



Cyber resilience health check

The 10 essential questions you should be asking about your
Cyber Resilience

a ramsac guide



Safeguarding your organisation against cyber threats has become increasingly vital, and assessing where you are currently in your cyber resilience journey is a fundamental step in understanding how best to protect your organisation moving forward.

This guide will give you the 10 simple questions you need to ask to verify your organisations level of Cyber Resilience.

1.	What are the main risks for your organisation in the event of a cyber breach?	4
2.	How well do you train your staff on IT security?	6
3.	Are your backups air-gapped /segregated from your local systems?	7
4.	Do your employees know what to do in the event of a cyber breach?	8
5.	Are all your laptops and servers kept up to date?	10
6.	Is MFA enabled for your most critical business systems?	12
7.	How much control do you have over your devices?	14
8.	Can you afford a cyber breach?	15
9.	Have you tested your cybersecurity measures ?	17
10.	Would you know if you were experiencing, or about to experience, a cyber breach ?	18



What are the **main risks** for your organisation in the event of a cyber breach?

The greatest assets to an organisation are its data, people, processes and technology. Every organisation relies on these assets to meet its goals and objectives. It is important to understand the interactions between these assets to ensure organisations function optimally and securely.

Cyber risk is the potential of exposing a business's information and communications systems to cyber criminals that could lead to a cyber-attack, data breach, or loss of access to data and technology assets.

Risk identification is the procedure taken to understand potential risks to an organisation that could affect the ability to conduct business. These risks are both internal and external. 81% of all cyber breaches happen to small and medium sized businesses globally. 97% of these breaches could have been prevented with the right security procedures and technology in place, but this can only be done if organisations understand the threat landscape, risk exposure and their current capabilities to defend against an attack.

To understand your current risk exposure, it is useful to undertake a detailed 'health check' of your IT estate. Your health check should identify your critical assets and should then consider each in the context of how those assets are stored, backed up, what access controls are in place and how well protected that part of your system is from external attack.



In IT circles we often say that a person shouldn't mark her own homework, so having someone independent from the person that's built or designed an asset to undertake the review is generally considered good practice.

After determining your current security posture and risk exposure, the next step is to determine your risk appetite and put together a risk mitigation strategy. Risk mitigation is the process of taking steps to prevent or reduce the severity of a cyber-attack.

Impact on Businesses

Businesses must adopt a multi-faceted and risk-based approach to cybersecurity. The implementation of comprehensive cybersecurity mechanisms, policies and procedures is a crucial part of a business's overall strategy for cybersecurity compliance and for protecting key IT systems and information assets. Testing implemented measures regularly to assess their effectiveness, as well as upgrading and enhancing them from time to time to remain current with wider technical developments is key.

Legal compliance requires the implementation of robust cybersecurity measures. Maintaining customer confidence requires businesses to continually adapt and react quickly as attack vectors change and new vulnerabilities are identified. Understanding the evolving nature of the threats they face, the weaknesses in their systems and identifying high-value information assets will enable businesses to deploy a strategy that offers the best protection.

Source <<https://www.whitecase.com/insight-alert/cybersecurity-and-uk-legal-landscape>>



How well do you **train your staff** on IT security?

Attackers often target company employees using phishing attacks to gain access to company corporate networks. Cyber defence technology alone is not sufficient to protect an organisation from a cyber-attack. Cyber criminals often use social engineering (such as phishing) which is a manipulation technique to exploit human errors and gain sensitive information such as usernames and passwords. These social engineering attacks try to lure unsuspecting employees to expose sensitive data, spread malware infections or give access to internal systems.

According to the NCSC 2022 cyber breach survey, in the UK, 83% of reported cyber breaches were caused by phishing attacks. Given that phishing generally relies on end user's behaviour, rather than an attempt to breach a physical security product, staff training is arguably one of the most critical elements of an organisation's cyber defence strategy. Training staff once does not provide enough protection against

cybercrime. Training should be comprehensive and regular, and the Information Commissioners office (ICO) has now mandated this for organisations.

The Information Commissioners Office (ICO) is the UK body that is responsible for prosecuting organisations that fail to keep data safe. In December 2021, the ICO issued new guidance saying that they expect all staff and volunteers that have access to data, to receive cyber awareness training as part of their induction, within 30 days of starting and before the employee is granted access to any databases containing personal or sensitive data.

Furthermore, they mandated that training should be ongoing for all employees and that the employer should be able to track and report on the completion of cyber training.

If an organisation suffers a cybersecurity breach and (as is required) reports it to the ICO, the ICO will expect that organisation to be able demonstrate completion of training by all new starters and ongoing training for all employees, including the management of non-attendees of prescribed training. A UK company was fined 4.4 million pounds after falling victim of a ransomware attack that breached the confidentiality of human resource databases that contained personal data of employees. This attack was via a phishing email sent to an employee which the employee opened on their computer that deployed a malware in their internal network. The ICO fined the company because they failed to put appropriate security measures in place.

In the UK, money is paid from a corporate account to a criminal's account every 15 minutes of each working day. The cost of a single data breach to Small and Medium Businesses (SMBs) typically ranges up to £186,000.



Are your **backups air-gapped/segregated** from your local systems?

Imagine writing a report that has taken a long time to complete only to realise that the report has been deleted and can no longer be retrieved, how upsetting would that feel?

Then imagine losing access to business-critical data that halts your daily operations due to a cyber-attack such as a ransomware attack, an unintentional deletion by an employee or a disk failure, and you do not have a backup to restart operations, what impact would that have on your business?

You really only know how good your backup system is when something has gone wrong. But that's the worst time to find out that your system isn't quite what you hoped it would be! Not all backups are created equally, and you need to ask some important questions about your own system.

Air-gapped backups serve as the last line of defence against data loss and it's a key component of a disaster recovery plan.

An air-gapped backup is a backup copy of your business critical data stored in a completely separate location to the original source. In days of old, this was achieved by backing up a file server to a tape, and then storing that tape away from the main site. In modern cloud based systems, too many organisations rely on the primary supplier to be backing up their data, but this is often being done in the same tenant as the main data application. A proper backup should always be completed in a way that is independent of the primary source – to provide an air-gap between primary and recovery data.

This protects your data from being destroyed, accessed, or manipulated in the event of a ransomware attack or any other type of cyber-attack because it is stored on a storage infrastructure that is not accessible from an external connection or the internet. Air-gapped backups serve as the last line of defence against data loss and it's a key component of a disaster recovery plan. Air-gapped copies should be monitored and updated regularly.



Do your **employees** know what to do in the event of a cyber breach?

- Do you have a breach response plan in place?
- Do your employees have clearly defined roles and responsibilities in responding to a cyber breach?
- Do you have a business continuity plan outlining procedures for restoring critical affected systems?
- Do you have a plan in place to respond to loss of availability of IT Infrastructure?

For as long as any of us can remember, testing your fire evacuation plans has been a core component of UK Health & Safety Laws. The reason for this is that, in the event of a fire, you want your staff to almost have 'muscle memory' for what to do to get themselves to safety, and to prevent the spread of fire within your building. Regular training and testing, together with clearly indicated procedures and well signed exits, prevent panic from breaking out, and means that everyone knows instinctively what to do.

A cyber breach plan works in exactly the same way. You take time to think in advance of the possible risks and the steps that people should take once the alarm has been raised.

Every organisation needs to have a breach response plan. The breach response plan defines the organisation's use of processes and technology in detecting and responding to cyber

threats, cybersecurity breaches and cyber-attacks. The breach response plan should have clearly defined strategies in planning for, responding to, managing and mitigating cybersecurity breaches.



A breach response plan lists the activities which must take place during and immediately after a cyber breach. These activities include determining the extent of the breach, managing the immediate impact, preventing the spread, rectifying the compromise of the systems and managing the aftermath including any potential PR impact. The breach response should also cover producing a report that documents the scope of the problem, its technical impact, its impact on the organisation, its partners and lessons learnt.

Disaster recovery on the other hand, is the method of regaining access to IT infrastructure by an organisation after an unplanned incident such as a cyber-attack, power outage, natural disaster or other disruptive event. These unplanned disruptive incidents can lead to financial losses, reputational damage and unhappy customers. The longer it takes to recover from an incident, the greater the impact it has on the business. A disaster recovery plan is a formal document every organisation should create detailing steps to take to minimise the effect and methods to rapidly recover from a disaster that causes a loss of availability of business-critical assets such as information and technology assets. The Disaster Recovery plan should highlight the disaster

recovery team, the business-critical assets, what should be backed up, who should perform backups, the frequency of backups and how backups should be implemented amongst other DR steps. It is important that every organisation has a clear disaster recovery plan and the resources to support this plan in order to enable rapid resumption of operations when a disaster occurs.

It would be catastrophic if a company assumes they know what to do in the event of a disaster only to find out their DR plan is not fit for purpose by then it might be too late. Hence, a disaster recovery plan should be tested regularly to check its effectiveness. Firstly, a table top exercise should be carried out regularly that discusses different IT and Cyber-attack incident scenarios that could occur. This exercise allows members of the recovery team to better understand their roles and responsibilities in responding to a disaster.



Having a comprehensive breach response plan will lessen the impact of a cybersecurity breach.



Are all your **laptops and servers** kept up to date?

Operating systems, firmware and software are constantly being exploited by cyber criminals, taking advantage of vulnerabilities found in them. The developers of software usually send out regular fixes or 'patches,' to address vulnerabilities that have been found. It is important to update software and hardware with the latest updates from the developer to prevent the chances of the vulnerability being exploited using currently known vulnerabilities or vulnerabilities that might be discovered in the future.

End-of-Life (EOL)/End-of-Support (EOS), software is no longer supported by the developer which implies that developers stop updating and patching the software. Using software that is no longer supported opens businesses up to hackers who can exploit unpatched vulnerabilities in outdated software.

The ICO considers that regularly updating Operating system, Firmware and Software is good cybersecurity practice and recommends this should be done by every organisation. In the event of a cyber-attack, if this hasn't been done it would be



It's
an arms
race between
cyber criminals
and cybersecurity
professionals in
attacking and
defending against
cyber exploits.

deemed as a failure to have taken appropriate measures to protect business and personal information, which could attract a fine from the ICO.

It is important every business has a procedure in place to monitor and automatically update operating systems, software and firmware with security patches and new features. EOL/EOS usage should be discontinued. Hardware without warranty should be updated or discontinued if warranties are no longer available.

Anti-Malware/Anti-Virus software is designed to detect and remove all kinds of malicious software such as viruses from servers, workstations and laptops. Anti-Malware software undoubtedly helps to protect against cyber-attacks.

Once a device is infected with malware, it can steal data, encrypt it so you can't access it (ransomware attack), or even erase it completely. Hence, Anti-Malware software must be installed and functioning on all servers, workstations and laptops. Anti-Malware software should be kept up to date to protect your data. Anti-Malware with the latest update contains the most recent virus signatures which make it possible to defend against recently discovered malware exploits.

A centrally managed Anti-Malware solution, that can automatically update Anti-Malware software and monitor that it's working properly, reduces the human errors that can occur from leaving this entirely in the hands of employees.





Is **MFA** enabled for your most critical business systems?

In traditional systems, all you need to know to gain access to an IT system, is a username and password. Passwords are not the most secure way to protect your organisation resources, because they are vulnerable to brute force attacks plus users often use the same password over multiple systems, that are often not complicated enough and not changed frequently enough.

Multi-Factor authentication (MFA) is a method of authentication that requires a user to provide more than one verification

method to gain access to company resources such as data and applications. MFA will enhance the security of an organisation and it's a strong component of a robust Identity and Access Management policy. MFA increases security because even if one credential becomes compromised, unauthorised users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database.

There are generally three different types of authentication factors:

- **Something you know:** Usually passwords or PIN numbers and the more complicated the better, but anything you need to remember falls into this category.
- **Something you are:** Use of a biometric feature, such as fingerprints, facial recognition or voice recognition. If you're using a mobile app as part of your MFA, the fact that the device itself needs to be unlocked using a thumb print or facial recognition, has added an additional factor in the process to access your data.
- **Something you own:** This could be smartcard or a hardware token that generates a code. It could also be a code that is sent to a separate device to the one you're logging on to. In most cases, MFA involves the sending of a time limited code as either a text message or mobile app on a mobile device enrolled by your organisation to receive the code.

It is important to configure MFA on admin accounts and enable it to be active at all times barring special circumstance. Accounts with administrative rights are targeted by attackers because these accounts have privileged rights. Enabling MFA is an easy way to reduce the risk of admin accounts getting compromised.

Increasingly, more and more businesses have employees working remotely and accessing company data over the inherently unsecure internet. Furthermore, companies are increasingly using cloud services for storing data in the cloud, for email services etc. and whilst previously users needed a VPN to access company data, access is now much more straight forward. This has led to a significant increase in cybercrime with criminals

Something you are
Something you own
Something you know

focussed on stealing email addresses and passwords. Hence, it is important that employees use MFA before they can access company data and resources.

Microsoft estimates that the use of MFA reduces the risk of cyber breach by around 97%. Most insurance companies will no longer pay out for data loss claims if MFA was not in use. Making MFA an absolute essential for all organisations.





How much **control** do you have over your devices?

Many organisations today tend to have employees working remotely, either fully or partially in a hybrid model. This has created a situation where company data and resources are accessed using both company and personal devices from anywhere. Companies are challenged with finding a secure way for employees to collaborate and access company resources in a secure manner. Company admins need to protect organisation data, manage end user access, and support users from wherever they work.

Mobile device management (MDM) is a type of security software that enables organisations to manage and secure mobile devices such as smartphones, tablets, and laptops, from a central location. The goal of MDM is to ensure the security of corporate data and applications on these devices while still allowing employees to use their own personal devices or company-issued devices to access work-related data and services.

MDM allows IT administrators to remotely manage and monitor devices, enforce security policies, and push software updates to devices. This helps to ensure

that devices are up-to-date with the latest security patches and that employees are following company policies, such as password requirements and device encryption.

Using MDM
to remotely lock
or wipe, a lost or
stolen device, gives
organisations piece of
mind that their data is
safe.

In addition to security, MDM can also help organisations to improve productivity by providing employees with access to company resources and apps from their mobile devices. This can enable remote work and improve collaboration among team members.



Can you **afford** a cyber breach?

39% of UK SMBs reported a cyber-attack or data breach in 2022. The cost of a cyber-attack to UK SMBs typically ranges up to £186,000.

The impact of a data breach can be financially damaging to businesses, 60% of SMBs go bust after a successful cyber breach.

Cyber Insurance is an insurance policy that covers your organisation's liability for a data breach and covers your costs of responding to and mitigating a

cyber-attack – such as extortion costs, breach notification costs, loss of revenue and regulatory fines. Cyber insurance obviously doesn't prevent cyber breaches from occurring, but it provides peace of mind that business disruption and the associated financial impact, will be minimised. Different insurance policies will cover different things and it is important to understand in detail what the policy covers, and equally important, what is excluded.

Cyber Insurance considerations

Cyber insurance policies will include different types of coverages that span first-party loss, first-party expenses, and third-party liability, each with specific parameters.

- **First party loss:** typically includes loss of revenue due to business interruption.
- **First party expenses:** would include the many services and resources needed to recover from an attack.
- **Third party liability:** may cover expenses and legal fees related to the potential damage caused by the incident to third party.

Cyber Insurance Requirements

To successfully buy a policy at the level of cover a business requires, will be dependent on their ability to show they have appropriate controls in place to reduce cyber risks. These requirements will vary depending on the insurance company but most insurers will ask questions including:

- Do you require all your employees to complete a security training course? What about all your contractors?
- Do you have a formal information security program in place?
- Do you use multi-factor authentication (MFA)?
- Do you backup your data?
- How do you process data while in transit and at rest? (Do you encrypt data?)
- Do you have a risk management disaster program in place? What about a disaster recovery program?
- How do you perform third-party due diligence with vendors and contractors?
- Do you carry out regular Security Testing?



The impact of a data breach can be financially damaging to businesses, 60% of SMBs go bust after a successful cyber breach.



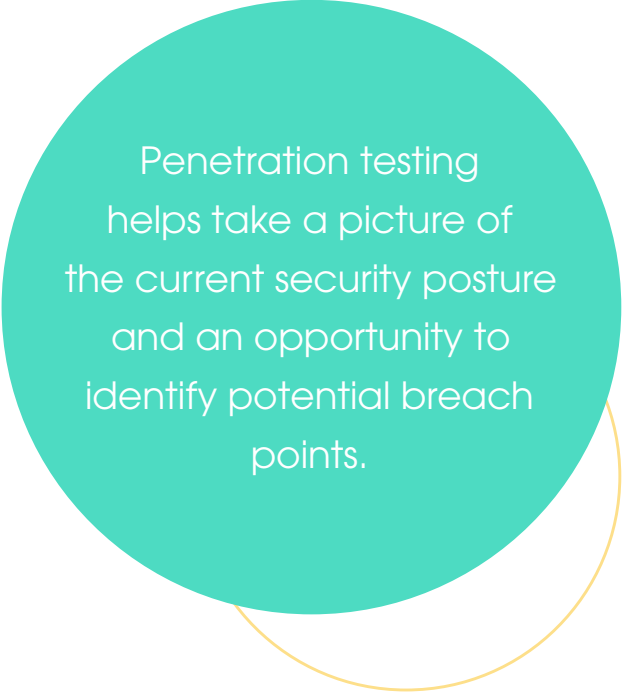
Have you tested your **cybersecurity measures**?

Penetration testing allows a cyber professional also known as an ethical hacker, to test your organisation's cyber resilience as if they were an attacker, using similar methods a cybercriminal would.

A comprehensive pen-testing exercise will encompass both social and technical attack techniques. In a social pen-testing exercise, the penetration tester uses typical social-engineering techniques deployed by cyber criminals, to understand the organisations extent of vulnerability to this type of exploit. Social pen-testing is designed to test employee's compliance to security policies and procedures. The outcome of a social pen-testing is to provide companies an overview on how easily an intruder could convince employees to give out sensitive information or break security rules defined by management. The outcome of a social pen-testing would give a better understanding of the effectiveness of the company's security training and what changes needs to be made.

Technical pen-testing involves the pen-tester testing a company's computer systems, network infrastructure and applications to expose security weakness that could be exploited by cyber criminals.

The threat landscape is constantly changing, vulnerabilities in software are found regularly, business network architecture may change with time and misconfiguration of networks and cloud infrastructures are very common, it is important we continue to test our cyber resilience to constantly improve on cyber defence.



Penetration testing helps take a picture of the current security posture and an opportunity to identify potential breach points.



Would you know if you were experiencing, or about to experience, a **cyber breach**?

Imagine the UK without police officers, intelligence services, and CCTV surveillance, how difficult would it be to prevent or solve crimes?

Monitoring in a cybersecurity context is like an intelligence agency using surveillance camera, police patrol, and the exchange of intelligence between various security agencies to detect, prevent and solve crime.

A Security Information Events Management (SIEM) and Security Orchestration, Automation and Response (SOAR) tool ingests data from across an organisation's applications and network to have full visibility of your organisations estate to protect the network from cyber threats and vulnerabilities.

The purpose of SOAR and SIEM tool is to identify security vulnerabilities and mitigate any potential cyberattacks by taking specific actions to resolve and eliminate any cyber threats or vulnerabilities.

SIEM software identifies potential threats by collecting, logging events data (collected

from applications, firewalls, endpoint devices, anti-malware software and authentication activities) and analysing this data. Based on the potential threat identified, it alerts the cybersecurity team to investigate and resolve.

A SOAR tool on the other hand, minimizes the decision making a cybersecurity team needs to do to resolve a potential threat by automating the response process, reducing any manual tasks done by security teams. A SOAR tool uses artificial intelligence and machine learning to analyse data gotten from internal and external sources, makes security recommendations and automates responses to security incidents.



About ramsac

**If you take cybersecurity seriously,
ramsac are the secure choice**

ramsac provide so much more than just IT support. We help our clients to get the best out of technology – implementing, managing and supporting secure, resilient, flexible IT solutions. We work with small and mid-sized organisations, providing them with strategic IT input, proactive management, jargon-free IT support and solutions that help them to grow their own organisations efficiently and securely. Our exclusive Cyber Resilience Certification programme helps organisation achieve the highest level of cybersecurity protection and allows them to demonstrate their commitment to their own stakeholders via our Gold certification standard.

Whether it's designing a new infrastructure, migrating services to the cloud, implementing enhanced security practices or providing end users with really efficient and friendly 24 hour IT support, ramsac manages IT on your behalf, so that you can focus on achieving your organisation's goals, safe in the knowledge that IT is secure, staff are working efficiently, and the IT investment is delivering tangible benefits to the business.



More information

For more information on cyber resilience from ramsac please contact us on **01483 412040**, email **info@ramsac.com** or visit **ramsac.com**

ramsac Limited

www.ramsac.com
01483 412 040

