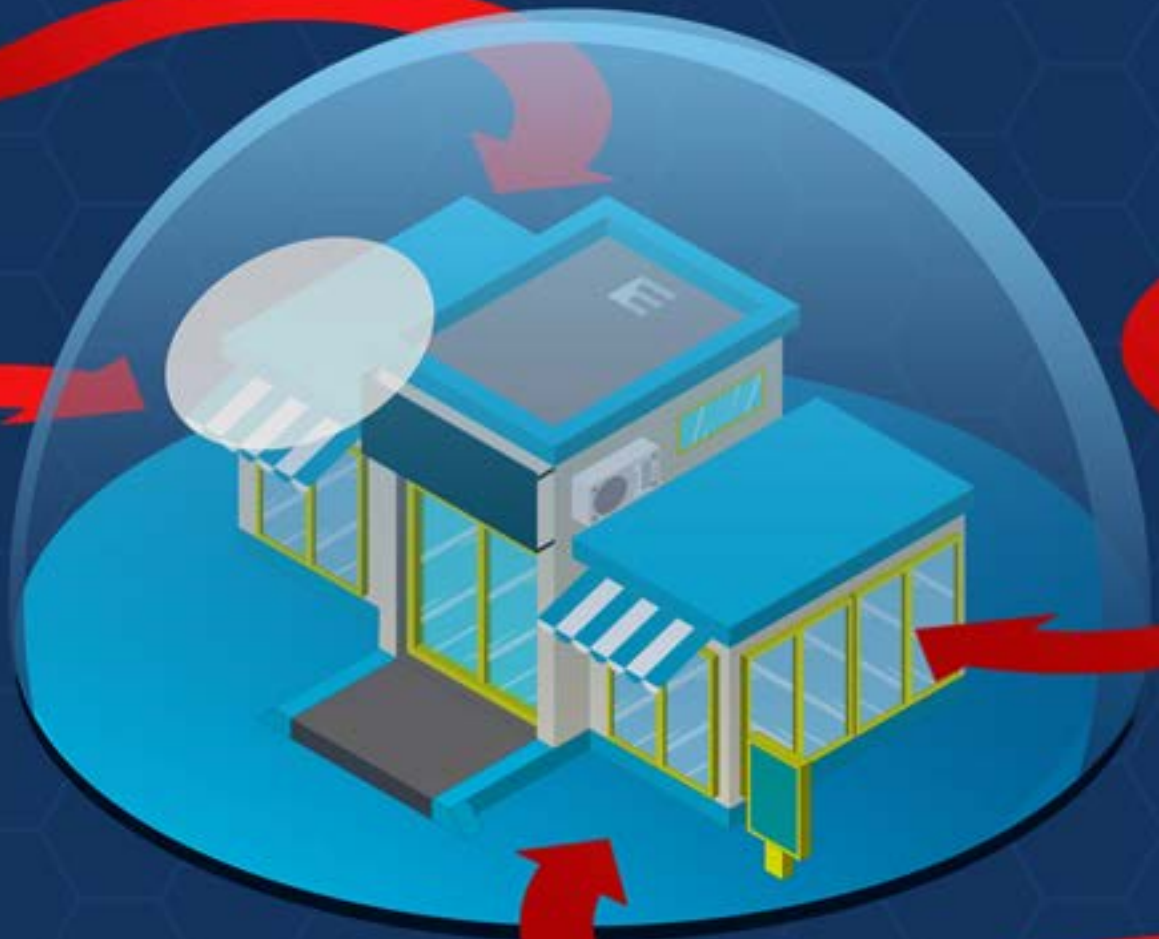


Does Your Business Need A Cyber Security Assessment?



SUMMARY

Ever thought “that won’t happen to me” in the face of bad news? Many businesses think they’re invulnerable to cyberattacks or data breaches: “we’re too small to be a target”, or “we don’t have anything cybercriminals want to access”. Yet cybersecurity needs to be a top priority for everyone.

Don’t rely on false confidence. Consider whether your business shows any of these signs indicating you need a cybersecurity assessment.





What is a Cyber Security Assessment?

First, let's be clear what we mean by cybersecurity assessment. Like an annual check-up at the Doctors, this assessment aims to diagnose potential risks before something serious happens. This proactive assessment aims to detect or identify any system, network, software, device, physical, and other threats or vulnerabilities. The assessment findings help your business plan what it will do to respond to and manage the risk.

The depth and breadth of a cybersecurity assessment can depend on your business size, industry, risk threshold, timeline, and budget. Still, there are several signs suggesting your business needs to schedule a cybersecurity assessment soon.





#1 Something's off.

Your Spidey senses are tingling. Or you've seen something suspicious that makes you question your cyber security.

This might be:

- Finding strange files on your network
- Your computers behaving oddly
- Competitors knowing information about your company that isn't yet public knowledge

#2 Compliance requirements.

Most industries today understand the threat of cybercriminal activity. Your business may need to meet regulatory requirements. For instance, there are many rules about testing for cyber exposure in financial, healthcare, energy, and educational settings. Compliance starts with a comprehensive cyber risk assessment.





#3 Your staff isn't tech savvy.

Humans remain one of the biggest cybersecurity threats. Your investment in security to lock down your “virtual house” doesn't help if your staff open the door to anyone who knocks.

Most employees aren't malicious. They just have poor habits. Some don't see a problem in securing their accounts (all of them) with a passcode such as “1234” or “password”. Others are naive enough to actually believe a Nigerian prince wants to send them millions!

Even those with security awareness can fall victim to business communications scams. Busy people may not notice when they get an invoice that looks exactly like a supplier's but with a bad actor's banking details.






#4 Your staff is unhappy.

Depending on your size and the volume of work, you may not yet have a clear process in place for handling terminated employees' technology access. Are unhappy people quitting? Have you fired staff? Not everyone leaves on good terms, so revoke all former employees' access and change passwords. Providing former staff with continued access to your cloud-based platform leaves you seriously exposed.

#5 Your technology hasn't been updated.

We've all been there. We try to get more done with the tools we have rather than having to invest in and learn something new. Yet the "if it ain't broke, don't fix it" approach is not applicable to technology.





Old software or operating systems are more likely to expose you to cyber risk. Once software reaches a certain age, the provider stops supporting that solution. Microsoft, for example, has phased out security patches and updates for Windows 7.

Don't plod along with decades-old technology, thinking you're safe because there hasn't yet been a failure or crash. The bigger danger is the small, unnoticed openings you don't know about, but cybercriminals do.

#6 You don't have data control policies.

The number of technology entry points to control is always growing. There may be USB drives floating around your business environment holding essential data. Company laptops can be misplaced or stolen. Remote employees may sign on to unprotected WiFi networks and portable devices aren't properly encrypted.





WARNING CYBER ATTACK

Without policies in place to control data throughout your business environment, it's difficult to determine your vulnerabilities.

#7 Your employees use their own devices.

A Bring Your Own Device (BYOD) environment makes employees happy. The cyber criminals are pleased too. Sure, this approach can save money. Your business no longer has to ensure every employee has the latest available technology. But, there are drawbacks:

- Employee devices may not be the latest, which could make them more susceptible to cyber attack.
- Staff could download malicious software or apps onto their personal devices that give cyber criminals access to your systems.





- Users may be entirely unaware their devices carry malware and could infect your systems when connected.
- The employee may not be the only user of the phone which has access to business information.
- Disgruntled employees can use their own devices to damage your network.



STOP

Don't Ignore the Signs!

We compared the cybersecurity assessment to a check up at the Doctors. Maybe you tend to put those off, too! Well, if any of these signs sounded familiar, it's time to schedule an assessment.

Cyberattacks and data breaches are seriously damaging for business. If something does happen, your business could lose access to its network or systems for hours or even days. Every moment of downtime proves costly in terms of:

- Productivity decline;
- Lost revenues and possible fines;
- Customer churn;
- Damage to brand reputation.






Why Get Your Assessment Done by Pros

A business can do its own cybersecurity assessments, but it's a little like going to the Internet to diagnose your persistent cough. Is it a common cold or proof you're dying? Having a managed services provider (MSP) perform the assessment gives you an objective, expert opinion.

MSPs understand potential threats and know where to look to identify internal and external vulnerabilities. They can also help gauge the likelihood of something negative happening, as well as the possible harm to your business.

An MSP doing a cybersecurity assessment should survey and inventory all your assets to determine what might happen and how devastating it could be to your business bottom line. Reviewing the network, hardware, systems, and your business tools, the MSP can map remote access points and confirm the right protection is in place.





In addition to running vulnerability scans, the MSP can also offer a prioritized plan for addressing any risks identified. The best MSPs will also stick around to help your business implement the fixes and even recheck to be sure your cyber security is now up to snuff.

Key Takeaway

A cyber security assessment gives you a clear picture of your business's risk exposure. If you recognised any of these symptoms, don't put off a cyber security assessment any longer. Working with an MSP, you can identify potential security gaps and benefit from their expert input to improve your cyber security health long-term.

Cloud backup typically has file versioning in place to make it easy to retrieve files. Even previous or deleted versions of files can be accessed. Note: ask your provider about the time-window for recovering previous or deleted versions.



Your IT Department

Unit 8 Farrington Way
Eastwood
Nottingham
Nottinghamshire
NG16 3BF

T: 0115 822 0200

E: info@your-itdepartment.co.uk

W: your-itdepartment.co.uk

Follow us on social media:

