A SMALL BUSINESS GUIDE TO IT SECURITY

micropro
Business IT Experts

Why do so many small businesses fail?

Securing your office network should be a priority for small business owners. Our small business IT security strategy guide helps you to get started.

According to the 2020 edition of the Business Population Estimates, released annually by the Departments for Business, Energy & Industrial Strategy, there were an astounding 6 million businesses registered in the UK last year.

Of these businesses, 5.94 million were classified as small businesses. When combined, SMEs (small or medium-sized enterprises) account for 99.9% of the entire UK business population.

Despite this high number, only 43% of start-ups and small businesses survive their first 5 years. According to an article from The Telegraph, as many as 60% of SMEs will go under this year.

Something you might be surprised to discover is that 43% of cyber attacks are aimed at small businesses. And it makes sense. For cyber criminals, a small business is an easy target as you’re more vulnerable to security risks. This is due to the fact you likely have limited resources

And according to Cyber Crime Magazine, around 60% of all small businesses fail within six months of falling prey to a cyber attack or data breach. This is why having the right IT security strategy in place is so important to the success of your business.

It can be tempting for many business owners to assume that IT security is something to work on later down the line. But without secure data and processes from the onset, you’re putting your business at risk.

A Guide to IT Security for Small Businesses

In this guide, we'll examine some key considerations when putting an IT security strategy together.

Follow our guide to ensure you're not included in the above statistics.

What would you do if suddenly, your business data disappeared? Or if your customers' sensitive data was breached? Would you know what to do if your network was attacked?

The answers you give to the above questions can determine whether your small business is primed for success or failure.

Do you have a plan or contingency measures in place for these very real risks?

If you answered "no" then chances are your business is in danger of falling prey to those aforementioned survival statistics.

But fortunately, it's not all doom and gloom. There are a few things you can do to ensure your business is as secure as possible. We've outlined five of these below.

Backup your data and protect against data loss

First thing's first, make sure you have a data protection solution in place. This will protect your business from security breaches and subsequent data loss.

A business that can't prevent data loss or doesn't have a disaster recovery process in place, will lose money and consumer confidence.

A data protection or back-up solution will protect your data from power outages, theft, fires, floods and other natural disasters. But it will also ensure you don't lose all your data if a cyber criminal tries to steal or delete it.

Off or on-site servers: which one is right for your small business?

If you work in a fixed location, as a general rule, you should have multiple copies of your original data stored on separate disks. Of course, these data backups need to be somewhere safe. For instance, on a separate site or stored remotely via cloud storage.

The benefit of cloud storage is that these backups can be scheduled at regular intervals. As a result, you reduce the risk of forgetting to do so manually.

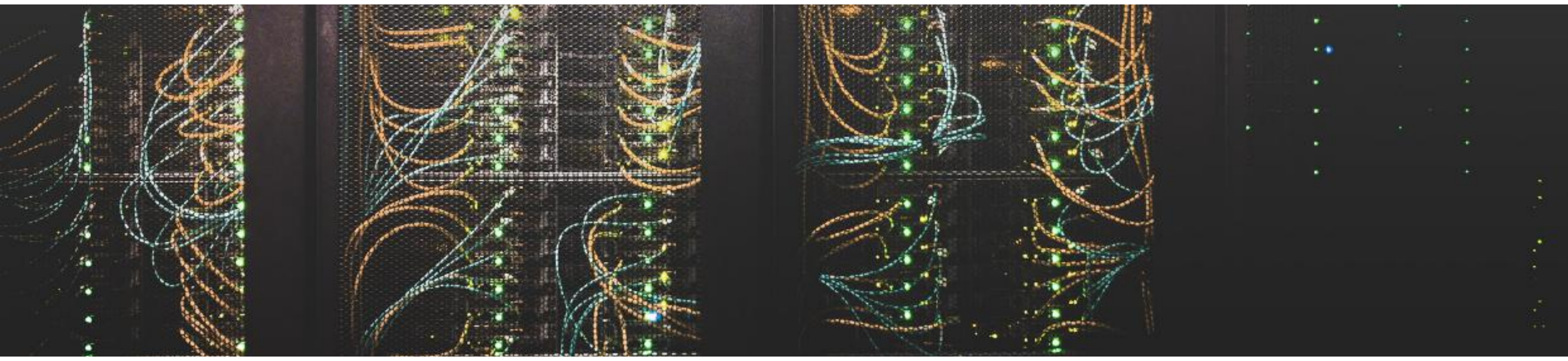
However, many small businesses opt to copy and save all files and data to a dedicated server, usually located on-site. This means all devices are backed up to a single server.

This is incredibly useful as a data solution when a single file gets deleted. Or if you need to retrieve some lost data. However, if your server gets damaged or the building it's in burns down or suffers from flood damage during heavy rain, you will lose everything.

> It's worth investing in disaster recovery and cloud backup. As a result, you can feel safe in the knowledge that your sensitive data won't suddenly disappear overnight, rendering your business helpless.

And, at Micro Pro, we provide expert advice on data and disaster recovery. We provide secure and reliable data back-up solutions and disaster recovery. Whether you want server support or a combination of on-site and cloud backup. And, following a disaster, we can enable your business operations to resume as quickly as possible.

As a result, this will mitigate any lost time for your business – so that you can focus on what matters.



Install firewall protection and monitor your traffic closely

Browsing the Internet without a firewall to monitor and control incoming and outgoing traffic across your network is dangerous. In fact, unmonitored and controlled traffic can lead to unintentional infected downloads, unsafe website use and threats to your data.

Of course, you can install a firewall yourself, but without understanding how it works this can still be risky.

Firewalls use a set of defined rules to determine whether or not to allow or block traffic coming to your website or network. As such, it's important to utilise a specialist with a high degree of skill who can configure your firewall and its rules.

If you want to stay safe, consider hiring an IT expert

An IT expert can actively monitor your traffic, ensuring your IT infrastructure remains secure and runs smoothly.

For instance, at Micro Pro, we offer 24/7 monitoring of servers, network infrastructure, backup systems and can monitor all company desktops and laptops.

Closely monitoring a network in this way can generate alerts and highlight suspicious activity. In fact, one of the biggest issues of an unmonitored network is that suspect activity such as bulk deletion of data or copying of sensitive documents may go undetected.

But with the fast response time of an IT security specialist, data and GDPR compliance can be upheld. Therefore, saving small businesses from having to pay hefty GDPR fines. As well as avoiding a loss of consumer trust and confidence.

After all, these fines could bankrupt a small business, so investing in IT security now could save your company.

Not to mention, 24/7 monitoring will lead to fewer service disruptions. Which means your infrastructure will remain more stable.

Ensure you have anti-virus protection in place

This ties in with network monitoring and regardless of your business industry or niche, good anti-virus protection is a necessity. Anti-virus software scans, monitors and blocks unwanted or dubious programs and processes.

However, having anti-virus software installed isn't always enough. After all, we're talking about your business, not your personal laptop. While most anti-virus programs are capable of defending your business, in that they provide a basic level of security against a limited set of threats. Having a fully-managed anti-virus system provides an extra level of security and protection.

As a result, your business can maintain fully-operational at all times. And you can avoid any disruption to day-to-day activities that may affect productivity.

At Micro Pro we offer fully-managed anti-virus solutions. Our service will protect you from the latest threats. And we offer up-to-date protection from computer viruses, infections, trojans, malware and ransomware.

In fact, we offer software designed to augment your anti-virus or endpoint IT security, giving you an extra level of protection. As such, we can secure your business from any potential new threats or unknown viruses much more efficiently.

Plus, we'll be on standby if an employee accidentally opens an email attachment they shouldn't have. Which brings us on to our next point.

Train your staff and employees on relevant security protocols

Even in the most secure of environments, data breaches happen. You can have a firewall in place and monitor your traffic closely but poorly trained staff can cause your IT security measures to crumble.

Unsurprisingly, the majority of these data breaches happen due to human error. In fact, according to the UK Information Commissioner's Office, 9 out of 10 data breaches were caused by human error in 2019.

We're all human and part of that experience is the fact that humans can easily make mistakes. As employees, we all have our strengths and weaknesses. An employee in the customer service department doesn't understand the complexities of spreadsheets in the same way someone on the accounts team does. And why should they?

Thus, the same goes for IT security. Your employees all have different specialisms and can't all be expected to know every part of your business inside out. However you can reduce the risk of human error if your staff are trained properly in IT security.

Avoid common errors with effective communication and access to essential IT security information.

Of course, this doesn't mean forking out for expensive training courses. Nor does it mean ensuring your staff understand IT and technology processes like the back of their hand.

In fact, a brief overview of what to do in an IT emergency and an IT compliance guide within your staff handbook should suffice. As well as ensuring you have a policy in place for dealing with suspicious or unsolicited emails.

Most attacks come from spam emails or phishing. Phishing is a when single or multiple targets are contacted (mostly via email, but sometimes via telephone or text message) by a criminal posing as a legitimate organisation or trustworthy individual in order to obtain sensitive information. This information may include passwords, credit card numbers and any other identifiable personal data.

Ensure your staff are aware of any phishing attempts and know to report anything that seems suspicious.

All staff should also have the correct details of your IT department or IT support team to hand too. As a result you can reduce the number of common IT support related issues.

Of course, you can outsource your IT support to experts too. This may be a good idea if your business is starting out and you haven't hired enough staff to carry out IT processes.

However, if you need help identifying your security protocols and mapping out your security processes, we recommend hiring an IT strategist.

Update your passwords regularly and use two-factor authentication

This is something which may seem obvious to most, however many businesses fail to update their passwords regularly. Or those that do, find that not all employees know how to create a secure one.

But, all computers, laptops and tablets belonging to your business contain critical data. Whether this is the personal details of your customers or the payroll details of your employees. All data that you access needs to be available to authorised personnel only.

While regularly changing passwords is a good tactic for avoiding breaches or unauthorised access to your data, emails and sensitive information, two-factor or Multi-Factor Authentication (MFA) is essential.

Two-Factor Authentication (2FA), requires users to provide two different methods that prove you are who you say you are. For instance, you've likely come across 2FA if you use online banking services and MFA is a basic requirement for modern security.

However, properly configured 2FA or a Single Sign On (SSO) can streamline this process and take care of your password security. SSO is a user authentication service that permits a single set of login credentials to access multiple applications.

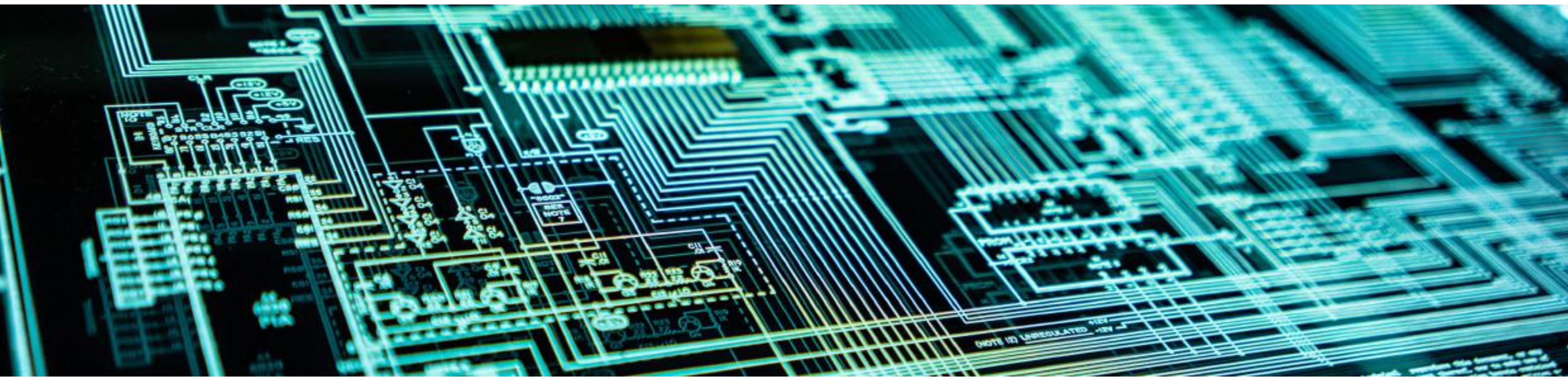
An example of SSO is Google. They implement this approach so that users can access all their software products using one login.

Many IT support companies can assist you with 2FA, MFA, or SSO processes and it will likely form a part of their overall cyber security service.

What Cyber Security Solutions Are Right For Your Business?

Naturally, problems and security risks will occur. However, if you're a small business owner you might not be able to accurately troubleshoot these problems. Knowing which cyber security solutions to utilise can be difficult, especially as there are so many potential attack vectors.

Overall, IT security issues are incredibly varied and complex so it's best to leave it to the professionals.



Summary

Of course, while our guide works as a checklist to reduce IT security risks, no security defence is 100% impervious. That's why you need an effective IT strategy and security protocol in place.

Our suggestions barely scratch the surface of IT security. SMEs will likely encounter even bigger risks as they grow, which is why it's important to invest in IT security early on.

However, if you're a small business owner, you need an IT department with the ability to identify potential risks. One that will find and control any IT or data breaches that will inevitably occur.

If you need IT security solutions or you need to secure your network, Micro Pro can help. We can work with your business, assessing your IT infrastructure.

Whether you need cyber security support, network security services or, an entire IT security strategy; we can help your small businesses to succeed. Here are just some of the IT security solutions we offer:

- A full IT security audit
- A bespoke IT security strategy
- Protection of IT infrastructure from cyber attacks
- 24/7 monitoring of your network
- Anti-virus support
- Mitigation against data breaches
- Compliance with GDPR
- Part or fully-managed IT support
- Data loss prevention
- Disaster recovery

We can offer support in one area or provide fully-managed IT security services to ensure security is one less thing you need to worry about.

Don't let cyber attacks or security threats get in the way of making your small business a success.

Email us at hello@micropro.com or
Call us on 01932 300314
Head office: 1 Station Road, Addlestone, Surrey, KT15 2AL

micropro
Business IT Experts