Breathe 10 Step Cyber Security Checklist

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

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

You should be able to give a positive answer on all 10 questions. If not, then you have identified a risk and need to rectify it!

And if you need help, call us on 01223 209920 or email Lucy@Breathetechnology.com

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 and communicated to employees, contractors and suppliers. Don't over complicate it, make it practice but ensure it's understood and followed. You need this by law to cover your GDPR responsibilities anyway.

If you require Cyber Essentials or ISO27001, this is a must.

Question 1: I have security procedures and policies in place

Check 2: Secure configuration

Administrator access should be limited to the appropriate personal or IT Support Partner. Equipment configurations should be standardised where possible. This include 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, most of the time 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?

Check 3: Network Security

The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. This is a fact! And regardless if you believe that you have a small organisation and your data is not valuable to anyone…is a false sense of security. They might not

want your data but they would like the money from your business or staff bank accounts, add you to their spam network or use your systems to hack other networks.

Your organisation's networks almost certainly span many sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

The basics:

****Emails and the web are the high-risk targets and where most compromises occur**

3.1 Another factor to consider is if your **firewall/ Webfilter** has 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.

3.2 **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 lives.

3.3 **Remote Access/ Home working** should ideally be provided via SSL or IPSEC VPN. 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.

3.4 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!

3.5 Ensure you have a working and documented **backup process.** Ensure that it covers all relevant data. On premises and in the cloud including Office 365 and Exchange Online. Your physical and Virtual Servers need to be backed up and you need an offsite copy for disaster recovery purposes as a minimum. 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.

3.6 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 is critical. Imagine a smart phone or tablet with customer, staff or student data, emails and images, bank details and cached login information lands in the wrong hands. The ICO would only be the cause of one of the headaches.

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

Check 4: Managing user privileges

If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as 'least privilege'.

Question 4: Only authorised staff have admin rights?

Check 5: User education and awareness

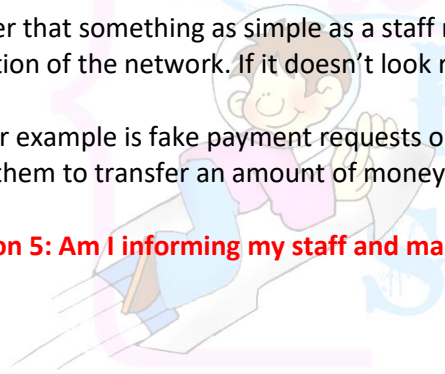
Users have a critical role to play in their organisation's security.

It's important that security rules and the technology provided enable users to do their job but also keep 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 MD to the Finance Manager asking them to transfer an amount of money to someone. So many people have fallen for that scam.

Question 5: Am I informing my staff and making them security conscious?



Step 6: 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 6: Do your staff know how to identify a breach and how to deal with it?

Step 7: Malware prevention

This is a 'biggie'….

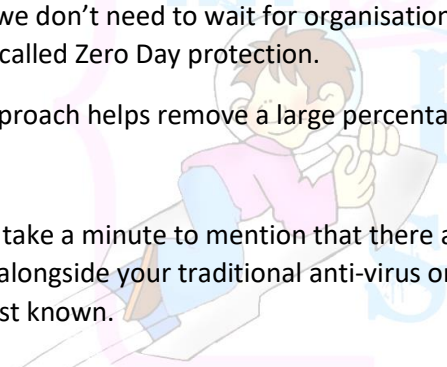
As a Managed Services organisation with a specialist security skillset we deal with this on a daily basis. And truth be told…it's a pandemic. We see the effects from infamous Malware attacks like WannaCry and Petya on the news…but there are real life cases in schools and businesses every day.

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 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 SonicWall because they have implemented market leading technology called Capture ATP (Advanced Threat Protection) that has the ability to stop Malware attacks without the malware being previous identified. In order words we don't need to wait for organisations to be infected and then to create the finger print and 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 also take a minute to mention that there are also '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 7: I have the systems in place to prevent Malware compromising my network?

Step 8: 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, your IT Support partner will monitor this if you have a good one! It's about being pro-active!

Question 8: I can say for sure that all my critical systems have monitoring setup and someone is managing this?

Step 9: Removable media

The age-old problem of using USB stick and other forms of external storage. Over the years this has been a real bug bear. Especially in our education sector customer sites.

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 business need to use removable media and apply appropriate security controls to its use.

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

If you need it…then you need to manage it. You will also most likely need to encrypt it.

Luckily encryption has become easier and cost effective these days. We prefer using the encryption module on your 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 complex in our opinion.

Typically, use of this technology should also be contained in your IT policies.

Consider your GDPR responsibilities and guidance from the ICO.

Question 9: Removable storage has either been blocked or we have policies and management or encryption in place?

Step 10: Home and mobile working

Mobile working and remote system access offers great benefits but exposes new risks that need to be managed. You should establish policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. 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.

Question 10: Our remote access is managed by a policy such as our acceptable use policy and we access via a VPN Technology?

Your Results?

Requirement	Pass or Fail	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: User education and awareness		
Step 6: Incident management		
Step 7: Malware prevention		
Step 8: Monitoring		
Step 9: Removable media		
Step 10: Home and mobile working		

PS. Remember the Breathe team can help! Please call us on 01223 209920 or email lucy@breathetechnology.com. Just mention that it's regarding the 10 Step Security Check List and your call will be directed to the relevant team.