IT 365

BEST PRACTICE GUIDE

Business cyber security

It seems that barely a week can go by without another cyber security story hitting the headlines. Global businesses have their websites or data compromised. Celebrities have their photos stolen. Systems that were perceived to be secure turn out to be far from it.

While it's the big brands that hit the headlines, every day sees small and medium-sized firms falling foul of digital security issues that cost them money. A recent survey by the Federation of Small Businesses identified that on average, cyber crime costs the typical business £4,000 a year.

But the true cost is likely to be much higher. It's not just the value of goods or services stolen, but of lost sales and additional administration as a result of running into a security problem.

Last year saw a 60% increase in reports of cyber crime. Criminals have realised that it's a lot safer than traditional forms of theft. Smaller businesses are an easier target because their security is often weak. Another survey revealed that a third of small firms wouldn't know what to do if their security was breached and a quarter would not be able to recover lost data.

This means millions of UK businesses are at serious risk of falling victim to cyber security failings. To help you be better aware of the risks, we've put together this brief guide to the main areas where your business could be exposed.

5 tips for improving your cyber security

1 Watch what your employees are up to

In a poll by the British Standards Institute, 37% said rogue members of staff were the biggest risk to security. Here are the most common ways in which your staff can let you down:

- Downloading viruses through casual surfing.
- Deliberate damage or destruction of business data.
- Theft of commercially-sensitive information.
- Clicking on links in phishing emails, despite being warned not to.

All of these occur more often than you might think. Many firms don't want to admit to it, or worse, they don't know about it. Many still put too much trust in free or low-cost firewalls or anti-virus systems that don't offer comprehensive protection.

Watching what your employees are up to is now relatively easy, with the latest generation of network monitoring tools.

2 Stay in control of your mobile devices

Around 1.5 million mobile phones are lost or stolen in the UK every year, along with a growing number of tablets. Despite our dependence on them, we're not very good at looking after our mobile devices. How many has your firm lost in the last few months?

Every business phone or tablet that contains company data or can access your internal systems is a security risk. Even if it can only get to email, it's a potential doorway for cyber criminals or simply someone looking to cause mischief.

You can't lock mobile phones and tablets to the desk, because that defeats the point. But you can install apps that let you keep track of an item's location, let you change its passwords remotely, or even allow you to delete its contents without having access to the physical device.

3 Audit your systems and your risk

One in five small businesses have assessed their digital security risks, according to research by the FSB last year. This figure suggests that an alarming 80% of firms have not given the matter that much thought.

An audit of your systems and risk means asking questions such as:

- How often are users required to change their passwords?
- Does our firewall or antivirus comply with recognised security standards?
- Are our staff trained in how to spot and deal with phishing attacks?
- Are all activities on our computer network logged?

Unfortunately, too many businesses only discover the extent of their risk when they are hit by a digital security problem. While an audit does not provide protection, it helps you spot the weak points, allowing you to put preventative measures in place.

4 Choose the right hardware and setup

While you're generating some excitement by putting new computers, smartphones and tablets into the hands of your staff, you can't afford to neglect some of the less glamorous pieces of business hardware.

Wireless routers and hardware firewalls may not be exciting to look at or to set up, but configured correctly, they're an essential part of your protection against cyber risks. However, many firms simply plug them in and assume they work correctly, not realising the need for proper configuration.

When you're installing hardware, it pays to have experts who can optimise its effectiveness.

5 Know what to do when it goes wrong

The head of research at security specialists Sophos estimates that four out of the five companies hit by malware every day are small and medium-sized firms. Many of these businesses have no contingency plans in a security crisis, resulting in days lost to finding a solution. The cost, in downtime, recovering data and missed sales, can be huge.

Firms who assume that at some point their security will fail, and who plan for how to recover the situation, are positioning themselves for minimal disruption and costs.

A contingency plan begins with agreeing a process with your IT support team for what to do when a problem strikes. Handing the issue over to technical specialists secures a faster, more effective fix than trying to muddle through in the hope the issue isn't as bad as you think.

How IT Support 365 can help you with cyber security

We're helping small businesses across the south of England to manage their digital security. Our solutions include:

- Internet usage monitoring, keeping track of all web traffic across the business, on any device.
- Mobile device management, allowing firms to remain in control of smartphones and tablets.
- IT security audits, which come as standard to all our customers.
- Correct configuration of key security hardware, such as routers and firewalls.
- 24-hour support, replacement servers and data back up, allowing firms to recover from security breaches as fast as possible.

If you're concerned about cyber security in your business, we'd be pleased to have a no-obligation conversation about potential solutions. Get in touch with us today, because it's better to be safe than sorry.

www.itsupport365.co.uk 08450 510600

IT 365
PROACTIVE IT SUPPORT