Cyber scenario planner

UK EDUCATION SECTOR

Contains promotional material

ecclesiastical

Cyber scenario planner

Introduction

As connectivity spreads and improves, and as schools move beyond a patchwork of often small and uncoordinated systems to become increasingly more dependent on their ICT infrastructure at the school, classroom and system level. A data breach or 'cyber attack' can lead to lost income, a damaged reputation, and legal and regulatory costs, not to mention the associated business interruption loss to the school.

Like all organisations making greater use of technology and the internet, it is vital that schools take all the steps they can to keep their systems, people and data secure and safe from harm.

This assessment has been created to raise awareness of the cyber threat to schools. Completion of this assessment does not replace the need for a wider cyber security policy, disaster recovery plan or certification under the Government's Cyber Essentials scheme.

The purpose of a cyber scenario planner

In considering a set of potential related scenarios and implementing a set of concrete actions, you may end up saving yourself from a lot of aggravation, damage, downtime or loss of trust. Or maybe you won't: no one is perfect, after all, mistakes happen, technologies change and the bad guys can be quite good at what they do.

You may also come to have a better understanding of where some of your most critical security vulnerabilities may lie. This may not only help you to respond if and when they are exploited, but also might just help you better protect yourself and stay on your feet in the first place.

The purpose of this scenario planner is to help inform decision makers and to support the appropriate response.

The planner serves as a summary to help all involved parties make informed decisions about security and the need for additional action such as insurance or technical management measures.

Reviewing the cyber risk posed to the school will also help identify where you may have a weakness or areas for further investment. Completing an assessment with all stakeholders helps organisational visibility of the risks and also enhances communication.

The planning should be handled by those that have knowledge of the school network, as well as trustees, governors or other parties who may have information that would be useful such as regulatory or budgetary knowledge. It should not be a one off task and is something that can become a repeatable process which could be picked up by others in the event of staff turnover.

Step 1 - Identify high-value assets

An inventory of assets is a critical element to understanding cyber risk exposures across the school. To begin, you should identify assets from all teaching and operational areas that could potentially be subject to a cyber attack.

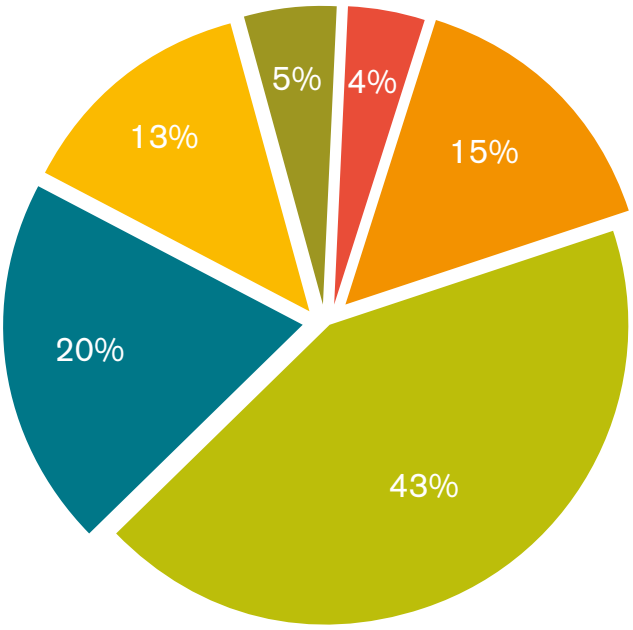
The list should include both digital assets – such as critical data that should be protected or operational services that can be disrupted – and physical assets, such as computing hardware and connected infrastructure that can be damaged or destroyed.

The goal is to identify assets that, if lost or compromised, would lead to significant loss to the school. In some cases, the asset might have little or no cash value – but loss of the asset might have implications for the school's reputation (e.g. losing sensitive data) to operational interruptions (e.g. inability to teach lessons due to system failures).

The cost of a data breach

According to the IBM 2017 Ponemon Cost of Data Breach Study[1], a data breach can cost as much as £72 per record in the education sector. The pie chart shows IBM's percentage breakdown of this cost by factor.

- Investigation and forensics
- Lost business
- Contact costs
- Legal services and compliance
- Audit and consulting services
- Other



1. 2017 Cost of Data Breach Study, sponsored by IBM Security, conducted by Ponemon Institute Research Report, June 2017 https://www.ibm.com/downloads/cas/ZYKLN2E3)

Step 2 - Identify threats

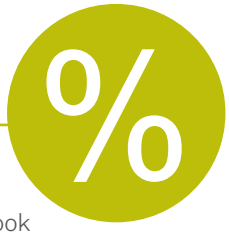
Once the **What** i.e. the high-value assets are identified, you should develop a list of cyber threats by identifying each potential situation to which each high-value asset could be subject.

The key for the success of the exercise is to consider the most relevant possibilities for potential actions. Your school should be asking **Who** - might attack (e.g. a cyber criminal, an insider, a student etc.), the **Why** - what might be the motive for the attack (e.g. the disruption, damage, etc.) and the **How** - what form the attack might take (e.g. phishing, malware, ransomware, etc.), and what specific assets might be targeted.

"Who"	"Why"	"How"
Types of individuals who are motivated to attack the school	Actions taken by threat sources	Event by which the threat source accesses the assets
Cyber criminal	Extort	Ransomware
Accidental insider	Disruption	Lost device
Tech savvy student	Curious	SQL injection

For more information on the threats, please refer to the **cyber threats explained guide**.

Step 3 - Estimate frequency of cyber events



Now that you have identified the threats, and how they apply specifically to your school. It's time to take a look at how likely these attacks and events actually are. And not just whether you might face one of these events at some point, but what its potential for success might be. The 'frequency' is an equation that weighs the likelihood of initiation or occurrence of an event against the possibility that said event would have an adverse effect. The threat, their motivation and method must be considered in addition to the current controls in place and their effectiveness in preventing a successful action.

High	The threat source is motivated and sufficiently capable and is almost certain to initiate the threat action which is likely to occur between **10-100** times a year. Current controls to prevent the threat action are **not effective**.
Medium	The threat source is motivated and sufficiently capable and is almost certain to initiate the threat action which is likely to occur between **10-100** times a year. Controls are in place that may impede successful exercise of the threat action.
Low	The threat source lacks motivation or capability and is unlikely to initiate the threat action which is likely to occur **less than once a year**. Controls are in place to prevent, or at least significantly impede, the threat action from being exercised.

Example

Due to the ease with which thousands of emails can be sent out by cyber criminals, a phishing attack is a very common threat action that is deployed to steal login credentials or gain additional information for a more sophisticated follow-on attack.

If a spam filter on the email system is the only control that is in place, this is unlikely to be sufficient as phishing emails may bypass this filter - as a result it could be classed as having a **High** frequency.

Additional risk management features that are listed in the **Cyber risk management guide** may reduce the frequency to **Medium** or **Low**.

Step 4 - Estimate severity of cyber events

Like you did in **Step 3**, the next major step in measuring the level of threat is to determine the adverse impact resulting from a successful threat action.

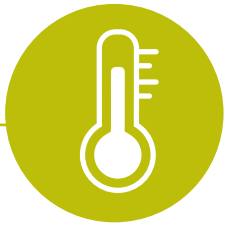
High	The threat action may result in the **costly** loss of assets or resources; or may **violate**, harm, or impede the school's functions or reputation.
Medium	The threat action may result in the **costly** loss of assets or resources; or may **violate**, harm, or impede the school's functions or reputation.
Low	The threat action may result in the **loss** of some assets or resources; or may **noticeably affect** the school's functions or reputation.

Example

Ransomware continues to be an easy way for cyber criminals to extort money from a school. If an email attachment was opened and subsequently downloaded ransomware, every computer and server on the network could be infected with all important school data encrypted. The ransom demand could be considerable and it's also possible that the encrypted data was taken by the attacker - as a result it could be classed as **High** severity.

Additional risk management features that are listed in the **Cyber risk management guide** may reduce the severity should an attack be successful.

Step 5 - Determine your school's risk



You'll never completely mitigate all risk. It's foolish to even think that you can. But you can minimise risk by continually assessing it and then working to implement safeguards that diminish the likelihood and impact of any security event.

The matrix below shows how the overall risk levels of **Severe, Elevated** or **Normal** are derived. The determination of these risk levels or ratings may be subjective.

		Frequency		
		Low	Medium	High
Severity	High	Elevated	Severe	Severe
	Medium	Normal	Elevated	Severe
	Low	Normal	Normal	Elevated

The table below describes the risk levels shown in the above matrix. This risk scale represents the degree or level of risk to which a school might be exposed if a given threat action was exercised. The risk scale also presents suggested actions that the school may take for each level.

Severe	There's a strong need for risk management actions. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Elevated	Risk management actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Normal	You must determine whether risk management actions are still required or decide to accept the risk.

Step 6 - Record results

List the following:

- Asset and value
- Threat, motivation and method
- Frequency (e.g. High, Medium, or Low frequency)
- Severity (e.g. High, Medium, or Low severity)
- Risk range based on the risk level matrix (e.g. Severe, Moderate, or Normal risk level)
- Current controls in place to recommended controls for reducing the risk.

Step 7 - Risk management

The starting point of risk management is an acceptance that risk can't simply be abolished. Risk must be recognised and then managed in some way or other (classically to either avoid, reduce, transfer or retain). This can be easier said than done, particularly when confronted with a demand to 'abolish risk', as if that were an easy and simple option.

There are four ways you can treat a risk:

Generally, you need to do everything 'reasonably practicable' to protect the school from harm.

This means balancing the level of risk against the measures needed to control the real risk in terms of money, time or trouble. However, you do not need to take action if it would be grossly disproportionate to the level of risk.

Look at what you're already doing and the control measures you already have in place. Ask yourself if you can get rid of the hazard altogether? If not, how can you control the risks so that damage or loss is unlikely?

Step 8 - Update planner

Once you have reviewed each scenario and addressed any risk management measures, then it's time to update the planner. As the threat is constantly evolving, it's a good idea to periodically revisit the planner or when there are changes to the ICT structure or roles within the school.

Cyber scenario planner (example)

Step 1		Step 2			Step 3	Step 4	Step 5	Step 6					
Asset type	Asset value	Threat source	Motive	Method	Frequency	Severity	Risk rating	Current controls	Risk treatment action	Recommended controls	New frequency	New severity	New risk rating
Computer equipment	Value £478,000	Cyber criminal	Extort	Ransom ware	Medium	High	Severe	Controls: Firewall and anti-malware installed. Backups made every friday to network 'D' drive.	Reduce	Controls: Automatic patch updates. Improved anti-malware. Daily backups to cloud storage, regular staff training and simulated phishing tests.	Low	Medium	Normal
Personal information	Value £192,000	Accidental insider	Disclose	Phishing	High	High	Severe	Controls: All staff are free to use USB sticks to transfer work between school and home.	Avoid	Controls: Stop the use of USB sticks to transfer data, restrict USB access to admin level users for limited cases and enforce encryption.	Medium	Medium	Normal
Money	Value £235,000	Cyber criminal	Theft	Spear phishing	Medium	Medium	Elevated	Controls: Dual approval required on all money transactions over £5,000.	Reduce	Controls: Verify identity of person requesting payment and recipients (via known contact details) made before action is taken. Report anything suspicious.	Low	Medium	Normal

Notes

Notes

More than just insurance

With over 55 years spent securing the future of educational establishments, our education product and specialist service is tailored to give you peace of mind.

- A tailored insurance product that provides protection for staff, pupils, buildings, contents and business interruption.
- Access to helplines to support with PR and crisis management, legal advice and counselling.
- A bespoke risk management assessment, followed up with a risk tracker report, providing a before and after picture of risk improvements. Plus a unique view of where you sit in relation to your education establishment peer group.
- Access to our risk advice line providing quality support over the phone, helping you to manage your changing risks.
- Support from an award winning claims team[1] should the worst happen.
- Online advice via our "Education Hub". Here you will find useful information ranging from staff training and health and safety advice, to easy to use forms and templates and market insights.
- A 25% discount for EduCare, a leading provider of online duty of care and safeguarding training[2].

Visit **www.ecclesiastical.com** for further information on education insurance from Ecclesiastical.

[1] Winner at the Insurance Times Claims Excellence Awards and the Post Claims awards 2018.

[2] To claim the 25% discount you must have an active education policy with Ecclesiastical Insurance Office plc on the date of purchase. This discount cannot be used in conjunction with any other offer.

ecclesiastical

Ecclesiastical Insurance Office plc (EIO) Reg. No. 24869. Registered in England at Benefact House, 2000 Pioneer Avenue, Gloucester Business Park, Brockworth, Gloucester, GL3 4AW, United Kingdom. EIO is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Firm Reference Number 113848

PD3169 1 03/21