AKITA The IT People

GUIDE TO CYBERSECURITY

Protect your organisation from the rise in cybercrime.

THE CHANGING THREAT LANDSCAPE

With unprecedented challenges and changes in working practices in recent years, technology adoption has evolved at a speed few could have dreamt of.

As ever, with new technologies comes new threats. And with small and medium-sized enterprises (SMEs) racing to improve their systems and meet requirements, IT security is not always keeping pace.

According to recent stats[i], the rise of remote and hybrid working in response to the COVID-19 crisis has resulted in reduced IT protection, with only 83% of small businesses reported to have up-to-date security software as just one benchmark for this.

At the same time, cyber threats that would once have been the reserve of multi-national companies and enterprise-level organisations are being increasingly directed at SMEs and less obvious targets, such as education and healthcare providers. This has required a fast adaptation to a new threat landscape.

With such significant shifts both in technology and threats, this guide aims to cover some of the recent trends in cyber security.

IT SECURITY FOR REMOTE WORKING

Home working became a sudden requirement across the UK in 2019/2020 with up to 50% of the population working at home at times. With the technology to support it now in place, many organisations are exploring remote or hybrid working as a permanent option.

However, home-based users do not by default have the advantage of the same security features of office-based workers. The less visible security measures may be missed. Firewalls, encryption and filtering technologies all protect business networks and sensitive data - only some will extend to remote workers.

Similarly, poor device security (whether a business-owned device or personal one) can expose an organisation's systems in unpredictable ways.

To prevent issues arising among remote workers, tailored IT policies and strategies need to be considered.

1. Invest in a **virtual private network (VPN)** that allows all users to access corporate IT systems and resources securely.

2. Provide users with **business-issued devices** equipped with the latest security software (and remote management to allow for future updates to be made remotely). IT policies should also be drawn up to stop the use of personal devices for work tasks. This will ensure that staff members use only the safest and most secure technologies.

3. Adopt a **virtual desktop environment**. In addition to a VPN, this allows for greater protection of work-related data and reduces exposure to threats associated with remote working (such as compromised Wi-Fi connections).

PROTECTION FOR DEVICES

With a move to remote and hybrid working, device security is growing in importance.

The very act of transporting a laptop to work and from every day constitutes a data risk for businesses. So the use of passwords and encryption to secure PCs is common. But what about smaller devices? Most organisations would struggle to tell you how many mobile devices are accessing their systems, and how many of those have protection. Yet in many ways they pose the greatest risk.

Since 2007, a staggering 98 million mobile phones have been lost in the UK alone. And there's no knowing how many of those devices had access to systems (such as email) or company data (CRMs, SharePoint etc.).

Remote and mobile device management (MDM) is, therefore, highly important if you're managing a dispersed team. An MDM solution will give an organisation control over the usage of that device. That can extend to ensuring anti-virus is always up to date, that the device has to be protected by a passcode, or restricting the applications that can be downloaded onto the device.

An MDM solution will also allow organisations to wipe data from devices remotely. So if a device is lost or stolen, all company information can be removed.

There are a few extra steps you can take to protect from device-related cyberattacks:

1. **Use multi-factor authentication (MFA) across all devices**. This adds an extra line of defence on top of passwords (which are often weak). MFA usually takes the form of text messages or push notifications asking users to confirm their identities.

2. **Provide employees with webcam covers**. Cybercriminals have become increasingly adept at accessing user webcams thanks to the rise of remote conference calls. Once a webcam has been hacked, criminals may be able to view sensitive files or record key logging of passwords.

3. **Ask staff members to avoid sharing their work devices with family or friends.** This reduces the risk of accidental, harmful downloads.

PROTECTING AGAINST RANSOMWARE

One of the major resurgences in cyberthreats is ransomware, with 29% of UK businesses targeted in the first half of 2021[ii].

Ransomware is a form of malicious software that encrypts then prevents victims from accessing their valuable files and documents until a ransom is paid. Most cyber criminals who deploy this technique threaten to delete or share the files with others unless the money is paid within a certain timeframe.

Should an organisation become victim to such attacks, business owners are often tempted to pay the criminals to try to avoid the disruption and reputational damage. However, it is advisable not to pay: files are generally difficult to decrypt and there is no guarantee that your files will be returned.

Despite the threat, many organisations seem reluctant to invest in specific ransomware defences. This is somewhat surprising given not only the prevalence of attacks but also the costs: the average SME IT security incident costs £8,460[ii] which typically includes several days of business interruption.

The best way to avoid losing precious data is to protect your systems against infection and malicious activity ahead of time. Here are a few key steps to take:

Install anti-virus software with specific anti-ransomware protection. While most credible programmes catch threats before they're downloaded, anti-ransomware detects and stops the rapid file encryption that's a hallmark of ransomware.

Back up all of an organisation's files to a cloud resource. Simply backing up files locally is not enough - we've known ransomware attacks consume backups held on in-house servers. Keeping backups separate from in-house systems ensures data is secure and ready to be reloaded if you're victim to a ransomware attack.

Educate staff members about cybersecurity attacks, how to spot threats and best practice to protect IT systems.

GET A HANDLE ON PHISHING

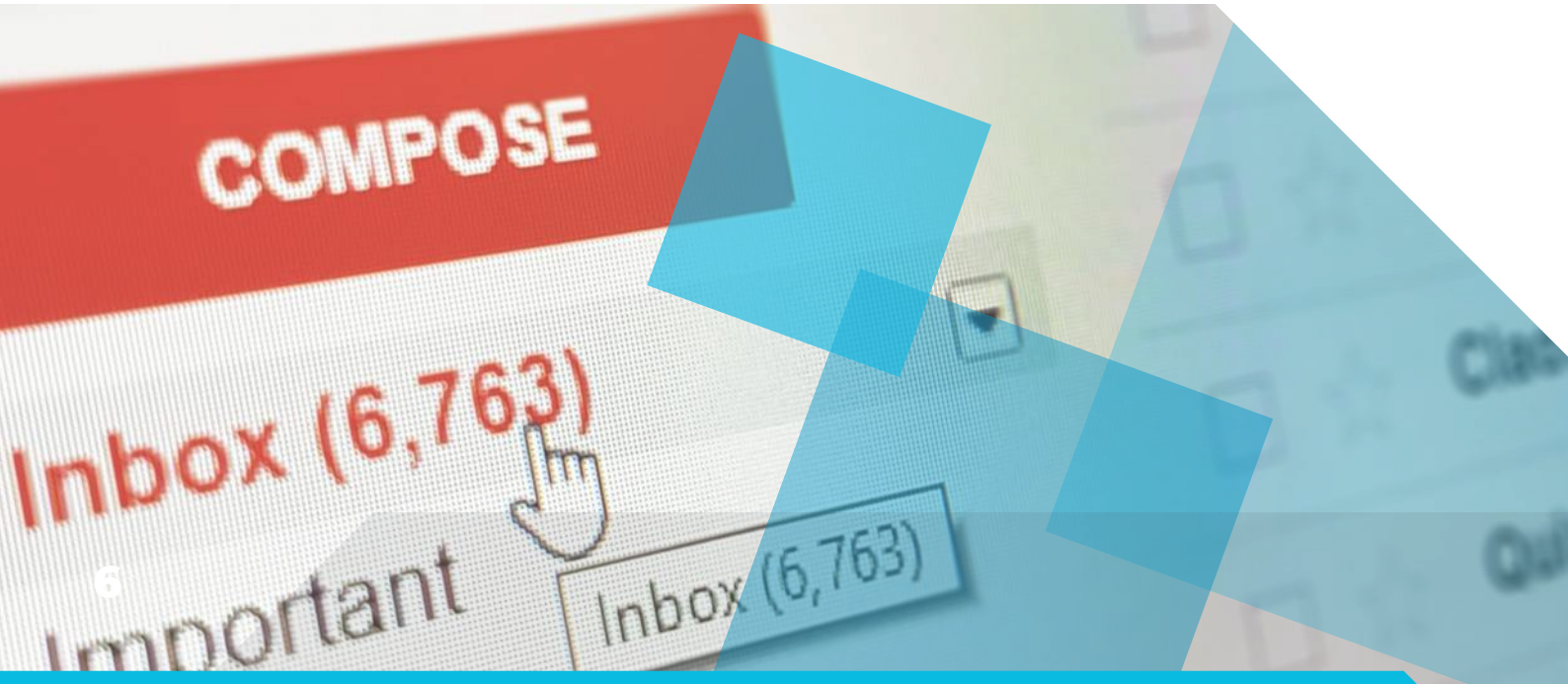
Like ransomware, there has been a rise in phishing attacks recently. Unfortunately, it's become a more successful tactic as a result of remote working, as users seem less likely to question what they're receiving.

Phishing is a very common form of cyberattack that works by luring users into handing over sensitive information such as their username, passwords, address details, or even bank account information.

Cyber criminals typically pull off this stunt by sending fraudulent emails claiming to be from an important organisation (such as a bank or delivery firm). The messages are often marked as urgent and demand that recipients pay a fee, download content, click a link, or hand over personal information to avoid negative consequences.

However, there is also a rise in fake supplier invoices. Cyber criminals clone an organisations quote or invoice documents, add their own details, then send a fake invoice to the organisation's customers.

Unfortunately, it is very difficult for businesses to avoid phishing emails, with 75% of organisations worldwide reporting phishing attacks in 2020[iii].



TEN TIPS TO AVOID BEING 'PHISHED'

1. **Approach emails labelled "urgent" with caution.**
2. **Remember to check email addresses** - scam emails often come from addresses that do not correspond to the sender's name or suspect domain names (eg. Barclaysbanking.net rather than Barclays.co.uk). Be wary of attachments and only open files you expect to receive.
3. **Be wary of attachments and only open files you expect to receive** - Organisations should have an attachment scanner as part of their anti-virus.
4. **Be suspicious of emails full of spelling and grammar error** - Legitimate companies tend to proofread their communications thoroughly. Oddly phrased greeting lines are another indicator.
5. **Avoid clicking links straightaway** - Links could trigger automatic malware download. Hover your mouse over the link and your email client will show you where that link is pointing to. Only click if it's a location you trust.
6. **Remember that even legitimate email addresses can be hacked** (known as business email compromise). So, use common sense before responding to an email, even if you think you know who sent it.
7. **Never hand over private or sensitive information via email.**
8. **Verify any request for a changes in payment details in person or by phone** – and don't necessarily trust the phone number given on the email!
9. **Approach sales enquiries with caution** – an easy quote could be an attempt to get your quote/invoice stationary.
10. **Remember that phishing is not just conducted via email.** Smishing (SMS phishing) and fraudulent messages on chat systems such as Slack are becoming increasingly common.

INTERNAL THREATS

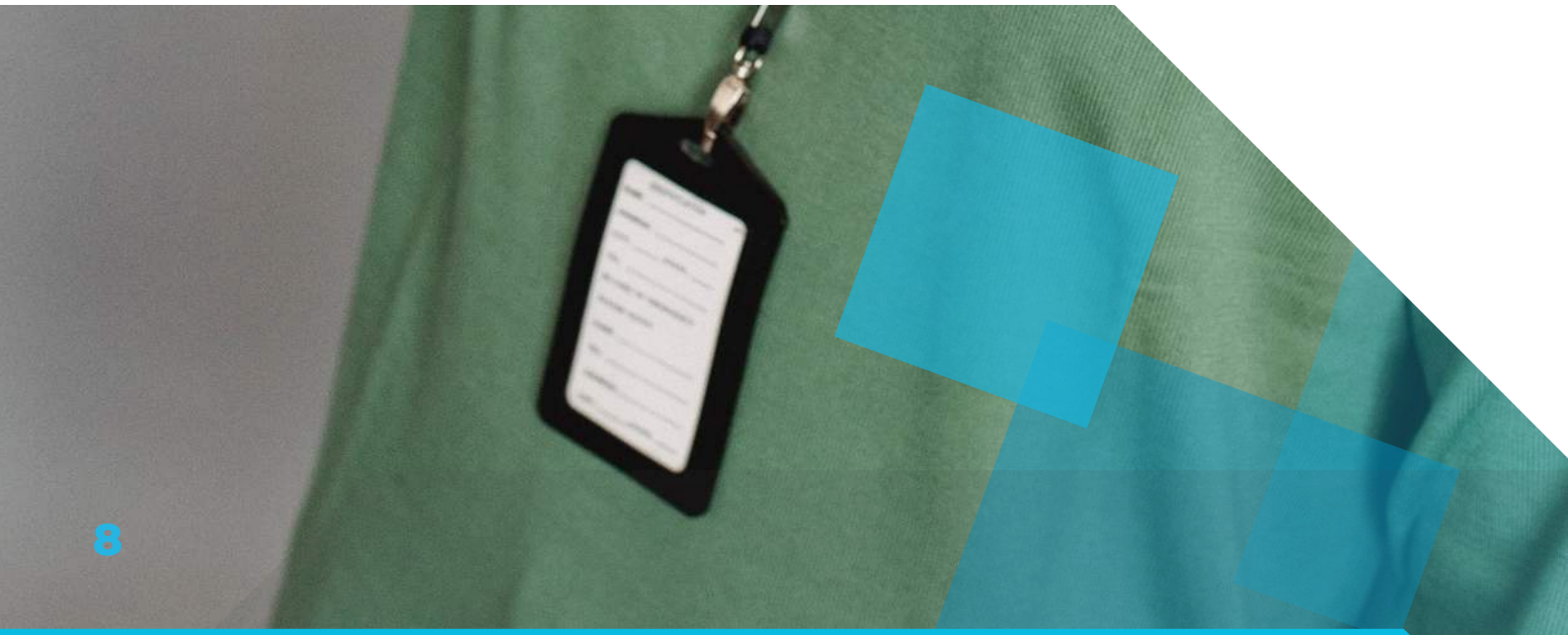
We all try to think the best of people. But in terms of IT security, this can result in organisations overlooking the risk from within.

Insider attacks come in a variety of formats but break down into three broad areas

Negligent Insiders
The most common form of threat, this is an individual who has not absorbed security training, doesn't follow IT security processes and leaves systems exposed as a result. Unfortunately, negligent insiders can exist at all levels of an organisation. And if they're in management with access to more advanced systems, this can increase the danger.

Compromised Insiders
A user whose account has been hacked or accessed in an unauthorised way. This can be linked to negligence (easily hacked passwords, careless link clicking etc.) or just pure bad luck. If an organisation is lucky, cybercriminals will act in a way that clearly demonstrates an account is compromised. But in the case of whaling (highly-tactical phishing directed at high-value individuals) activity can be difficult to detect.

Malicious Insiders
Some attacks or data breaches are simply product of malevolence. Commonly these will be users whose contracts are being terminated or are ending soon, but other less obvious individuals may also commit actions either as part of collaboration, coercion or avarice (eg. stealing your data to sell).



STEPS TO PROTECT FROM INTERNAL THREATS

Here's are few steps you can take to help protect against most forms of insider attacks:

1. Have a comprehensive security policy that covers use of IT systems and data. You should include information about handling customers' personal information, incorporating issues surrounding GDPR and other vital legislation.

2. Secure important hardware by storing it behind locked doors. This prevents interference or damage.

3. Only give your users access to the data and programs they need to complete their jobs. Have all users' access documented (a User Access Matrix is useful), so that should a user leave your organisation you know exactly what access needs to be removed.

4. Deploy software to monitor employee activity. This should look not only for misuse (access to harmful websites etc.) but also look at odd patterns of access (such as time and geography) that may indicate an account has been compromised.

5. Limit data transfer options. Remove the ability for general users to perform large data downloads from applications such as CRM systems, and stop the copying or deletion of files in bulk. Prevent data leaving your organisation by disabling USB storage devices and access to online file transfer sites. And set up email security measures that automatically scan and quarantine emails that contain sensitive data (until approval can be sought).

USER EDUCATION

Educating your users and ensuring they're aware of the tactics cybercriminals use, is one of the most important steps your organisation can take to defend against attacks.

Defence Against Phishing
As detailed on page 7, there are a number of ways you can avoid being 'phished'.

Phishers use information that they find about you online to make their emails more convincing. That's why ensuring your users are mindful about what they post publicly online is so important. Anyone can be tricked into thinking a malicious e-mail is genuine so cyber awareness is essential.

Password Security
Perhaps the most basic part of security is also one of the most essential. Users should be encouraged to practice good password security, for example:

1. **Passwords shouldn't be shared across different accounts**
2. **Using three random words** - and thinking of your password as a pass-phrase - is better than using predictable passwords like dates of birth or names of your pet or children.
3. **Passwords should be just one step of accessing an account.** Multi-factor authentication should be activated wherever available.

Introducing Thinking Space
One of the most effective ways of stopping a cyberattack is to stop and think. When you receive an email, stop and consider if it is genuine and from a legitimate source. When you receive a pop-up ad, stop and think if you should click it. Likewise with web browsing; stop and check if the website is secured by an SSL certificate before inputting data.

90% of data breaches in the UK are due to human error.[iv]

IMPROVING IT SECURITY WITHIN YOUR ORGANISATION

With this guide we've aimed to cover just some of the IT security tasks that an organisation should be undertaking.

Managing them all is a herculean task, particularly if you don't have an internal IT resource.

Akita can provide a holistic approach to an organisation's security, covering every aspect from system protection to guidance on IT policies as part of a managed IT support service. But we can also provide ad hoc IT security services.

If IT security is on your organisation's agenda (and it should be), an IT security audit is the best place to start. This will not only help assess the success of current security measures, but also identify additional protection required in line with your organisation's risk profile.

To discuss an IT security audit or other security services, please get in touch.

i https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975732/20-046099-01_CSBS_2021_micro_and_small_trends_infographic_310321.pdf
ii https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021
iii https://www.tessian.com/blog/phishing-statistics-2020/
iv https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/

AKITA
The IT People

info@akita.co.uk | www.akita.co.uk | 0330 058 8000

Head Office:
Unit 15 Nepicar Park,
London Road, Wrotham,
Kent, TN15 7AF