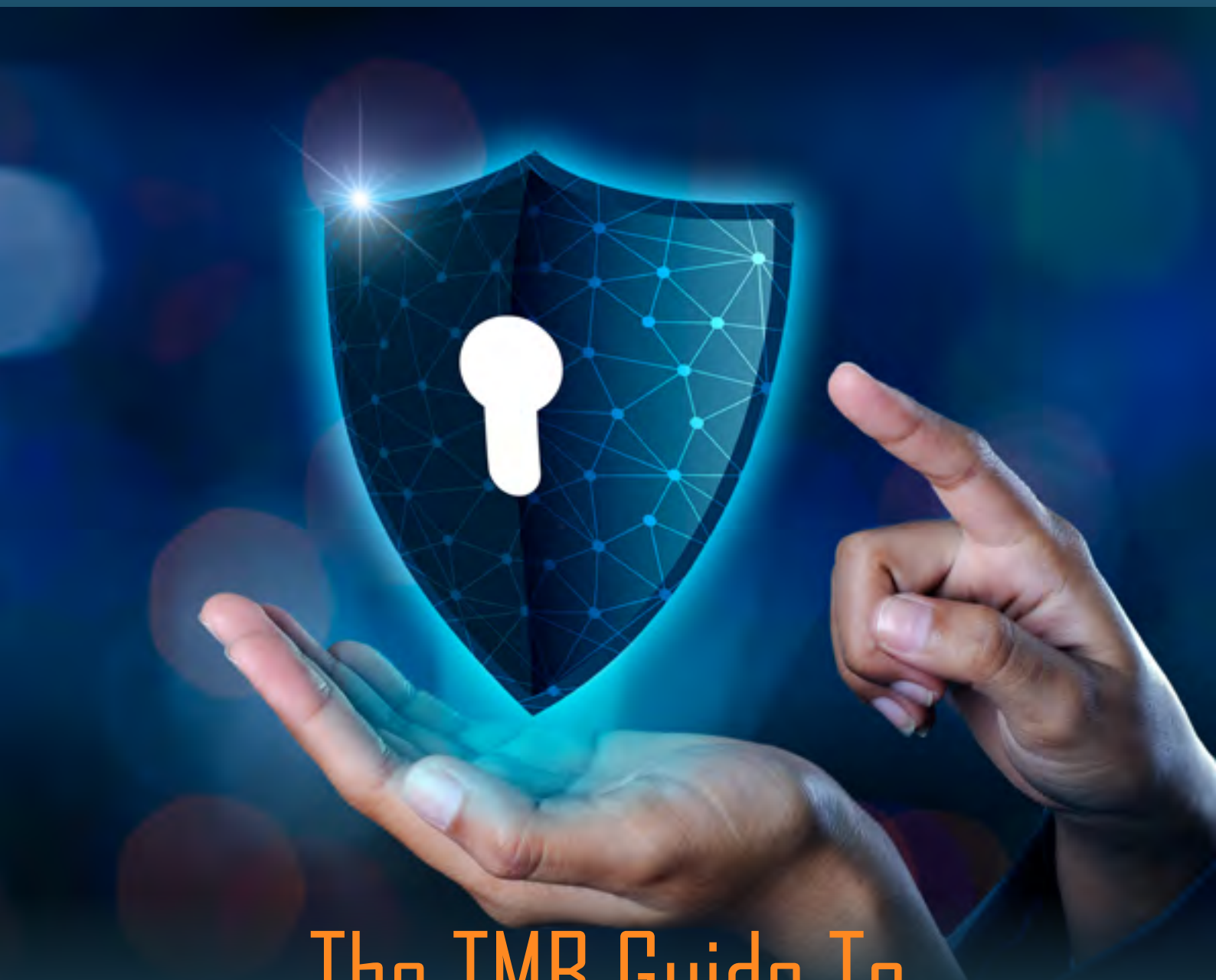
tmb Group | technology means business



The TMB Guide To Cyber Security

Cyber Security In Numbers | Tech Jargon Buster | Essential Cyber Security Tips & Advice | Backup & Disaster Recovery: The Ultimate Insurance Policy | How Cyber Secure Are You? | Visibility & Cyber Security

About TMB

Technology Means Business is a provider of IT services and products, with more than 30 years of experience working with businesses, charities and other organisations. With offices in London, Hampshire, Essex and Kent, we cover a large part of the South East, and our clients range from small, family owned businesses to large, multinational corporations.

As well as cyber security solutions, such as firewalls, email filtering and disaster recovery, we also specialise in fully managed IT support, network infrastructure projects, backups, disaster recovery, technical consultancy and cloud software.

info@tmb.co.uk 0333 900 9050 www.tmb.co.uk

Gold Microsoft Partner

WEBROOT

Microsoft

CYBER ESSENTIALS

SONICWALL

TMB London
318 Worple Road,
London,
SW20 8QU

TMB Hampshire
A1 Endeavour Business Park,
Penner Road,
Havant, Hampshire
PO9 1QN

TMB Essex
9-10 King's Court,
Newcomen Way,
Severalls Business Park,
Colchester, Essex
CO 4 9RA

TMB Kent
The Joiners Shop,
The Historic Dockyard,
Chatham, Kent
ME4 4TZ

Welcome

At TMB, we believe cyber security isn't just about technology – it's also about education. Robust security solutions like antivirus applications and firewalls play an important role in keeping businesses safe, of course, but to be truly effective, they have to be backed by a workforce that knows what it's doing.

That's why we created this ebook. We want to show not just our customers but everyone why it's so important to be on the ball when it comes to cyber security. After all, we're all in this fight together, and the more we collaborate to tackle this problem, the closer we get to beating it. We'll probably never get rid of cyber criminals completely, but we can definitely make things harder for them.

Richard Shuker, technical director, Technology Means Business

CONTENTS

10 ESSENTIAL CYBER SECURITY TIPS

Taking a few simple precautions can make a huge amount of difference...

According to the government's Cyber Security Breaches Survey 2018, more than 40% of businesses in the UK have experienced a cyber breach, and more than 70% say cyber security is a high priority for them. Yet less than a third of them have any kind of formal cyber security policies in place.

Clearly more needs to be done, and to give you a head start, we've put together 10 cyber security commandments that every business should follow. There are, of course, many more tips and pointers we could include, but hopefully this will at least help you to get started.

1) Assume you're a target

First and foremost, never assume that you won't be hit by a cyber attack. If you're lucky, it will never happen, but absolutely anyone can be a target, because many attacks use automated software, which doesn't necessarily discriminate. Small businesses may also be more likely to fall victim to security breaches because criminals consider them soft targets.

2) Use strong, unique passwords

Although other forms of authentication exist, such as fingerprint scanners, passwords remain the most common way of logging into websites and systems. Don't make life easy for criminals by using weak or easily guessed passwords like 'Pa$$w0rd' or '12345678', and don't reuse your passwords in different places.

3) Keep software and hardware up to date

If possible, use automatic updates to keep your IT solutions up to date. Otherwise, ensure that you regularly check for updates, particularly those that include security patches. Cyber criminals will be well aware of any weaknesses, and they'll waste no time trying to exploit them.

4) Report any suspicious activity

It's not necessary to report every single dodgy email you get, as long as they're automatically getting sent to your spam folder, but if you see what you think might be a phishing attempt and it hasn't been filtered out, tell your IT people. By getting the word out, you can make sure no one in your business falls victim to a scam.

5) Secure all devices including phones

In the modern workplace, it's not just workstations and servers you need to be concerned with; many workers also carry phones and tablets that are connected to the corporate network via WiFi. These need to be secured or limited to a guest network, because they're all potential entry points for hackers.

6) Identify and fix your weaknesses

All businesses should be aware of their weak points. That could include many things, including operating systems that are no longer supported, people who aren't trained to spot phishing emails, routers that don't use the latest security protocols and systems not configured to deliver the maximum security benefits. Arrange a security audit to gain clarity and to plan ahead.

7) Be careful when clicking links or files in emails

Booby-trapped files and websites are a favourite way for hackers to install malware or to steal data, and email is the most common way of getting people to open them. If you receive an email from someone you don't know and it's urging you to download a file or follow a link, stop and think about it first.

8) Don't leave your computer unattended without locking it first

This is especially important if you're using a laptop or other mobile device and you're not in the office, because if criminals gain physical access to your computer, it's no problem for them to install malware on it. To lock your system, simply press the Windows key and L. You'll need your password or PIN to log back in.

9) Review your cyber security measures every year

Cyber criminals are always looking for new ways to rip people off, so cyber security cannot be considered as a one-off, static purchase. At least once a year, you should assess your current security solutions, to see if they're still up to the task, and if they're not, then you need to upgrade. This is also a good time to look at your security budget, to make sure it's being spent effectively.

10) Make multiple backups, with at least one kept off site

Never put all your backup eggs in one basket: backups can and do go wrong. In the majority of cases, one backup will be enough if your main copy of data is damaged by mechanical failure or human error, but if you're unlucky, your backup could be lost at the same time. The chances of your backups being affected increase when malware enters the equation. Viruses, ransomware and so on can spread over a network and take out all your backups, as well as your main copies. Keep one of them off-site, though, and you should be safe. ■

This article first appeared on the TMB blog. Head to www.tmb.co.uk to read more of our posts.

Confused by tech talk? Let us TMB lend you a hand...

Understanding cyber security has never been more important for businesses – but it's not easy. Experts sometimes use so much technical jargon, it's like they're talking a completely different language!

But you don't have to become a tech whiz to learn about security essentials. As long as you know a few of the basics, you can make informed choices about how you're going to protect your business from criminals.

tmb technology means business

Adware
A form of unwanted software that automatically displays adverts, often at particularly intrusive times.

Bot
Short for robot, a bot is an automated program that works over the internet.

Botnet
A network of bots.

DDoS
A distributed denial of service is a type of attack that involves flooding a computer system with requests for information. This essentially overloads that computer, causing it to crash.

Encryption
By encrypting data, it becomes unreadable to anyone who doesn't have the code to unlock it.

Exploit
An attack that takes advantage of a weakness in a computer system or piece of software.

Firewall
A security system or program that prevents unauthorised access to a computer or network.

Hacker
Someone who gains unauthorised access to data, networks or computers.

Malware
Software designed to disrupt, damage or gain unauthorised access to computer systems.

Phishing
The practice of sending fraudulent emails, with the intention of gaining personal information.

Ransomware
Malicious software that encrypts data, which will only be unlocked once a ransom is paid to the criminals behind it.

Spear-phishing
Like phishing, but tailored specifically to a person.

Spoofing
To fake certain information. In the case of email spoofing, criminals make it look as if they're contacting you from an email address different to the one they actually are.

Spyware
Just like it sounds, spyware covertly sends information from your computer to a third party.

Trojan
Also called a trojan horse, this is a computer program that seems to be legitimate, but which contains hidden code that unleashes malware.

Virus
A type of malicious software that attaches itself to files on your computer and which is able to replicate itself.

Whaling
Like spear-phishing, where a particular person is targeted, but aimed specifically at high-profile employees such as CEOs or CFOs.

Worm
Similar to a virus, but a worm can spread across a network to other computers, and it doesn't need another file to act as a host.

Backup & Disaster Recovery
The Ultimate Insurance Policy

Data loss and downtime have real financial consequences for businesses. Don't find out the hard way...

If you have strong cyber security measures, such a business-class firewall, spam filtering and DDoS protection, there's a good chance you'll never experience a significant breach. But even with the best made plans, it's still possible to be hit by a breach that knocks your business out of action, perhaps deleting data or making it otherwise inaccessible.

A typical example might be a ransomware attack that encrypts important files and systems, making them inaccessible and probably causing your business to grind to a halt.

Data loss may also occur due to hardware failure, human error or catastrophic incidents like fire, flooding and natural disasters.

Whatever the cause, these incidents quickly translate into financial losses. Lost data can mean not being able to process orders or keep track of receipts, and system downtime can simply prevent you from doing anything productive at all.

The average cost of IT downtime for a UK company is estimated at £3.6 million per year. Obviously, that figure will vary according to the size of individual companies, but so will the amount of financial loss they can withstand. In any case, the cost can be anywhere from £4,300 to £258,000 per hour.

Even if you never experience a cyber attack, your business could experience downtime and/or data loss at some point. Considering the associated costs, it makes sense to be prepared for the worst.

The answer in most cases is backup and disaster recovery (BDR).

IT Fail Hall of Shame

The NHS

As if the National Health Service didn't have enough to worry about, in May 2017, it fell victim to a major ransomware attack that ended up affecting multiple hospital trusts and other NHS organisations. The total costs were about £92 million, and the subsequent investigations found numerous failings in the NHS's IT and cyber security, including failure to do basic things like applying software updates.

IT Fail Hall of Shame

British Airways

In May 2017, a major system failure forced British Airways to cancel all flights from Heathrow and Gatwick, affecting more than 75,000 passengers. Not only did this cost the airline about $68 millions in customer reimbursements, it also led to a 28% fall in its stock price.

Best Practice

All responsible businesses will make backups of important data, but how often they do so makes a huge difference to their usefulness. If you only back up files once a month, what happens if you suffer a data breach right before your next scheduled backup? That's a whole month of files gone. You should instead be making backups at least once every day.

It's also important to make multiple backups, with at least one kept off site or in the cloud, because whatever destroys your originals might also take out your backups. An on-site networked backup device, for example, could also be affected by a ransomware attack, and if there's a fire at your premises, you could lose everything all at the same time.

By following good backup practice, you should never lose so much data that your business can't recover.

The Whole Story

But backing up is only half the story, because backups alone do not ensure business continuity. For a start, restoring data takes time, and the duration is determined not only by the amount of data you have but also the speed of your network or internet. That time, of course, will likely mean wasted work hours.

Furthermore, while backups enable you to restore data, they may not restore whole systems, including configurations, applications and so on. In other words, they don't usually offer business continuity; for that, you need a disaster recovery solution.

Going hand in hand with backups, the whole point of disaster recovery is to give organisations a system they can fall back on, if they ever need to. The idea is that they replicate the corporate network in real time, and if there is some kind of IT disaster, the user can simply spin up the backup server and work from that, until the problem is fixed.

Recovery At Any Time

With TMB's own BDR solution, data can be sent not only to a local backup server but also a cloud server. That extra redundancy in the system could be vital and could even save your business.

Also important is the fact that it's a fully managed, 24/7 service. That matters because disaster can strike at any time, and if you experience a problem outside of normal business hours, you'll want to get it fixed before you open shop.

As a fully managed service, TMB's BDR solution is proactively monitored too, which means we're constantly keeping an eye on your backups to make sure they're completing properly and that your disaster recovery servers are up and running.

To get the most from your BDR service, no matter who it's provided by, you should also have a disaster recovery plan or policy, documenting exactly what needs to happen, when and with whose authority. Ignoring this part of the process could result in a delay in getting your business back on track.

Once all of this is in place, you will have an effective insurance policy against disaster. Hopefully, you'll never need to use it, but if you do, you'll be glad you got it sorted while you had the chance. ■

IT Fail Hall of Shame

TSB

The now legendary IT problems of TSB all started in April 2018, when it tried to migrate its customers to a system created by its new owner, Sabadell. The result was chaos, as customers were locked out of accounts, given access to other people's details and generally shown how not to complete to complete a major IT project. The cost of this failure? About £330 million and 80,000 customers switching to a different bank.

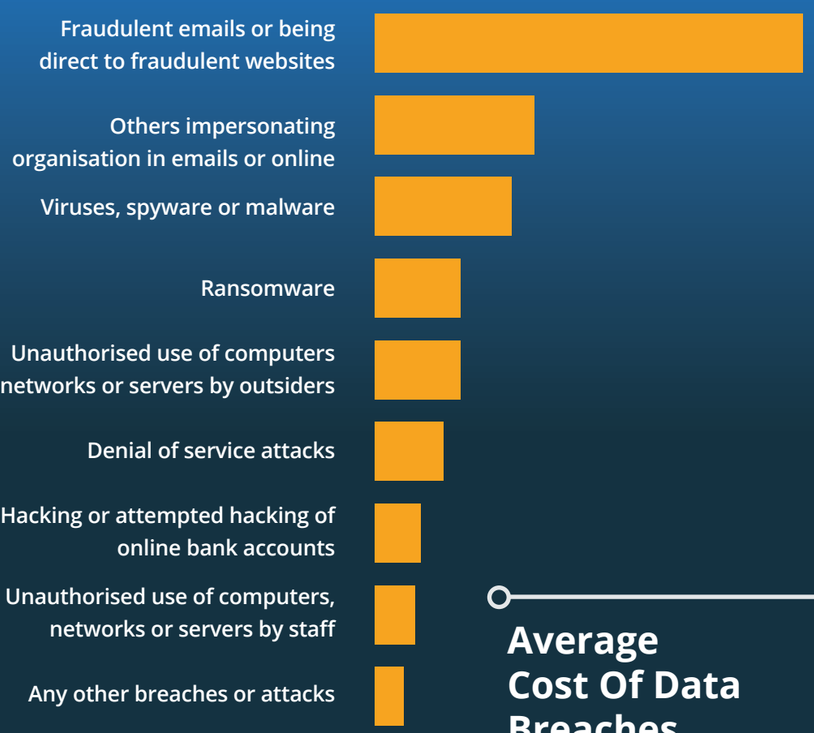
CYBER SECURITY

Facts & Figures

How much do UK businesses lose to hackers? What are they doing to protect themselves? Read on to find out...

tmb technology means business

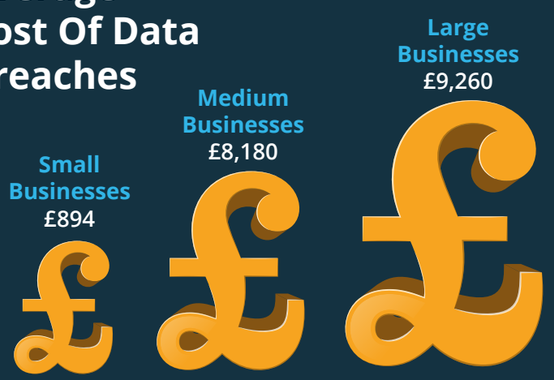
Types of breaches or attacks suffered among the businesses that have identified breaches



The source of 35% of ransomware infections is unknown. Most common known sources are email links (23%) and email attachments (17%).

Only 9% of small businesses have cyber security insurance

Average Cost Of Data Breaches



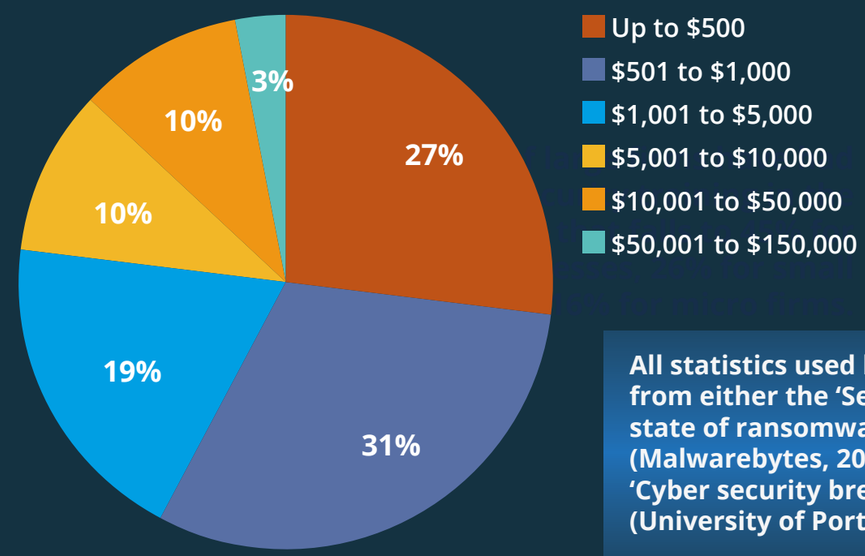
DOWNTIME

is often the worst problem caused by ransomware. More than 50% of ransoms are for $1,000 or less – but not being able to work can be even more costly.

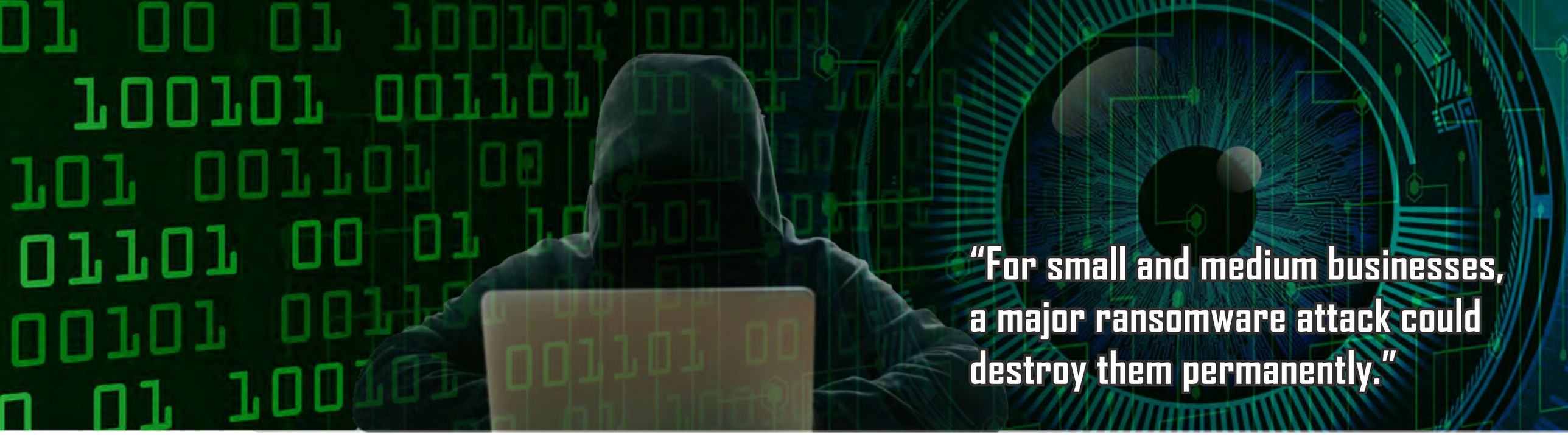
43% **of all businesses identified at least one cyber security breach in the last 12 months.**

The average UK business reports **998** breaches in a year

Largest Ransom Demanded From Businesses Affected By Ransomware



All statistics used here are taken from either the 'Second annual state of ransomware report' (Malwarebytes, 2017) or the 'Cyber security breaches survey' (University of Portsmouth, 2018).



Understanding The Long-Term Damage Caused By Cyber Attacks

Recovering from a security breach can be time consuming and expensive, as a high-profile ransomware case in the United States illustrates

In 2018, the long-term impact of cyber crime was felt sharply in the USA. In March of that year, the city of Atlanta was hit by a massive ransomware attack, in which criminals demanded a $50,000 ransom.

At the time, vital systems and departments were said not to have been affected, but almost three months later, it was revealed that the extent of the damage had far exceeded early reports. At a public meeting on 6th June 2018, the city's IT chief suggested another $9.5 million would be needed to help clean up the problems left in the malware's wake.

This came just a month after Atlanta's government already spent $2.7 million trying to repair the damage.

Such huge costs are difficult to comprehend, until you put them into context. Reports suggest that over a third of the city's 424 software programs were knocked offline, and a third of those were 'mission critical', meaning they were related to vital services like policing, water systems, courts and so on. Clearly, it was a matter of urgency that these be restored to full working order as soon as possible, and combined with the complex nature of public services, it was not surprising that Atlanta had to pay some hefty bills to private firms just to keep things running.

Is It Best To Pay The Ransom?

It's not clear whether officials tried to pay the ransom or not, but it's widely thought that they refused or were unable to do so. Considering the original ransom was only $50k, it's tempting to think that paying it would have been the better option. Maybe it would have been; after all, it was tax-payers' money at stake. But there are some good reasons to avoid paying up in a ransomware attack. For a start, there's no guarantee that the criminals behind the attack will actually supply decryption keys once they've got their money. In fact, in some cases, they might not even be able to. And paying ransoms might also attract repeat attacks – a very real possibility for a high-profile target like a government body.

If anything positive can be said to have come of Atlanta's troubles, it's that they provide a lesson to the rest of us. No, we probably wouldn't have to spend millions on getting our systems up and running again, but we also don't have the same depth of funds to aid the recovery process. For small and medium businesses, a major ransomware attack could destroy them permanently.

It's important, then, to understand what the long-term impact of cyber crime could be for you. If your business were to lose all record of invoices, you could lose money for work already done. If payroll were affected, you might be liable to pay compensation to employees. If ordering systems go down, you could lose the ability to bring in vital stock or equipment. The list goes on. And all these things could lead to customers taking their money elsewhere or business operations having to cease.

How could all this pain be prevented? With comprehensive, top-to-bottom cyber security policies and systems. As well as modern firewalls, antivirus and so on, you also need to think about staff training, to help reduce your chances of being attacked by criminals. Plus it should be considered essential to have a robust disaster recovery strategy in place, because even the best protective measures in the world aren't perfect.

It's also worth considering moving over to a proactive support and security arrangement with a managed services provider such as TMB, rather than relying on reactive, 'break-fix' solutions, which by their very nature are only employed when something has already gone wrong.

Most importantly, you shouldn't make the mistake of thinking that once a cyber attack is over that's it. In many cases, the worst is yet to come. ■

This article first appeared on the TMB blog. Head to www.tmb.co.uk to read more posts.

Why Visibility Is Vital To Cyber Security

Knowing who and what can access your network is vital for effective security...

Could you say, with complete confidence, what devices and which people, at any one time, are able to access your company's digital resources and data? Sure, you might have a list of all the PCs and servers your business owns, but what about those mobile phones in your colleagues' pockets? If they're personal devices, it's likely they're not being tracked at all, yet they're quite possibly connected to the company wi-fi, which in turn means they could be connected to every other device in the workplace.

From a security point of view, this is less than ideal. Every one of those phones is a potential risk, a gateway into your corporate network, just waiting for cyber criminals to wonder in and wreak havoc. All it takes is for one of them to accidentally download malware from an email, an app or a website, and it can quickly spread around your business. The same, of course, applies with other personal devices such as laptops and tablets.

Avoiding any kind of BYOD (bring your own device) arrangements in your business could help to reduce your risks, but it would certainly not be a guarantee of safety. Even company-owned devices can cause problems if they're not properly tracked and regulated.

Also, the threats aren't always external. Every year, there are numerous cases of insider threat, where employees or other parties within an organisation use IT systems to commit fraud or cause damage. One of the ways they might do this is unregulated devices.

Businesses might also find themselves having to contend with staff members storing valuable data and then taking it to a competitor or their next employer.

These are worst-case scenarios, but sadly they occur all too often in the real world.

Thankfully, there are solutions, some of which involve technology and some that require a change in the way you think about your business.

The first step is to simply acknowledge and understand the cyber security risks within your business. What you absolutely shouldn't do is assume you won't be a target or that the people within your organisation will always be on your side. Once you made this step, you can think about the technology that will resolve the problem: user and device management tools.

One popular solution is Microsoft Enterprise Mobility + Security. This collection of tools does various things, including enabling businesses to easily prevent unauthorised devices from accessing their systems and data, while allowing enough flexibility for even personal devices to be used safely at work.

It also allows businesses to determine which apps can be installed on which devices, and it can also be used to remotely delete corporate data from devices.

But perhaps the key benefit is visibility. If you can track where devices are and how they're being used, you're better positioned to protect yourself. Indeed, as well as device management, Enterprise Mobility + Security manages user identities and tracks changes to data.

Maybe, though, you might find some employees don't want to install on their personal devices the software necessary to make such systems work. For that reason, you want to set up a guest wi-fi connection in the workplace, one that has full internet access but is separate from the company network. This is fairly simple to set up, but a useful preventative measure all the same.

> "What you absolutely shouldn't do is assume you won't be a target or that the people within your organisation will always be on your side."

But technology can only take you so far. To avoid confusion among staff, you should implement clear policies and procedures about how they use company and personal devices while at work. People need to know what kinds of things they should be doing and which they shouldn't; they need to know what data they're allowed to take from your premises, and they need to informed of the possible penalties for any infractions. You might also want to make it a contractual obligation for all personal devices to have security software on them if they're going to be used at or for work. ■

5 NOTORIOUS CYBER CRIMINALS WHO GOT CAUGHT BY THE LAW

Crime, they say, doesn't pay. Yet every year, billions of pounds are lost to cyber criminals, and the chances of recovering anything are often slim. So, it would seem, crime does, in fact, pay quite a lot of money, quite a lot of the time, which is no doubt why so many people are engaged in it.

But that doesn't mean the authorities are completely powerless. Identifying and capturing cyber criminals is often difficult and time consuming, but it happens all the time, and to celebrate the work of law enforcement professionals, we've put together a list of notorious cyber criminals who were caught and prosecuted.

Kevin Mitnick

Who: Arguably the most famous cyber criminal of all time, Kevin Mitnick, unlike many black hat hackers, wasn't motivated by profit. Instead, he committed multiple computer and communications crimes just for the sheer hell of it. From the tender of age of 12, he learned the power of social engineering, convincing a bus driver to tell him where to buy the special punch that was used to mark transfers, and then using it to mark blank transfers he dug out of station bins – thereby getting free bus travel all over Los Angeles. He also used social engineering and phone phreaking to explore the phone networks of the day, getting free long-distance calls and access to secret information.

What he did: The social engineering and phone phreaking were just the start of things to come for Mitnick. It was when he started gaining unauthorised access to computer networks that he really got into trouble. In 1989, he was sentenced to a year in prison, followed by three years' probation, for hacking into computers at Digital Equipment Corp. and stealing $1 million of software. While on release, he hacking into voicemail computers at Pacific Bell, and an arrest warrant was issued. But rather than go quietly, Mitnick went on the run for two and a half years, before eventually being arrested in 1995. Yet it wasn't until 1999 that he pleaded guilty to wire fraud, possession of unauthorised devices and unauthorised access to a federal computer, among other things.

Length of sentence: 46 months, plus another 22 months for violating his 1989 parole. He served a total of five years in prison – four and a half of which were served pre-trial. He also spent eight months in solitary confinement, because law enforcement officials convinced a judge that Mitnick could launch nuclear missiles by whistling down the phone.

Where is he now?: After being released in 2000, Mitnick was banned from using computers and other communications technology, but he appealed against that and won. Today, he's turned legit and makes a living as a cyber security expert, as head of Mitnick Security Consulting LLC. He also, controversially, started selling security exploits.

Michael Calce

Who: A Canadian schoolboy from Île Bizard, Quebec, who went by the handle MafiaBoy.

What he did: In February 2000, Calce launched several high-profile denial-of-service attacks against companies like Yahoo, Amazon, Dell, eBay and CNN. He began by targeting Yahoo, under a project he called Rivolta (Italian for 'riot'), before turning to other firms, bringing each of their websites to their knees. It was later reported that these attacks caused a total of around CAD$1.2 billion.

Length of sentence: Because he was only 15 at the time of the offence, Calce got off relatively lightly. The Montreal Youth Court sentenced him to eight months of 'open custody', a year of probation, restrictions on his internet use and a small fine.

Where is he now?: Calce wrote a book, called Mafiaboy: How I Cracked the Internet and Why It's Still Broken, which was published in 2008. He also set up his own company, Optimal Secure, which tests other firms' cyber security measures, and has worked with HP on a security-related documentary.

Max Butler

Who: Max Ray Butler grew up in Idaho, USA, and was known online as Iceman. Growing up, Max was expelled from school, arrested for burglary, and convicted of assault. He would later change his name to Max Ray Vision, while living in a rented mansion with a group of other computer enthusiasts.

What he did: Butler was convicted multiple times for crimes spanning several years. As well as his previous scrapes with the law, he hacked US government websites in 1998, and was sentenced to 18 months in prison in 2001. After being released in 2003, he went back to crime, using WiFi to commit attacks, programming malware and stealing credit card information. In 2007, he was arrested and eventually pleaded guilty to wire fraud, stealing millions of credit card numbers and around $86 million of fraudulent purchases.

Length of sentence: Considering the nature of his crimes and his history, it's perhaps no surprise Butler was given a much more hefty sentence this time. In fact, at the time it was the longest ever sentence handed out for hacking in the US: 13 years.

Where is he now?: The Federal Detention Center, Victorville, probably sporting a rather fetching orange jumpsuit. He's due for release in 2019.

Albert Gonzalez

Who: Hailing from Miami, USA, Gonzalez had various screen names, including cumbajohny, soupnazi and segvec. When he was just 14, he hacked into NASA and was duly visited at school by the FBI.

What he did: Like Max Butler, Gonzalez had a long history of trouble with the law. In 2003, he was arrested for being part of ShadowCrew, a group that stole and then sold card numbers online. Proving there really is no honour among thieves, he did what all good hackers do in this situation – he turned grass, working with the authorities in exchange for his freedom.

But this was just the beginning. From around 2006, Gonzalez was involved in a string of hacking crimes, once again stealing credit and debit card details. Before his arrest in 2008, he managed to steal millions of dollars, which he used to pay for lavish parties and hotels. Among the companies targeted were TJX, Heartland Payment Systems and Citibank.

Length of sentence: He was eventually indicted on charges in several different cases, in Boston, New York, Massachusetts and New Jersey. As part of a plea deal, his sentences in all these cases were allowed to run concurrently, but he still got 20 years – beating the previous record set by Max Butler.

Where is he now?: Gonzalez is serving his time in the Federal Correction Institution, in the wonderfully named Yazoo City, Mississippi. He's due for release in 2025.

Roman Seleznev

Who: The son of Russian Parliament member Valery Seleznev, his hacker handles included nCux and Track2.

What he did: Between 2009 and 2013, Seleznev hacked into more than 500 businesses and 3,700 financial institutions in the US and stole card details, which he would then sell online. Doing this, he is said to have made tens of millions of dollars. Many of the businesses affected were small firms, and in at least one case, this led to their bankruptcy.

Eventually, the law caught up with Seleznev. US Secret Service agents picked him up in the Maldives, as he headed back to Russia from a holiday with his girlfriend. His father has since gone on to claim Roman was kidnapped by the US.

Length of sentence: They really pushed the boat out for this one. In April 2017, a judge gave poor Roman 27 years in the slammer. And to compound his misery just that bit more, in December 2017, he was given another 14 years for a separate case.

Where is he now?: Roman currently resides in the Federal Correctional Complex in Butner, North Carolina, USA. His release date is set as 2038, which would make him 53 by the time he gets out.

This article first appeared on the TMB blog. Head to www.tmb.co.uk to read more of our posts.

Cyber Security Checklist

Run through our list to see how prepared you are

- [ ] All business software, including your operating system, is up to date.
- [ ] You can identify all devices connected to your network.
- [ ] You have full control over what software your team are running.
- [ ] The passwords on your wi-fi and your router (if you use one) are strong and aren't displayed out in the open.
- [ ] There's a clear policy about reporting data breaches, and your whole team are aware of it.
- [ ] You have professional antivirus and firewall solutions.
- [ ] Sensitive data is encrypted.
- [ ] Regular backups are made to an internal destination and to an external one.
- [ ] You and your team use password managers to remember and share passwords securely.
- [ ] Your company website uses https, rather than http.
- [ ] When employees leave the company, their passwords and network access are revoked.

Got a few ticks missing from your list? Contact TMB to find out how we can help you. We're fully Cyber Essentials accredited, and we have decades of experience, helping small and medium-sized business to get the IT solutions they need.