I.T. is not ROCKET SCIENCE

Breathe 11 Step Cyber Security Risk Assessment

breathetechnology

infrastructure | support | security | cloud

Breathe 11 Step
Cyber Security Risk Assessment

As an experienced Security Business, we realise that there is a balance between security and what's practical for the Trustor or school to achieve. Apart from cost and skill-set, the network should not be locked down, to the point where it prevents your organisation from functioning seamlessly.

This checklist has been created to help you cover the basics and is based on the guidance from the National Cyber Security Centre. https://www.ncsc.gov.uk/guidance/10-steps-executive-summary

Date of Assessment: _____

Person responsible: _____

Check 1: Security and Risk Management Process and Policies

You should have an approach which is documented with some basic policies and procedures. This should then be supported by the management team, if you have one in place, this should be communicated to employees, contractors and suppliers. Don't over complicate it, make it practical but ensure it's understood and followed. You need this by law to cover your GDPR responsibilities anyway.

Question 1: I have security procedures and policies in place?

Yes ☐ No ☐

Comments: _____

_____

_____

_____

Check 2: Secure configuration

Administrator access should be limited to the appropriate person or IT Support Partner.

Equipment configurations should be standardised where possible. This includes the version of Windows, MS Office and other applications. Mapped drives and access to system resources. Critically important is system updates and patches.

Most customers we ask, believe that someone is looking after this. When we audit the network, often we find that updates are not being managed to expectation. A simple method to check is, to ask how updates are being done. Unless it's centrally managed via a programme like GFI LanGuard or Windows WSUS/ or Windows Systems Centre, it's unlikely that it's being efficiently done.

Question 2: My computers are locked down and we perform patches and updates?

Yes ☐ No ☐

Comments: _____

_____

_____

_____

Check 3: Network Security

The connections from your network to the Internet, and other partner networks, expose your systems and technologies to attack. This is a fact! And regardless if you believe that your systems or your data is not valuable to anyone… it is a false sense of security. They might not want your data but they would like the money from your organisation or staff bank accounts. You could also be added to their spam network or use your systems to hack other networks. Actually, your data would be great too, especially in an encrypted format! Bitcoin always comes in handy as part of a ransomware attack.

These days your networks almost certainly go further than the school LAN, if you consider the use of mobiles, remote working and teaching, and cloud services. This makes defining a fixed network boundary very difficult.

Rather than focusing purely on physical connections, think about where your data is stored and processed, and whether an attacker would have the opportunity to interfere with it. It does sound a bit like a 'GDPR Data Eco System document', but it's ultimately the same fundamentals that apply.

THE BASICS:

****Emails and the web are the high-risk targets and where most compromises occur! That includes HTTPS web pages.**

3.1 The first factor to consider is your Gateway Firewall/ Web filter. Does it have a subscription service on it for things like Anti-Virus and Anti malware, and does it filter your web browsing? If the answer is no…then you are exposed.

Yes ☐ No ☐

Comments: _____

_____

_____

_____

3.2 Can your web filter scan encrypted pages? In the old days, many firewalls and web filters simply passed through HTTPS pages because it wasn't practical to scan them. In todays world, a large number of pages are encrypted and the attackers make use of this to hide malware. We call this shadow malware. Security vendors now offer technologies such DPI SSL and variations of this, which allows the security solutions to scan encrypted pages. It's becoming a must have security technology.

Yes ☐ No ☐

Comments: _____

_____

_____

_____

3.3 **Emails** should be filtered for **anti-spam** and **anti-virus**. Regardless if it is on premises, hosted or in Office 365. There is a misconception, that your email is safe in Office 365. You still have the same security considerations, regardless of where your email is hosted.

Yes ☐ No ☐

Comments: _____

_____

_____

_____

3.4 **Remote Access/Home working** has become a 'Biggy'. Covid-19 has definitely changed the way we work. Remote working and learning will surely be a standard way of life for many of us. But is your infrastructure ready for this?

SSL or IPSEC VPN, Remote Access Servers and Two factor Authentication should be in place for remote access to the schools' network. Consider carefully who you provide it to, and manage their access. In an ideal world, two factor authentication should be implemented as user passwords is very often the weakest part of the system. This could be a fob or an app on your smart phone providing an additional code for logon. Open remote desktop access should be a 'no no' as it has too many vulnerabilities.

Lastly, SharePoint and OneDrive are available as part of Office 365. Is there a clearly defined plan on how access rights are setup and integrated with Active Directory?

Yes ☐ No ☐

Comments: _____

_____

_____

3.5 **Up to date Anti-Virus** with a subscription and a central management console should be deployed. Review this console and ensure that the AV agent has been distributed to all machines and they are up to date. Machines that are not up to date provide a weakness. Your network defences are only as strong as the weakest link! Consideration to be given on how remote workers update their AV!

Yes ☐ No ☐

Comments: _____

_____

_____

3.6 Ensure you have a working and documented backup or **business continuity process.**

Ensure that it covers all relevant data, servers, applications and system settings. Consider your local on-premise systems, but also your Cloud Infrastructure, including Office 365 and SharePoint. Your Physical and Virtual Servers need to be backed up and you need an offsite copy for disaster recovery purposes as a minimum. Offsite, could be on the same campus but a separate building or hosted in the cloud or somewhere else. The restore process should be tested and you need to see evidence of this, to ensure it actually works!

Ideally you should have a local backup and a secondary location of hosted backup.

Yes ☐ No ☐

Comments: _____

_____

_____

3.7 With the increase of mobile devices in the work place and learning environments, considerations should be given to how these devices are managed and secured. MDM (mobile device management) is critical. Imagine a smart phone or a tablet with customer, staff or student data, i.e. emails and images, bank details and cached login information lands in the wrong hands.

The ICO and its fines would probably only be the start of your worries!

Question 3: I can confidently say that all these measures are in place?

Yes ☐ No ☐

Comments: _____

_____

Check 4: Managing user privileges

If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise will be more severe than it needs to be. All users should be provided with a reasonable (but minimal) level of system privileges and rights, required for their role. The granting of highly elevated system privileges should be carefully controlled and managed.

Admin/ IT staff should have relevant levels of access and there should really be a policy in place on their levels of data handling and access.

Careful consideration should be given to local installation rights. If the IT is outsourced completely and a local user with install rights is a must, then a super user should be assigned and trained.

Filer, folder and application rights should be documented, reviewed and managed. Ideally the employee onboarding and offboarding process should be linked to this process. This ensures that new starters or someone moving between departments or roles only get the relevant access rights and leavers rights are removed.

Question 4: Only authorised staff have admin rights?

Yes ☐ No ☐

Comments:_____

_____

_____

_____

Check 5: Passwords (Source: Sans Institute Top 20)

Passwords is on the list as one of the oldest vulnerabilities known to IT.

As time and technology changes, it is only becoming a more complex issue. We all now have multiple passwords for so many online systems and often two factor authentication to aid the security. The internationally recognised SANS Institute provides the following guidelines:

5.1 Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behaviour.

5.2 Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password.

5.3 Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

5.4 Ensure that all service accounts have long and difficult-to-guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.

Yes ☐ No ☐

Comments:_____

_____

_____

_____

Check 6: User education and awareness

End Users have a critical role to play in their organisation's security. It is important that security rules and the technology provided enable our users to do their job, but also keeps the organisation secure. It's critical that you create a culture of awareness and your staff understand that they should think before they act and realise that the world is not a safe place and cyber-crime is at an all-time high.

Consider that something as simple as a staff member click 'Ok' on a pop-up window could cause encryption of the network. If it doesn't look right … don't trust it.

Another example is fake payment requests or invoices sent from the Business Manager to the Finance Manager asking them to transfer an amount of money to someone. So many people have fallen for that scam.

Question 6: Am I informing my staff and making them security conscious?

Yes ☐ No ☐

Comments:_____

_____

_____

_____

Step 7: Incident management

Reality is, that you will experience a security incident at some point. Come to terms with this and think about having a process in place to deal with it.

Implement a practical and effective incident management policy and process that will help to support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. Also consider the GDPR requirements if relevant and the ICO process.

You should identify recognised sources (internal or external) with the relevant expertise and ensure your internal resources understand the process and what to do.

Question 7: Do your staff know how to identify a breach and how to deal with it?

Yes ☐ No ☐

Comments:_____

_____

_____

_____

Step 8: Malware prevention

This is another 'biggie'….

As a Managed Service Organisation, with a specialist security skill-set we deal with this on a daily basis. And truth be told… it's a pandemic. We see the effects from infamous Malware attacks such as WannaCry and Petya on the news… but there are real life cases in schools and businesses every day.

NOTE: Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach.

Security is normally implemented as a layered approached. See the network security section above.

Additionally, we believe that by scanning your email in the cloud, using an application like ProofPoint and having a good 'all in one' firewall like SonicWall at the gateway is a great start. The all-in-one approach means that you cover deep packet inspection firewalling, gateway anti-virus and web filtering with a single appliance and licensing method. We specifically like firewalls that have implemented market leading sandboxing technology, that has the ability to stop Malware attacks without the malware being previous identified. In other words, we don't need to wait for organisations to be infected and then to create the finger print and a fix. It's called Zero Day protection.

This approach helps remove a large percentage of the 'bad stuff' before it enters the network.

I'll take a minute to mention, that there are 'on demand' malware specialist scanners that can sit alongside your traditional anti-virus on your servers and desktops. Malwarebytes is probably the most known.

Question 8: I have the systems in place to prevent Malware compromising my network?

Yes ☐ No ☐

Comments:_____

_____

_____

_____

Step 9: Monitoring

System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

This can be provided from various layers in the network. Consider the following:

Email Security/ Anti-Spam reports e.g., Proofpoint

Firewall reporting e.g., SonicWall

Web Filter Reporting e.g., SonicWall

- Safeguarding Systems e.g., Net Support Software
- Anti-Virus e.g., Sophos or Kaspersky
- Anti-Malware e.g., Malwarebytes
- Patching and Vulnerability Scanning e.g., GFI Langured

- Network and Server Reporting e.g., Spice Works or Comodo RMM Software
- Backup Reporting e.g., StorageCraft
- System generated reports that are native to the hardware installed.

Typically, this is monitored by the IT Team and Managed Services Provider.

Question 9: I can say for sure that all my critical systems have monitoring setup and someone is managing this?

Yes ☐ No ☐

Comments:_____

_____

_____

_____

Step 10: Removable media

The age-old problem of using USB sticks and other forms of external storage….

Over the years this has been a real bug bear. Especially in our SME and School customer sites. Corporates and Universities generally have a defined policy and systems around this.

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the need to use removable media and apply appropriate security controls to its use.

The simple answer is…unless you really need it…. block it from your network and find other ways of working such as secure remote access, OneDrive or SharePoint.

If you need it…then you need to manage it. You will also most likely need to encrypt it too, as you do with Laptops. The risk here is actually much higher than laptops.

Luckily, encryption has become more mainstream and cost effective these days. We prefer using the encryption modules that come with end point security software like your anti-virus. As an example, both Sophos and Kaspersky have this feature available, but requires an additional license.

Yes, BitLocker is native with Windows. However, central management sometimes can be a more complex and integration with Active Directory is required.

The use of this technology should detail in your IT policies.

Consider your GDPR responsibilities, guidance from the ICO and definitely your ISO27001 or Cyber Essentials if you need to be certified.

Question 10: Removable storage has either been blocked or we have policies and management or encryption in place?

Yes ☐ No ☐

Comments:_____

_____

_____

_____

Step 11: Home and mobile working

Mobile working and remote system access, used to be seen as a luxury or suitable for some selected people.

Today it's mainstream, because of the pandemic, but surely has changed the way we work forever more. It does however expose new risks that need to be managed. You should establish policies and procedures that support mobile working or remote access to systems.

Train users on the secure use of their mobile devices in the environments they are likely to be working in. From a technology point of view, it would be suggested to have secure remote access via SSL VPN with two factor authentication to add an additional layer of security to the user passwords.

MDM and Encryption too, mentioned earlier.

Question 11: Our remote access is managed by a policy such as our acceptable use policy and we access via a VPN Technology?

Yes ☐ No ☐

Comments:_____

_____

_____

YOUR RESULTS?

Requirement	Status	Remedial Action
Check 1: Security and Risk Management Process and Policies		
Check 2: Secure configuration		
Check 3: Network Security		
Check 4: Managing user privileges		
Check 5: Passwords		
Step 6: User Education and Awareness		
Step 7: Incident Management		
Step 8: Malware Prevention		
Step 9: Monitoring		
Step 10: Removable media		
Step 11: Home and mobile working		

SUMMARY

** Summary and interpretation of the above results

LIST OF ITEMS TO ADDRESS:

**Task List of items to rectify or improve