files
- people telling you of strange emails coming from your domain
- internet searches being redirected
- requests for unauthorised payments
- unusual account activity.

If you experience any of the above then contact your IT support and ask them to investigate and report back as soon as possible, including recommendations for any actions that need to be taken.

The following questions are a starting point if you suspect something has gone wrong: they will help you identify what has occurred, and provide your IT support (internal or external) with the information they need to resolve the issue.

Some crucial questions…

1. What problem has actually been reported, by who, and to whom? This will enable you to go back to the source to confirm the details and ask follow-up questions.

2. What services, programs and/or hardware are not working?

3. Is there any evidence that data been lost? For example, have you received ransom requests, or has your data been posted on the internet?

4. Can you tell if any information has been disclosed to unauthorised parties, deleted, corrupted or encrypted?

5. Have you had any reports of problems from external users? Can they still access your website or VLE, for example?

6. Who is responsible for the affected system's design and/or maintenance?

7. When did the issue first arise or, if this is not known, when was it first reported?

8. What is the scope of the problem? What systems are affected and how critical are they to the functioning of the school?

9. Have there been any signs as to whether this problem was internally or externally instigated?

10. What is the potential impact of the running of the school itself, the ability of teacher to teach, and pupils to learn?

Stop the incident getting any worse

After gathering this information, you should have a clearer understanding of the problem. If the incident is ongoing, then check any cybersecurity software or logs you have to see if you are able to identify the specifics. Contact your IT Support who can see if there are any instructions from trusted sources that can be used to fix the problem.

- https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection
- https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- https://www.nationalcrimeagency.gov.uk
- https://www.jisc.ac.uk/cyber-security
- https://www.empsn.org.uk/knowledge-base/malware-removal/
- https://www.itgovernance.co.uk/blog/how-to-handle-a-ransomware-attack

Resolve the incident

Having identified the issue, the next step is to resolve it or minimise any further adverse effects. If your IT systems are managed by third-party suppliers, then simply call them, apprise them of the situation and get them to do what is required to clean up the systems and get them working again. If you manage your own systems then your IT team should follow the agreed Incident Response Plan and report back to the SMT.

The school's SMT will need to have a full report from the IT team.. It should identify the major factor(s) in the incident: were, for example, agreed processes correctly followed, was it a technical issue, or lack of staff training? The remedial actions taken should be noted together with the details of any changes that have already been made to prevent the problem recurring. Finally, it should note any further preventative recommendations: upgrading hardware/software, revising staff training, etc.

Reporting the incident

When the incident has been resolved it should be reported both internally and to any relevant external bodies. There are some incidents that you are legally obliged to report to the Information Commissioner's Office. Remember that a cyber attack is a crime and should be reported to the Police - usually, this is either to Action Fraud or, in Scotland, the Police Scotland call centre on 101.

Many cyber attacks go unreported: within education, this may be because of personal embarrassment or through fear of publicity and its impact on the school's local reputation. However, reporting to the NCSC or your local Police Regional Organised Crime Unit (ROCU) is confidential so local publicity should not be of concern. If you have suffered a cyber attack, then it is very likely that others have similarly suffered: the more incidents that are reported the greater the chance that those responsible will be arrested, charged, and convicted.

If the "attack" was purely internal - by a student, for example - then it may be best to take a low-key approach without involving the Police. Such a decision must be taken by the SMT and justified by the facts. For example, a prolonged attempt to defraud the school would be of a different order from a one-off, "experimental" hack. There is clearly a judgement call here which attempts to balance educational and societal needs against the strict legalities.

The National Cyber Security Centre (NCSC) has various schemes aimed at young people including CyberFirst and the ROCUs also work with schools in their area through the National Cyber Protect Network (https://serocu.police.uk/cyber-protect/). A full list of ROCUs can be found here.

In addition to any statutory obligations to report an incident to the ICO or Police, every school will have a range of other stakeholders who need to be kept informed. Clearly, this will include the Senior Management Team and Governors but may also include the Local authority, the wider staff, parents and, possibly, students as well.

If the incident is particularly serious (e.g. a major ransomware threat or personal data breach) that will probably affect the running of the school or its reputation, then you may want to consider seeking legal and/or public relations advice. This could be from your Local Authority, if they can provide this service in-house, or privately. However, this will incur significant cost so is probably only viable for large schools or Local Authorities.

If you (or your LA) have cyber insurance, then they will be able to provide more advice.

Learning from the incident

Once the incident has been resolved (or at least is under control) it is time to review what happened, learn from any mistakes, and take any actions to try to reduce the likelihood of it happening again.

While it is important to review technical controls and procedures, it is also an opportunity to review your staff training and to take measures to develop cyber security awareness among all the staff (teaching and administrative) and pupils. The twin aims of cyber security awareness training are:

(1) to make staff aware of the range of potential cyber threats they may come across and how to react to them. This may include training on how to spot suspicious emails, using strong passwords, and securing electronic devices.

(2) to instil a “no-blame” culture so that staff (and students) and not afraid to report something they think is suspicious even if they have acted unwisely. For example, if a member of staff replies to a scamming email but thinks better of it afterwards, they should know that it is okay to report it. A school will be more cyber secure if it adopts a culture where reporting is encouraged rather than one based on recrimination and blame.

The actions taken throughout the incident should have been documented so now is the time to review them and not just file them away. What went well? What didn’t? What could be improved? Update your incident plan accordingly and make users aware of any changes they need to know about - having a procedure is all very well but is useless if it is kept hidden or buried in a mass of other (equally important) procedures.

Your technical defences may need to be strengthened. Did your anti-virus software work well enough? Are your backup procedures robust? Is the firewall allowing too much access in or out? Is your password policy correct? Are user accounts being removed when they should be? Did your IT staff (whether internal or external companies) respond appropriately? Do you need to review your suppliers’ contracts? What about their access to your network - did they have enough access to resolve problems?

So, as Winston Churchill may (or may not!) have said: “Never let a good crisis go to waste”.

Use it to review procedures, to review your network security, train staff and reinforce the "no blame" culture.

Summary

Any school can fall victim to a cyber incident regardless of its size. Schools are perceived to be soft targets due to the low levels of cyber security some of them employ. They also hold sensitive personal data on staff, pupils and parents that can be valuable to attackers, and they have financial assets and processes that can be exploited by criminals to steal money.

School networks are also used by many different users and devices, including pupils who might wish to look for a readymade network to practise their cyber skills on.

A school is more likely to suffer an incident where they are not the explicit target but just get caught up in a more generalised, non-targeted attack (e.g DDoS or ransomware) or because they are using a particular piece of vulnerable technology.

Up to date cyber security and incident response plans (which may be combined into one document) will help prevent an attack or, at least, mitigate its effects.

To mitigate the effects of any cyber incident you may experience it is important to prepare for one. If the worst does happen, then identify what is going on, stop and resolve it, report it, and learn from it.

There are many types of cyber incident - from the accidental opening of a malicious email attachment to a concerted, targeted, professional attempt to steal money or data. An understanding of this variety of risk and the possible routes an attack may take will assist in keeping the network and its users safe.

Apart from the technical aspects of preparing for an attack one of the best ways prepare is to instil a culture of openness in reporting suspicious activity and a “no-blame” culture when mistakes are made, as they inevitably will be.

APPENDIX I: Types of breach

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.

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.

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.

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.

APPENDIX II: Where do incidents originate?

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.

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.

Useful Links

Information Commissioner's Office: https://ico.org.uk

Report a breach: https://ico.org.uk/for-organisations/report-a-breach/

Action Fraud: https://www.actionfraud.police.uk/report_fraud

National Crime Agency: https://www.nationalcrimeagency.gov.uk

National Cyber Security Centre (NSCS): https://www.ncsc.gov.uk

NCSC Weekly threat reports:

https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports

NCSC's CyberFirst:

https://www.ncsc.gov.uk/section/education-skills/11-19-year-olds

Regional Organised Crime Units (ROCU):

https://www.ncsc.gov.uk/information/regional-organised-crime-units-rocus

Jisc: https://www.jisc.ac.uk/cyber-security

National Cyber Protect Network: https://serocu.police.uk/cyber-protect/

Some examples from the TES:

https://www.tes.com/news/student-turned-cybercrime-after-college-rejection

https://www.tes.com/news/gcse-coursework-lost-ransomware-attack

https://www.tes.com/news/colleges-hit-cyber-attacks-12-times-week

https://www.tes.com/news/top-academy-trust-hit-ps77k-cyberattack

https://www.tes.com/news/fraudsters-are-intercepting-school-fee-payments-warns-charity-commission

https://www.tes.com/news/cyber-attack-readiness-colleges