# Cybersecurity confidence for the SME

Just as it is for large corporates, cybersecurity is a pressing issue for small businesses. The scale might be different, but the fundamental risk areas are similar. Indeed, criminals frequently target SMEs and start-ups in the knowledge they can often be a softer target with less resource for IT security.

It's risky for small business owners to assume that cybercriminals will overlook them in favour of larger targets. They understand that the typical SME simply can't invest in the same specialist technology or training as larger corporates, but that they still hold potentially lucrative data and information.

Under the general data protection regulation (GDPR), small businesses now have the same responsibility as large corporations when it comes to processing and protecting data. They are also subject to the same fines and penalty structures.

What's more, cybersecurity has moved from a technical specialism to a mainstream business issue over the last decade. Despite this, many companies are still not doing enough to protect themselves.

According to a 2019 cybersecurity study conducted by IBM, three-quarters of businesses do not have a plan in place to respond to a cybersecurity incident.  This is even more concerning in light of research published by the Department for Digital, Culture, Media and Sport, suggesting that every data breach or cyber incident results in losses of £4,180 on average - up from £3,160 in 2018 – for businesses.

Standards help SME owners act with confidence to protect themselves, their customers and partners from cyberattacks and data breaches. They introduce processes which build resilience against both deliberate and chance incidents – as well as assisting with legislative compliance.

A priority area for attention is information security. Every business, no matter how small, runs on data – its own and that relating to employees, partners, suppliers, customers and others. With new information generated every second, it's imperative to stay in control of how it's stored, who can access it and how it's managed.

Businesses can use ISO/IEC 27001 to design and implement an overarching information security management system, while ISO IEC 27552 will focus on improved privacy controls when it launches later in 2019.

Data storage is also important to control. Cloud computing has transformed the way most businesses store data and has now become commonplace. Standards can help SMEs make the right choices when selecting cloud service providers, as well as manage the resulting storage arrangements. ISO/IEC 27017 outlines guidelines for information security controls around the provision and use of cloud services.

Modern flexible, and home-based, working practices present new risks related to employees using their own devices for work tasks. Some companies now maintain a 'bring your own device' (BYOD) system. These situations require the right awareness and understanding from staff when it comes to their security responsibilities.

Creating a clear policy, in line with ISO 27001 requirements, is the best way to reduce risks associated with BYOD arrangements.

Human error is often cited as a common cause of cybersecurity incidents - employees make mistakes and misjudgements. They can also be exploited by criminals who understand how vulnerable busy, distracted people can be.

However, standards put security-awareness training at the forefront to help strengthen your cybersecurity chain, empowering employees to become an SME's best protection against attack. It's also worth considering ongoing internal communications and reminders on the subject, as well as running phishing simulations and other training scenarios to assess specific training requirements and risk areas.

Using this information, business owners can tailor plans to an employee's individual needs. The information security standard ISO/IEC 27001 helps small businesses create and structure training in accordance with international best practices, as well as define responsibilities in the event of a breach.

Given the consequences of failing to comply with regulations like GDPR, small businesses can't be too careful when it comes to cybersecurity.

Taking a standards-based approach helps you implement a robust approach to managing information security and building resilience in your business.

Certification to key standards also inspires greater trust in your business, demonstrating to customers, suppliers and the market that you can handle information securely.

**Summary:**

- Criminals frequently target SMEs and start-ups in the knowledge they can often be a softer target with less resource for IT security.
- Standards help SME owners act with confidence to protect themselves, their customers and partners – as well as assisting with legislative compliance.
- Small businesses can use ISO/IEC 27001 to design and implement an overarching information security management system, while ISO IEC 27552 will focus on improved privacy controls when it launches later in 2019.
- Any information security management policy based on ISO 27001 principles should also cover the use of personal devices for work tasks, as well as reduce the likelihood of human error causing a cybersecurity incident – helping to turn your staff into your own human firewall.
- Data storage is also important. ISO/IEC 27017 helps SMEs select cloud service providers, as well as manage the resulting storage arrangements.
- ISO/IEC 27001 also helps small businesses structure cybersecurity training in accordance with international best practices, as well as define responsibilities in the event of a breach
- A standards-based approach helps SMEs implement a robust approach to managing information security and build resilience.
- Certification to key standards also inspires greater trust in your business.

For more information on our business improvement standards, visit:

www.bsigroup.com/standards

bsi.

...making excellence a habit.™