How Businesses Can Ensure Cyber Security

TechRounder PDF Edition

Live article: https://www.techrounder.com/security/how-businesses-can-ensure-cyber-security/

By Vipin PG | Published June 19, 2025 | Updated March 9, 2026 | Format: Analysis | 4 min read

In brief

With the majority of businesses embracing digitalisation and relying on the internet to operate, cyber security is no longer an option - it’s a necessity.

With the majority of businesses embracing digitalisation and relying on the internet to operate, cyber security is no longer an option - it’s a necessity. Whilst going digital allows companies to be more flexible, efficient, and cost effective, it does leave them vulnerable to cyber threats, of which the consequences can be detrimental.

Especially since methods used by cyber criminals have become more advanced and cyber criminals are targeting businesses of any size across all sectors, the need for cyber security has dramatically increased.

So, let’s take a look at what cyber security actually is and how you can implement it to protect your business, its finances and reputation, and give yourself peace of mind.

What is Cyber Security?

Cyber security includes security measures that have been taken to reduce the risk of cyber attacks on individuals or organisations.

Cyber security is used to protect the devices and services used by an individual or a business from theft or damage and prevent unauthorised access to personal information stored online.

Why is Cyber Security Important?

50% of UK businesses have experienced a cyber attack, so it’s crucial that businesses have proper defenses in place to prevent these crimes. Here are just some of the reasons why cyber security is so important:

Prevents Financial Loss

From the cost of investigations into the crime to stolen assets, cyber attacks can cost businesses a significant amount in attempting to recover lost information or data.

Preserves Customer Trust

Customers who hand over personal information have to trust a business to protect that data. When a business experiences a data breach, future customers may be less trusting when it comes to sharing information.

Maintains the Reputation of the Business

People expect companies to have a reputation for operating safely and securely. A cyber attack can damage that reputation, resulting in a loss of existing and future clients.

How Businesses Can Stay Cyber Secure

Understand Potential Threats

Having an understanding of common threats is the first step in defending against them. Here are some of the most common cyber threats businesses face:

- Malware - 'Malicious software' refers to intrusive or harmful software designed to steal data or damage computer systems. Cyber criminals will employ a range of tactics to get malware onto a computer system. More often this involves an individual downloading a file disguised as something innocent.
- Phishing - These are scams that trick users into revealing sensitive information or installing malware. Most phishing attacks are via email.
- Impersonation - Cyber criminals will impersonate a trusted individual to steal funds or sensitive data. They are typically carried out via email.

Implement a Cyber Security Policy

Every business, regardless of size, should have a clear policy in place for cyber security. The policy should detail data handling, passwords, and incident response plans. All staff should be trained to understand and follow these policies.

Train Staff

95% of data breaches involve human error. Regular training ensures staff can recognise phishing emails, identify impersonation, and follow the best practices for data protection.

Limit Access Where Possible

Most employees don't need access to all company data. Instead, only provide people with the relevant access based on what is necessary for them to fulfil their role.

Regularly Update Software and Systems

Outdated software creates a weak link that cyber criminals can utilise. Ensure all software and systems, like business applications that contain personal information such as your payroll app, are up-to-date to enhance their security.

Use Multi-Factor Authentication

Multi-factor authentication (MFA) adds an extra layer of security by requiring the user to provide a second form of verification. Additionally, employees should be encouraged to use strong and unique passwords.

Don't Neglect Remote Working Security

With modern workforces often operating partially or fully remote, it's important to ensure remote devices also meet high security standards. This includes using VPNs and encrypting files that contain sensitive information.

Frequently Back Data Up

By backing up your data, you can restore operations in the event of a system failure or cyber attack, minimising data loss and the financial and reputational repercussions that come with this.

Conduct Security Audits

Security audits should be carried out every so often to identify any areas where security could be compromised.

Get Insurance

Prevention is key but cyber attacks can still happen even with all the right security measures in place. By obtaining cyber insurance, you get an additional safety net that can reduce the ramifications of a cyber attack should one occur.

Cyber Security is an Ongoing Process

Unfortunately, cyber security isn't a set and forget project - it requires ongoing attention as threats evolve. Businesses that take a proactive approach to cyber security by understanding the current threats, training staff on cyber threats and policies, limiting access, updating software and backing data up regularly, using MFA, and conducting audits to identify areas of weakness, can not only protect their data but also gain a competitive edge by building stronger trust between customers and stakeholders.

References

1. twenty-four.it - services / cyber-security-services - https://www.twenty-four.it/services/cyber-security-services/cyber-crime-prevention/cyber-crime-statistics-uk/#:~:text=50%25%20of%20UK%20businesses%20have,formal%20cybersecurity%20incident%20management%20plan.

2. scworld.com - news / 95-of-data-breaches-involve-human-error-report-reveals - https://www.scworld.com/news/95-of-data-breaches-involve-human-error-report-reveals

3. paycaptain.com - solutions / payroll-app - https://www.paycaptain.com/solutions/payroll-app