MYERS & Co. Accountants Limited

Chartered Certified Accountants and Registered Auditors

MYERS & CO. ACCOUNTANTS LIMITED
Suite 204A, East Wing, Sterling House
Langston Road, Loughton
Essex, IG10 3TS

Tel: 020 8418 8980
Fax: 020 8418 8981
Email: info@myersaccountants.co.uk

www.myersaccountants.co.uk

Safeguarding your business against cybercrime

Cybercrime is proving to be an increasing problem for UK businesses, and according to recent research, firms of all sizes have been affected.

More than four in ten UK small businesses have experienced a breach in their cyber security in the last year, according to the Cyber Security Breaches Survey 2018. Among larger businesses, the figure rises to seven in ten. While 74% of firms report that cyber security is high on the priority list for their senior management, the survey suggests that there are further steps that could be taken to help raise awareness.

In this factsheet, we review areas where many businesses leave themselves open to attack, as well as some key strategies to help protect your business.

Implementing technical controls

The survey found that around 50% of businesses failed to implement the basic technical controls set out in the government's Cyber Essentials scheme: **https://www.cyberessentials.ncsc.gov.uk/**.

Analysing what comes in

The first line of defence is to filter what's coming in. It may sound obvious, but the survey found that around one in ten businesses still do not routinely do so.

Firewalls and antivirus software filter incoming computer communications. Together, they establish what's safe to allow through, and block malicious software ('malware'). At the most basic level, for a laptop connected to the internet, a firewall may be included in the operating system. In this case, it simply needs to be switched on. However, many businesses will have a more complicated system, with various different types of devices. They may need a boundary firewall to protect the whole network. Some routers may contain a firewall, but this is not always the case, and your internet service provider can provide clarification. Another tip is that firewalls can be set up or 'configured' to block sites which could pose a risk to your business. This way staff cannot access them.

Antivirus software should be installed and switched on for all computers and laptops, running regular scans to delete malware such as viruses and ransomware. Antivirus software should be updated regularly. Smartphones and tablets also need protection, though they may not need separate antivirus software, depending on how they are configured. The National Cyber Security Centre (NCSC) offers guidance here: **goo.gl/3NmA9G**.

Keeping systems up-to-date

Many businesses continue to run outdated systems, assuming that they work sufficiently well to avoid the need to install updates. However, keeping systems up-to-date is critical, and the survey highlighted this as an area where many businesses were not sufficiently rigorous. Nearly one in ten businesses do not regularly update their software and malware protection. Everything needs to be up-to-date: operating systems, software and apps, on all IT equipment, including tablets, smartphones, laptops and PCs. The operating systems on all business devices should be set to 'automatic update,' and software likewise.

Applying updates is called 'patching'. Patches exist not just to offer new features, but because security vulnerabilities are regularly discovered. That means that businesses which don't apply patches are easy prey for cyber criminals – who are every bit as quick to find software errors as the software developers.

Another tip is to remove any unused software or services from devices. As the Information Commissioner's Office states: 'If you don't use it, then it is much easier to remove it than try to keep it up-to-date'.

Businesses also need to think about their replacement policy. There will come a point at which a device reaches the end of its supported life and updates will no longer be available. Replacements need to be arranged prior to this point.

Restricting access to system controls

Another area of concern highlighted in the survey relates to access rights. Who has access, and to what, within your business? Restricting user access to the system is another of the basic technical controls set out in the Cyber Essentials scheme.

Staff accounts should be configured so that if there is a phishing attack on your business, the risk is minimised. This means that users should be given the lowest level of user rights necessary to do their job. If, for example, a user account exists to create backups, it doesn't need to be able to install software as well – and it is safer if it cannot. Restricting access in this way is called the 'principle of least privilege'.

'Administrator' privileges are particularly important and should be kept to a minimum. An Administrator account can change security settings, install software and hardware and access all computer files: a security breach here therefore has more serious consequences than a breach of a standard user account. Most malicious software, for instance, needs Administrator privileges to install itself or gain access to protected files. Making sure staff do not use an Administrator account to browse the web or check their email can reduce the risk of an Administrator account being compromised.

When staff leave, remember to delete or deactivate their user accounts. This is also worth considering if staff are away from work for prolonged periods.

Making use of secure settings

The survey also found that many businesses are failing to use appropriate security settings – another basic control listed in the Cyber Essentials scheme. Selecting the most secure settings for devices and software is critical. The 'default' settings of new devices and software – those used by the manufacturers – will in many cases need customising before use to improve security. One tip would be to disable or remove functions, accounts and services that your business doesn't need. Default passwords should be changed before devices are used (see later). Fingerprint sensors or PINs can also be used to provide extra security.

The special dangers of mobile working

On business premises, servers can be stored in a separate room. Back-up devices, CDs and USBs can be locked away while they are not in use. But when staff are mobile, different risks arise.

Loss or theft of devices is a particular hazard. Many devices, however, now include free web-based tools which can track a device and lock it remotely so it cannot be used. They can also remotely erase data and retrieve a backup of data stored on the device. Mobile device management software can be used to set up a standard configuration on all your devices to do this.

Unknown Wi-Fi hotspots, for example in hotels and coffee shops, are a prime risk. Connecting to the internet in a hotspot can potentially give someone else access to what you're working on while connected, or to private login details which many apps and web services maintain while you're logged on. Using 3G or 4G mobile networks instead provides security. This has the advantage that you can also use 'tethering' (your other devices, such as laptops, share the 3G/4G connection), or a wireless 'dongle' provided by your mobile network. Another possibility is to use a Virtual Private Network (VPN), which will encrypt data before sending it.

The survey noted that where businesses allowed staff to connect their own devices to a business network, say for remote working, this added another layer of risk. A 'bring your own device' policy, setting out appropriate security, can help here.

Safeguarding removable media

The survey highlighted the fact that many businesses needed to pay more attention to removable media – disks and drives such as DVDs and USBs. Removable media can easily be lost, and important business and customer data with them. If infected, they also have the potential to spread devastating malware throughout the business. Key tips to help minimise such infection include blocking access to physical ports for most users, only allowing business-owned removable media to be used with business devices, and using antivirus tools. Not all staff will need access to USB drives, and it can be prudent to make an inventory of such drives, who they have been issued to, and monitor on an ongoing basis whether they are still necessary.

Creating a robust password policy

The National Cyber Security Centre (NCSC) describes a good password policy as 'a free, easy and effective way to prevent unauthorised users accessing your devices'. It's important to make sure password protection is operative on all devices – laptops, PCs, smartphones and tablets – and that manufacturers' default passwords are changed before devices are used.

The use of three random words and misspelled words is current best practice, and experts recommend training staff on how to create non-predictable passwords. 'Password' and '123456' still come high on the list of most-used – and therefore most dangerous – passwords. Secure storage, such as a locked cupboard, is advised, to give staff the ability to keep a written note of passwords safely. Password details should never be left with the device itself.

As part of a secure password policy, the use of two factor authentication (2FA) for important accounts like email, banking and IT admin is worth considering. 2FA works by using two different methods of verification before a service can be accessed – but is dependent on the service provider allowing its use. It usually works by using a password in combination with a code sent to a mobile phone. This means accounts can't be accessed even if an unauthorised person knows relevant passwords. Service providers are now starting to offer enhanced confidentiality and security settings for email, which may help here.

Detecting phishing emails

Good cyber security isn't just about technology: it's also about people. One of the most high risk areas relates to staff receiving fraudulent emails. Phishing attacks, where emails are sent out asking for sensitive information or containing links to malicious websites, are becoming more and more sophisticated. Just one click can introduce malware, with devastating consequences. Reputable 'brands', such as HMRC, can be used as a 'hook' – and the resemblance to the authentic brand can be very convincing. Invoice-related scams are increasingly common, as are banking security notifications. Other scams operate by requiring staff to 'enable content' or 'enable macro' before they can view. Configuring your accounts to give least privilege (as mentioned previously), and training staff in these matters, will help to keep your business cyber secure.

How we can help

Ensuring that your business is adequately protected against cybercrime and cyber-attacks is vital: it has never been more important to have secure systems in place. Please do not hesitate to contact us for help with carrying out a security or information audit, or training staff on security issues.