NEWS BITES AND INSIGHTS

# Protect your business against cybercrime

**Are you worried that cybercriminals may be targeting your business?**

If your answer is 'no', your confidence flies in the face of all the evidence. Tens of thousands of UK firms, of all sizes, have already fallen victim to cybercrime and many have lost tens or even hundreds of thousands of pounds.

If your answer is 'yes', you're taking a more realistic view. Criminals are increasingly turning to online crime because it extends their reach and makes them harder to track. They target businesses because many firms have gaps in their cybersecurity that are easy to exploit.

We know of businesses in the South West of England that have lost hundreds of thousands of pounds to cybercriminals. Their stories don't make the headlines and they're not big brands, but that doesn't lessen the pain felt by the business owners and their teams.

## Top tips for boosting your firm's cybersecurity

**According to research by the BBC, cybersecurity is the number one concern for big companies in 2016. It should be an even bigger concern for smaller firms, which have less inhouse expertise for tackling digital threats.**

### 1. Make someone responsible for cybersecurity

Your entire business should be made aware that cybersecurity is everyone's responsibility. Most cybercrime starts by fooling someone into giving away access to internal systems, meaning anyone could be targeted.

That said, someone in your business should take overall responsibility for managing cybersecurity. They will understand the main forms of threat and the best types of defence. It's their job to communicate with the rest of the business, keeping people informed and alert.

New government research shows that three out of four small businesses (fewer than 250 employees) suffered a cybersecurity breach in 2014-2015. This level of attack highlights the level of threat and the importance of this responsibility.

### 2. Conduct a cybersecurity health check

An audit of your cybersecurity measures should definitely be on your firm's to-do list for 2016. As with a financial audit, this is best carried out by someone independent of your organisation, who can bring a fresh perspective and isn't afraid to ask challenging questions.

Last year, one region of the UK took the cybercrime threat so seriously that it set up a business unit of ethical hackers with the specific objective of helping smaller businesses. Ethical hackers are invited into firms to expose weak points in their security systems, by carrying out activities similar to cybercriminals.

You might not want to go so far as to hire an ethical hacker, but a thorough health check is recommended.

A health check includes:

- Making an inventory of all your digital assets.
- Carrying out a risk assessment.
- Reviewing procedures for handling a cybersecurity breach.

### 3. Educate your staff about their cybersecurity role

A survey by security specialists Kaspersky Labs revealed that over 80% of smaller companies felt they would not be targeted by cybercriminals because they were too small and had nothing worth stealing.

If business owners and directors believe their firm to be small enough to be safe, employees are unlikely to give cybersecurity a second thought. But it is the employees who are likely to be targeted by criminals.

Educating your staff in how to spot and avoid attacks should be a cornerstone of your cybersecurity strategy. Making them aware of the risks could prevent someone being fooled into clicking on a rogue link which allows the installation of a virus onto your network.

Ransomware is predicted to be one of the biggest cyber threats in 2016. This is a virus which, once installed, encrypts all your company data, making it inaccessible. It's accompanied by a demand for payment. Even if you pay up, there's no guarantee that your data will be unencrypted.

Educating your staff about the importance of their role in cybersecurity should also raise their awareness of what may happen if your company falls victim. Not all businesses survive an attack, meaning your staff could lose their jobs.

## Make your cybersecurity easier by talking to us

As specialists in supporting IT networks and mobile devices, we're proactive in helping our clients develop and maintain their cybersecurity strategies. By keeping ourselves up to date with current best practice, we're well placed to advise our clients on current cybercrime threats and trends.

**If you would like to know more about the cybersecurity issues facing your business, or how to protect yourself from the growing risks from cybercrime, give us a call on 0808 168 9135 or email enquiries@itsupport365.co.uk. We would be pleased to have a no-obligation conversation with you.**

Alternatively, you can follow us as we share news on Twitter, Facebook or LinkedIn.

Cybercrime, which comes in many forms, is now the single largest category of criminal activity affecting the UK. For many people and businesses, it's only a matter of time before they fall victim to phishing, malware or some form of online fraud. Take action now to cut the chances of your business experiencing the pain of significant financial loss.