cyberlab

10 Steps to Cyber Security

The Ultimate Cyber Security Guide

cyberlab

Smaller Organisation? Discover Security 101: Cyber Essentials

Clear and concise guide to fundamental cyber security practices, helping businesses protect themselves against common threats. By following these guidelines, small organisations can significantly reduce their vulnerability to cyber attacks, safeguarding their operations and customer data in a cost-effective manner.

CYBER ESSENTIALS

Visit Cyberlab.co.uk or scan QR Code

Introduction

This eBook explores the 10 Steps to Cyber Security framework developed by the National Cyber Security Centre (NCSC) and how to keep your data secure, and your organisation protected.

This guidance is best suited for medium to large organisations that have someone dedicated to managing the organisation's cyber security.

This guidance is designed to assist organisations in handling their cyber security risks by dividing the task of safeguarding the organisation into 10 components. Adopting the security measures outlined in the 10 Steps greatly diminishes the likelihood of a successful cyber attack and mitigates the impact on your organisation should an incident occur and outlines effective strategies to mitigate risks.

Contents:

Risk Management

Risks are a natural part of any business, as is managing the risks that represent a threat to your business be they from competitors, shifts in market trends or as is increasingly the case, cyber threats.

Cyber risk management is something that should support your companies' objectives and goals, not obstruct them. It can be used to set limits on risks that are and are not, acceptable with regards to technology use.

"...by 2025, 60% of organisations will use cyber security risk as a primary determinant in conducting third-party transactions and business engagements."

Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23

Five Steps of Cyber Risk Management

Identifying Risks

Assess your systems, processes, and data to pinpoint vulnerabilities and threats, understanding critical digital areas by evaluating the impact of potential disruptions.

Assessing Likelihood and Impact

Determine the probability and consequences of each risk, from data loss to financial risks.

Prioritising Risks

Prioritise risks based on their likelihood and impact, focusing on credible risks that could significantly disrupt operations and using risk assessment frameworks to compare and understand severity.

Implementing Controls

Mitigate or eliminate identified risks by implementing technical solutions like firewalls and antivirus software, alongside operational changes, and security features, considering cost-effective measures.

Monitoring and Reviewing

Continuously monitor systems and processes to ensure effectiveness of implemented controls, promptly identifying, and addressing new risks for ongoing risk management.

Cyber Insurance

Cyber insurance is an essential safeguard for businesses, providing financial protection against the growing risk of cyber incidents, such as data breaches or ransomware attacks. It complements your cyber security measures by covering costs associated with recovery, legal fees, and potential liabilities.

Tales from the CyberLab:
Cyber Insurance Explained with Marsh Insurance

To better understand how cyber insurance can benefit your organisation, tune into Tales from the CyberLab podcast episode featuring Eric Alter, Senior VP Risk & Cyber Engagement Leader at Marsh, who discusses key considerations and strategies for securing your organisation.

Solutions For Risk Management

Network Device Discovery & Identification

Gain visibility of the devices connected to your environment, using such as Forescout and Microsoft Defender for Cloud and IoT. Identify devices that could present significant security risks with Vulnerability Assessments.

Security Posture Review

Conducting a detailed review of your security posture to pinpoint areas of significant risk and allow you to manage those risks by building defences and taking action to minimise the risks. CyberLab can assist in this area with Cyber Essentials assessments, Penetration Testing, Red Team exercises, Microsoft 365 health checks and secure workshops.

Engagement & Training

User education and awareness of cyber security is more important today than it ever has been before. People in your organisation are one of the most effective layers of defence you can have against cyber threats, but they can also be one of your greatest weaknesses.

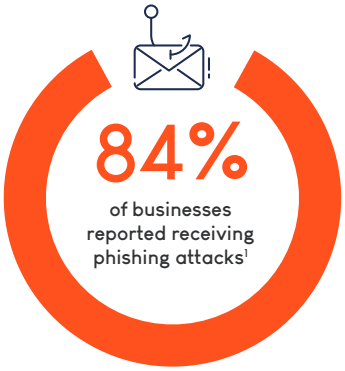
The primary, and arguably the most insidious, threat our users face today is from phishing emails that entice us to give away information or access that we wouldn't normally do.

Building Security that Works for your People

The best security strategies do not get in the way of people doing their job but allow them to work how they want to work. One of the best countermeasures to the growing threat of social engineering attacks like phishing is regular and effective user education. Alongside this, organisations can implement realistic simulated email threats to test the effectiveness of the training.

Going Beyond Email Security

User awareness is not only limited to email security. It is recommended that organisations should also train their people to be aware of data handling best practices and it's important to create a positive cyber security culture so that your people report potential breaches in confidence.



- Insights from the UK Gov Cyber Breaches Survey 2024

Solutions for Engagement and Training

Visibility

The use of products that give you visibility to devices connected to your environment, such as Forescout and Microsoft Defender for Cloud and IoT, ensuring they are connecting in a secure way, and identify devices that could present significant security risks through the use of Vulnerability Assessments.

User Training

Ensuring that your users understand the correct and incorrect ways to safely handle data is essential. Training platforms can educate users on this aspect of cyber security.

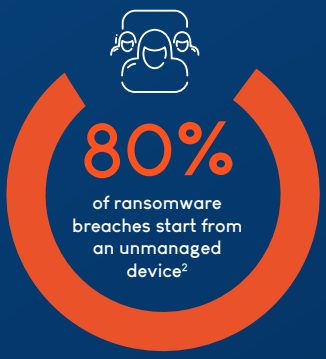
Asset Management

Organisations should understand how data is being accessed, whether the access is through secure mechanisms, and how to control that access. You can't control or protect what you can't see. Which is where asset management comes in.

Asset management is the process of identifying all devices connected to an environment, managing their level of access, and establishing business processes to record new devices. The main goal of asset management is to ensure that an organisation's assets are being used effectively and efficiently while minimising security risks and ensuring regulatory compliance.

Five Steps to Asset Management

1. **Identify who is responsible for what:** Establishing clear ownership of systems within an environment streamlines operations and enhances efficiency by removing ambiguity in responsibilities.
2. **Identify business critical areas:** Recognising devices supporting critical business services and using robust backup strategies ensures the reliability and continuity of essential operations, including safeguarding data assets.
3. **Identify areas of vulnerability:** Utilising asset information to identify security concerns such as unsupported systems, and outdated software.
4. **Remove what you don't need:** Streamline operations by identifying and decommissioning redundant or obsolete devices.
5. **Maintain and improve your asset management:** Sustain the accuracy and relevance of asset management systems through automated updates.



Solutions for Asset Management

Device Management

Managing the devices that your users use to access and process your valuable data is more important than ever in the mobile-cloud era. Devices are no longer contained securely within your network perimeter, they are now dispersed and having an effective means to effectively manage them with Endpoint Security Solutions.

Data Handling Training

Effectively audit the devices connected to your environment, such as Forescout, allow you to ensure that connected devices are being managed and that if unmanaged devices are being connected, you can manage how that happens so as not to compromise your secure systems.

1 Cybersecurity Asset Management: Know What's on Your Network - Forescout 2 Microsoft Digital Defense Report 2023 (MDDR) | Microsoft Security Insider

Architecture & Configuration

Cyber security is easier when you build a system or service with it in mind. It is also essential that those systems and services can be maintained and updated to adapt effectively to emerging threats and risks.

Secure by Design

Architect infrastructure and applications with cyber security baked into them that can be adapted over time. It's recommended that organisations use secure design principles by following frameworks such as MITRE ATT&CK Configuration.

Adopt a change control process to manage, assess and co-ordinate changes that need to be made. Change control can minimise unforeseen effects and ensures unauthorised changes from a malicious source are obvious.

Remote Working

Whether your people are working entirely remotely or are working hybrid, an organisation should adopt a device management strategy suitable for effectively managing remote workers devices. Tools such as conditional access can minimise the risk from compromised devices.

Minimising Impact

The best approach is to assume malware will, at some point, affect your systems and plan accordingly. Traditional anti-malware software is becoming increasingly ineffective at spotting modern malware, so it's essential for organisations to adopt next-gen anti-malware software. Use network segmentation and zero trust principles to prevent and inhibit unauthorised lateral movement in your systems and make it harder for an attacker to be effective.

Vulnerability Assessments and Penetration Testing

A simple but effective way to monitor and manage vulnerabilities is to gain visibility and awareness of them through regular vulnerability scans. We recommend that vulnerability scanning should be conducted at least quarterly.

Solutions for Architecture and Configuration

Vulnerability Assessment

A Vulnerability Assessment is an automated activity that actively scans for possible security vulnerabilities within an internal or external infrastructure (including all systems, network devices and communication equipment connected to that network) that cybercriminals could exploit.

It is conducted against infrastructure IP addresses and produces a report to identify any issues found and allow you to resolve them.

Penetration Testing

A Penetration Test will include a vulnerability assessment for an initial sweep of the infrastructure, but the key here is that a penetration tester will use the output of the Vulnerability Assessment and combine it with their experience and skillset to penetrate further into your network.

They perform research and reconnaissance, threat analysis and exploitation of the vulnerabilities identified to reveal the full extent of your security and its weaknesses.

Vulnerability Management

The software we use to conduct business globally changes daily. Whether that is adding new collaboration features or integrating with other software products to enable us to work smarter rather than harder, the changes are continuous.

Infrastructure changes constantly too, perhaps to add new web applications for our customers to access or to provide a new level of access for our users who work remotely.

Identifying Vulnerabilities

By ensuring we keep internal and external vulnerabilities in our environment to an absolute minimum it makes it harder for attackers, taking them longer to make progress and improving our chances of detecting their presence.

Checking for and identify vulnerabilities should be a key component of your security strategy. A simple but effective way to monitor and manage vulnerabilities is to gain visibility and awareness of them through regular vulnerability scans.

Patch Management

Looking for vulnerabilities is only a single part of vulnerability management however, manually having to deploy patches across your estate – and beyond, for home workers – is an impractically huge undertaking.

Patch management solutions automate the deployment of patches into your environment, having OS patch management configured and managed at an organisation level is essential and, fortunately, is generally included with your OS.

3rd party patching, on the other hand, is often difficult to automate. Much of today's software will automatically perform updates – the catch being that many updates will only be implemented when the software is run, so infrequently used applications can lay there for weeks harbouring a well-known vulnerability.

Solutions for Architecture and Configuration

Vulnerability Assessment

Protect your operating systems and third-party software from vulnerabilities with vRx from Vicarius. A complete patch management system that discovers, prioritises, and remediates software vulnerabilities across your estate, including the smaller applications that are often forgotten.

Penetration Testing

Penetration Testing is a way to identify vulnerabilities before attackers do, evaluate how effectively you can respond to security threats, assess your compliance with security policies, and improve the level of security awareness amongst your staff.

Identity and Access Management

Understanding who or what needs access, under what conditions, is as important as knowing who needs to be kept out. Identity and access management (IAM) involves selecting appropriate methods to verify the identity of users, devices, or systems with sufficient confidence to make informed access control decisions.

Audits

Regular audits are essential for gaining a comprehensive understanding of your security status. Audits help identify the number of administrator accounts in use, the age of passwords, and the activity and utilisation of user accounts. This process can reveal unnecessary accounts that should be removed. Audits should be conducted at least annually.

Password Management

Implementing a password management solution ensures passwords are securely stored in an encrypted vault, preventing users from keeping them on post-it notes or other insecure locations. This allows for the use of complex, hard-to-guess passwords without burdening users with memorisation. When certain passwords need to be shared, an enterprise-grade password management system facilitates secure and controlled sharing that can be audited.

Multi-Factor Authentication

Multi-factor authentication (MFA) requires more than one method of verification. Typically, this involves a password followed by a second factor such as a phone, SMS, or mobile app verification. MFA should be enabled for all privileged accounts as standard and is recommended for all users to enhance security.

User Behaviour Monitoring

User behaviour monitoring tracks user activities to detect potential threats such as breaches or insider threats. User Entity Behavioural Analysis (UEBA) solutions create a baseline of normal behaviour within your environment. Deviations from this baseline are flagged as potential issues, allowing suspicious behaviour to be reviewed and addressed before escalating into a cyber incident.

Solutions for Identity and Access Management

Monitor User Activity & Behaviour

Solutions such as Logpoint UEBA or Forcepoint UEBA that will silently monitor and analyse User Entity Behaviour in your environment to identify possible insider threats or potential compromise of your systems.

Audit User Accounts & Best Practices

Keeping on top of the user accounts present in your active directory or other directory systems can quickly become an unmanageable task.

CyberLab's Microsoft 365 Health Check service solutions can greatly simplify the task as well as offering valuable insights into user account and license utilisation that could represent subscription savings to your organisation.

Data Security

Data is the lifeblood of any organisation, and the scale of cyber threats aimed at stealing or denying access to data underscores its importance.

The initial step in safeguarding data is to identify the types of data held, assess its sensitivity, and understand the risks associated with it. With this information, you can implement appropriate controls to protect the data, such as access control, encryption, and digital rights management.

Secure Interfaces

All interfaces that protect sensitive data must be rigorously scrutinised to ensure they are secure and only accessible through the intended mechanisms. It is also essential to verify that the cryptographic algorithms in use are up to date and not obsolete.

Remote Working

Establishing a policy for remote and hybrid working begins with understanding how remote workers will interact with business systems and ensuring adequate access controls. Identify systems that should only be accessed from trusted locations to enhance security.

Data in transit must also be protected, ensuring it is accessible only by intended recipients. This can be achieved by controlling the network paths the data will traverse, such as using VPNs.

Zero Trust

Adoption of a zero-trust model is an invaluable tool to effectively control the flow of data within your environment. A Zero trust approach can revolutionise your system and data security, by assuming that no-one or no device should be allowed access until their identity has been established via multiple factors almost guarantees your data is protected from unauthorised access.

Email Security

Email security is one of the somewhat-simpler elements which again has been around for a long time, but this technology too has undergone quite radical transformation from what it once was. Microsoft Defender for Office 365, Mimecast and Sophos Web Security for example take similar approaches to how they function by looking at content and known junk senders to block content.

Solutions for Data Security

Monitor User Activity & Behaviour

Solutions such as Logpoint UEBA or Forcepoint UEBA that will silently monitor and analyse User Entity Behaviour in your environment to identify possible insider threats or potential compromise of your systems.

Audit User Accounts & Best Practices

Keeping on top of the user accounts present in your active directory or other directory systems can quickly become an unmanageable task. CyberLab's Microsoft 365 Health Check service solutions can greatly simplify the task as well as offering valuable insights into user account and license utilisation that could represent subscription savings to your organisation.

Logging & Monitoring

Collecting logs is essential to understand how your systems are being used.

When a security concern or potential cyber incident occurs, good logging practices can help you understand the impact of the incident by retrospectively looking at what happened.

Monitoring

Email security is one of the somewhat-simpler elements which again has been around for a long time, but this technology too has undergone quite radical transformation from what it once was.

Microsoft Defender for Office 365, Mimecast and Sophos Web Security for example take similar approaches to how they function by looking at content and known junk senders to block content.

Solutions for Logging and Monitoring

Security Information and Event Management

Also referred to as SIEM, this is a solution that combines legacy tools; SIM (Security Information Management) and SEM (Security Event Management).

Modern SIEM solutions also include technology such to automate threat response and to detect threats based on abnormal behaviour. Together they provide accelerated detection and response to security events or incidents within an IT environment.

Endpoint Detection & Response (EDR)

EDR or sometimes now called XDR (eXtended Detection & Response) is arguably a simplified version of a SIEM solution. It performs a similar function but instead of drawing security and event telemetry from multiple different sources and solutions it uses information from the vendors end-points.

Managed Detection & Response

An extension of EDR/XDR capabilities is to employ threat specialists to both monitor the dashboards for signs of possible compromise.

Incident Management

Cyber incidents can have a significant impact on an organisation, affecting cost, productivity, and reputation. However, a robust incident management plan can mitigate these effects. Detecting and responding to incidents quickly can prevent further damage, reducing the financial and operational impact.

An effective incident response plan should ensure clear lines of communication within the organisation and keep stakeholders informed as the incident progresses towards resolution. Learning from incidents post-resolution will strengthen your preparedness for future incidents.

Always Backup

Backups are a key component to any business contingency plan, although this is often not understood or appropriately financed. Having a good backup solution in place can mean major hardware, cyber, or force majeure incidents can be shrugged off with minimal downtime – conversely, not having a good backup solution could mean serious trouble for a business should the worst happen.

Solutions for Logging and Monitoring

Audit user accounts & best practices

Keeping on top of the user accounts present in your active directory or other directory systems can quickly become an unmanageable task.

CyberLab's Microsoft 365 Health Check service solutions can greatly simplify the task as well as offering valuable insights into user account and license utilisation that could represent subscription savings to your organisation.

Monitor user activity & behaviour

Solutions such as Logpoint UEBA or Forcepoint UEBA that will silently monitor and analyse User Entity Behaviour in your environment to identify possible insider threats or potential compromise of your systems.

Supply Chain Security

Supply chains are often large and complex, and effectively securing the supply chain can be hard because vulnerabilities can be inherent, introduced or exploited at any point within it.

The first step is to understand your supply chain, including commodity suppliers such cloud service providers and those suppliers you hold a bespoke contract with.

Solutions for Supply Chain Security

Cyber Essentials

Cyber Essentials is a UK government backed scheme owned and run by GCHQ. The aim of the scheme is providing a simple framework for UK businesses to follow to achieve a basic standard of cyber security.

It has two levels of certification, Standard which is an online self-assessment, and Plus which is an on-site audit of the responses provided by your organisation in the Standard version of the assessment.

Penetration Testing

Penetration Testing is a way to identify vulnerabilities before attackers do, evaluate how effectively you can respond to security threats, assess your compliance with security policies, and improve the level of security awareness amongst your staff.

Using research and reconnaissance, threat analysis and exploitation of the vulnerabilities identified to reveal your cyber security strengths and weaknesses.

cyberlab

Understand your security risks and how to fix them!

Take our FREE Cyber Security Health Check

Take the first step to improving your cyber security posture, looking at ten key areas your organisation should be focusing on, backed by National Cyber Security Centre (NCSC) guidance for UK SMEs.

Completed alongside a CyberLab expert, the CyberLab Posture Assessment is completely free and will review all the most relevant aspects of your security posture.

1. Take our Online Assessment

Our quick-yet-comprehensive questionnaire will review the most relevant aspects of your security posture within half an hour.

2. Assess Your Score

We will assess your results and provide a total score out of fifty, as well as a breakdown of your highest priority areas to review.

3. Review With an Expert

Our expert consultants will reach out to review your assessment and discuss the steps you can take to strengthen your security posture

---

Book Your Free SME Security Posture Assessment

Our People. Our Platform. Protects You.

CyberLab is a specialist cyber security company that provides a wide range of security solutions and services.

Your one-stop cyber security advisor, the CyberLab team is equipped with the right technology, knowledge, and expertise to help businesses of all sizes, including large public sector organisations.

By leveraging world-class technology, decades of experience, and our vendor partnerships, we have helped to secure thousands of organisations across the UK.

Our unique Detect, Protect, Support approach makes us the perfect partner to review and reenforce your cyber security defences.

Speak With an Expert

hello@cyberlab.co.uk | cyberlab.co.uk

Awards and Accreditations

CREST

VA | PEN TEST

IASME CONSORTIUM

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

cyberlab

cyberlab.co.uk