Beaming

CYBER SECURITY FOR ACCOUNTANTS

Practical steps for securing business-critical data

Introduction

Accountancy firms are at high risk of becoming victim of cybercrime because they are often trusted with the kind of information that's valuable to cyber criminals.

Things like financial data, personnel details for payroll and bank account information can all be used to commit fraud or theft. And because clients need to trust their accountant, extortion through ransomware can be a successful route for cyber criminals, because accountants may be more likely than others to pay a ransom to stop the reputational damage caused by sensitive data being exposed or lost.

We've created this guide to give accountants practical steps to take that will make their systems more secure against cyber attacks. We've divided it into two sections, one which describes the best practice measures that can easily be adopted by all members of staff in an accountancy firm (and by accountants that work alone, too), and a second that recommends the technology and procedures that should be put in place by partners or IT teams.

Contents

ADVICE FOR ACCOUNTANTS

Our easy-to-follow guidance helps accountants play their part in protecting data and networks.

>

Seven simple ways to improve cyber security

Everyone can play their part in keeping the company network safe, and in fact it's often people that are targeted as an entry route to the network. These easy-to-follow tips will help you feel confident in your ability to prevent cyber attacks.

*** PASSWORDS

Your log in credentials give access to company systems, your own private data and confidential client data, so they must not be easy to guess. Bear in mind that the "guesser" here is not human – you're up against sophisticated computers with databases full of common and previously breached passwords. **Ensure passwords are unique, long and strong by following our guidance >**

MULTI FACTOR AUTHENTICATION

Try to enable multi-factor authentication (MFA) on any accounts that make this possible. This means that even if your password is breached, an attacker couldn't gain access to your account without meeting at least one other requirement such as entering a PIN sent to your mobile, details from memorable information you've provided, or even biometric data such as your thumbprint.

BEWARE PHISHING

Phishing emails can be used to trick you into installing malware on your computer (and in turn, the whole network) or sharing sensitive data, usually by clicking a link or downloading an attachment. These attacks have become increasingly sophisticated and while many take a "scattergun" approach by sending out mass emails to try and hook your attention, others may be extremely targeted to you and the organisation you work for. **Here's more advice on spotting & dealing with phishing attacks >**

USB USE

Your company may restrict your use of USB memory sticks, but if you do use them, be very wary of plugging anything in to a USB port unless you know exactly where it's come from. Instead of storing sensitive data on portable memory devices, which are easily lost, try to use secure cloud storage or even better, when you need to access network files from a remote location, use a VPN.

PHYSICAL SECURITY

Don't forget physical security – a cyber attack could be initiated by someone with unauthorised physical access to a computer on the network, so be wary of allowing access to your computer unless they're a recognised member of the IT team. If you work using a laptop or tablet in a public place, consider using a privacy screen to ensure no prying eyes can see confidential information over your shoulder.

PROTECT MOBILE DEVICES

Protect laptops and tablets with automatic screen locks and multi-factor authentication, and activate remote data wiping so that if it were to be lost or stolen, others would not be able to access data or the network.

RUN UPDATES

It can be annoying to run updates when you have work to get on with, but operating system and software updates often fix bugs you're unaware of which could otherwise be exploited. Allow updates to run as soon as they become available.

Good password practice

Your password is the key to a wealth of data on your school systems, from confidential emails to customers' sensitive financial data. If it's easy to guess or you re-use the same password (or even the same one with slight variations each time), cyber criminals may already have it in a database and could use it in an automated attack to gain access to the network.

How to choose a strong password & keep it safe

1. Avoid easy to guess passwords (birthdates, sports teams, pets name etc).
2. Use a combination of 3 random words to make a strong but memorable password.
3. Use completely different passwords for work and personal accounts.
4. Ideally, you'd have a separate password for every log in, but at the very least ensure that you keep your most important accounts (access to student records, your email) secure with a totally unique password.
5. Don't share your passwords with anyone.
6. Use multi-factor authentication for added security where available.
7. Consider using a password manager, which makes it easier to create & use unique passwords without having to remember them all.

Focus on phishing

We've seen some clever, and very targeted phishing emails sent to accountancy firms. Phishing emails use psychological tactics to trick the recipient into carrying out an action such as sharing personal or financial information, or downloading malware. The problem may not be immediately obvious, for example you may receive a (fake) request to reset your password and be taken to a website designed to capture your information. Those details will later be used to orchestrate an attack. Otherwise, you may be persuaded to download an attachment, which when opened allows ransomware to take over your computer and in turn the network.
Email users should follow these steps to help prevent becoming a victim:

1. Always check the email addresses
Look for deliberate mis-spellings in the email address designed to trick the eye or nonsense addresses full of random characters. When you reply, check where your email is being sent to as scammers can redirect your messages, giving them the opportunity to continue a conversation without raising alarm.

2. Look at how the email is written
Some phishing emails contain poor grammar and spelling that would not pass the proof-reading or normal written style of the legitimate sender or organisation. That said, not everyone uses perfect grammar, particularly not busy business owners that need to fire off a quick email to their accountant, so this isn't a fool-proof way to distinguish a scam.

3. Don't automatically click
Be wary about clicking links or opening attachments in emails you hadn't expected, even if you (think you) know the sender. Store internal documents in a shared location instead of sending them to colleagues via email. When unsure, contact the sender via another means to validate their intent.

4. Use shift+delete
Delete suspicious emails straight away. Use shift+delete to make sure the email bypasses your recycling bin and is permanently deleted.

5. Be extra cautious on mobile devices
It may differ slightly from device to device, so make sure you know how to view the full email address of senders and how to check the full URL of any link you're directed to.

6. Don't overshare
As someone that works in education, your social media accounts are most likely private already. Be careful to remove any "friends" or "followers" you aren't certain you know in real life. Giving away personal information will make it much easier to scam you.

7. Being pressured should ring alarm bells
Think twice, especially if you are requested to carry out an action or share sensitive information. If you receive an email that asks you to click a link, download a file, share confidential information or divulge financial details, think before you act, especially if there's a sense of urgency.

8. Don't be scared to double check
If a request seems odd then always follow up verbally. You're demonstrating your commitment to data security so no one should be offended!

Working from home

Accountants often work late from home or log in to their company network from clients' business premises. Follow our guidance to keep data secure as you work remotely.

Stay up to date

Ensure that all of the software you are using when working from home is up-to-date. Use the latest version of your browser software and up-to-date antivirus that is actively blocking threats.

Please note that Windows 7 is now 'end of life', meaning Microsoft no longer offers patches and security updates. Some PC's running Windows 7 can still be upgraded for free to Windows 10.

Don't allow device sharing

Don't share access to work devices with family members.

All of the excellent work you've done to protect your school from the risks of cyber attacks can be undone in an instant if someone you live with accidentally downloads key-logging software or some other form of malware.

Secure data in motion with a VPN

You should be provided with a VPN or Virtual Private Network, which encrypts Internet traffic and makes the flow of data more secure.

This is the way to access documents containing confidential data – don't remove them from the school's systems.

Update your router & password

Secure your home broadband router. As well as ensuring that the firmware is up-to-date, change the default WiFi password within the router settings to something longer and more secure.

This will disconnect old devices (which is a reasonable security precaution in any case) and ensure new devices are accessing the network more securely.

IT TEAMS AND PARTNERS

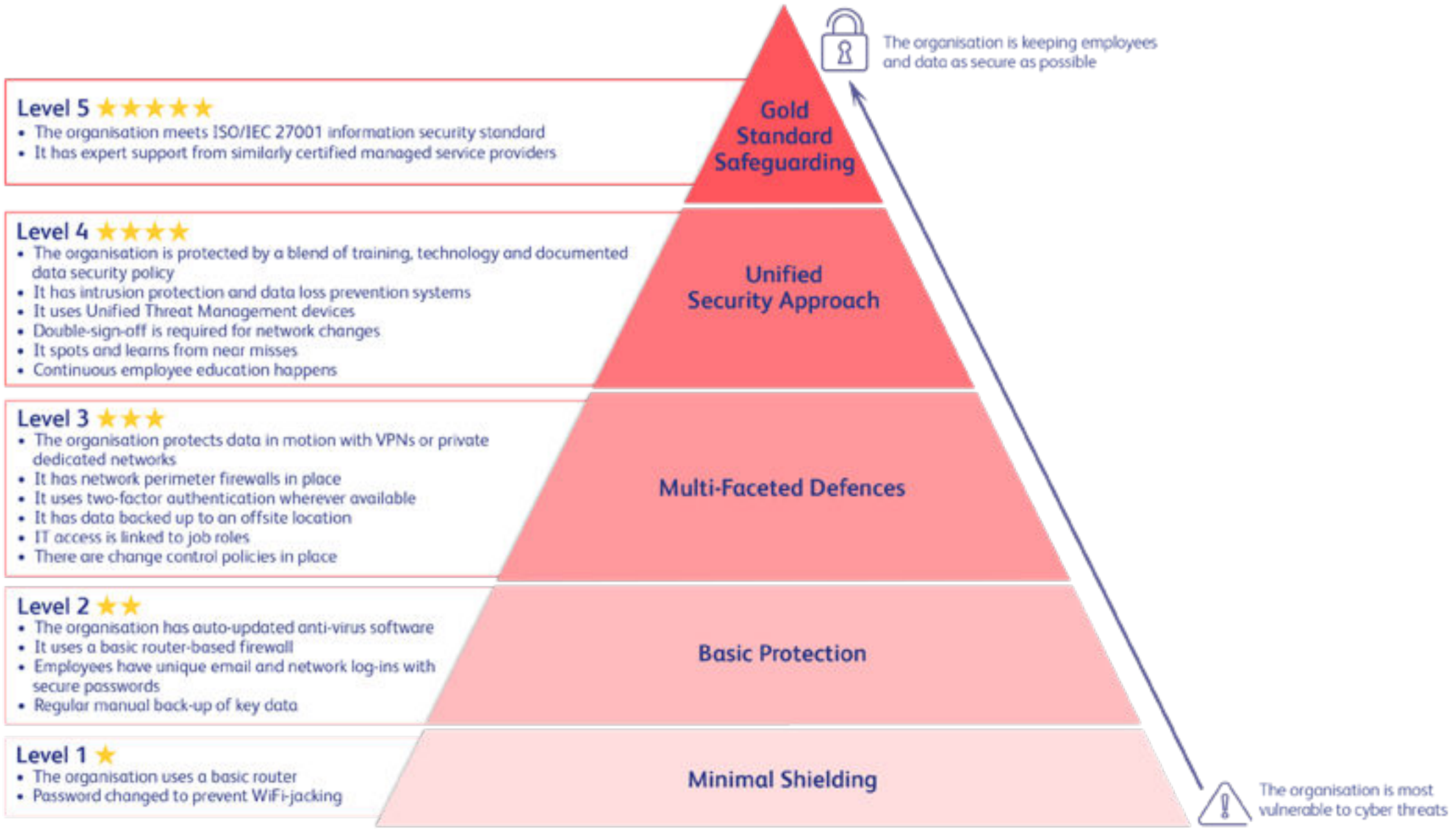
Technology and procedures that should be put in place by partners or IT teams

Evaluate your level of cyber security

Your people can't be the first and last lines of defence; Following the guidance outlined so far is a great way to strengthen your accountancy firm's defences against cyber attacks but you'll also need to have in place the right technology to protect your company network and data.

That's why we have developed the Hierarchy of Cyber Security Needs, which allows you to assess how well you are doing with cyber security and data-protection, based on the technologies and processes you are currently using, and shows a clear path to improving your defences.

We recommend that all small and medium sized businesses should achieve at least level three on the hierarchy, but as an accountancy firm you're a well-known target for cyber attacks and have access to a lot of sensitive data, so we'd advise that when you've reached level three, you don't stop there and strive to reach level four or five.



Secure data backups

Backing up data in itself won't protect you from falling foul of a cyber attack, but having in place thorough data backups that are stored securely away from your core network will be instrumental in helping you recover quickly should you suffer an attack.
Having to restore from backups is inconvenient, but it's nothing compared to the expense and stress of either paying up in a ransomware attack or trying to reverse the damage done when your data has been encrypted or destroyed.

When you're deciding a backup strategy, these are the five key points to consider.

1

Think 3,2,1

Keep three copies of any data that's integral to your ability to operate, using two different systems, one of which is offline. This may mean using a combination of backing up to an external hard drive and removing it from the premises, backing up to a server in a colocation facility, using a private cloud or a or a public cloud service.

2

Consider cloud

Backing up to the cloud is a convenient option for small businesses and means data can be accessed quickly from almost anywhere, but do your due diligence to make sure you know where data is held and that it is secure.

3

Or colocate

An alternative to cloud data storage is the use of remote company data centres and colocation facilities, which allow companies to backup their data remotely and in real time to their own dedicated servers.

4

Do you actually need to back it up?

Whichever means of backup a company uses, they must first consider which data is worth duplicating. That means making multiple copies of the important data your business needs to function; it probably doesn't mean incurring the extra cost associated with backing up employees' personal photographs and iTunes libraries.

5

Don't forget data in transit

Consider how your data travels between the business and its backup location. You'll need connectivity that's secure, reliable and resilient.

The cyber security measures you need to know about

We bust some jargon to help you get to grips with the key terms you need to be aware of when it comes to cyber security.

Anti-virus software: Also known as anti-malware, this is a computer programme used to prevent, detect, and remove malware. Keep up to date: Cyber-crime evolves fast. Heed the advice and install updates from your software and IT platform providers.

Bots: Bots are used on the internet to automate simple, repetitive tasks at high speed. When programmed maliciously, they can be used to carry out denial of service attacks or log keystrokes and gather passwords.

Clearing up after leavers: Don't leave old email accounts and access routes to the network dormant. Delete them to eliminate a potential source of vulnerability.

Cyber insurance: An insurance policy that covers financial losses if you're the victim of a cyber-attack or data breach.

Cybersecurity policy: A documented set of procedures stating what your business will do to protect itself and employee responsibilities. Make sure you have appropriate policies and procedures for data security and access control. Make sure they are regularly updated and communicated to all members staff, including the Board.

Data back-up: Making copies of business data that can be accessed if the original source is corrupted or stolen. While this can be done manually using storage devices, or automatically to a public cloud provider such as Google or Amazon, it is safest to mirror your systems and data to your own dedicated servers located in a data centre or a colocation facility.

Data breach: When people who should not see secure or sensitive information gain access to it. The data might be financial, confidential or contain trade secrets.

Denial-of-service attack: An attack that stops businesses using a vital IT resource, or which prevents customers from connecting with you.

Employee education: A policy is useless if it doesn't become part of your practice. Provide a simple guide and set of procedures for staff, and train them in simple cybersecurity.

Intrusion detection/prevention system: A device or software that detects anomalies to catch hackers before they do real damage to your network.

ISO/IEC 27001: Top level information security standard requiring organisations to adopt overarching management processes to ensure controls continue to meet the security needs on an on-going basis. Organisations must examine cyber risks systematically, and implement comprehensive controls to address risks deemed unacceptable.

Least-privilege policy: This means making sure each employee has the lowest level of user rights required to do his or her job. This minimises the number of potential sources of vulnerability and the impact of successful attacks.

Malware: Software designed to infiltrate and then disrupt or damage a computer system. Viruses, worms, spyware and Trojans are all malware. Almost always disguised as something innocent-looking.

Manual back-up: Backing up is making a copy of your data somewhere you can get to it if your original data is corrupted or stolen. Manual back-up means someone has to take on the job of backing up and make the copies themselves.

Multiple eyes on the prize: Don't rely on one person for firewall configuration, software updates and access control. If you have only one IT person, use another company's support. Make sure significant IT changes have two experts checking them for security before completion. Work with ISO27001 certified suppliers wherever possible.

Network-perimeter firewall: The first line of defence against external attacks, unwanted traffic and dangerous content. This is a secure boundary limiting network access to trusted data and sources only, and stopping outgoing traffic from accessing potentially harmful networks and hosts.

Phishing: Attackers send fraudulent emails that look like they are from a reputable company to dupe victims into granting access to malware or divulging sensitive information such as usernames, passwords and credit-card details.

Proactive vulnerability scanning: Software used to identify weaknesses in a computer network. This allows network security to be improved ahead of any potential cyber-attacks.

Ransomware: Malware that blocks access to data on your computer or network, often by encrypting access to it, and demands payment for access.

Record near-misses: Have processes in place for documenting and analysing near-misses for data breaches and use this as the basis continuous improvement.

Router-based firewall: A firewall built into the router you use to connect to the internet, providing a barrier between your internal systems and untrusted external networks.

Trojans: Just like the mythical Trojan Horse, Trojans mislead IT users about their intentions. They are programmes that look innocent but are dangerous. Ransomware attacks often rely on Trojans to infect a victim's computer.

Two-factor authentication: Two-factor or multi-factor authentication is the practice of asking a user for two or more pieces of identity information. An employee might, for example, have to use a password and an approved device, to gain access to a system.

Unified threat management: A cybersecurity tactic which employs a single hardware or software installation to do several security jobs. This holistic approach simplifies installation, configuration and maintenance.

Unique email and network log-ins: Don't share log-ins. Make sure all your passwords are strong, only used by one user, and that employees are not using their company passwords anywhere else.

Virtual Private Networks: A Virtual Private Network or VPN is a secure connection linking users in different locations. The VPN encrypts the data, meaning anyone who intercepts it will not be able to read it.

Web-application firewall: Many businesses now depend heavily on web-based applications such as Microsoft 365. A Web Application Firewall helps protect web applications from attack and corruption by monitoring traffic between a web application and the Internet.

About Beaming - www.beaming.co.uk

If you want support with keeping your accountancy firm safe, call Beaming. We are an Internet Service Provider (ISP) that works with organisations of all shapes and sizes, and unlike most providers, we own our network, which has been built for top-quality performance. We supply thousands of businesses across the UK with fast, reliable, and secure voice and data connectivity and managed services.

Cyber security is at the forefront of everything we do, and we are ISO27001 certified - the gold standard in data safeguarding. We can help you increase your resilience to cyber-attacks.

Our teams are handpicked, not only for their great technical capabilities but their great people skills too. Our customers never end up talking to robotic sounding call centre operations.

Follow Beaming **online** and on **Twitter** to get regular updates on cyber threat analysis and new cyber security insights.

How to get in touch

Speak to our experts:
Call 0800 082 2868
Or email hello@beaming.co.uk
Or visit www.beaming.co.uk

Certificate Number 9849
ISO 9001, ISO 27001