CyberSmart

The state of UK SME Cybersecurity

CONTENTS

CyberSmart & Software Advice

UK SMEs have faced a turbulent few years. The COVID-19 pandemic altered the way many of us work forever. The conflict between Russia and the international community has raised the spectre of cyber attacks on UK businesses. And cyber threats for SMEs continue to rise.

So with all these factors in play, how are the UK's SMEs managing? Has the rise in remote working led to a change in cybersecurity practices? How often are SMEs facing cyber threats? Most importantly, what can they do to better protect themselves?

To answer some of these questions, Software Advice – a company that provides advisory services, research, and user reviews on software applications – surveyed 500 managers at UK SMEs.

What follows is our interpretation of Software Advice's research. We hope it provides you with some key insights into the current state of cybersecurity in UK SMEs and what can be done to improve it.

How often are UK SMEs being attacked?

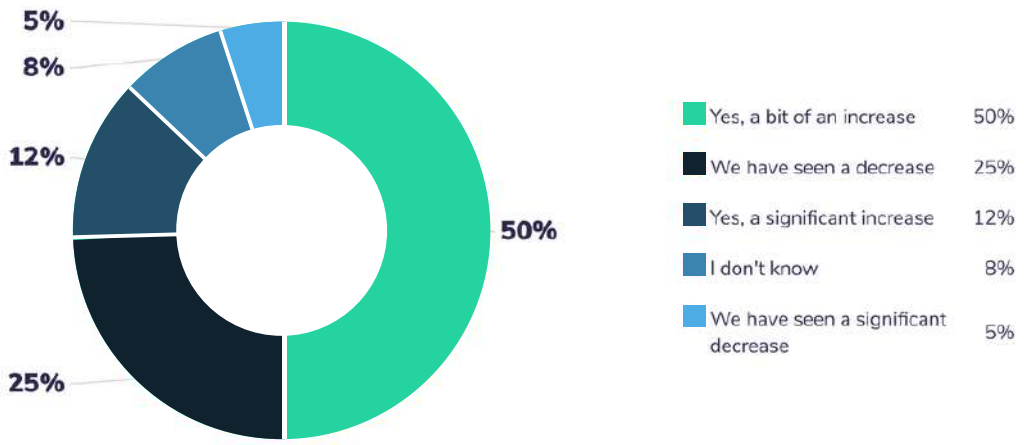
Let's begin with a simple question. Just how regularly are UK SMEs being attacked? We know that UK businesses are being hacked at alarming rates. According to the Department for Digital, Culture, Media & Sport's (DCMS) Cyber Security Breaches Survey 2021, 39% of businesses and 26% of charities report having cyber security breaches or attacks in the last 12 months.

Unfortunately, the picture isn't any rosier when it comes to small businesses. The insurer, Hiscox, estimates that, while most attempts fail, a small business in the UK is successfully hacked every 19 seconds. When you consider that the Federation for Small Businesses estimates that there are over 5.5 million SMEs in the UK (and that they account for 99.9% of all businesses), it's clear that this represents a monumental problem.

But what about how SME owners themselves feel? Sadly, the general trend towards increasing numbers of attacks on SMEs is borne out there too.

Of the SME managers Software Advice surveyed in late 2021, 62% said they had seen an increase in attacks in the last 2 years. And of those, 12% said that the increase was significant.

Have you seen an increase or decrease in cyber security threats in the last 2 years?



What effect has COVID-19 had on SME cybersecurity?

It's not an exaggeration to say that the COVID-19 pandemic radically transformed the world of work, possibly permanently. As the virus swept across the world, many UK businesses were forced to adopt remote working for the first time. And this switch wasn't just the preserve of globe-striding corporations. 43% of UK SMEs made the jump to remote working, within a week of lockdown measures being implemented in Britain.

What's more, after being exposed to the benefits of remote working, such as improved staff morale and lower operating costs, many SMEs have decided to stick with it. Research from communications company NFON reveals that over a quarter (27%) of UK SMEs are now planning to move to hybrid or remote working permanently as soon as their lease allows.

However, this move to remote working has brought with it heightened cybersecurity risks. As we outlined in the previous section, many SMEs have seen cyberattacks increase in the last two years.

Why is this happening? It's partly down to cybercriminals seeing a new opening for attacks and opportunistically taking it. VM Ware's 2020 Global Threat report revealed a 91% rise in cyberattacks during the first few months of the pandemic.

But it's also about the cybersecurity practices (or sometimes lack thereof) of SMEs themselves. Remote working comes with some defensive drawbacks which many small businesses just haven't prepared for.

For example, there's the potential psychological element. As ZDNet has reported, 52% of employees believe they can get away with riskier behaviour when working from home. This includes behaviour like sharing confidential files via email instead of the usual, safer channels.

Part of the reason employees are exposing themselves to risk at home is simply a lack of knowledge of these risks. The COVID-19 pandemic developed so quickly that many businesses didn't have time to put in place clear policies and procedures for working from home so employees were literally left to their own devices. This makes cybersecurity a bit of a guessing game, particularly for less security-literate staff.

On top of behavioural challenges, many SMEs have faced plain old equipment problems. When COVID-19 hit, many businesses were forced to send employees to work from home networks with relatively poor cybersecurity. Many small businesses have spent the pandemic with staff working on insecure personal devices and networks, without VPNs or regularly patched software. In short, a recipe for cyber disaster.

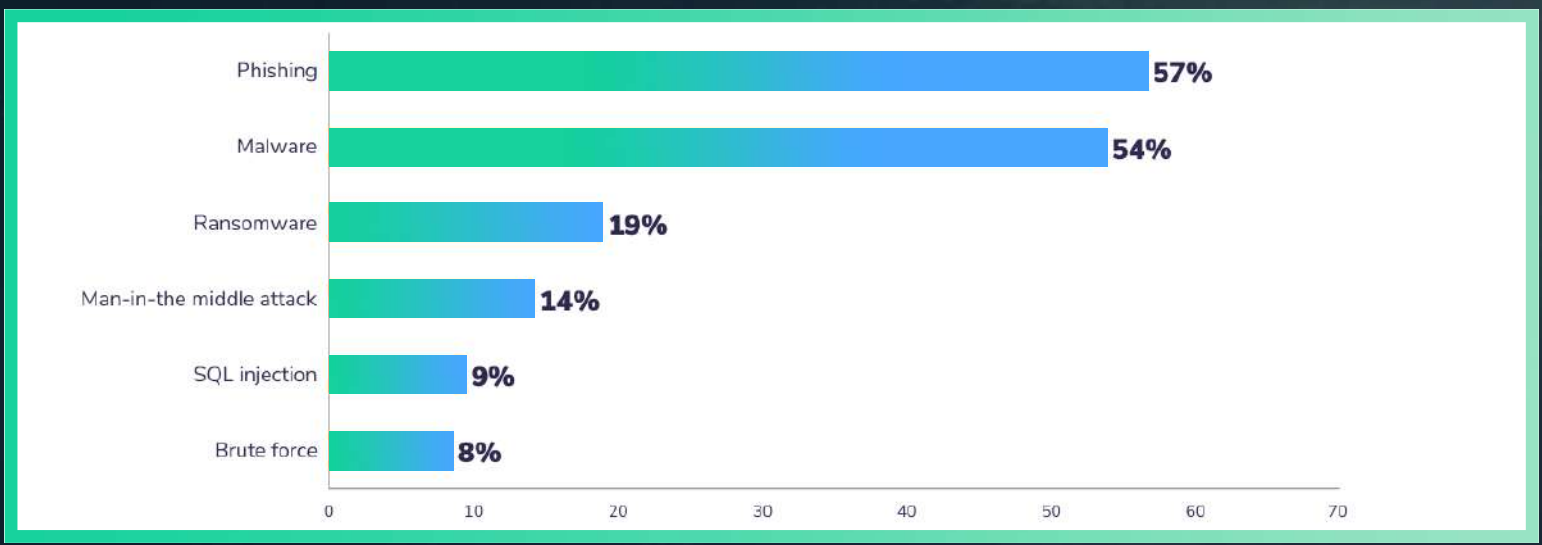
What are the biggest threats facing SMEs?

We've established that COVID-19 has presented SMEs with a host of new challenges. But what are the most common cyber threats small businesses face day-to-day?

According to Software Advice's survey results, one in five (21%) SME managers said that their business has been hit by a cyberattack or data breach in the past 2 years.

The most common attack on SMEs was phishing, which affected 57%. However, this is closely followed by malware (54%). Most surprising of all, given the media attention it generates, ransomware attacks were a long way behind at 19%.

What kind of cybersecurity attacks has your company experienced?



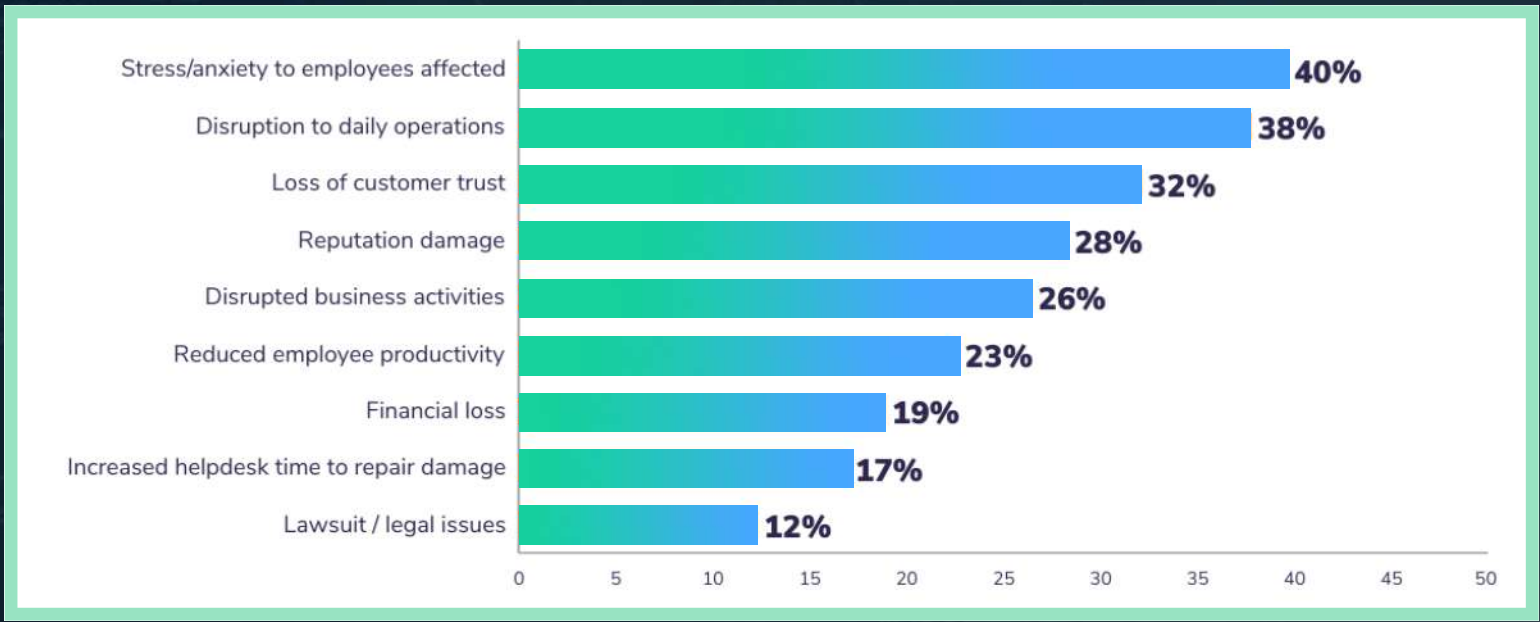
This points to SMEs largely being targeted by less sophisticated attacks and those that require an element of human error for success. It's not difficult to understand why. Small businesses typically have limited staff numbers and heavy workloads. And, when you combine this with limited cyber knowledge, it becomes the perfect blend for opportunistic cybercriminals.

What is the impact of a breach or attack on SMEs?

A successful breach or attack can have severe implications for a small business. The DCMS' Cyber Security Breaches Survey 2021 revealed that 39% of businesses ended up losing money, data or other assets due to a breach. And the average cost of all the cyber security breaches these businesses have experienced in the past 12 months is estimated to be £8,460.

These findings from the DCMS were echoed in Software Advice's survey with financial loss impacting nearly one in five.

What impacts have cyber attack/s had on your company?



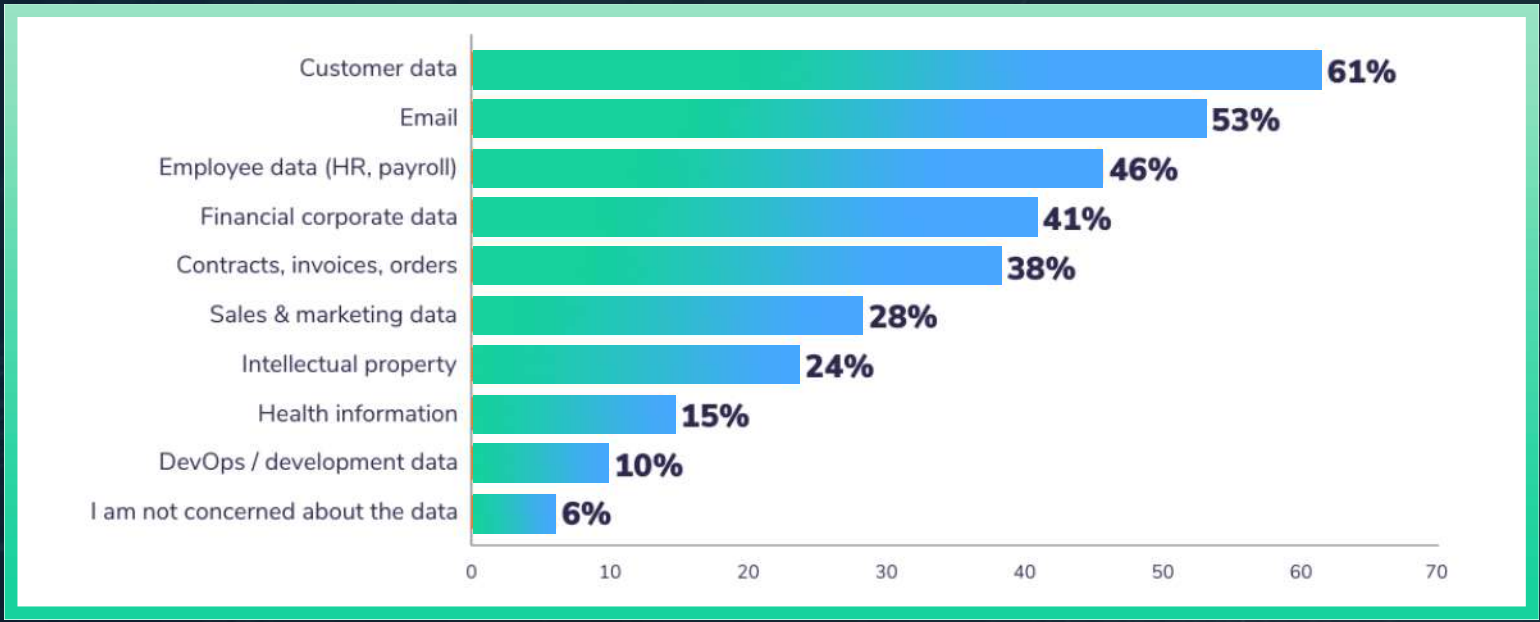
Alongside this, disruption to daily operations, loss of customer trust, and reputational damage also ranked highly. This highlights just how dangerous a successful breach can be.
For SMEs, who often have a limited customer base, any impact on service or customer trust can be hugely damaging, sometimes even terminal.

What are SMEs most worried about?

There's a common misconception that SMEs are ignorant of or don't care about cybersecurity and data protection. Sadly, it's a narrative heard all-too-often in cybersecurity circles. However, this is extremely misguided if not wholly wrong.

From Software Advice's survey, it's clear that not only do SMEs recognise the need for protection, but it's also something they actively worry about.

What types of sensitive data are you most concerned about protecting?



The introduction of strict regulations such as GDPR and the Payment Card Industry Data Security Standard (PCI-DSS) appears to have shifted the needle for many SMEs. As can be seen in the figure above, there's a broad range of data SMEs are keen to protect, none more so than customer data.

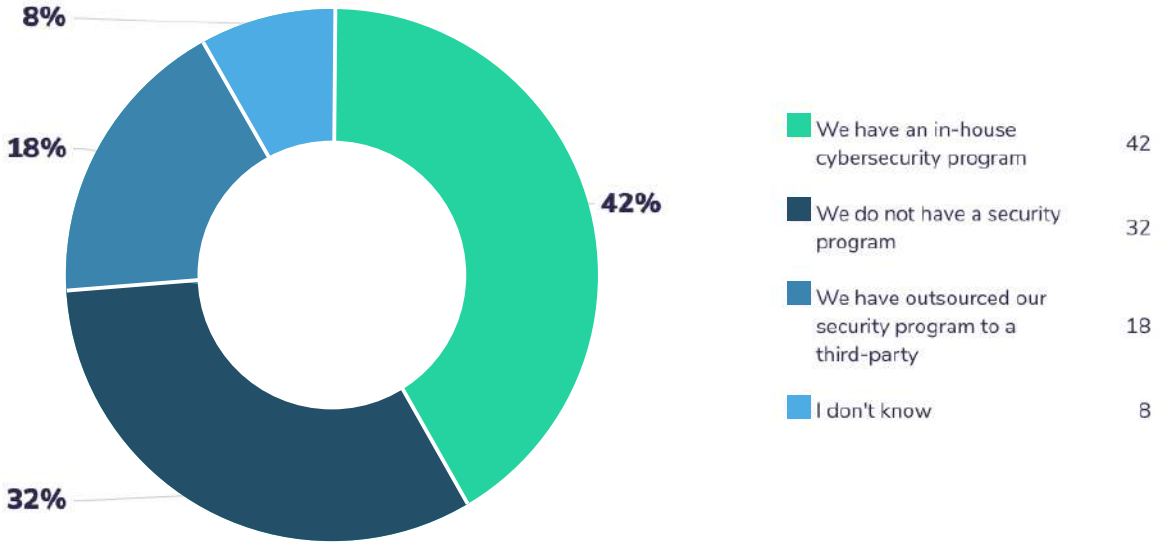
Given the consequences of a breach of GDPR, this perhaps isn't surprising. However, what it also illustrates is a clear recognition amongst SMEs that data is the lifeblood of their business and needs to be protected as such.

How good are SMEs' cyber defences?

So, if SMEs are increasingly aware of the risks posed by cyber threats, are they protecting themselves better than in the past?

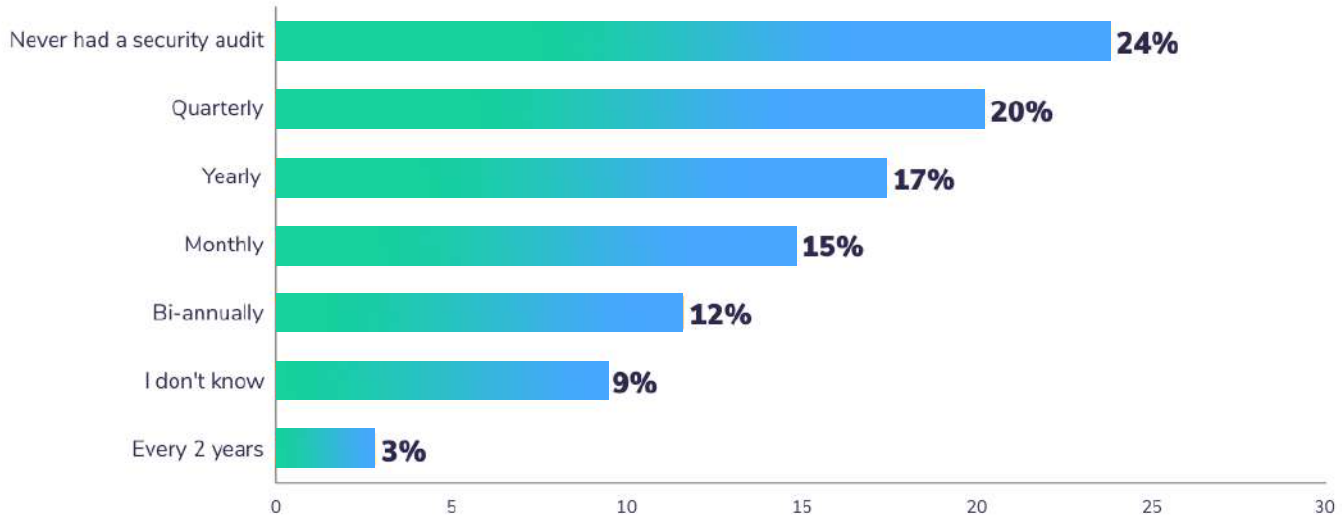
Unfortunately, this is where things become a little less positive. 32% of the UK SMEs surveyed still don't have any form of cybersecurity program at all (whether in-house or outsourced).

Which of the following best applies to your business?



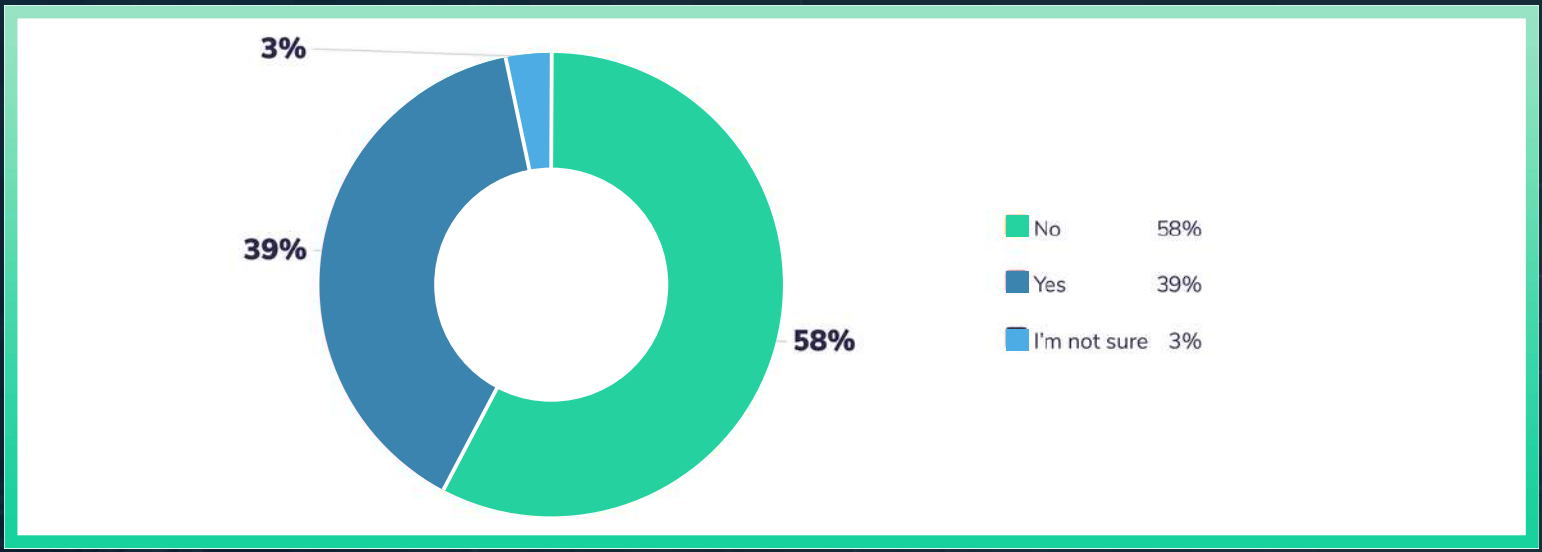
What's more, nearly a quarter of SMEs (24%) had never carried out a security audit.

How often does your company conduct security audit?



And passwords remain a major issue (although this is a problem in businesses of all sizes) with 39% of SMEs using the same credentials for multiple accounts.

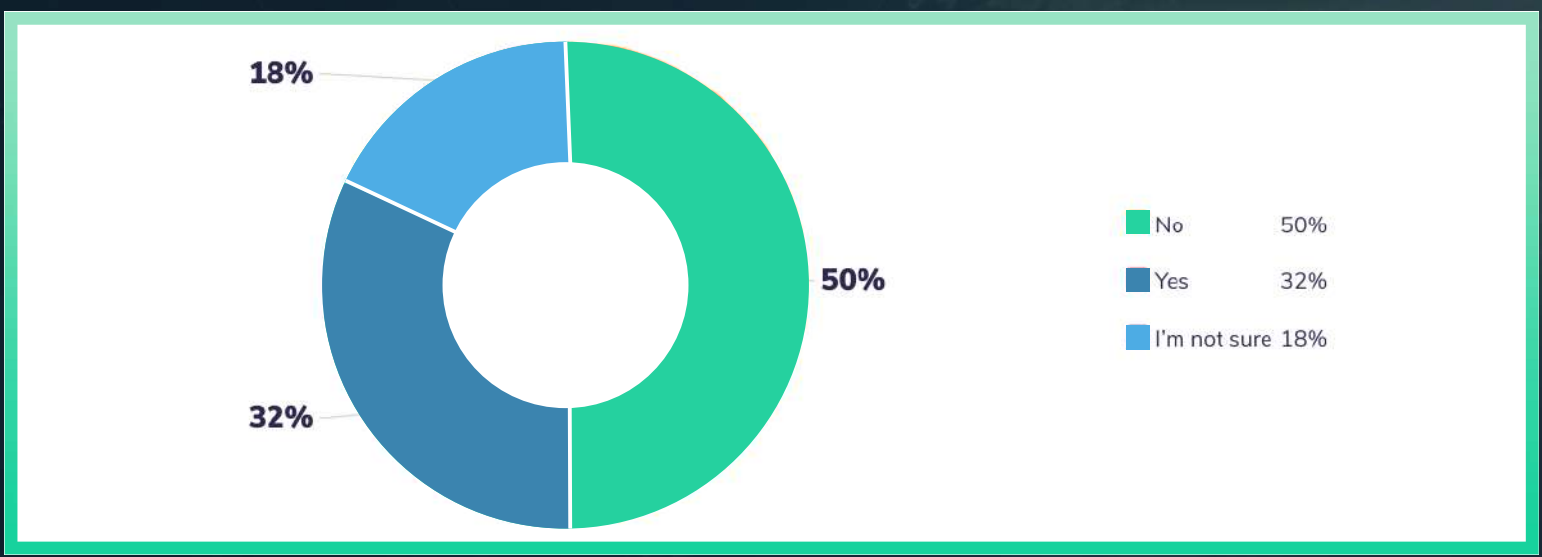
Do you ever use the same password for multiple work accounts?



These issues likely stem from two things: awareness and cost. Although, small business managers are aware of the risks presented by cybercrime, what they're less sure about is what to do about them (as demonstrated by the findings on passwords and security audits).

This also applies to how SMEs respond to a successful attack. 50% of SME managers said they did not have a formal cyber-incident response plan. Again, suggesting that while small businesses might be aware of the risks, that doesn't necessarily mean they have a plan in place to deal with them.

Does your company have a formal cyber security incident response plan?



In addition to problems of awareness, cost is also a large inhibiting factor. Many SMEs work with tight budgets; it's a part of being the little guy. And, cybersecurity has a reputation for being costly and complex. This means that a formal cybersecurity programme can feel financially out of reach for many SMEs.

So what can be done to help SMEs better protect themselves? We'll look at a few options in the next section.

What can SMEs do to better protect themselves?

Fortunately, many of the most effective things a small business can do to protect itself are simple. And few require expensive experts or tools. Here are just a few examples.

Start patching and updating software regularly

We bang the patching drum a lot at CyberSmart. Regular readers of our blog will have noticed we mention it at every possible opportunity. But, as repetitive as it might be, there's a very good reason behind our love affair with patching.

Regularly updating software and operating systems is the easiest, most time-efficient way to improve your cybersecurity. Even the best software becomes outdated or develops gaps and, when it does, cybercriminals suddenly have an easy route into a business.

Fortunately, avoiding the worst is incredibly easy and it shouldn't take more than a couple of minutes each month. All it requires is that employees check now and then for any new updates to tools and software you use. Or, for an even easier solution, simply turn on auto-updates in your device's settings, and you won't even have to think about it.

Create a password policy

Creating a secure password policy is by far the simplest tool for improving your security. Most of us know the importance of strong passwords, but that doesn't stop us from using the same easily-guessable phrase we've been using since 2001 for everything. We're only human after all.

The problem is this poses a huge security risk. It only takes a cybercriminal to crack one insecure password in your business for disaster to strike. But the good news is fixing it is simple.

Set up a password policy and ensure everyone in the business follows it. Often, it doesn't take much more than a well-worded email and a few friendly nudges to get everyone on board.

What should go in the policy? Well, a strong password policy should have four key points:

- Use complex passwords, we recommend the NCSC's 'three random words' approach
- Change passwords regularly
- Set up different passwords for different accounts, tools and software. If you struggle with remembering them, consider using a secure password manager tool like LastPass or 1password
- Use multi-factor authentication (MFA) wherever possible

Use Encryption

Encryption is one of those technologies that everyone has a vague notion they should be using. However, many of us get put off by the misconception that it's difficult to set up or hard to understand if you're not a techy type.

In reality, this couldn't be further from the truth. You probably already use encryption a lot in your daily life, you just don't know it. Ever sent a message using WhatsApp? That's encryption. Bought something from a web store? Encryption.

We won't go into exactly how it works (if you'd like to know more we have a whole blog on the subject) but, essentially, encryption randomises data so that only an authorised recipient with a key can see it.

Due to the complexity of the randomisation process, encryption is near impossible to break so it offers a level of security passwords alone can't match. Better still, once you've set it up and are used to using it, it's unlikely you'll ever have to think about it again.

Budget for cybersecurity spending

Given the risks, you would expect cybersecurity to be top of most businesses' budgeting lists. However, that's often not the case. It's not hard to see why; if you're an SME performing financial wizardry each year just to keep things ticking over, cybersecurity can feel like a 'nice to have' rather than a priority. It's this that leads to many smaller businesses making do with anti-virus and little else.

However, this needs to change. Cybersecurity needs to become an integral part of yearly budgets, in much the same way as operational costs or business insurance.

Get Cyber Essentials certified

The UK government's Cyber Essentials covers everything a business should do to protect itself from cyberattacks. Think of it as 'cyber hygiene' – a bit like washing your hands, brushing your teeth or wearing a face mask.

The scheme assesses five key criteria:

- Is your internet connection secure?
- Are the most secure settings switched on for every company device?
- Do you have full control over who is accessing your data and services?
- Do you have adequate protection against viruses and malware?
- Are devices and software updated with the latest versions?

According to research from Lancaster University, simply being certified can help reduce a business's cyber risk by up 98.5%. And, it's a great way to demonstrate to new customers and partners that you take cybersecurity seriously – helping you grow as well as stay safe.

Build clear, easily accessible cybersecurity policies

This is the most important step on this list. If your people aren't aware of which behaviours are harmful, they can't correct them. Ensure all security policies for workers are clear, easy to follow and stored somewhere everyone can find them. If you don't have a cybersecurity policy, now's the time to draft one.

Alongside this, work to foster a culture of communication. That way, employees will feel comfortable asking for help with anything they don't understand and reporting anything suspicious to internal security teams. All too often, security mistakes are made because staff feel 'silly' raising their concerns.

Use a VPN

Use a Virtual Private Network (VPN) for all remote work. If your employees are using public networks or their home router it's likely to be far less secure than your office network. According to a report from BitSight, home office networks are 3.5 times more likely than corporate networks to be infected by malware.

A VPN can help you counter this by creating a secure connection to business systems and data, from wherever your staff choose to work.

Take out cybersecurity insurance

Cybersecurity insurance uptake is extremely low among SMEs. Just 13% of those surveyed by the DCMS had a specific cyber insurance policy. Much like budgeting for cybersecurity, this needs to change.

Cyber insurance can provide a vital last line of defence for small businesses against cybercriminals. It could even be the difference between staying in business or not. What's more, many insurers will help you with incident response and cleanup.

Training, training, training

Research suggests that 90% of cyber breaches can be put down to human error. Or, in simpler terms, if your employees aren't aware of what cyber threats look like, they're much more likely to fall foul of them.

The best way to beat this is through training. Training can help your people better recognise and understand the threats they face. And, more importantly, learn how to counter them.

What this training looks like will depend on your staff and their knowledge gaps. For some businesses, this means starting with the basics. Meanwhile, in others, training addressing specific weak spots in employee knowledge will prove the best route.

Get in touch

68 Hanbury Street
London
E15JL
T: 020 7993 6990
E: hello@cybersmart.co.uk

www.cybersmart.co.uk