centrality

Microsoft Experts. Client Focussed. Delivering Excellence.

MASTERING CYBER SECURITY

THE 10 ESSENTIAL STEPS

PART 1

centrality.com

+44 (0) 1462 857 014

info@centrality.com

Microsoft
Solutions Partner

32% of businesses experienced a security breach or attack in the last 12 months. As cyber attacks become more severe – are businesses considering the steps that they could be taking to help keep themselves secure?

As an IT leader security is always top of mind. With shifting regulatory requirements, plus the ever-changing digital threat landscape, staying on top of your security infrastructure can feel like a full-time job in itself.

In this guide we look at the first five essential steps for all businesses to consider when reviewing their cyber security infrastructure.

Keep an eye out for our part two – coming soon!

centrality

Microsoft Experts. Client Focussed. Delivering Excellence.

01

STEP ONE

Risk Management

- Consider your businesses priorities when it comes to managing cyber risks.
- Understand where within your digital landscape you need to apply risk management.
- Continuously assess your chosen risk management approach.
- Seek external confidence from cyber security professionals.

Risk management is a crucial process for businesses to consider when thinking about security. By identifying, assessing and controlling risks you can ensure that your business is protected to the highest degree.

Only 3/10 of businesses have undertaken a cyber security risk assessment within the last year. Poor risk management can have a significant impact on any business, and many businesses do not have an effective risk management approach in place.

An effective risk management process plays a crucial role in enhancing cyber security measures and has many benefits.

Identifying potential threats and vulnerabilities associated with your technology allows for a comprehensive understanding of your cyber landscape and the specific risks that your organisation could face.

By assessing the risks, you can prioritise your resources effectively. This process helps save both time and money whilst ensuring that resources are used efficiently and allows you to focus on mitigating risks with the greatest potential for harm.

Effective risk management allows you to build greater trust within your business relationships, attract new customers, and improve your organisation's reputation.

Demonstrating a solidified management process influences trust among stakeholders as it illustrates that your organisation takes security seriously.

02

- Continuously look to build a trusting dialogue with staff across the business.
- Personalise cyber security training relating to your business's weaknesses and needs.
- Run internal cyber awareness campaigns.
- Use a business with cyber security experience to run effective internal training.

centrality

Microsoft Experts. Client Focussed. Delivering Excellence.

STEP TWO

Engagement & Training

Employees are at the heart of any cyber security strategy. An effective cyber strategy relies on accounting for the way people work whilst not preventing them from getting their work done.

Only 18% of businesses have carried out employee or awareness training. As employees are the primary recipients of various cyber-attacks such as phishing, by not conducting the appropriate training you leave your business open to greater opportunity for an attack to happen.

Running internal awareness engagements and training on cyber security is very beneficial.

Employees are the first line of defence against threats. By delivering training on security best practices, policies, and safe online behaviour, you can ensure that your workforce is prepared when it comes to cyber security. This, therefore, reduces the likelihood of an attack succeeding as a result of human error.

As cyber threats continue to develop and become more harmful, regular awareness training ensures that employees stay up to date on the latest emerging threats. This also allows them to learn what new measures they can take to prevent an attack from succeeding.

03

Understand your critical functions and identify the associated technology dependencies.

Develop your knowledge.

Only keep the assets you need.

Find a provider who can assist you with managing your technology landscape.

centrality

Microsoft Experts. Client Focussed. Delivering Excellence.

STEP THREE

Asset Management

Establishing and maintaining knowledge of your assets is crucial when it comes to cyber security. As systems grow over time it can be difficult to maintain all of the assets within your digital landscape, which therefore leads to the opportunity for security incidents to occur.

Only 26% of businesses have a list of their critical assets. Curating a list of these assets is a fundamental measure to being able to discover if you have any risks that quickly need to be resolved.

Asset management plays a critical role in enhancing cyber security and provides many key benefits to your organisation.

Asset management helps you to maintain and accurately keep an up-to-date inventory of your IT assets, including software, hardware and network infrastructure. It provides better visibility into your digital landscape and allows you to ensure that all of your assets are tracked, identified and managed efficiently.

Effectively manage the lifecycle of your assets, from acquisition to disposal, with asset management. This allows you to ensure that your assets are decommissioned securely, minimising the risk of data exposure.

Managing your assets correctly helps your business both save costs and spend money more efficiently in the future. It enables you to identify assets that are rarely used or redundant, therefore reducing unnecessary costs.

04

- Always understand what you're building and why.
- Make systems easy to maintain and update.
- Make it easy to detect and investigate compromises.
- Find a provider who can assist you to ensure that your systems are secure from the offset and throughout.

centrality

Microsoft Experts. Client Focussed. Delivering Excellence.

STEP FOUR

Architecture & Configuration

As the technology landscape continuously evolves, ensuring that cyber security is embedded into your systems from the beginning, and continuing to maintain this throughout is vital. By doing so, you then have the opportunity to keep the systems updated and adapt them effectively to emerging threats and risks.

Architecture and configuration play a vital role when focusing on cyber security and provides many benefits to any organisation.

When architecture and configuration have been considered, it enables you to implement a centralised monitoring and logging system. Therefore, allowing for the collection and analysis of security events from all systems and devices across your landscape, allows you to be able to respond to security incidents quickly and more efficiently.

When you implement tight security measures at the stage of design and build within a system it will allow for the opportunity of scalability and flexibility for your business. Having a robust architecture and configuration approach enables you to adapt to changing business needs as well as evolving cyber threats without ever having to compromise your security.

Designing resilient architectures and configurations can be a big task for any business, but the long-term benefits outweigh this. If a security issue was to occur, having this in place means that your business will have little to no downtime to resolve the issue. It enables you to recover quickly and maintain essential operations throughout.

05

STEP FIVE

Vulnerability Management

- Always look to keep your systems updated.
- Develop an effective vulnerability management process.
- Focus on the management of your legacy equipment.
- Introduce managed services provided by a partner into your landscape to reduce your management burden.

centrality

Microsoft Experts. Client Focussed. Delivering Excellence.

Attackers will first seek to exploit a company's vulnerabilities before they make their attack. It's crucial to have an effective vulnerability management process to ensure that you can find possible vulnerabilities straight away, fix them, and keep your assets as secure as possible.

Only 15% of businesses carried out a cyber security vulnerability audit within the past year. Being aware of the vulnerabilities within your environment, and keeping informed of any new vulnerabilities that arise, is essential for keeping your business cyber secure.

Vulnerability management plays a crucial role in enhancing cyber security by providing many key benefits.

Having a strong vulnerability management process ensures that your systems and software are kept up to date with the latest security patches. Quickly applying patches allows you to address vulnerabilities promptly and protect your assets.

By regularly including something such as a vulnerability audit in your cyber security strategy, you quickly enhance your security posture. Doing this helps to reduce the possible attack surface, strengthens your defences, and enhances your resilience if a cyber threat was to happen.

Effective vulnerability management has long-term cost-saving benefits. By proactively addressing vulnerabilities you can prevent future security incidents from happening, therefore saving your company from any financial losses. This means that there is no need for expensive incident response, recovery, or remediation efforts that would be necessary after a cyber-attack has taken place.

centrality

Microsoft Experts. Client Focussed. Delivering Excellence.

MASTERING CYBER SECURITY

WOULD YOU LIKE TO LEARN MORE?

Contact us today to see how Centrality and the Microsoft Workshop program can help.

centrality.com
+44 (0) 1462 857 014
info@centrality.com

Microsoft
Solutions Partner