Citation ISO Certification

Top 10 Cyber Security Threats

v01

Introduction

Cyber security threats are ever evolving, with new strategies and technologies used to compromise your business. In fact, in 2023, there were 7.78m incidents of cyber crime nationwide, and it was reported that 50% of business have experienced an attack or breach over the last 12 months.

The fallout following an attack or breach can be catastrophic, causing significant financial losses, reputational damage, non-compliance, and company downtime. To safeguard your business, it's crucial to understand the current cyber threats, where they come from, and how you can take proactive steps to protect your business.

Keep reading to discover the top 10 cyber security threats facing your business today.

1. Phishing and social engineering

Social engineering is the act of deceiving individuals into providing sensitive information or gaining unauthorised access to a system or device. This can include impersonation of reputable sources, pretexting on social media profiles or company websites, baiting or phishing attacks.

In 2023, 84% of attacks and breaches were the result of phishing communications, and this continues to be the most common initial attack vector cyber criminals use to compromise your business.

To protect against social engineering, your workforce needs to be up to date on these tactics, establish clear procedures for verifying identities, and limit user access to company data, minimising damage and data loss in the event of an attack.

2. Ransomware

Ransomware is a type of malicious software that prevents the use of a system, either by locking the system's screen or locking the user's files unless a ransom is paid.

Ransomware is commonly distributed through infected email attachments, malicious downloads, or compromised websites.

To protect against ransomware, it's important to regularly back up your company data and keep this in an isolated location separate to your company network. Implement malware detection tools and strong firewalls, and train employees to recognise and report any suspicious activity.

3. Supply-chain attacks

Over the last 12 months, only 11% of businesses report reviewing the risks posed by immediate suppliers. Cyber criminals are beginning to see the benefits of supply-chain attacks as they are able gain access to a multitude of data and devices just by targeting one business.

If one of your immediate suppliers fell victim to a cyber attack, how much of your company data would the cyber criminal also have access to? It's important to consider the security level of your suppliers and introduce a minimum level of security requirements to reduce risk. Implement policies and procedures when looking to take on new company suppliers by verifying that they have appropriate defences in place.

4. Misconfigurations

Misconfigurations are systems, applications, or networks whose settings are not correctly arranged, leaving your business exposed to potential cyber attacks.

This can include not updating default configurations, unnecessary features enabled, permissions set too broadly, or human error when implementing new systems.

Most businesses use external software as part of their daily operations – but these aren't always secure by default. Implement measures to effectively secure, configure, and update these to prevent data breaches and exploited vulnerabilities.

5. Zero-day vulnerabilities

Zero-day vulnerabilities refer to unknown security holes in your systems and networks. By exploiting these unknown weaknesses, cyber criminals are able to remain undetected for longer periods of time without the organisation even knowing they're being targeted and attacked.

Zero-day vulnerabilities can lay undetected for days, months, or even years – software and hardware vendors will look to release updates and patches as soon as they're identified, but sometimes cyber criminals are faster.

Ensure all devices are up to date with the latest software and download these as soon as they're released.

6. Stressed budgets and lack of resource

All businesses have budgets and need to make decisions on where/what they spend this on. When budgets are stressed, businesses tend to cut areas including information security, which can leave your business vulnerable.

7. Insider attacks and human error

This is your employees and workforce who put your business at risk of an attack or breach, either with or without malicious intent. There are occasions where employees may become disgruntled and wish to do your company harm, but in most cases, this is a result of lack of awareness and human error.

Cyber security is everyone's responsibility – all members of staff need to understand their role with mitigating risk, and they need to be provided with the tools and knowledge to defend against potential threats and attack attempts.

8. Legacy systems

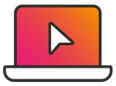
Typically, a symptom of stressed budgets – old systems that are still used for daily operations can lead to vulnerabilities and weaknesses that cyber criminals look to exploit.

For legacy systems, vendors no longer deploy patch-management and software updates that look to remediate risk and bug fix.

9. Home working

Home working can bring many benefits, but also leave your business vulnerable. As we see more companies adopt the remote-working environment, there have been spikes in cyber criminal activity looking to exploit this.

Personal devices and networks used to access company-owned data may not be up to par with the security requirements needed to protect your business.



10. AI and machine learning

With the increased implementation of AI and Machine Learning within business operations, these can help boost efficiency and productivity. However, they can also present certain vulnerabilities and cyber risks.

From inputting sensitive and confidential company information which could result in a data breach, to malicious actors automating and streamlining their attacks.

To combat AI threats, businesses need to implement strong authentication protocols, encrypting sensitive data, train staff on the proper use of AI tools, and regularly monitoring networks for any unusual activity.

Are you ready to respond?

With the continued growth and evolution of cyber crime, protecting against these attacks is one of the biggest challenges facing business owners.

Any of these cyber security attacks could be detrimental to your business – but there are measures you can take to effectively secure your vital devices and data.

One popular approach is to implement an information security management system that's compliant with ISO 27001.

ISO 27001 is the leading international Standard for information security management. It's designed to help organisations of any size and sector protect their information security, giving you peace of mind that valuable information assets are secure and compliant.

Citation ISO Certification – proud to support businesses across the UK

If you want to protect your information security and achieve ISO certification, we'll be with you all the way. Even if you're going it alone, you're not on your own and it's not as scary as you might think. It's based on how your business systems currently operate and basically makes them better and helps fill the gaps to get your business up to Standard.

At Citation ISO Certification we help businesses of every size and sector with a fast, simple, and cost-effective route to ISO certification. We are one of the UK's leading certification bodies and we're by your side throughout your ISO journey. No complicated jargon just simple expert advice to help you achieve certification in as little as 45 days.

If you have any questions or would like the help, guidance and advice of our expert team, you can call us on **0333 344 3646** or email **ISOsales@citation.co.uk** for a chat about what you need and to get the ball rolling.

Citation ISO Certification