Cyber threats

General Features

01 January 2019

Andrew M from the National Cyber Security Centre provides practical guidance for SMEs on preparing for and dealing with a cyber security breach

Key Points

What is the issue?

There’s around a one in two chance you or your client will suffer a cyber security breach.

What does it mean to me?

Think about what you'd do if you lost your or your clients' sensitive personal or business critical data.

What can I take away?

By following the steps in this article organisations can improve their cyber security and better protect themselves and their clients from loss online.

If you're a Small or Medium Sized Enterprise, you'll probably know how vital you are to the UK economy. SMEs make up 99.9% of all UK registered businesses, employ 60% of private sector employees and account for 47% of UK turnover.

What you might not know is that there's around a one in two chance you'll suffer a cyber security breach, which wouldn't be good for you or your livelihood. And when you consider the economic importance of SMEs, it wouldn't good for the UK overall.

So, when the National Cyber Security Centre (NCSC) was formed in late 2016, we committed to supporting SMEs with tailored products and services. This forms part of our role as the UK Government's authority on understanding and reducing cyber security risks to make the UK the safest place to live and do business online.

While cyber security might seem a daunting challenge for you, it no longer need be and there's no reason to put your livelihood at risk with the same odds as a toss of a coin.

Simply take a little time to understand the threats and act on them. By following our quick, easy and low-cost advice, you can protect yourself from the most common attacks.

So, what are the threats? Motivated largely by financial gain, the threats from cyber criminals are significant and growing. They range from high-volume opportunistic attacks, which are bought, not learned, to highly sophisticated and persistent attacks involving bespoke malicious software designed to compromise chosen targets.

And as we become more connected to the internet, opportunities for cyber criminals continue to grow. Not only are there more devices connected to the internet than

there are people in the world, the UK's highly digitised economy means that the data we're using on it is increasingly business critical, and therefore attractive to criminals.

For most SMEs, the risks are often from high-volume, untargeted attacks which can be bought and launched with little technical know-how from so-called 'script kiddies'.

A step up from that, hacker groups can run much like your own business. They use both 'commodity attacks' (malicious software that can be purchased) as well as creating or adapting attacks themselves and, like you, return on investment is important to them, so large-scale attacks that cost little to launch are an attractive proposition.

Typically, these might involve sending out phishing emails to implant a virus, allowing criminals to steal your data or passwords, or it may encrypt your data, seeking a payment to unlock it: a ransomware attack.

Think about what you'd do if you lost your, or your customers', sensitive personal data or business critical data like your accounts? Could you spare the time and money to get back up to speed? Would you be ready for the reputational damage that a loss of data might cause? And from 25 May 2018, the General Data Protection Regulation (GDPR) introduces the chance of increased fines if you fail to meet your responsibilities. Could you spare the cost of potential fines?

Again, are you prepared to take a chance with cyber security on a toss of a coin?

Those are some of the threats. But the NCSC has products available that can significantly reduce your chances of becoming a victim and will help shield you from potential threats.
We can't guarantee total protection, but you'll be protected against the majority of attacks that SMEs most commonly face.

By following the steps in our Small Business Guide, organisations can improve their cyber security and better protect themselves from loss online:

1. Backing up data. If you have an up-to-date copy of your data, there's no need to pay to unlock it if you fall victim to a ransomware attack.
2. Keeping smartphones (and tablets) safe. If you lose your phone, or it's stolen, you can limit the loss to just the cost of the hardware and not risk allowing

access to all your business and sensitive personal data too.

3. Preventing malware damage. Use antivirus software and keep your software updated, ideally turning on automatic updates. There's a reason why companies offer updates to their software, and if it's driven by a cyber security vulnerability you can be sure someone will aim to exploit that.
4. Avoid phishing attacks. Don't punish staff if they get caught out by a phishing email, it's better to encourage people to report it so you can act upon it quickly.
5. Using a password to protect your data. We've all got more passwords than we can reasonably remember, so consider using a password manager or provide secure storage so you can write passwords down and store them securely.

SMEs looking to improve their cyber security further can also seek certification under the Cyber Essentials scheme, which helps protect against common threats and demonstrates to customers and prospective customers that you take the protection of their data seriously.

The NCSC website features more simple and practical guidance covering the 10 Steps to Cyber Security, supply chain guidance, avoiding phishing attacks, what makes a good password and so on. It's worth a look.

With a little time and effort, you can go a very long way to reducing your cyber risks, but if you do suffer a cyber breach then Action Fraud should be your first port of call.

The facts are clear: large numbers of SMEs suffer from cybercrime. But taking some very easy steps now could allow your business to grow without the worry of basic cyber threats.

My ask? Do your bit for your business, and help us make the UK the safest place to live and do business online.

Image

PROFESSIONAL STANDARDS AND CYBER SECURITY

Members regularly deal with client sensitive information. As well as having to comply with a number of legislative requirements in relation to the data they hold as a result of GDPR and the Data Protection Act, holding sensitive data opens up significant risk to members in the event of any cyber attack. In addition, there is a fundamental principal of confidentiality which all members are required to adhere to. As set out in both Professional Rules and Practice Guidelines (tinyurl.com/ybl49r9m) and Professional Conduct in Relation to Taxation (tinyurl.com/j9ej35u and tinyurl.com/ya2vv3ga) members must 'respect the confidentiality of information acquired as a result of professional and business relationships and, therefore, not disclose any such information to third parties without proper and specific authority, unless there is a legal or professional right or duty to disclose, nor use the information for the personal advantage of the member or third parties.'

It is essential that all members maintain cyber security and that those who run their own businesses consider the implications throughout their organisation. Resources are available on the Cyber Security pages of both the CIOT and ATT websites (tinyurl.com/leasmwx and www.att.org.uk/cyber-security). This includes Cyber Security training, useful articles on cyber security essentials and password protection and a link to the GDPR frequently asked questions prepared by both bodies and reviewed by the ICO. If you have any further queries in relation to professional standards relating to cyber security please email standards@tax.org.uk.