wanstor

Putting the right IT security controls in place

A Quick Start Guide

Introduction

Business and not for profit organisations across the UK are facing increased security threats from a wider range of people, groups, competitor businesses and government agencies than ever before.

The result of security attacks on many UK organisations include: Credit card breaches, identity theft, ransomware, theft of intellectual property, loss of privacy, denial of service plus many more. Many victims of these attacks actually do have the right levels of cyber security budgets in place to buy the right technology to keep their organisations safe from cyber-attacks.

However they still fall short in efforts to defend against these. What's even more disturbing is that many attacks could have been prevented by well-known security practices such as regular patching and secure configurations.

So how do organisations with small budgets and limited staff respond to the continuing cyber security problem?
This guide aims to demonstrate that owners can still protect their IT environments with a small number of high priority actions based on the Wanstor IT Security Controls Guidance.

Wanstor's IT Security Controls are a comprehensive set of cybersecurity best practices developed by Wanstor's IT experts that address the most common threats and vulnerabilities, including:

Theft of company information: External hackers and dissatisfied employees steal company information and customer lists

Website defacement: Hackers corrupt your website to benefit competitors

Phishing attacks: Email is designed to look like legitimate correspondence that tricks recipients into clicking on a link that installs malware on the system

Ransomware: Types of malicious software block access to a computer so that criminals can hold your data for ransom.

Data loss: due to natural events and accidents.

On your marks

At Wanstor, we believe IT security and good IT management go hand-in-hand: a well-managed network is far more difficult to attack than a poorly managed one.

To understand how well your organisation is managing its cybersecurity, start by asking the IT team these questions.

+ Do you know what is connected to your computers and networks?
+ What software is running on your systems and networks?
+ Do you set your computers up with security in mind?
+ Do you manage who has access to sensitive information and who has additional privileges?
+ Are your staff clear about their role in protecting your organisation from cyber incidents?

To help you prioritize your efforts, this guide recommends using a phased approach:

Phase 1 involves knowing what devices are active on your network and understanding your cybersecurity baseline

Phase 2 focuses on protecting this security baseline through education and prevention

Phase 3 helps your organisation to prepare in advance for disruptive events

Each phase has specific questions that you will want to answer, along with items to be actioned and tools that will help achieve your goals.

IT Managers may want to assign one person in their team to oversee cybersecurity and report regularly on security activities.

Phase 1: Know and understand your IT environment

The first step that will help IT Managers move forward with their cybersecurity efforts is to know their company network, including connected devices, critical data, and software.

Without a clear understanding of what needs to be protected, IT Managers will have trouble ensuring coverage of cybersecurity efforts.

Key questions to consider at this stage:

+ Discover potential cost-savings that can be made through migration to Azure
+ Easily discover and assess workloads that need to be migrated whilst quickly identifying those that can and cannot be migrated to Azure
+ Provide estimated monthly costs for running workloads in Azure

Know what is connected to your environment

If your data is lost, stolen or corrupted this could prove catastrophic. Accidents and natural disasters also have the potential to destroy valuable information. Additionally, criminals target data with potential value to them; hackers or employees who wish to exploit customer data, credit card information or intellectual property. Your network is their means to an end.

To understand the value of data, we recommend all IT Managers identify and inventory the following:

+ Credit card, banking and financial information
+ Personally identifiable information (PII) such as health information, usernames and passwords, home addresses and birth dates
+ Customer lists, product lists and pricing
+ Company trade secrets, formulas, methodologies and models

Know which devices are connected to your network

IT Managers can reap multiple benefits from having a good understanding of which devices are on their network. The IT environment becomes easier to manage once you know what devices need to be protected.

Below are steps which managers should take in identifying the devices active on a network.

+ If on a wireless network, check your router to see which devices are connected and password-protected by using strong encryption (WPA2)

+ For larger networks, use a network scanner (commercial or open source) to identify all devices on your network

+ Enable Dynamic Host Configuration Protocol (DHCP) logging on your networking devices to allow for easy tracking of all devices that have been on your network

+ For smaller organisations, keep an inventory list of hardware assets and critical data on a spreadsheet, ensuring to update this whenever there are new devices or data added

Know what software is on your systems

Managing software is a key component of both good IT management and effective cybersecurity.

Rogue software within an IT environment poses risks that must be mitigated, including legal liability for using unlicensed software.

Additionally, unpatched software allows malware to infiltrate and attack systems.

By understanding the software on a network, controlling individuals' ability to add software, and protecting accounts with administrative privileges, IT managers can reduce both the likelihood and impact of cyber events.

On the following page, we consider a detailed list of precautionary measures that IT specialists must take in order to protect networks from unwanted or malicious software.

What IT Managers can do

+ Create application inventory running on your systems and the web services or cloud solutions your organisation uses
+ Manually check the install and uninstall features of the operating system for a list of software that has been installed
+ Periodically check to see what software is running on your systems using available inventory or auditing tools
+ Check with employees to identify online services like file sharing platforms or HR systems they use in their roles
+ Limit the number of individuals with administrator privileges
+ Use unique strong passwords for all accounts. Provide instructions to employees on developing strong passwords
+ Ensure that system administrators use separate non-administrative accounts for reading email, accessing the Internet, and composing documents
+ Develop a company process for downloading software, and prevent unapproved applications via whitelisting tools

By understanding software on the network, controlling the user's ability to add software, and securing accounts with administrative privileges, IT managers reduce the likelihood and the impact of cyber events.

Phase 2: Protect your assets

Employees are your most valuable asset, especially when it comes to IT security.

Protecting information requires not only technological solutions but employee awareness to prevent damage to IT systems. This phase will focus on both protecting your organisations devices and educating users on their role in cybersecurity.

Here are some questions you'll seek to answer:

+ Do you set up your computers with security in mind?
+ Does your network run up-to-date anti-malware software?
+ Do you educate your users on cybersecurity best practices?

Configuring a secure baseline

Malware and cyber attackers take advantage of insecure configurations or vulnerabilities in system apps. IT professionals should ensure that operating systems and applications are updated and securely configured.

What IT Managers can do

+ Ensure browsers and all browser extensions are kept up to date with automatic updates.
+ Run anti-malware software to protect systems from malware. Utilise cloud based lookup capabilities to check for updates if your anti-malware product supports this.
+ Limit the use of removable media.
+ Require the use of MFA where available, especially for remotely accessing your internal network or email.
+ Change default passwords for applications, operating systems, routers, firewalls, wireless access points, printer and scanners when adding them to the network.
+ Use encryption for secure remote management of your devices, to pass sensitive information, and to protect hard drives, laptops and mobile devices that contain sensitive information.

Remember, cybersecurity is not just about technology, but process and people. Security tools and software are not sufficient.

To help secure an organisation, employees and staff must practice strong cybersecurity behaviour, with two key considerations - what information you communicate, and how you communicate it.

What to communicate

+ Identify those in your organisation with access to sensitive data and communicate their role in safeguarding that information

+ Two common attack methods include phishing email and phone call attacks. Ensure employees can identify and explain common indicators of an attack, including someone creating a strong sense of urgency, requesting sensitive or private information, using confusing or technical terms or asking an employee to ignore or bypass security procedures

+ Clarify that common sense ultimately represents the best form of defence. If something seems odd, suspicious, or too good to be true, it is most likely an attack

+ Encourage the use of strong, unique passphrases for every account and two-step verification where possible

+ Make sure all staff keep their devices and software updated with the most current operating systems or build

How to communicate

+ Engage your employees at an emotional level, making sure they understand how to protect your organisation and how this protection also applies to their personal lives

+ Be sure all staff understand that cybersecurity is an important part of their job

+ Disseminate relevant cybersecurity awareness material amongst your staff

+ Use online resources to encourage good behaviour concerning cyber security

Phase 3: Prepare your Organisation

Once your organisation has developed a strong cybersecurity foundation, IT Managers should build relevant capabilities for a response.

This includes the ability to handle a cybersecurity incident and resume business as swiftly as possible.

Here are key questions for IT teams to answer:

+ Do you know the last time your critical files were backed up?
+ Do you periodically verify that the backups are complete?
+ Do you know who to contact if an incident occurs?

Managing backups

Making and managing backups can be a tedious task; however, it is one of the best ways to secure data, recover after an incident, and get your organisation back on track. This is crucial considering that ransomware can encrypt all your files and hold data to ransom.

A robust response plan, complemented by current and well-maintained backups, are the best protection when dealing with any cyber incident.

What you can do

+ Perform weekly backups of all computers that contain important information in an automated fashion.
+ Consider using secure cloud solutions where available.
+ Periodically test your backups by trying to restore a system using a backup.
+ Make sure that at least one backup destination is not accessible through the network.

This will help protect against ransomware attacks since those backup files will not be accessible to the malware.

Preparing for an incident

No-one chooses to face the reality of cybersecurity incidents, but advanced preparation may mean the crucial difference in getting your business running again.

Cyber incidents include denial-of-service attacks disabling websites, ransomware attacks disabling systems or data, malware attacks resulting in loss of customer or employee data and the theft of hardware containing unencrypted data.

What IT Managers can do to prepare

+ Identify those within your organisation who will serve as the lead in case of an incident
+ Update contact information for IT staff and 3rd party organisations
+ Join InfraGard or other associations that focus on sharing information and promoting cybersecurity
+ Keep a list of external contacts as part of your plan. These could include legal counsel, insurance agents if you carry cyber-risk coverage, and security consultant

What to do if an incident occurs

+ Consider contacting an IT or cybersecurity consultant if the nature and extent of the incident isn't clear to you
+ Consider contacting legal counsel if it appears that personal information was involved in the incident
+ Prepare to notify any affected individuals whose personal information was involved in a breach
+ Inform law enforcement as required

For more on Wanstor's IT security solutions and how they can help protect your organisation from attack, please contact us on 0333 123 0360, email us at info@wanstor.com or visit us at www.wanstor.com

Whilst moving your current IT environment into the cloud can bring benefits like increased productivity and lower costs, the complexity of cloud migrations can be daunting.

Wanstor have significant experience in helping customers optimise Azure environments. Our two-day workshop explores what a migration could look like for your business.

Our workshop follows Microsoft's best practice Cloud Adoption Framework, ensuring the right infrastructure and workloads are considered for your migration strategy.

"Wanstor have been epic - from implementing massive migrations seamlessly to huge improvements in efficiency and functionality."

Daniel Swithinbank, Catch22

Strategy

Define business case and expected outcomes of adoption

Plan

Align actionable adoption plans to business outcomes

Ready

Prepare the cloud environment for the planned changes

Adopt

Migrate and modernise existing workloads

Manage

Operations management for cloud and hybrid solutions

Govern

Govern the environment and workloads

Moving to Microsoft Azure Public Cloud

When you partner with Wanstor to move your workloads into Azure, our certified engineers follow Microsoft's Cloud Adoption Framework best practise ensuring that no stone is left unturned, and your deployment will be right first time.

Azure Migration Workshop

Our three-day assessment is carried out by our team of Azure cloud consultants alongside your business and IT leaders.

Day 1 Onsite or remote workshop to develop business case for cloud migration, understand key drivers, motivations and concerns, define expected outcomes

Day 2 Undertake a readiness assessment to review current estate and overall business readiness for a cloud migration and adoption

Day 3 Discuss our recommended migration strategy including estimated requirements and costs and next steps to begin your journey

The Readiness Assessment

We deploy all the necessary tooling into your estate to get a clear picture of your resources.

Total Discovered Servers
62 (Includes 8 inactive servers)

Different OS types
7 (58 Windows, 2 Linux, 2 other)

Servers with SQL Server
19

Total Memory
677 GB (589 GB / active servers)

Total vCPU Cores
210 cores (186 cores / active servers)

Total Storage (GB)
26914 GB (25264 GB / active servers)

Dependency Status
47 VMs enabled, 15 VMs disabled

Assessment Target Location
UK South

We then make a full analysis of what is ready to migrate and provide a breakdown of migration scenarios with the cost implications of each.

Ready for Azure
58

Ready with conditions
4

Not ready for Azure
0

Unknown
4

Monthly cost estimate (Existing Infrastructure)
£16,895.40

Monthly cost estimate (Migrated to Azure)
£ 2624.80

*Costs assume moving into a Reserved Instance Subscription (3 year) performance based with hybrid benefits. Cost-savings of up to 85% can be achieved through migration.

The five steps to a successful migration with Wanstor

Discovery workshop

Install tooling

Analyse results

Feedback on findings

Provide strategy report

Benefits of our Azure Migration Workshop

Using Wanstor as your trusted Azure migration partner can help you revolutionise IT infrastructure for your business.

+ Discover potential cost-savings that can be made through migration to Azure
+ Easily discover and assess workloads that need to be migrated whilst quickly identifying those that can and cannot be migrated to Azure
+ Provide estimated monthly costs for running workloads in Azure
+ Identify and provide information on any specific application and system dependencies
+ Receive recommendations on what the size of your Azure environment should be to run as efficiently as possible and remove any guesswork
+ Obtain a strategic roadmap for your own Azure migration

Our Customers

We've worked with many customers to migrate their infrastructure and applications into the cloud whilst providing ongoing management and support.

catch 22

The Restaurant Group plc

wagamama

The Fostering Network

"The great benefit of working with Wanstor is direct access to such a large pool of IT specialists from different disciplines giving us exceptional levels of support. The calibre of their technical team is exceptional."

Geoff Wilson, The Fostering Network