The Guide for B Corps and Purpose-Driven SMEs

Stop Sleepwalking into a Cyber Nightmare:

The requirement for secure IT for growing businesses.

Introduction: The Cost of Ignoring Cyber Security for SMEs

As a small to medium-sized business, especially within the B Corp and purpose-driven business space, you may be thinking, “Cybersecurity isn’t something I need to worry about yet.” It can be easy to pretend or even believe that breaches are something that happens to someone else. That everyone in your company is too smart to accidentally click on a bad link or assume that everyone, including those contractors or freelancers who have access to your files, have up-to-date virus protection.

But believing it’s all okay means you could be sleepwalking on your cyber security obligations, only to face an unexpected, devastating cyberattack or compliance breach.

While it may feel like your business is too small to be a target, statistics tell a different story: 43% of cyberattacks target small businesses, and over 60% of those businesses close within 6 months of a cyber breach. For businesses like yours, which rely on a strong sense of purpose and community, the damage of a cyber incident goes beyond financial loss—it can hurt your reputation, stall growth, and cost you clients who trust you with their data.

This guide is designed to show you why scalable, adaptable, and secure IT systems aren’t just nice-to-haves—they are the backbone of your business’s long-term success. We’ll explore the dangers of neglecting IT security and give you actionable steps to secure your organisation and support your growth.

Certified B Corporation

© 2024 ITGUYS. ITGUY London Limited is a registered company in England and Wales.
Registered Number 09390513. Registered Office: 8 Woodberry Down, London N4 2TG.

The growing SME cyber threat landscape
Data-driven insights: The risk is real

Many SMEs mistakenly believe they are too small to attract cybercriminals, but in fact, they're often the ideal target. In 2023, the UK's National Cyber Security Centre (NCSC) reported that cyber threats aimed at SMEs increased by 50% over the last 12 months, with more businesses falling victim to ransomware, phishing, and data breaches.

For B Corps and purpose-driven SMEs, the consequences are even greater. Not only do you face the financial and operational impacts of a cyber attack, but your brand's credibility is at risk. Your customers expect the highest level of security and trust, especially if you're handling sensitive data such as financial details or personal information.

In the UK, 32% of businesses and 24% of charities reported experiencing cyber breaches or attacks in the past year. Cybercrime cost UK businesses over £30 billion in 2023, with small businesses among the hardest hit.

Small businesses are facing a diverse array of cyber threats, including:

- **Phishing Attacks**: Fraudulent emails or messages designed to steal sensitive information.
- **Ransomware**: Malicious software that encrypts data, demanding payment for its release.
- **Business Email Compromise (BEC)**: Deceptive emails that manipulate employees into transferring funds or sensitive information.
- **Data Breaches**: Unauthorized access to confidential data, leading to potential identity theft and financial loss.

Several factors contribute to the increasing vulnerability of SMEs. Predominately, a lack of expertise hinders the implementation of robust cyber security measures. When no one is taking responsibility consistently from education through to the right software, you lack the comprehensive security measures and staff training to combat the growing wave of cybercrime.

The end result? You become an attractive target for cybercriminals.

© 2024 ITGUYS. ITGUY London Limited is a registered company in England and Wales.
Registered Number 09390513. Registered Office: 8 Woodberry Down, London N4 2TG.

The Growing Consequences of Sleepwalking

When you neglect to acknowledge the real risks and threats lurking in the background, you put your data, operations, and client trust in jeopardy.

1. Increased Vulnerability to Evolving Cyber Threats

- *Why it is dangerous*: Cyber threats are becoming increasingly sophisticated, and a "sleepwalking" attitude towards IT security means you may be relying on outdated systems and protocols that can't defend against modern threats. In 2023, the average number of cyberattacks targeting small businesses increased by 45%. Threats such as ransomware, phishing, and insider attacks have become more advanced, and those who don't continuously adapt their security posture are left exposed.

- *Impact*: If your business isn't actively keeping pace with cyber security trends, it becomes a prime target for cybercriminals who know SMEs are often underprepared. Hackers know how to exploit old software, weak passwords, and employees who haven't been trained to spot phishing emails or scams. This is how they gain access to your systems, your data and even your bank accounts.

2. Reputation Damage That Can Be Irreparable

- *Why it is dangerous*: One of the most significant risks of sleepwalking through cyber security is the potential damage to your reputation. If a cyber-attack exposes customer data or disrupts your service, it can erode the trust and loyalty that your customers have placed in your brand.

- *Impact*: Reputation is everything for SMEs, especially those in the B Corp and purpose-driven space. These organisations often market themselves on values like transparency, trust, and responsibility. A data breach or ransomware attack can create a public relations nightmare, leading to customer distrust, negative reviews, and a significant loss of business. The damage isn't just financial—it's emotional and relational and can take years to recover (if ever).

3. The Financial Toll of Being Unprepared

- *Why it is dangerous*: A cyber-attack is expensive, but when SMEs sleepwalk through security, they don't plan for this potential financial burden. Small businesses typically don't have the resources or budget to recover from a significant cyber incident. The cost of ransomware, downtime, and recovery can drain your cash flow.

- *Impact*: The financial toll from an attack can be devastating. SMEs that suffer a ransomware attack, for example, may spend an average of £120,000 or more to recover. If your systems are compromised, you may face additional costs like lost productivity, the price of restoring compromised data, and even compensating customers or clients for their losses. And for some SMEs, these expenses can be enough to close the business down entirely.

4. Operational Slowdowns and Missed Opportunities

- *Why it is dangerous*: One of the more subtle consequences of neglecting cyber security is the operational slowdown that often follows a breach. Many SMEs find themselves spending weeks or months trying to restore lost data, rebuild systems, or deal with legal fallout after a cyberattack. During this time, your business operations can grind to a halt, causing missed sales opportunities, lost contracts, and decreased productivity.

- *Impact*: If your business is forced to divert time and resources to address the fallout from an attack, that means fewer resources are available for customer acquisition, product development, or service delivery. In an increasingly competitive market, this operational downtime can result in losing your edge, making it harder to recover or grow after an attack.

5. Regulatory and Compliance Risks

- *Why it is dangerous*: Many SMEs fall behind in maintaining compliance with regulations such as the General Data Protection Regulation (GDPR) or the Data Protection Act. Cyber security is not just a matter of protecting your business; it's about protecting your customers' data and meeting regulatory standards. For example, failing to implement proper data security measures under GDPR can result in severe fines if you are hacked.

- *Impact*: If your business experiences a data breach and you haven't taken the necessary precautions, the legal consequences can be far-reaching. In addition to hefty fines, non-compliance could mean long-lasting reputational damage. Customers expect companies to protect their sensitive information, and regulatory authorities are increasingly stringent in ensuring that businesses meet security standards. Plus, data breaches can damage your relationship as a trusted partner with your clients and customers. Damage to your brand that is hard to rectify.

Secure IT solutions: The fallacy of "good enough" IT systems.

As your business grows, so do your IT needs. Starting with basic systems may seem sufficient in the early days, but as you scale, vulnerabilities multiply if those systems can't grow and adapt with you.

When companies take shortcuts with their IT, opting for quick fixes or outdated systems, they often find themselves dealing with:

- **Limited scalability**: Systems that can't grow with your business or handle increased data traffic.

- **Costly rigid structures**: Systems that lock you into costly service contracts or expensive hardware that offers little flexibility.

- **Security risks**: Outdated or patched systems that cybercriminals can easily exploit.

© 2024 ITGUYS. ITGUY London Limited is a registered company in England and Wales.
Registered Number 09390513. Registered Office: 8 Woodberry Down, London N4 2TG.

For growing SMEs, security and scalability should be non-negotiable.

A secure, scalable IT infrastructure will allow you to scale up your operations without disrupting service. It enables flexibility to help you adapt to new opportunities, team members and even customers. And in today's world, meet your obligations to keep sensitive data safe, with modern security protocols, encryption, and up-to-date software.

What you can do right now: Steps to secure your IT infrastructure

You don't have to wait for a cyber-attack to shake your business—there are immediate, actionable steps you can take to ensure your IT systems are scalable, adaptable, and secure.

1. Conduct a Cyber Security Audit

A cyber security audit is the first step to understanding where your vulnerabilities lie. It will identify weak points in your current system and highlight areas for improvement. This audit should include:

- Reviewing access controls (who has access to what data).
- Assessing your network's security (firewalls, encryption, antivirus).
- Examining your backup and recovery plans.

2. Invest in Scalable Cloud Solutions

Cloud computing offers businesses an affordable way to scale without locking into expensive, inflexible infrastructure. Choose a cloud service that:

- Offers high levels of encryption and secure backup.
- Allows for flexible growth without costly infrastructure updates.
- Adapts to meet regulatory compliance and data protection laws.

3. Train Your Team

Cyber security isn't just an IT issue—it's a company-wide responsibility. Ensure that your team is educated on:

- Recognising phishing and social engineering attacks.
- Using strong, unique passwords and two-factor authentication.
- Regularly updating software and security patches.

4. Partner with a Trusted IT Services Provider

As a purpose-driven SME, your focus is on your mission, not on managing complex IT systems. Partnering with a trusted IT provider who understands the needs of growing businesses is key to securing your infrastructure, improving system performance, and reducing risks. An IT services partner can help you implement scalable, secure solutions and monitor your systems 24/7.

Take Action Now—Before it's Too Late

Your business's growth depends on your ability to manage risk, and this includes the risk posed by cyber threats. A proactive approach to IT security will safeguard your business and empower your organisation to grow sustainably and efficiently.

It's time to stop sleepwalking through your IT systems and take control of your cyber security. By adopting scalable, adaptable, and secure IT solutions, your business can grow sustainably without the risk of falling prey to cyber-attacks. Secure IT is not just about protecting your data—it's about future-proofing your business and continuing to deliver on your mission with confidence.

Don't wait for a cyber nightmare to disrupt your growth. Take the first step toward securing your IT infrastructure today.

Book your ITGUYS Cyber Security Audit today.

Partner with Us

ITGUYS delivers IT Freedom. We want to ensure purpose-driven businesses are confident that they are safe and protected from the risks and complexity of IT. Free to focus on what matters, confident they have the strategy and tools in place that are right for them to proactively support their business growth free from the worry of IT while still reducing their IT impact on the planet.

> *"I love that I don't have to think about my IT. That feels weird, right? But it's true. If it is so important operationally and you don't have to think about it, gives me the bandwidth to worry about other things. ITGUYS have dropped everything to ensure we're up and running.*
>
> *I continue to be really impressed with their commitment to us."*
>
> *Lettie Graham*

**BOOK A CALL WITH
BEN AT
BEN@ITGUYS.COM
OR ONLINE HERE**

Let's chat about how you work, what you like and how we can help you. We want to empower businesses of all sizes with the IT they deserve. If that sounds good to you, pick up your phone or send us a message.

© 2024 ITGUYS. ITGUY London Limited is a registered company in England and Wales.
Registered Number 09390513. Registered Office: 8 Woodberry Down, London N4 2TG.