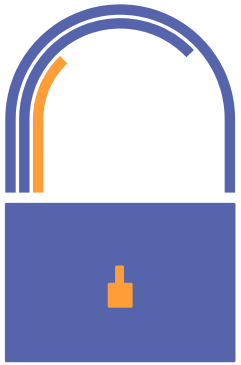
Best Practice to Improve Your Cyber Security.

Basic steps and key areas to address to maximise your protection.

Fordway

Cloud Services. Excellence Delivered.



Fordway's security review helps you check your organisation existing controls and threat posture.

We take customers through a review process similar to this high-level security review to audit their existing environments and identify any remedial action required. The findings can be used to assist with:

- ✔ Broad level risk analysis
- ✔ Ensuring your organisation is fulfilling your security obligations
- ✔ Enabling you to prepare for Cyber Essentials, Cyber Essentials Plus or ISO 27001 allowing your organisation to demonstrate best practice

This guide helps you check nine key areas and provides guidance and easy tips to improve your security:

01 → Network infrastructure

02 → Password policy and access control

03 → Data loss prevention

04 → Software licensing and OS review

05 → VoIP phone system

06 → Physical security

07 → Monitoring and logging

08 → Asset management and inventory software

09 → Accountability and Organisational Management

Network Infrastructure

Every organisation needs several layers of network security, so that if one level fails the others will continue to provide protection. Reviewing the items in this checklist will help you ascertain if your network is deployed securely and provide suggestions to harden it further.

CHECKLIST

- ✓ Network Configuration
- ✓ **Network design** including subnets and site-to-site configuration
- ✓ **Device security configuration** including port access and control
- ✓ **Firewall infrastructure** - are they configured correctly and maintained regularly
- ✓ **VPN review** – check your VPN arrangements are appropriate and effective for your business

Password Policy & Access Control

81% of hacking-related breaches leveraged either stolen and/or weak passwords

–
Verizon Data Breach
Investigations Report 2017.

Having the right policies and controls in place can radically minimise the threat should anyone gain access to your network.

FOR EXAMPLE: local machines should not be configured with the same local administrative password. Similarly, normal business user activity (such as email or internet access) should never be done under an admin password as this enhances the risk of being exploited.

Fordway recommends that this is covered through an Access Control Policy and monitored appropriately.

CHECKLIST

- ✓ **Review accounts and permissions** to ensure the concept of 'least privilege' is applied. Remove unused accounts.
- ✓ **Local accounts –** Review administrative policy for local machines and implications
- ✓ **Admin accounts –** Is best practice followed? Is administrator access being abused?
- ✓ **Password policy –** Are your staff setting secure passwords and do you make use of 2FA for remote access?

Data Loss Prevention

Data Loss Prevention (DLP) is the ability to maintain a network-wide inventory of all data within your organisation and have visibility of data movement both over the network and on mobile devices and removable media.

A review of the measures your organisation needs to protect its data includes:

- Encryption review
- USB key access
- Endpoint review including MDM
- Remote wipe
- GDPR Compliance

Only 19% of businesses have a policy covering personally owned mobile devices used for work

—

Cyber Security Breaches Survey 2018
Department for Digital, Culture, Media and Sport

Software Licensing, Patching and OS review

Management, configuration and security can be greatly improved by deploying a single standard software suite across the organisation. It is important, however to review your OS configuration to ensure that you are making use of the relevant design features available to improve your security.

Malware protection is an essential safeguard but must be kept up-to-date

CHECKLIST

- ✔ Ensure patching is done on web, email and application servers; endpoints including mobile phones; firewalls; and routers. Check it is up-to-date.
- ✔ Verify that operating systems on all devices are set to ‘Automatic Updates’
- ✔ If you are using SaaS services ensure they are configured securely
- ✔ Review tools used by staff, identify the ones that could be compromised and address
- ✔ Remove or disable unnecessary and unsanctioned software (including applications, system utilities and network services)
- ✔ For legacy systems or unsupported or end of life OS perform a risk assessment and create a plan to mitigate the reliance
- ✔ Disable any auto-run feature allowing file execution without user authorisation and configure instead at the policy level.

VoIP Phone System

The phone system is central to BAU for all organisations. If your business has a VoIP phone system then it is reliant on an internet connection and could need further protection. VoIP phone systems are susceptible to the same kind of attack as your internet connection and emails.

CHECKLIST

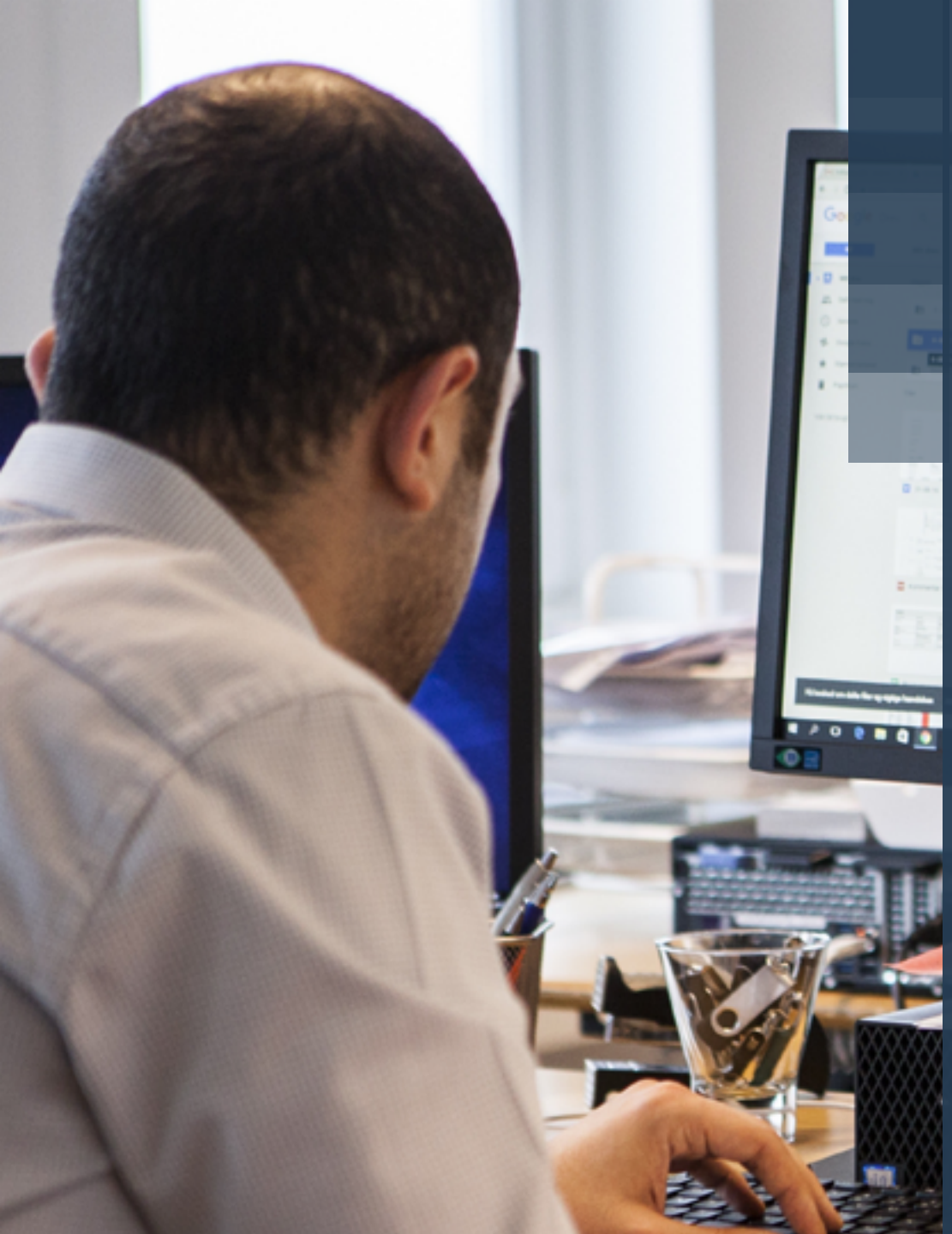
- When was the last time the software was updated?
- Is your current system vulnerable to attack?
- Could your VoIP phone system be a back door into your network?
- Consider limiting call types by extensions to prevent against toll fraud
- Ensure it is connected to the firewall.

Physical Security

An area easily overlooked by organisations. Without a comprehensive physical security strategy and the right tools, your employees and company assets are at risk. A fresh pair of eyes can identify the gaps in your physical security.

CHECKLIST

- Review access to your comms room or cabinets held on premise
- How easy is it to access a user laptop/ device from the moment you walk into the premises?
- Ensure that physical security measures are sufficient to prevent someone wandering off the street from gaining unauthorised access to your premises
- What are the potential risks to systems and equipment?



Monitoring and Logging

Monitoring and message logging are useful for a variety of IT tasks. From a security perspective reviewing authentication records, resource access and suspect malware activity will help you recognise security problems and respond to them.

CHECKLIST

- ✔ What logging is performed routinely? What are the gaps? What is required in order to comply with regulations?
- ✔ Review your environment and external monitoring to ensure they are fit for purpose and retained to provide information should forensic work be required
- ✔ If using third parties to monitor your environment, are they meeting their SLAs?

Asset Management and Inventory Software

Inventory tracking and management are crucial to obtain detailed device information to help you troubleshoot user issues, stay ahead of potential device problems, and be ready for budget and audit talks about your devices.

CHECKLIST

- How are assets within the organisation monitored and managed?
- Do you have the auditable trail for your assets to ensure that you know you haven't lost any?
- Should a particular model of device prove vulnerable, do you know precisely where they are deployed?
- Are devices disposed of correctly?

If you don't have inventory tools due to cost barriers, Fordway recommends free tools such as Spiceworks or Snipe-IT

Accountability and Organisational Management

In most organisations preparations often fail to anticipate the test of a real-world cyber-attack or are not adequately designed to fully mitigate the potential business impact. This is because information and cyber risk remains poorly understood outside the information security profession. To bridge this gap you need to provide training so all staff understand the risks and to raise awareness.

1

Are those making decisions aware of the risks involved for the organisation?

2

Does the prevailing culture support security practice?

3

What are the gaps and what management support and understanding is needed to embed best practice?

Next Step

It's easy to get started with your security assessment:
Fordway helps IT departments check existing security controls, identify threat posture against established best practice and regulations. We start with a high-level review to provide a plan of action.

FIND OUT MORE →

SCHEDULE A CONSULTATION →

Or contact us:

01483 528 200

www.fordway.com

Fordway