The Nature of Cyber Crime

Part 2 How to secure your business against a cyber attack.

www.complete-it.co.uk | info@complete-it.co.uk

Complete I.T.

Part 2 of 2. This report will look at the unique challenges SMEs face today and how to prepare for a cyber security attack.

90% of businesses back up their data, but only 41% do it daily.

The Challenges

SMEs today are facing a unique set of challenges when it comes to cyber security. Although infiltrating large corporations is far more lucrative for a cyber criminal, SMEs are increasingly being targeted because of their weaker defenses, limited resource and lack of knowledge.

Historically SMEs have been fairly relaxed when it comes to cyber security, however with the increasing rise of high profile cyber attacks, small business owners are beginning to take note of the evolution of threats and research highlights that SMEs are more afraid of cyber crime than Brexit (Bonhill Group Plc, 2020).

Internal challenges

With high level cyber security management positions estimated to earn an average salary of £70,000 (Prospects, 2020), a huge chunk of any SMEs resource.

Coupled with this, technical professionals will be sure to face some internal conflict when it comes to cyber security resource.

Many decision makers will view investment in cyber security as an insurance policy and struggle to see its worth until it is too late. This internal conflict can be hard to resolve without your business itself becoming the victim of a cyber attack.

Data and GDPR

Under the GDPR, if your business suffers a data breach you could face a fine of up to £10 million, or 2% of your annual turnover, enough to put most SMEs out of business instantly.

However despite the surge in cyber security awareness since the introduction of the new regulation, research by Acronis found that although 90% of businesses do back up their data, only 41% do it daily, which leaves valuable gaps in the data that is available to be recovered.

With 42% of organisations suffering data loss resulting in downtime in 2019, it emphasises the need to back up your data on a regular basis in order to limit business downtime in the event of a cyber attack.

Educating Employees

While SMEs are beginning to make significant investments in technology to defend against threats, they often miss the biggest cyber security threat; their own teams.

Employees are your biggest asset but can also be your biggest downfall. If you do not take the right steps to help educate your team on cyber threats the chances that you fall victim to a phishing attack or click on malicious links and attachments is high.

We stated in part one that 90% of data breaches are down to human error, this can be rectified by implementing regular training and knowledge sharing with your teams.

Within the UK it is stated that 63% of small businesses and 46% of medium sized businesses have not provided cyber security training to their team (Statista, 2019).

Bring your own device (BYOD)

More often than not, employees choose to use their own technology to assist with their daily tasks both inside and outside of working hours.

Although this may help with productivity, what often gets overlooked is how employees own devices create weaknesses in your cyber security and data protection plans.

BYOD gives your businesses data a clear path outside of the organisation, should your team's devices get lost or stolen. With this in mind, organisations need to rethink their IT policy to not only continue to maintain and encourage a use of technology that can assist in productivity, but also one that does not compromise on security risks.

With teams working remotely your security defences may well suffer. Threats such as Man in the Middle attacks can be prevalent when your teams use public networks outside of the office, and so relevant training and the use of VPN connections needs to be encouraged.

63% of small and 46% of medium sized businesses have not provided training.

cit Complete I.T.

No Magic Solution

There is a misconception that cyber security and security defences fall under IT, when in reality it is an issue faced by every department. Cyber criminals use whatever means are available to them to attempt to penetrate your business defences, whether that's via the phone, phishing, ransomware or password attacks, therefore your defences should reflect this structure.

There is not one solution that can tell you whether an email is a phishing attack, whether an attachment is riddled with ransomware, whether your password is no longer secure. To fully protect your business from the threats, it is essential that you implement a multi-layered cyber security approach underpinned with user education.

How to reduce business downtime

Hackers evolving faster than technology

As discussed in part one, the strategies and attack methods that cyber criminals rely on are constantly evolving and becoming increasingly more intelligent.

This creates a cat and mouse cycle where IT teams are continuously trying to secure every possible entry point, but with the rate at which attack methods are evolving it is impossible to secure every known vulnerability before the next one arises.

Disaster Recovery at the core

Disaster recovery is no longer just about protecting your business from natural disasters, it is now about being able to bounce back after human error, natural disasters and malicious attacks.

It can be hard to plan for the unknown, but with the combination of natural disasters, cyber attacks, hardware failure and human error, it is a matter of when you might experience data loss, not if. Therefore, it is essential that you have a reliable Disaster Recovery plan in place to act as the foundation for your multi layered approach.

The cost of creating a disaster recovery plan might seem high initially, but when disaster strikes, this plan could be the difference between a bad day at work or putting your organisation out of business.

To create A Disaster Recovery Plan, follow our 6 steps.

Step 1: Management

As we discussed in section 1, there is often a discourse between IT or security professionals and top management. There is potential for them to see a disaster recovery plan as a wasted insurance policy for something that may never happen.

The reality is that at some point in time your business will lose data, whether through error, natural disaster or malicious activity. As your disaster recovery plan will draw on the whole business, you will need approval and commitment from your top management team to ensure your plan is as effective as it can be.

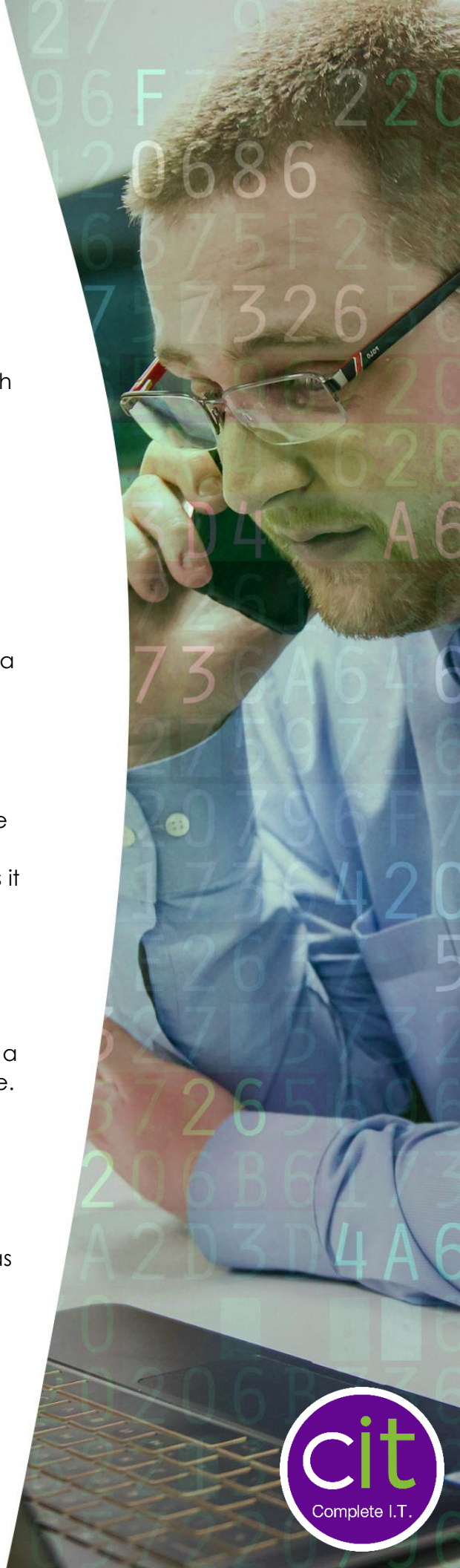
Step 2: Your Disaster Committee

In the run up to and after a disaster, you will need a solid team around you to lead the planning process. There is not one department in your business who are exempt from this – a cyber attack or hardware failure could come from anywhere. It is important that your disaster committee contains representatives from all areas of the business.

Step 3: A Risk Assessment

Your first actionable activity should be to perform a risk assessment. Throughout this process, you should identify areas of your business which present a larger risk than others.

Unfortunately, you won't be able to plan for every single threat so it is important to understand your high risk areas.



For example, high risk employees may be remote workers who rely on public networks, or those who work using their own device. High risk departments will be those who handle sensitive personal data, for example the finance teams or customer service department.

Step 4: Set Priorities

Now that you have identified your high risk areas, you can focus on your priorities and how to overcome certain issues should they arise.

Some areas will need to be restored urgently to prevent business downtime and a loss of revenue, and some will take longer to fix than others. These areas should be tackled first in the wake of an attack or data loss.

It is important to identify these high risk areas in order to prioritise and plan to limit business downtime.

Step 5: Data

Before you create a document outlining your plan, you need to collect data from each department. You will need to know things like key members of staff, insurance policies, power providers and inventories.

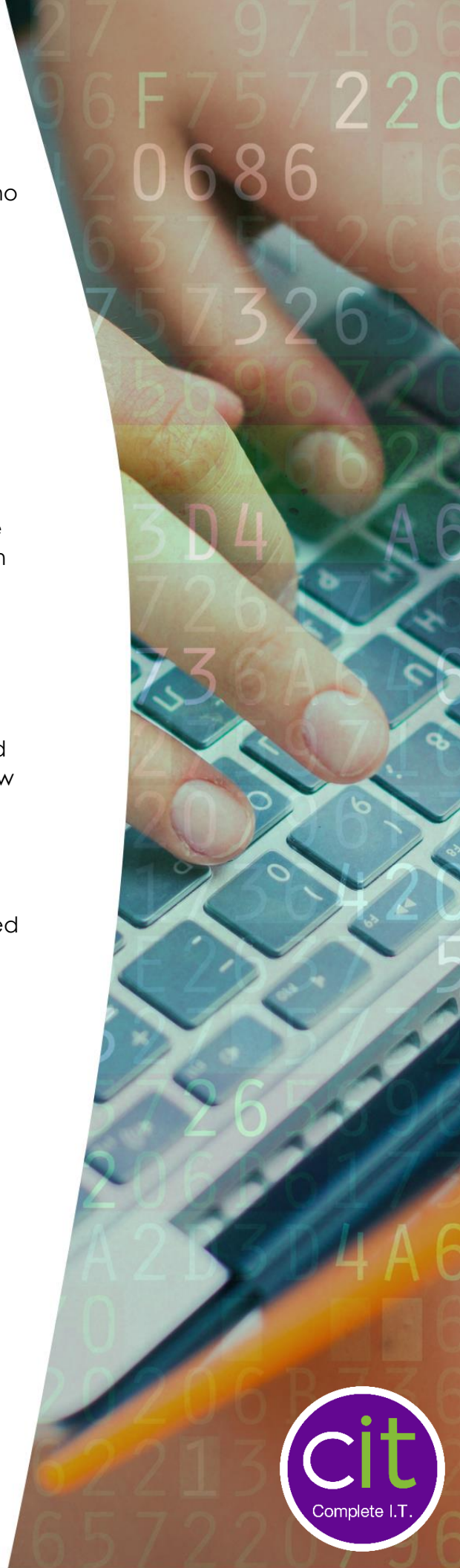
Step 6: Document and test

Now you have collected the above information, you will need to document a plan for each threat you have identified.

These should all follow a similar framework:

- Identify and address the source of the threat.
- How you will secure your premises or infrastructure.
- How you will assess whether you can continue to operate.
- How you will begin the process of recovering your data.

You will need to test this plan against certain criteria, for example an acceptable time frame of recovery or whether your business can recover at all. It is essential to perform this test so that you can address any grey areas as soon as possible.



Reliable Backup Solution

Underpinning your Disaster Recovery Plan should be a reliable backup solution. A common issue for SMEs when it comes to a backup solution is the reliability of traditional methods.

Onsite Backups

Onsite backups relate to the traditional method of storing a backup of your businesses data, usually on a tape or disk.

Once the primary method for data backup, tape-based backup is the practice of periodically copying data from the primary storage device to a tape cartridge, a manual activity.

In the event of a hard drive crash or failure, data can be recovered from the tape cartridges. While tapes do have some benefits of lower cost and minimal infrastructure changes, they can bring a huge risk to your business in terms of data loss.

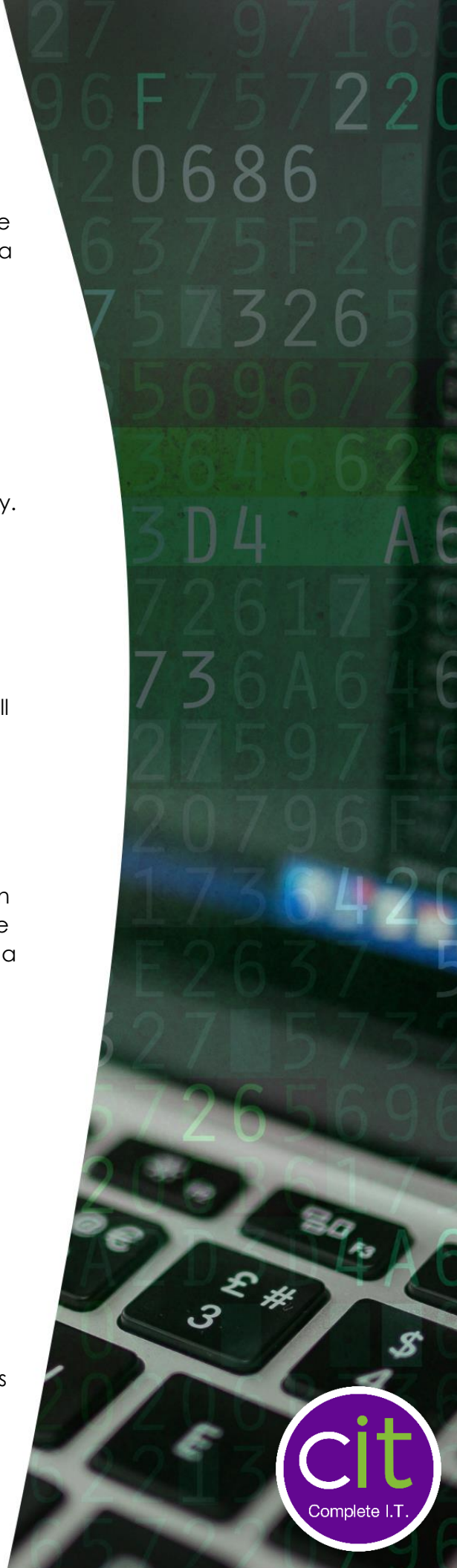
Take maintenance for example, any form of data backup will likely be stored for a long time. The thing with tapes is that they take a lot of maintenance in order for them to remain somewhat reliable over time and you will need controls in place to moderate humidity, sunlight and temperature to reduce any damage to the tapes.

On top of this, tapes have a known single point of failure. If on the same day your business is hit with ransomware and a pipe bursts and damages your tapes, you would find yourself with a set of encrypted files and no way of restoring your data – enough to put most SMEs out of business.

Cloud Backups

Now the primary method for data backup, a cloud based backup is the practice of sending a copy of data to an off-site server, normally hosted by a third-party service provider and is an automated process. In the event of ransomware or network failure, the data can be recovered straight from the cloud.

Cloud backup solutions are gaining popularity among SMEs for a number of reasons. The use of a cloud backup solution can be cost effective for businesses as they take advantage of existing infrastructure already in place. Once the backup is complete your businesses data will be stored at an offsite data center which can be restored to your local machine at any point.



A huge advantage here is that the backup process can be fully automated, taking place many times a day, to suit your business needs. Cloud backups also offer the best protection and reliability when compared with any other data backup and recovery service.

Since your backup is held offsite, in the event of a natural disaster or even an attack on your infrastructure or network, you can quickly recover your files to prevent major business downtime. You can even replicate your servers in the cloud to get you back up and running until the disaster has been resolved.

Password Policies and 2FA

Whether or not you still have a secure backup in place, this in no way protects you from a data breach or cyber attack.

Thinking of passwords as the key to your business – yes you would put the key in to unlock the front door, but the chances are that you will have a security alarm, extra bolts or maybe a security camera. If we protect our homes like this, we should also be protecting our businesses in the same way.

Your backup is the last step in this layer and is drawn upon should your other defences fail to protect you. Passwords are ultimately the key into your business. With it, attackers can access your businesses network and therefore confidential and personal data. Should this happen, you could be facing huge fines under the GDPR.

As we all become more and more dependent on a plethora of e-commerce and SaaS sites, it is not uncommon for some of us to have over 30+ passwords at any given point in time. If you think about those passwords for a second, at least one of them probably contains the year you were born, one contains the name of a family member or pet, and more than a few contain the trusty exclamation mark.

Not only that, it is likely that you use just one of those passwords across a range of sites. This may seem like an easy way to keep track of your small directory of passwords, but in reality, you are making it far too easy for potential hackers.

Your social media accounts probably make it relatively easy for anyone to find out the names of your family members, most definitely your pet's name and an idea of what you get up to in your spare time.

Enable 2FA on all accounts and logins.

Imagine what a hacker could find out while armed with a host of automated brute force programmes.

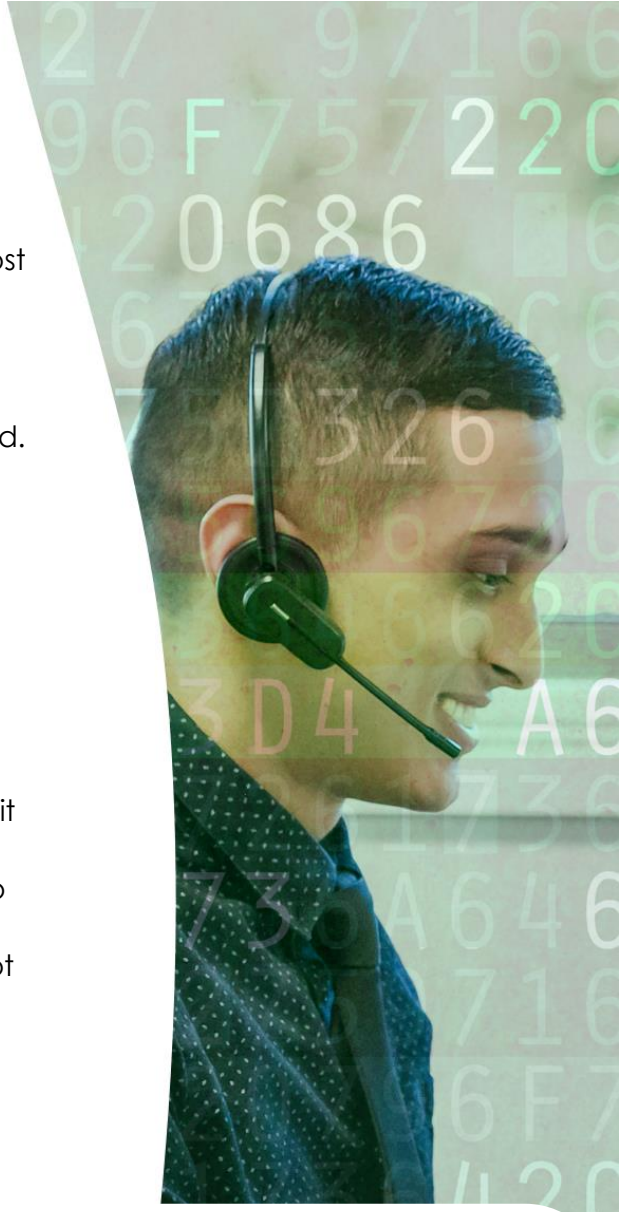
With a cyber criminals' host of automated brute force applications, it would be somewhat foolish to attempt to secure your devices and online accounts with just a password.

Now is the time to really promote the use of two-factor authentication (2FA) in adding an extra layer of protection and securing our devices and accounts.

In recent years, 2FA has become readily available to enable on most consumer websites, including banking, social media sites and your email accounts.

It takes just a few clicks for the end user to add two-factor authentication through account settings. With 2FA enabled, it does not matter whether an attacker has one of your user's passwords, without the authentication code that gets sent to your users phone each time they enter their password (or on different time frames based on your preferences) they will not be able to gain access to your system.

There is no need to rely on SMS either – there are a host of authenticator apps that can be used in place of a text. To remain secure in this new age of cyber security it is vital that you do not rely on passwords as your only line of defense.



People

Even the most secure IT infrastructure can feel the brunt of cybercrime. While attackers are getting increasingly more intelligent in their attack methods, the number of attacks due to end user error is continuing to rise.

The weakest link when it comes to cyber security, can often be your employees which is why empowering them with knowledge and training on a regular basis is one of the most important actions to take when trying to secure your business.

Empower your team with knowledge.

cit
Complete I.T.

Resources

Education is the key.

We have a host of information and resources for you and your team to utilise. Including:

- Cyber Security Resources
- GDPR Resources
- Microsoft Resources
- Complete I.T. Blog
- 60 Second Tech Videos

Phishing

Employees within your organisation should have clear guidelines on what to do if they are suspicious of an email.

It's important that they do take the time to inspect suspicious emails and do not take everything at face value.

- **Blog -**5 Ways To Spot A Phishing Email
- **Blog** - Phishing Emails: How Criminals Are Infiltrating Your Systems
- **60 Sec Tech –** Spam Emails: 4 Things to Look out For
- **Quiz** - Take the phishing quiz!

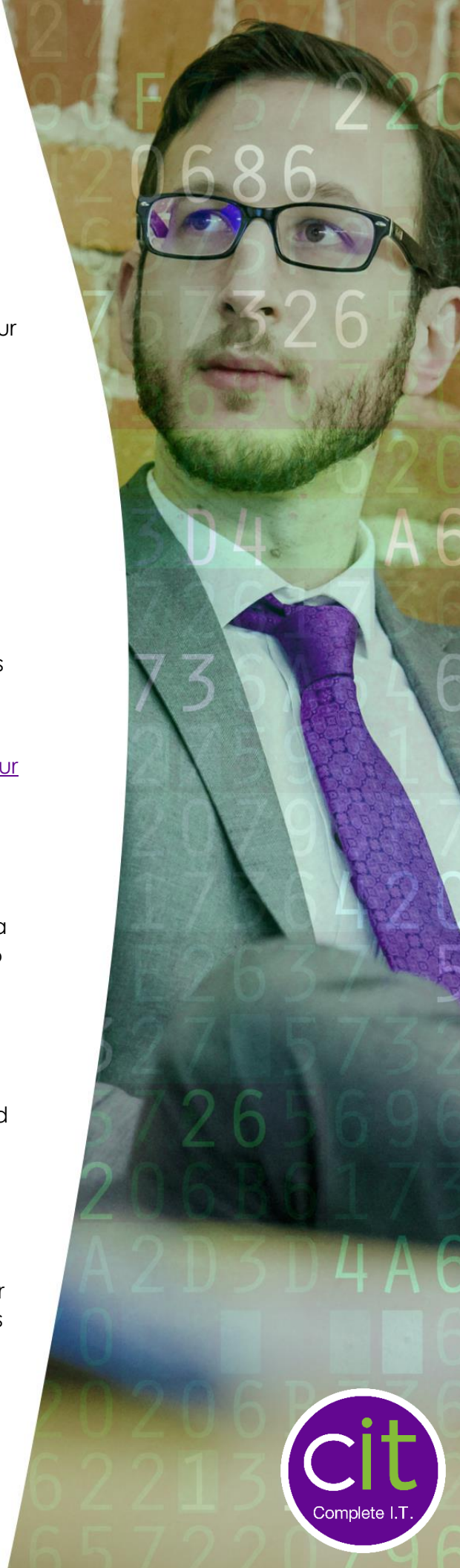
Ransomware

Ransomware can come in many forms. However, there are a number of tips that should be shared with your teams to help them determine whether an attachment or download is riddled with ransomware.

The list below presents popular file extensions that are employed to spread ransomware. Again, this is by no means an exhaustive list but encourages good practice by your end users: .EXE .DOCX .DOCM .TXT .HTA .JS .VBS .PY .BAT.

On top of encouraging your end users to check the types of file extensions they are clicking on, we also strongly advise ditching the use of USB sticks altogether.

While once a widely popular method of data transfer and/or storage, it has been increasingly more common for USB sticks to be used as a method for ransomware delivery.



Once plugged into your machine, if your USB drive is infected with ransomware it is only a matter of seconds before this infection spreads to the rest of your network. Ditching USB sticks gets rid of one clear path for attackers to enter your businesses network.

- **Blog** – Ransomware? What is it?

Passwords and Enabling 2FA

Letters numbers and a whole lot of nonsense is needed when creating a strong password.

Never use the generic "password" or replicate the same password over numerous accounts.

Enabling 2FA is also strongly recommended, in most cases all you will have to do is open settings and set up an alternative method of authentication, such as your mobile number.

- **Blog** - 5 Tips To Create A Strong Password
- **Blog** - What Is MFA and Why Do You Need It?
- **60 Sec Tec** - Why Are Password Managers Important?
- **60 Sec Tec** - What and Why Do We Need 2FA?

Thank you

At CIT we love taking technology problems off your hands, providing high level, flexible, IT support services at whatever level of support you need.

Our support not only enables your team to work more productivity, more collaboratively or smarter but we also give you peace of mind that your data is secure from cyber criminals and in the event of a disaster, we will be able to recover your data with cloud backups and enable you to bounce back with limited downtime.

We hope that you have enjoyed reading our two part ebook and if there are any aspects of this report which you would like some more guidance on, please do not hesitate to get in touch:

- www.complete-it.co.uk
- enquiries@complete-it.co.uk
- 01628 552 850