breathetechnology

support | cloud | security | infrastructure | comms

EMPOWERING EDUCATION THROUGH SECURE TECHNOLOGY

Cyber Security Audits

FOR MAT'S, TRUSTS & SCHOOLS

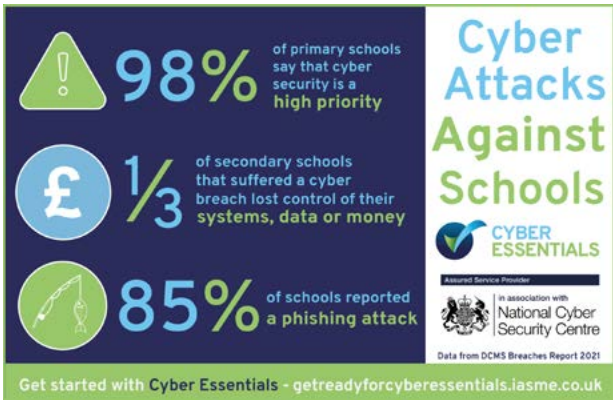
Security has never been more important

ISO 9001:2015 COMPANY | ISO 27001:2013 COMPANY | bcs Chartered IT Professional | Chartered Institute of Information Security | CISP | National Cyber Security Centre | CYBER ESSENTIALS | TOP CYBERSECURITY CONSULTING COMPANIES

Cyber Security Audits

FOR MAT'S, TRUSTS & SCHOOLS

Security has never been more important



When talking about **Cyber Security,** each school has a moral and legal responsibility to protect its students, staff, other stakeholders, systems, and data. The trust's responsibilities are to protect its schools and drill down to the details in the event that there are shared services. As the organisation's size increases, so do its complexity and risks.

Senior leaders and governors need to be aware that cyber security is a management and assurance issue and have assigned responsibilities in terms of cyber security. It's a bigger issue than simply relying on the IT team to manage.

Cyber security is about protecting the devices we all use and the services we access online, both at home and at work or in the classroom, from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices and online. From that point of view, the trust or school has a wider responsibility affecting the local community.

Often, a trust or school will require the help of a specialist MSP with cyber security experience and accreditation. Not all IT providers are suitable.

Effective cyber security management starts with the allocation of roles and responsibilities, understanding the current state of play and the risks and threats that could affect your trust or school, and then creating a plan to mitigate the risk and clarify how you will respond to an attack or breach.

This Cyber Security Audit is your first step in understanding the risks, how to deal with them, and putting together a plan.

Why Cyber Security is Essential for Schools

An increasing number of schools and colleges are being seriously impacted by cyber incidents, perhaps a phishing attempt to steal money and passwords, or a ransomware attack that encrypts files preventing access. ***But why?***

- **Many cyber incidents are untargeted.** They can affect any school that doesn't have basic levels of protection.
- **Schools hold plenty of sensitive information.** For example, staff and parents' bank details, medical information about students, and safeguarding records. All this has to be kept safe and confidential.
- **Cyber criminals want to make money.** They understand that an organisation's information is often sufficiently important to that organisation that they might be prepared to pay a ransom to get it back.

Who is behind cyber attacks?

Online Criminals

Are really good at identifying what can be monetised, for example, stealing and selling sensitive data or holding systems and information to ransom.

Hackers

Individuals with varying degrees of expertise often act in an untargeted way – perhaps to test their own skills or cause disruption for the sake of it.

Malicious Insiders

Use their access to an organisation's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Honest Mistakes

Sometimes staff, with the best intentions, just make a mistake, for example, by emailing something sensitive to the wrong email address.

School Pupils

Some students simply enjoy the challenge of putting their cyber skills to the test.

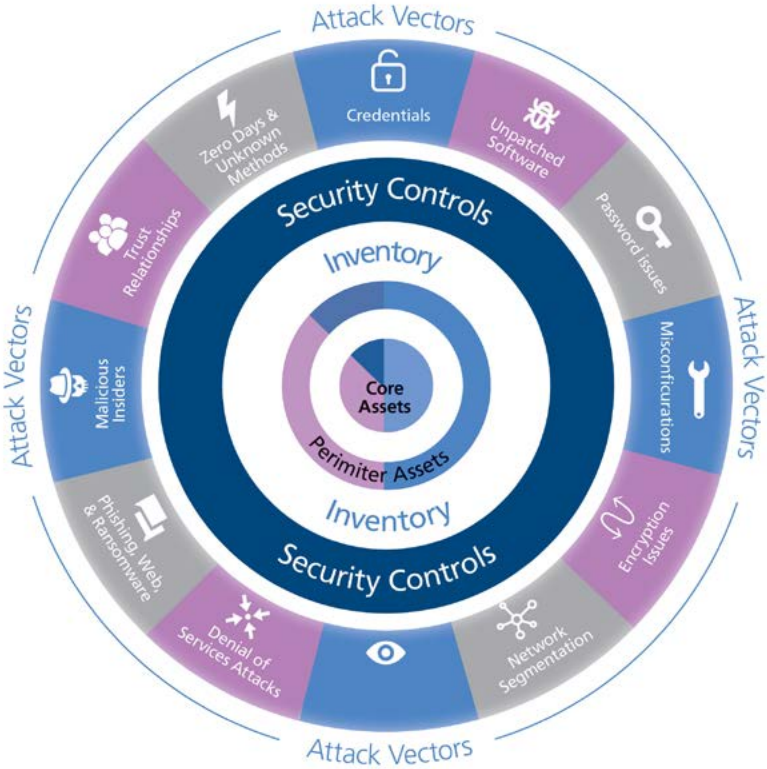
Anatomy of a ransomware attack

What is a Cyber Security Audit

A Cyber Security Audit for Schools is a comprehensive assessment of the information technology systems, policies, and practices in educational institutions to identify and mitigate potential cyber security risks.

Given the sensitive nature of student data and the increasing reliance on technology in educational settings, cyber security audits for schools are crucial for ensuring the protection of students' personal information, maintaining the integrity of academic records, and safeguarding against cyber threats.

Often, when trusts form and expand, audits help with the planning and risk mitigation processes as the organisations become larger and more complex.



Aspects that a cyber security audit for schools may focus on:

1. **Department of Education and NCSC Digital Standards and Best Practice:** The National Cyber Security Centre (NCSC) is the government security department that advises the Department of Education (DFE), which in turn has been great in guiding schools in terms of the minimum standards that should be achieved. In our experience, these standards are very achievable and make complete sense. They closely align with the global gold standard for security, which is called ISO 27001. Breathe has developed a simple-to-understand process, helping you understand how you compare to the Digital Standards Guidelines and how to achieve them where they are not being met.

2. **Network Security:** Assessing the security of the school's network infrastructure, including Wi-Fi networks, routers, switches, and firewalls, to ensure they are properly configured and protected against unauthorised access.

3. **Endpoint Security:** Evaluating the security measures implemented on computers, laptops, tablets, and other devices used by students, teachers, and staff, such as anti-virus software, endpoint detection and response (EDR) solutions, and device encryption.

4. **Data Protection:** Reviewing the policies and practices for protecting sensitive student data, such as personally identifiable information (PII), academic records, and health information, including data encryption, access controls, and data backup procedures.

5. **User Awareness Training:** Assessing the effectiveness of cyber security awareness training programmes for students, teachers, and staff to ensure they are educated about common cyber threats, phishing scams, and best practices for maintaining security online.

6. **Access Controls:** Reviewing user access controls and permissions to ensure that only authorised individuals have access to sensitive information and systems, and implementing multi-factor authentication (MFA) where appropriate.

7. **Incident Response Planning:** Evaluating the school's incident response plan for handling cyber security incidents such as data breaches, malware infections, or denial-of-service (DoS) attacks, and testing the effectiveness of response procedures through simulated exercises.

8. **Compliance Requirements:** Ensuring that the school complies with relevant regulations and standards concerning student data privacy and cyber security, such as the Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act (COPPA), and state-specific data breach notification laws.

9. **Third-Party Risk Management:** Assessing the security practices of third-party vendors and service providers that have access to school systems or handle student data, such as cloud service providers, learning management system (LMS) vendors, or educational software providers.

10. **Office 365:** Office 365 is widely used in schools, and it is a no-brainer. However, there is a real misconception that it is safe. You need to consider scanning not only email but also OneDrive, SharePoint, and MS Teams. If you held this data on your server, you would surely have protection such as Sophos Anti-Virus and Email Security or an alternative. The same principles apply when moving data to the cloud.

11. **Backup, Disaster Recovery, and Business Continuity:** Yes, that's right. We are now talking about business continuity too. This is no longer only reserved for the corporate world. The latest government and DFE guidelines are standards that require at least three copies of the data. Additionally, there should be an offsite/offline copy that is ideally hosted off the trust or school network, and it's only open and visible for short periods of time. While it accepts an offsite backup, that will eventually become your very final defence in a cyberattack. Traditionally, schools would keep two backups that would cover traditional risks such as natural disasters, fire theft, etc. This is no longer sufficient, as the risk of a cyberattack is now the primary risk to protect yourself against.

    It's also critically important that the backup, DR, and business continuity plan are actually approved by the SLT and Trustees. So everyone understands what is possible in terms of backup and, actually, how long it will take. IT can then implement the approved and documented plan. The audit will review the current state of play and provide clear guidelines on what is required by the DFE and NCSC and how Breathe has helped other schools with real-life examples.

    By conducting regular cyber security audits, schools can identify vulnerabilities, strengthen their security defenses, and protect the sensitive information entrusted to them by students, parents, and staff members. Additionally, it helps foster a culture of cyber security awareness and resilience within the educational community.

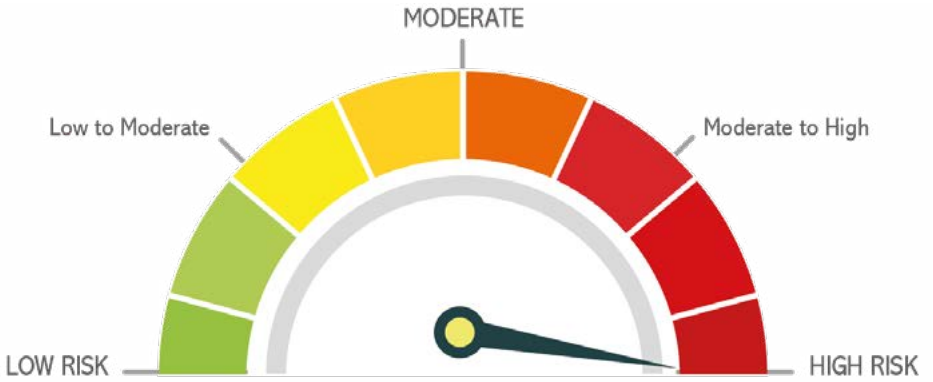
12. **Penetration Testing:** Penetration Testing: Penetration testing has now become common practice in schools. It should ideally be done annually. The goal is to review the external attack surface and understand if there are any vulnerabilities to exploit, as an attacker would.

    During this audit, a Breathe White Hat Hacker will use industry-recognised tools to perform a real-world attack on the school systems. No systems are broken, but possible scenarios can be detailed with remedial action. Ensuring we find it before the cybercriminals do.

13. **Simulated Phishing Attacks: Phishing attacks are one of the most successful strategies for** exploiting schools. They are common and get results. It's important to understand the levels of staff awareness and their ability to identify these email or text messages. Systems alone cannot always protect everyone. A critical component is then how these results are communicated to all staff and linked in with cyber security training. If run annually or biannually, it then helps to create a culture of suspicion and awareness.

Why schools do Cyber Security Audits

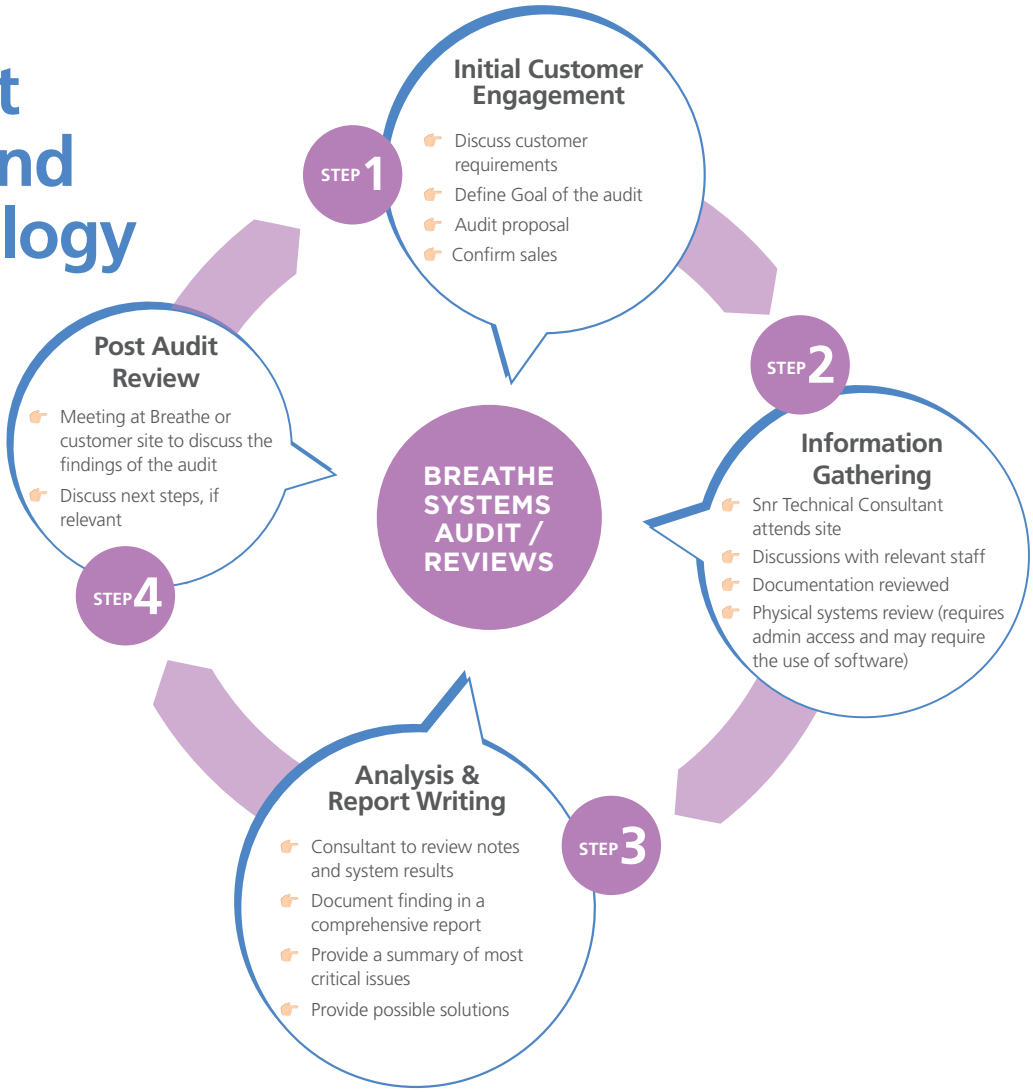
- To gain clarity on their security posture and their cyber-attack exposure
- The management team needs to gain an understanding of the cyber security status.Especially when there are multiple schools in a trust
- It's an incredibly good process to understand the current state of the system, performance, costs, or risks, which are then followed up with advice and recommendations
- To obtain a 3rd-party expert view on the resourcing requirements and IT support team setup
- Concerns regarding the cyber security posture of the school or trust or possible data or security breaches
- Multi-Academy Trusts often audit to help them centralise the IT function and to ensure the schools get the most out of being part of a trust
- An audit can help to ensure that the school or trust is meeting the latest guidelines, such as the KCSIE or DFE Standards for IT
- Meeting the latest government guidelines for security and backup
- A gap analysis can be performed if there is a goal to be Cyber Essentials Certified. The audit ensures that the work is done upfront and simplifies the certification process
- Often, the trustees will request that an independent cyber security assessment be performed
- When starting a new managed services/support agreement, the audit is ideal to document the system and help everyone understand what is in place and needs to be handed over. It then creates a plan for the IT to be proactively managed based on issues, risks, best practices, or technical problems highlighted during the audit
- It's the perfect starting point when building a cyber security strategy or plan



Types of audits and tests available from Breathe

- (Show the types with icons and bullet points of what's include)
- Breathe offers the following Cyber security Audit Services to businesses and schools
- IT Systems Audit (includes High Level Cyber Security Review)
- Penetration Testing (Using real-world tools)
- Simulated Phishing Attack (Using real-world Tools, not Office 365 simulations)
- Cyber Security Audit
- Managed Cyber Essentials and Gap Analysis (We assist with the end to end process in obtaining Cyber Essentials certifications
- Gap Analysis and consultancy for ISO27001
- Gap Analysis for Schools, against the DFE Digital Standards

Our Audit Process and Methodology



How is the audit presented to the school?

- Detailed Audit Report with Cyber Security Posture Score
- Management Summary Report – For easy ongoing management and planning
- Internal Vulnerability Assessment Report
- Simulated Phishing Attack report
- Penetration Test Report
- DFE Digital & Technology Standards Gap Analysis Report

Where do we get our best practice guidelines from?

Breathe have conducted hundreds of audits and have many years of experience in designing, installing and supporting IT in Schools. However, we are trained and certified as a Cyber Security Socialist.

In the audit we will provide our professional opinions, but we will also reference best practice guidelines and formal advice or recommendations. We get this information from the following organisations:

Gov.UK
https://www.get-information-schools.service.gov.uk/

Information Commissioners Office (ICO)
Schools, universities and colleges | ICO

National Cyber Security Centre (NCSC)
All topics - NCSC.GOV.UK

SANS Institute
Information Security Policy Templates | SANS Institute

ISACA
CISA Certification | Certified Information Systems Auditor | ISACA

Cyber Essentials for Schools
Cyber Security for Schools - NCSC.GOV.UK

DFE
Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Gartner
https://www.gartner.co.uk/en/methodologies/research-methodologies-gartner-critical-capabilities

Professional memberships and accreditations

BCS – Chartered Institute for IT

- British Computer Society
- BCS, The Chartered Institute for IT | BCS
- Our management Consultants are Chartered by the British Computing Society, which means we are externally vetted in terms of qualifications and real-world senior IT management experience. A formal certification and qualification is provide and referred to as CITP.

NCSC

- National Cyber Security Centre
- CiSP - NCSC.GOV.UK
- Breathe partner with the National Cyber Security Centre to ensure we are up to date with Cyber Security and the Government (Our Sponsor is the UK Police Anti-Terrorism Unit)
- The NCSC advises all government departments including the DFE on security advice, guidance and best practice.
- The NCSC is the official Cyber Security Department of the UK Government.
- Breathe rely heavily on best practice advice, security methodologies and audit or risk assessment guidelines.

CIISEC

- Chartered Institute of Information Security
- https://www.ciisec.org/
- Breathe Technology are an official member of the CIISEC and follow the advice and guidelines of the UK's official Cyber Security institute.
- Our consultants are Chartered Cyber Security professionals that are certified in a similar way to how the BCS certify IT Professional, but this qualification being Cyber Security specific.

ISACA

- ISACA provides training and certification specifically for IT and Cyber Security Audits
- https://www.isaca.org/
- As a globally recognized leader in IS/IT for over 50 years, ISACA is a professional membership organization committed to the advancement of digital trust by empowering IS/IT professionals to grow their skills and knowledge in audit, cybersecurity, emerging tech and more.
- Members receive personalized training, educational resources and can earn the most in-demand credentials – all backed by the support of industry-leading IT experts from around the world.

SANS Institute

- Globally recognised institute for Cyber Security. They are responsible for the SANS Top 20 Security System
- https://www.sans.org/uk/
- Launched in 1989 as a cooperative for information security thought leadership, it is SANS' ongoing mission to empower cyber security professionals with the practical skills and knowledge they need to make our world a safer place.

IASME

- IASME works with the government and most other Cyber Security authorities and provides training and certification in Cyber Security
- IASME is responsible for the Government backed Cyber Essentials Certification Programme
- Breathe currently undergoing the programme to become a Certification Body and Auditor for Cyber Essentials. We already have a partnership in place to accredit schools/ Trusts.
- https://iasme.co.uk/about/

ISO 9001

- ISO 9001 is the international gold standard for ensuring high quality services to your customers
- Breathe are ISO 9001 Certified and have a Quality management System in place
- https://www.iso.org/iso-9001-quality-management.html

ISO 27001

- International standard for security best practice within your organisation.
- Breathe are ISO27001 certified and have a Security Management System in place
- https://www.iso.org/standard/54534.html

Police Cyber Alarm

- The police Cyber alarm provides log information from it's members security systems such as attack logs from a firewall. Similar to CCTV on an IT network.
- In return for helping the Police Cyber Security Team, you receive regular reports and intelligence feeds about the information that the police have gathered, helping to secure our networks.
- Breathe Technology helps install the Cyber Alarm servers at our customers sites and we use the information provided by the Police to improve our customers security systems.

We get our best practices from these organisations, especially the NCSC (National Cyber Security Centre), which advises the DFE. Breathe is sponsored by the Police Anti-Terrorism Unit, as NCSC member ships require a sponsor. Additionally, we use the DFE Digital & Technology Standards and Cyber Essentials requirements to perform a gap analysis as part of the process.

What are the benefits in the short and long term?

In the short term:

Risks are identified, and professional suggestions are made to mitigate the risks.

A DFE Digital Standards Gap Analysis will clearly show where the trust or school is not meeting the latest standards, with realistic suggestions on how to achieve them.

Longer Term:

The audit is the first step in understanding the current state of play and highlights any risks with suggestions and recommendations for mitigating the risks and meeting the standards set by the NSCS and DFE.

That means it is actively helping you protect your students, staff, wider community, systems, and data.

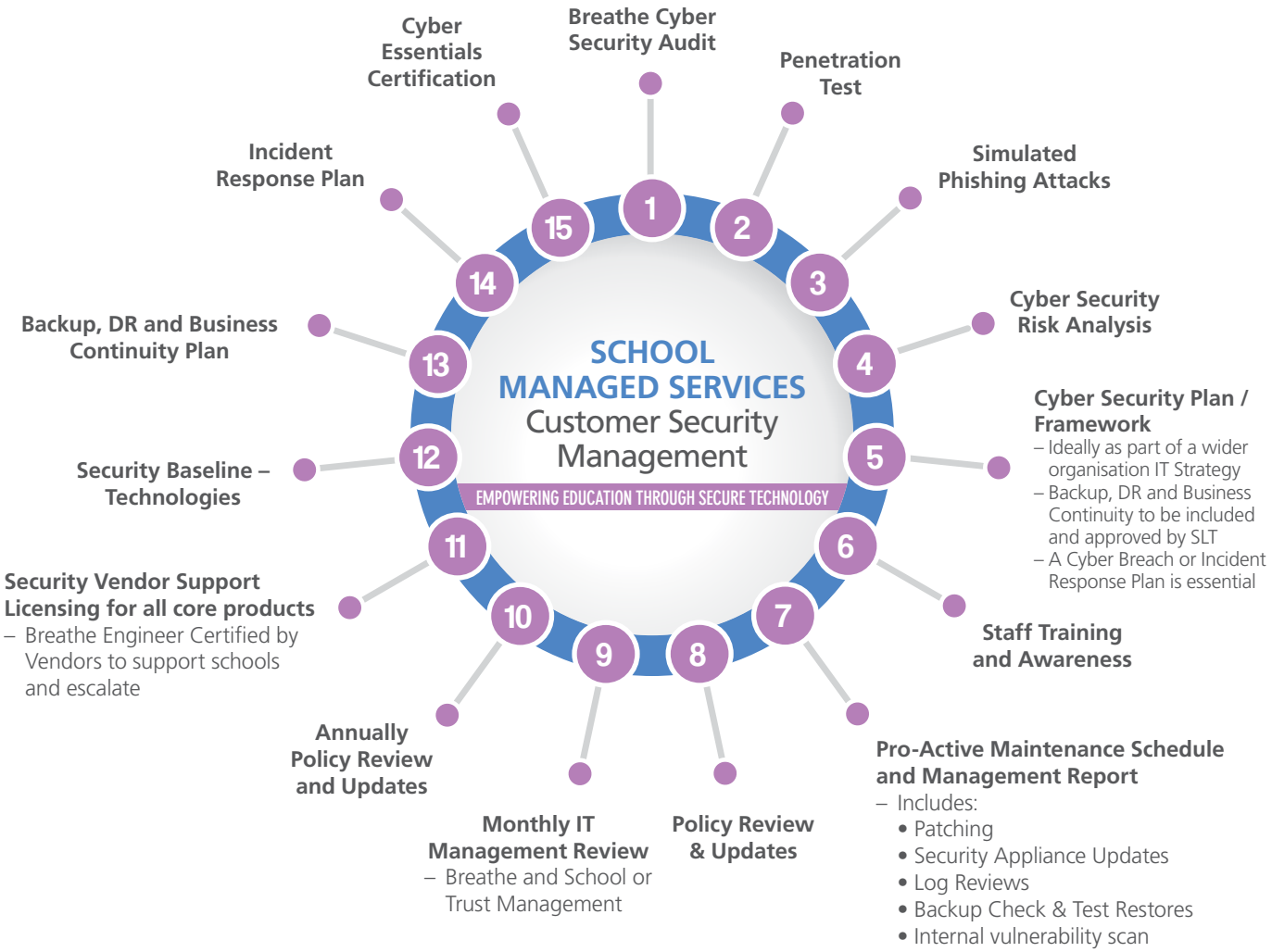
The next steps are:

Assigning roles and responsibilities for Cyber Security. It's often a combination of the internal IT team (if one is in place), SLT, and an MSP with a strong cybersecurity skillset.

- Creating an action plan to address the findings of the audit
- Continuously reviewing the action plan to ensure that risks are mitigated and standards are met.
- Creating an IT strategy
- Creating a Cyber Security Policy or Plan
- Implementing a Cyber Security Framework
- Implementing a Trust-approved Backup, DR, and Business Continuity Plan
- Creating an Incident Response Plan and its Relevant Processes
- Implementing regular penetration testing and simulated phishing attacks
- Ensuring staff awareness and training

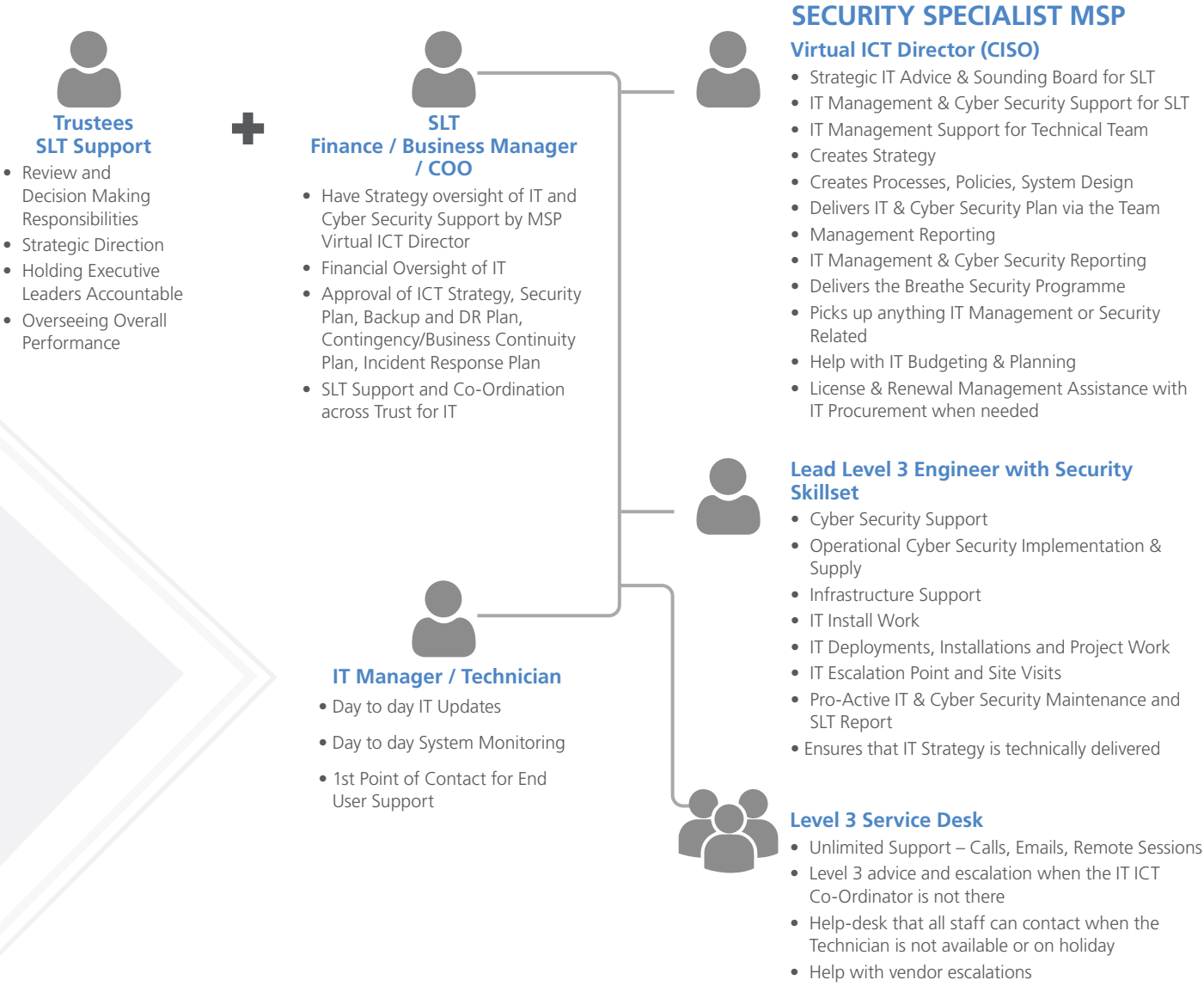
Breath would be more than happy to help implement these processes and can show you how we have done this for other trusts and schools.

15 Step Cyber Security Framework – Schools & Trusts



Cyber Security Management Org. Diagram

This diagram represents a common organisational setup, which consists of a wider team created through the MSP Partnership approach.



From our view as a security-focused MSP that works with schools, we can clearly see when a trust or school has a good MSP that helps with cyber security. What we see is that Larwood is not uncommon, and we see the same scenario at many other trusts, even trusts with bigger teams where the IT systems and support teams have already been centralised.

The reality is that we are expecting business managers or heads of finance to manage IT and cyber security. This is often not their skillset.

We are expecting IT technicians who often only really have experience in desktop support and sometimes a bit of networking, gained from only working in one or two roles previously, to look after probably the most complex IT subject. The technicians do their best, but unfortunately, they don't have the experience or professional training.

The conclusion here is that the ideal team structure or skillset would look as follows:

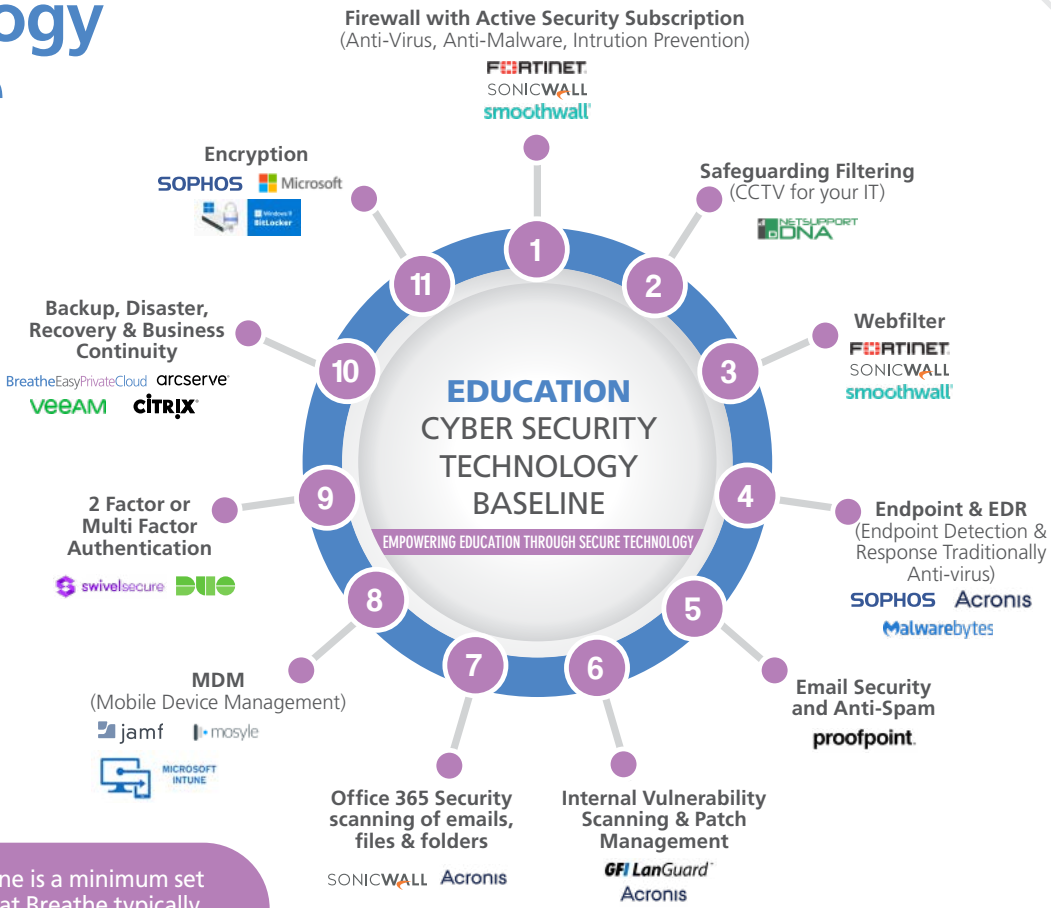
- An IT Director
- A Security Consultant or CISO (Chief Information Security Officer)
- Senior Infrastructure Engineer
- Desktop Support Engineer

Especially considering that school networks are often classified as enterprise networks based on the number of users and devices.

The reality is that these skillsets may be required in order to manage IT and cyber security well, but it's not financially feasible for schools, nor do they need these roles full-time. Which is why it lends itself to the managed services model.

The MSP supplies these resources only for the amount of time the school needs and works as part of the extended IT support team. The MSP picks up the burden of employment, HR, holidays, and sick cover, ensuring that the engineers are trained, certified, and exposed to enough projects and customer sites to create an experience that is second to none.

Cyber Security Technology Baseline



The security baseline is a minimum set of technologies that Breathe typically implements as a standard within the schools we work for. Advanced technologies are listed, but these don't always feature at all of our customer sites. It depends on the complexity and size of the organisation and what level the school or trust is at in terms of developing a Cyber Security Strategy.

Advanced Systems:

- SIEM (Security Information and Event Management)
- Automated Penetration Tests
- Automated Phishing Attacks
- DRP – Digital Risk Protection

intruder
Secure Schools
SKURIO

Breathe Services Overview

Empowering Education through Secure Technologies

Full Service MSP

- Breathe was created to work with schools by design. Today, we do work with businesses, but we still spend the majority of time in Trusts and Schools.
- A full-service MSP is certified to provide specialist services and support, such as IT Strategy, Cyber Security and Cloud Services.
- We don't believe in break-fix support but rather pro-active management of the IT systems, processes, infrastructure, and end-user support.

Which Cyber Security Packages are available?

ENTRY LEVEL	MID LEVEL	PRO LEVEL *(Most Popular)*	CERTIFIED LEVEL
Enhanced Cyber Security	**Enhanced Cyber Security**	**Enhanced Cyber Security**	**Enhanced Cyber Security**
✔ Mini Pen Test / External Scan (Non evasive)	✔ Detailed External Penetration Test using recognised Real Life Hacker Tools	✔ Details External Penetration Test using recognised Real Life Hacker Tools	✔ Details External Penetration Test using recognised Real Life Hacker Tools
✔ Security Topology Review	✔ Security Topology Review	✔ Security Topology Review	✔ Security Topology Review
✔ IT Risk Analysis (NCSC)	✔ IT Risk Analysis (NCSC)	✔ IT Risk Analysis (NCSC)	✔ IT Risk Analysis (NCSC)
✔ Internal Vulnerability Assessment	✔ Internal LAN Vulnerability Assessment, using a software suite to identify vulnerabilities in software and devices	✔ Internal LAN Vulnerability Assessment, using a software suite to identify vulnerabilities in software and devices	✔ Internal LAN Vulnerability Assessment, using a software suite to identify vulnerabilities in software and devices
✗	✗	✔ Gap Analysis – DFE Meeting Digital & Technology Standards	✔ Gap Analysis – DFE Meeting Digital & Technology Standards
✗	✗	✔ Review of ICT Processes and Policies (related to Cyber Security)	✔ Review of ICT Processes and Policies (related to Cyber Security)
✗	✗	✔ Real world scenario, Simulated Phishing Attack	✔ Real world scenario, Simulated Phishing Attack
✗	✗	✗	✔ Cyber Essentials Gap Analysis prior to the Cyber Essentials audit to ensure a first time pass rate
✗	✗	✗	✔ Breathe engage with a 3rd party certification partner and manage the certification process
2 Consulting days	**3 Consulting Days**	**5 Consulting days**	**6 Consulting days**

Discount Available for Audits

- A 20% discount is available as part of an ICT network audit package.
- It is possible to add simulated phishing attacks, penetration testing, or the Managed Cyber Essentials Certification as a separate item at a later stage.

A closing word from our MD

Craig Van Aswegen
MD & Snr IT Management Consultant
Breathe Technology LTD

Our customers value their cyber security more than ever. Mainly due to a significantly increasing problem and user awareness.

It's probably important to state that our ideal customers are Education Trusts, Colleges, Secondary Schools, Primary Schools and Infant Schools. It's where we show the most value.

10 years ago, primary and infant schools, especially, had much simpler IT, and the younger students had very little to do with IT. Those days are no more!

Young people today are very IT-savvy! They even walk around with iPads provided on 1:1 computing programmes such as iLearn by the school.

The fact is that all schools have become completely reliant on the internet, cloud services, technology in the classroom, and even VoIP telephony.

Everyone has become aware of the high levels of cyberattacks against schools, the public sector, and small to mid-market businesses. Schools and small to mid-market businesses are the most affected.

The national Cyber Centre advises all government departments, including the Department for Education (DFE), and is constantly communicating and doing their best to educate us on the risks.

Their advice for schools and small to mid-market business sectors is second to none.

Gone are the days of criminals running into banks with Tommy guns. It's much easier to hold a school or business at ransom after a cyberattack, data theft, or to empty someone's bank account from the comfort of a desk. Less adrenaline-filled, octane-filled operations are much safer and more effective. As the use of cloud services rose after the pandemic lockdowns and our ways of working changed forever, so did cybercrime.

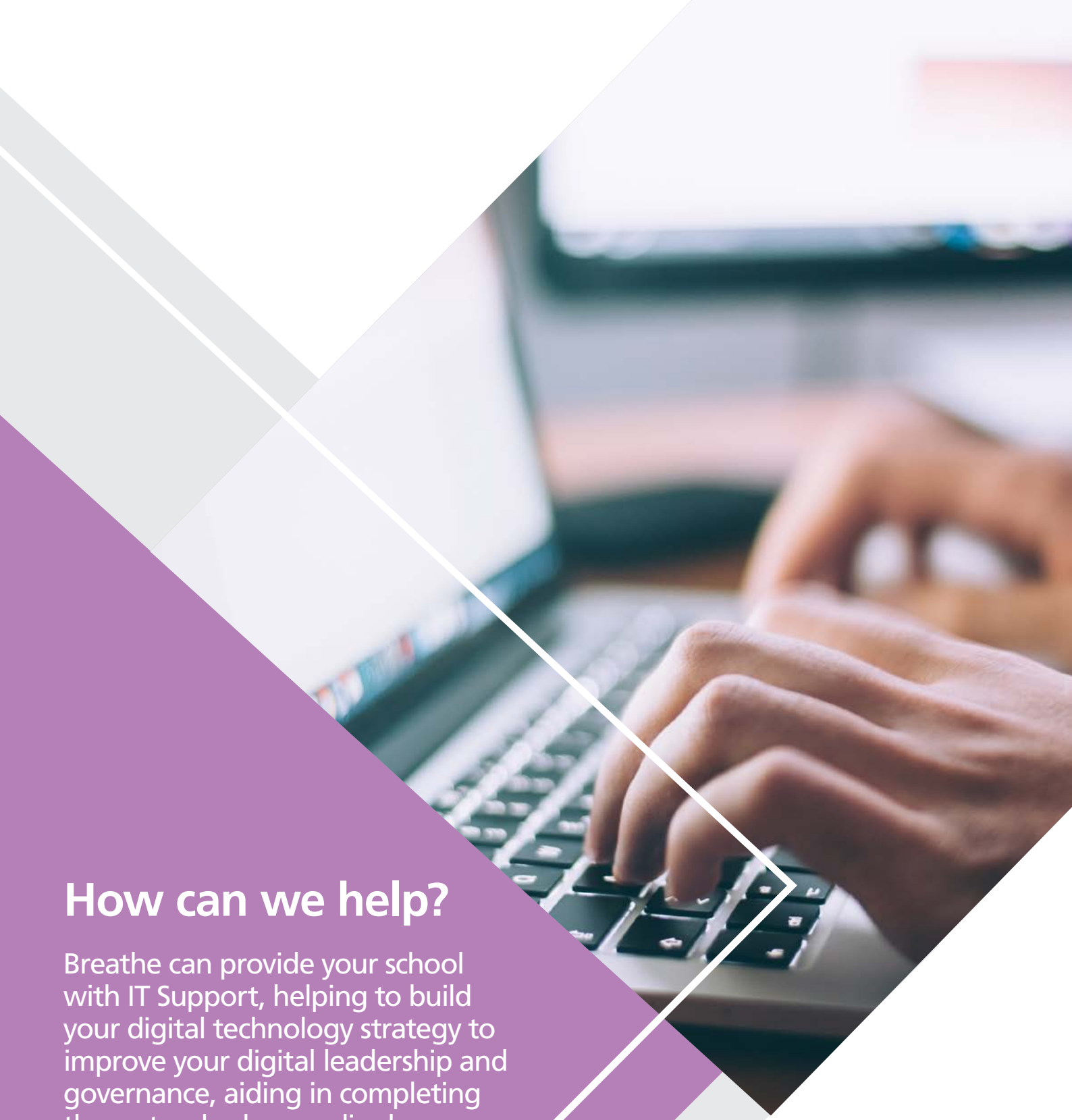
It would be ignorant to think that we will not experience a data breach, account compromise, phishing attack, or even a full network compromise at some point.

It's your duty to:

- **Protect Yourself.** Have your systems and processes reviewed or audited. Understand what the risks are, the latest threats, and the best proactive and mitigation measures.
- **Have the minimum security baseline in place in** order to protect your staff, your students or customers, your data, and your systems.
- Someone with the right experience needs to assume the CISO (Chief Information Officer) and DPO roles. You cannot manage cyber security or IT unless you hold someone qualified responsible. Regardless of whether this is in-house managed or outsourced.
- This is a big one. If you have a Managed IT Service Provider, do not assume that they are qualified for security. You must check their credentials and memberships and see what systems and processes are in place.
- It is also critical to have an IT Security Plan or Policy in place. Without a plan, there can be no structure or defined functionality and responsibilities. It should cover the defences, the risks they mitigate, if you have a Security Framework in place, and who is responsible. There should also be regular management reporting and meetings to effectively govern cyber security. Don't simply rely on IT. This is a management decision, and the plan should be agreed upon by the management team. Even if you are non-technical.
-

- The same applies to the Backup, Disaster Recovery and Business Continuity Plan. This definitely is not an IT decision! IT can guide, facilitate, import, and support the plan, but it is completely a management decision. Consider your risks! The risks of yesterday were staff errors, hardware failures, natural disasters, the server room overheating or flooding, theft, and power outages. The risks of today are all of those, and the biggest risk is cyberattack. Your plan should cover all scenarios with SLA's and an indication of how long disaster scenarios or even basic backup recovery will take and affect your ability to function.
- Both your IT Cyber security Plan and Backup Plan should include the latest government guidelines and best practices.
- Do you have an incident response plan? Or would a cyberattack cause pure chaos and your staff possibly cause more damage? Can you continue to operate? The NCSC has a response plan that can be adapted for your trust, business, or school.
- In the event that the attack has a severe impact or the attacker is demanding ransom, can you make your final stand? Often, this comes in the form of an Offsite/ Offline Backup, hosted outside of your network.
- The only way to know if your systems will provide the correct amount of protection is to test them. Examples include penetration tests to see the outside of your network as an attacker would, internal vulnerability scanning to check systems and applications for vulnerabilities, and backup and DR testing.
- Finally, if you are serious about your cyber security, consider certification. An external audit and certification does mean that you have done as much as you can to ensure you have the systems and processes in place to keep the organisation, people, and systems safe. A simple, cost-effective first step is the government's Cyber Essentials Certification. It's available for both schools and businesses. It also shows your stakeholders and customers that you are on the case. The next step is ISO 27001, which is a bit costlier and more involved. However, we truly believe in the benefits we get from the ISO certifications. The processes, global best practices, and independent checking of these.

Breathe is ideally placed to help you with the tasks above. Often, the best starting point is an IT or Cyber Security Audit. We look forward to helping you and sharing our experience.



How can we help?

Breathe can provide your school with IT Support, helping to build your digital technology strategy to improve your digital leadership and governance, aiding in completing these standards accordingly.

Get in touch

www.breathetechnology.com
(live chat available)

London	020 3519 0124
Cambridge	01223 209920
Sheffield	0114 349 8054
Suffolk	0144 059 2163

lucy@breathetechnology.com

breathetechnology
support | cloud | security | infrastructure | comms