Citation ISO Certification

The surprising security threats inside your business

v01

The surprising security threats inside your business

Think of a cyber security threat – are you imagining malicious software? High-profile hacks hitting the headlines? Whilst you're right these outside threats are real and a risk to your business, are you overlooking the dangers from within?

These internal threats can be less obvious and even come from employees you know and trust but are just as damaging – if not more so – to your business' sensitive data and operations.

In this guide, we'll uncover the surprising security threats lurking within your business, learn how big the threat is and look at the best solutions to protect your business.

People

Cyber security isn't just about making sure your network and devices are secure, it's about making sure the people who are using these networks and devices are secure too!

Unaware and untrained employees

One of the most common internal security vulnerabilities is the lack of awareness and training among employees. In fact, 74% of data breaches involve a human element (Verizon DBIR 2023). Your team, although well-intentioned, can inadvertently put your business at risk by falling victim to phishing emails, downloading malicious files, or unknowingly sharing sensitive information. It only takes one click of the wrong link sent in a phishing email to cause a big headache for your business.

Whether it's recognising a phishing email, handling sensitive data, or practicing secure password hygiene, your employees are the inside threat key to your cyber security success.

Top tips:

As one of the biggest risks – the human factor is also one of the biggest opportunities!

- ✓ Empower your employees at all levels of your business to be accountable and take ownership of cyber security measures.
- ✓ Educate your employees to spot the signs and know how to respond appropriately.
- ✓ Training your employees shouldn't be seen as a tick-box exercise but a powerful strategy to protect your business. So, encourage a culture of security awareness and best practice to turn your team into your first line of defence.

Malicious insiders

As much as businesses would like to trust their employees and believe they hold no ill will against the company, this is unfortunately not always the case. Sometimes threats come from the actions of employees, former employees, contractors or partners who for various reasons, decide to misuse their access. Although malicious insider attacks are rare - accounting for 6% of incidents, this was reported to be the costliest to businesses, totalling $4.90m (IBM Security 2023).

Malicious insiders and unwitting employees are particularly dangerous to organisations as they already hold some level of access to company accounts, data, office premises, and in some cases, finances. Even if an employee was to leave your company for a new job, if they take your company data hoping this will help them in their new career, this would be classed as a data breach and could cause harm to your organisation.

Top tips:

- ✓ Background screening during the hiring process can help to identify any red flags in a candidate's history.
- ✓ Put measures in place such as 'least privilege'. This means giving staff the lowest level of user rights required to perform their jobs, so if they are the victim of a phishing attack, the potential damage is limited.
- ✓ Prepare for an employee leaving the company by reducing and revoking access to company data and controls.

Physical factors

While we focus on digital threats, physical security shouldn't be overlooked. Think about access to your premises, unsecured server rooms or paperwork scattered on desks and printers. These seemingly ordinary occurrences often go unnoticed but can quickly turn into opportunities for data breaches and threats to your business' cyber security.

Top tips:

- ✓ Don't leave the door open to hackers – literally! Tailgating (when people take advantage of the politeness of someone holding a door for them) can invite unwanted guests into your business.
- ✓ Have protocols in place for guest access to your premises and networks and make sure all employees understand them.
- ✓ Introduce a clear desk policy so that no paperwork with sensitive information on is left in view.
- ✓ Encourage employees to screen lock when away from their desks, even if they're only away briefly.

Incident response

As the saying goes, fail to prepare and you prepare to fail. You may not know when an attack might occur but if you're prepared you can limit the damage, handle the fall out and recover quicker. With a response plan that's been tested and ready to go, you can make sure that if an attack happens it can be quickly identified and dealt with.

Imagine losing access to your emails – could your business continue its operations seamlessly? A business continuity plan can help you plan for any disruptive events. As cyber crime is constantly evolving, staying up to date on the different types of attacks and refining your response plan is essential to maintaining your defences.

Top tips:

- ✓ Do you have a response plan in place and have you tested it?
- ✓ Does your response plan include key contacts and clear roles and responsibilities?
- ✓ Make sure backups are available and regularly tested to help with a swift recovery.

Cyber security in numbers

Cyber security is one of the biggest challenges facing organisations of every size and sector. So how big is the threat to UK businesses today? Let's look at the numbers!

83%

of organisations have suffered from more than one security breach
(IBM Security's Cost of a Data Breach Report 2023)

74%

of breaches involve a human element (Verizon's DBIR 2023)

43%

The UK is the most cyber attacked country in Europe, accounting for 43% of all cases (IBM Security's X-Force Threat Intelligence Index 2023)

41%

of incidents involve phishing for initial access
(IBM Security's X-Force Threat Intelligence Index 2023)

60%

of cyber breaches in Europe involve social engineering tactics
(Verizon's DBIR 2023)

19%

of breaches are caused by stolen or compromised credentials
(IBM Security's Cost of a Data Breach Report 2023)

Security breach! What's the impact?

We all know that as technologies progress and become more integrated into our day-to-day, we're increasingly vulnerable to cyber attacks and data breaches. But what would be the impact of a security breach, and how would this affect your business?

- Your sensitive, intellectual property and data could fall into the wrong hands.
- You could see a loss in market confidence and reputational damage following an attack.
- Your business could face hefty fines as a result of incompliance with the UK GDPR 2021.
- Significant company downtime and a disruption to your business operations.

Let's keep your business safe

How can you stay on top of it all and create best-practice processes to protect your business? That's where ISO 27001 comes in.

ISO 27001 is the world's best-known Standard for information security management. systems. It helps organisations set up processes to pinpoint potential risks to sensitive information in their business, that also includes cyber security risks and maintaining data confidentiality. And the great thing about ISO 27001 is it looks at information security across all areas of your business - online and offline.

How can ISO 27001 help?

This best-practice framework helps your business have controls in place to combat threats to your data integrity. With policies and procedures in place to protect and manage sensitive information, you'll be well prepared to identify and handle security threats helping you to reduce breaches and build a culture of security.

And the benefits don't end there! ISO 27001 certification can help power your business growth. With a certificate that's recognised worldwide you can open doors to new opportunities and access new markets. It shows clients you're committed to safeguarding their information and take security seriously. Businesses with ISO 27001 certification are seen as safer to engage with and it's becoming more common for organisations to only do business with those that can show they have a recognised IT security management system in place.

Top benefits of ISO 27001

- ✓ Keep confidential information secure
- ✓ Reduce cyber attack threats and minimise the risk of data breaches (and the hefty fines that come with them!)
- ✓ Develop better legal compliance
- ✓ Give customers peace of mind
- ✓ Sharpen your edge and win more business
- ✓ Enhance your reputation and get recognised as being safe to work with

The latest protection

ISO 27001 was updated in 2022 to be brought in line with current cyber security practices and potential threats. With an ever-changing digital landscape and new business practices such as remote working, cloud computing and emerging technologies, ISO 27001:2022 is here to provide robust and relevant controls so you can stay one step ahead of cyber threats and protect your business. With organisational, people, physical and technological controls you can make sure your business is covered and ready for anything.

Psst! Did you know?

ISO 27001 includes business continuity planning helping you to maintain operations during and after security incidents, minimise downtime, recover quickly and keep your business running smoothly.

Citation ISO Certification – proud to support businesses across the UK

If you want to protect your business 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