

# The Nature of Cyber Crime

## Part 1

Cyber threats faced by SMEs today, including the evolution of attacks, targeting and key threats.



Part 1 of 2. This report will offer an understanding of the cyber threats faced by SMEs today, including the evolution of attacks, targeting and key threats

# The Evolution of Attacks

**No one is safe**

Year after year the cyber crime landscape becomes more complex and cyber attacks are often described as “highly sophisticated”.

High profile incidents, such as EasyJet and Facebook data breaches illustrate the severity and scale of these attacks but many SMEs believe they will not be on the receiving side of these acts when in fact they are easier targets to phish, infect and defraud.

According to the [Cyber Security Breaches Survey 2020](#) cyber attacks have become more frequent, and 46% of businesses report having suffered a cyber security breach or attack in the last 12 months.

Things are worse for medium sized businesses where this number rises to 68% (Gov.uk, 2020).

Traditionally, businesses had a well-defined area that needed protection, that being on premise servers and workstations. Outside those 4 walls, the data did not need to be protected but due to the shift to digital along and with [46.6% of people in employment working from home](#) due to COVID-19 (Office for National Statistics, 2020) it is essential that data protection is taken seriously.

Businesses are starting to reap the benefits of remote working and have realised that a vast majority of roles can be successfully carried out remotely. Many businesses want to continue to offer flexible and remote working in order to

**68% of Medium  
Sized Businesses  
report having  
cyber security  
breaches or  
attacks.**





keep and attract top talent, for environmental reasons such as reducing pollution from travel and to reduce fixed costs by negating the need for highly priced rented office spaces.

Although flexible and remote working has many benefits, with valuable business data now stored in [the cloud](#) and the ability to access everything, anywhere at any time, it is important that you are considering how you can work safely and securely, as cyber threats evolve and adapt to this new way of working.

A multi-layered approach to securing your systems is always recommended and your [Cyber Security](#) should be at the top of your organisation's agenda. Taking all the necessary steps to secure your business and data should not be an intimidating process as there are a host of top of the range support and services that can help protect your business.

## The Nature of Threats

### Hackers evolving faster than technology

Cyber criminals are often described as highly sophisticated, due to the increasingly intelligent methods they are using to administer attacks, from social engineering, ransomware, and phishing.

Cast your mind back to the "Happy New Year 1999" virus that stormed computer screens with innocent imagery of fireworks exploding in the night sky, no malware or ransomware attached, just a video to celebrate the New Year.

How things have changed. Cyber crime has evolved into a status symbol and is now a sophisticated, profitable and fraudulent business where personal data or credentials are stolen and often sold on the dark web for large sums of money.



It has developed from an obvious scam that we could mostly avoid, to “spray and pray” strategies where thousands of people are sent the same email and the hackers pray they catch out as many people as possible.

To today, where smart social engineering attacks are executed after years of research to pull off attacks without anybody batting an eyelid.

With the number of attacks growing and when [90% of data breaches reported are due to user error](#), your multi layered cyber security approach must include user education as educating your teams is one of the key ways you can help keep your organisation safe.

## Targeting

### Social engineering is at the core

One of the main differences is that our lives are now online. Everything about us is online, whether that's online services such as banking and shopping, or social media.

Almost every attack method contains some form of social engineering, a technique fuelled by the wealth of information uploaded to the internet each day, more specifically through social media accounts.

Social engineering tactics allow the attackers to take advantage of human vulnerabilities like trust, habits, or emotions to lure victims into clicking on fraudulent links or malicious sites. If you trust that the person knocking on your front door holding a large box is in fact your pizza delivery man, you would not think twice about opening the door to them.

With social engineering, if you suspect the person on the other end of the email is in fact your manager or best friend, you wouldn't think twice about doing what they ask.

Highly intelligent attacks take time and criminals study religiously to find out what makes their victims tick, often masking them as someone or something close to them.

**90% of data breaches are down to human error.**





If attackers say the right things to the right person, they could gain access to your network within a matter of minutes.

The more we know about cyber security and the more education we receive, we will become more aware and suspicious of the tactics criminals use which in turn will help reduce the number of successful attacks.

## Key Threats

What you should be looking out for

### Phishing Attacks

In 2020 phishing attacks are the main source of attack you should be watching out for, with [phishing attacks rising from 72% to 86%](#) (Gov.uk, 2020).

Deceptive phishing is something we have probably all experienced, this is when the attacker poses as a legitimate company, such as your bank, TV licensing or HMRC. These messages are usually sent by email or in the form of [smishing](#) (sent via SMS and text).

Spear phishing is a highly targeted form of attack which is tailored to a specific victim or group of individuals. Relying on social engineering, attackers will spend a lot of time researching which users they can and should be targeting.

Attackers may pose as an interested sales lead to begin conversation with your business, from there they may interact with senior members of staff such as Directors and will make note of the style of language they use in emails.

Attackers can then easily copy their email signature and set up a very similar domain, often changing just one character with the aim of tricking an untrained eye into thinking it is the correct address.

Once they have what they need, the attackers will then launch a highly targeted spear phishing attack, posing as someone of authority within the business. They could choose to target the whole organisation or a specific

**There has been a rise in phishing attacks, from 72% to 86%.**



individual, asking for early payment of an invoice that does not exist or to access log in credentials to gain a way into your businesses network.

CEO fraud is a type of phishing attack where a criminal will spoof a company email address and impersonate a member of an organisation, such as the CEO. Their hope is that the employee that receives the email won't realise they aren't in fact talking to the CEO and will action their request to transfer money to a spoofed client bank account, click a malicious link or send out sensitive personal information. CEO fraud is also known as Email Spoofing and is named Business Email Compromise by the FBI.

A spoofed email address looks exactly the same as the real persons email address making it very hard to identify. An anti-spam filter helps protect your business from receiving this type of email but it is important to invest in a good solution as the better the solution the better it will be at keeping these emails from landing in your inboxes.

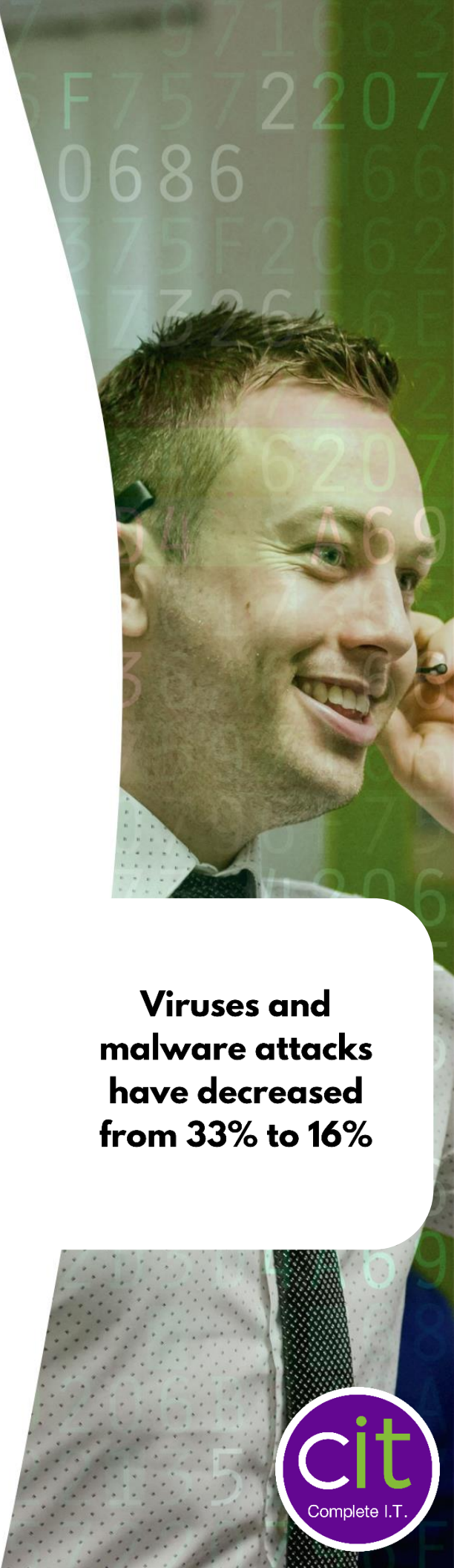
## Ransomware

Ransomware has been around for some time, the first case was called the PC Cyborg Trojan which infected computers using floppy disks (which is why we don't endorse the use of USB sticks today), encrypting the machine and all of the files on it.

Although viruses and malware attacks, such as ransomware has decreased from 33% to 16% in recent years (Gov.uk, 2020) they are still a highly targeted and intelligent tactic which businesses should be aware of and protect against.

Ransomware comes in many forms and is constantly evolving, making it very difficult to identify and detect before it infects your systems and network. One of the most prolific pieces of ransomware is WannaCry which caused chaos all over the world in 2017.

Individuals and businesses were hit with the ransomware which infected over 300,000 computers over the course of the weekend, bringing down several NHS trusts for a



**Viruses and  
malware attacks  
have decreased  
from 33% to 16%**





number of days, cancelling appointments leading hospitals to urge patients not to go to A&E unless absolutely necessary. Ransomware can be very scary and can cause huge potential loss to your business.

If your files have been encrypted and are not backed up, they are essentially lost forever, unless you pay the ransom and the attackers do actually stick to their end of the bargain (which we do not recommend). If you have properly prepared your systems for an attack, ransomware becomes more of an annoyance as opposed to acrippler.

### **Brute Force attacks**

Brute force attacks are one of the most common methods used to target websites, with the aim of gaining entry to user accounts to steal their login credentials and information.

Under the GDPR these attacks are classed as a data breach and can land your business with huge fines and tarnish your reputation. Attacks are often orchestrated via automated tools which are readily available on the internet, making it very easy for attackers to enter password secured systems.

One of the most common methods of conducting brute force attacks is set in motion if the length of the password is known. For example, if an attacker knows that the length of passwords for a site are equal to 8 characters, they will launch an automated attack that tries every known combination of numbers, letters and symbols equal to 8 characters until a match has been found.

Although this sounds like a slow process, an attacker could access an account within minutes using an automated process. Other brute force attack methods include a dictionary attack, where all words in the English dictionary are tried with the substitution of different numbers and characters.

While this method contains far fewer possible combinations when compared to traditional brute force attacks, they still give attackers a very good chance of identifying the



A man in a blue sweater is shown in profile, talking on a black mobile phone. The background is a blurred office setting with other people. In the bottom right corner, there is a large, stylized 'cit' logo in a purple circle, with the text 'Complete I.T.' underneath it.

When it comes to remote working it is proved that it can increase your teams productivity but your team must be made aware of the risks associated with unsecure networks and how to overcome them.





## Part 2: The Nature of Cyber Crime

We hope after reading Part 1 of this 2 part series you have a much better understanding of the current state of cyber crime. Part 2 will look at the unique set of challenges that SMEs face when it comes to cyber crime, and our recommended steps to stay one step ahead.

