CyberSmart

STRENTHENING YOUR DIGITAL DEFENCES

The SME's guide to cybersecurity on a budget

cybersmart.co.uk

Contents

INTRODUCTION

Cybersecurity isn't optional

SMEs suffer more than most during periods of economic downturn. Faced with rising costs and shrinking profit margins, business owners have no choice but to reduce operational expenses to keep their businesses afloat. And cybersecurity budgets are often first on the chopping block.

Many business leaders see any cybersecurity investment beyond the basic tools that come with Microsoft Windows as optional. A luxury, like a company holiday. But no matter what industry you work in, cybersecurity is business critical.

Cutting your cybersecurity budget is one of the biggest mistakes you can make. After all, you wouldn't remove the locks on your office doors to save money, would you? The idea that robust cybersecurity comes at a premium persists, but perceptions are changing.

Read on to discover why cybersecurity is vital for SMEs during a recession, the common threats to be aware of, and how to get maximum value from your cybersecurity budget.

DID YOU KNOW?

39% of UK businesses identified a cyberattack in 2022.

GOV UK

CYBERCRIME AND RECESSION

Why cybercrime goes up when the economy goes down

Studies show a clear relationship between economic instability and an increase in cybercrime. At the height of the 2009 recession, the UK saw a 40% rise in cyberattacks. The question is, why?

Corporate cutbacks

One of the biggest issues with reducing your cybersecurity budget is that it makes you more vulnerable to online threats. Cybercriminals are opportunistic. They know that many businesses will slash their cybersecurity budgets during a recession, and like any successful predator, they're quick to exploit that weakness.

DID YOU KNOW?

Cybercrime increased by 40% in the UK at the height of the 2009 recession

CSO

Similarly, staff redundancies can increase the pressure on employees. Stressed employees make more mistakes and are more likely to cut corners to stay on top of their mounting workload. Patch management can also suffer as the people responsible for monitoring, maintaining, and updating business systems are no longer around. This makes them the perfect target for social engineering attacks, like phishing emails, which work by generating a sense of panic or urgency to trick the victim into clicking on a spurious link or handing over their credentials.

Unemployment

Cybercriminals aren't immune to the effects of a recession. During periods of recession, cybercriminals often step up their efforts to protect their finances amidst rising costs and unemployment.

It's easy to demonise hackers as predators who prey on less tech-savvy people or vulnerable businesses. But not all of them are career criminals. For example, a software developer who suddenly finds themselves unemployed may turn to cybercrime to make ends meet. Or an ex-employee may steal sensitive business data and sell it on the dark web to make some quick cash – possibly in retaliation for being made redundant.

Even non-techies can get in on the act, thanks to the growing trend of cybercrime-as-a-service. The ransomware affiliate marketplace, for example, allows people to execute ransomware attacks using existing tools that require little or no expertise to use. In return, they earn a percentage of the money gained from the attack.

What is ransomware as a service?

Ransomware as a service allows users – known as affiliates – to execute cyberattacks using pre-built software tools. Affiliates don't need any technical knowledge or specialist tools. They simply pay a one-off fee or a monthly subscription to gain access to the software.

Affiliates earn a percentage of the gains on each successful attack, while the ransomware's author incurs less personal risk by distancing themselves from the attack.

The continuity imperative

SME business owners must make many tough decisions in a recession. They'll do anything to keep their business afloat, and that makes them the perfect target for ransomware attacks.

If they're struggling financially, many businesses will simply pay the ransom because it's better than the alternative: prolonged disruption, lost revenue, and public disclosure of potentially sensitive customer information. Cybercriminals know this, and deliberately target vulnerable SMEs.

CYBERSECURITY FOR SMES

Why every business needs cybersecurity

Cybercrime is on the rise

Cyberattacks are becoming more frequent and easier to launch. Automated tools and the ransomware as a service model mean perpetrators don't need in-depth technical knowledge to execute a successful attack. And with SMEs conducting more of their business online, they're more vulnerable than ever.

DID YOU KNOW?

31% of UK businesses in a recent government survey said they were attacked at least once a week in 2022

GOV UK

Hackers don’t discriminate

A common misconception among SMEs is that they’re too small to attract attention. It isn’t worth the hacker’s time or resources to launch the kind of sophisticated attack you see on the news at a small business. So, they think they can get away with the most rudimentary defences. This is true to an extent, but these aren’t the attacks you should worry about.

Opportunistic attacks are far more common, and cybercriminals often target SMEs specifically because they don’t have the expensive and rigorous cybersecurity framework of a Fortune 500 company. To a hacker, SMEs are low-hanging fruit.

The human element

What do you picture when you think about cyber threats? Chances are, it's a hooded youth sitting in front of a monitor in a dingy basement, forcing their way into a corporate system through a combination of skill and persistence. It's a popular image, but one that doesn't consider the human element of cybersecurity.

Human error is one of the biggest causes of data breaches. This could be a careless employee who left their work phone unlocked on a table in Starbucks when they popped to the toilet or downloaded pirated software harbouring malware onto a company laptop. Disgruntled employees may also deliberately leak company data in retaliation for being made redundant.

Then there are social engineering attacks that target humans instead of computer systems to steal business data, encrypt files, or install malicious software on corporate networks.

DID YOU KNOW?

82% of data breaches involve a human element

VERIZON

Every business relies on tech

No matter your industry, you have some form of online presence. Even a one-person consultancy firm will have a business email address, if nothing else. And without proper protection, that makes them a potential target.

When we say proper protection, we don't mean installing the most advanced antivirus software on the market or hiring an in-house cybersecurity team. Often, attacks happen because businesses run on outdated software and unpatched systems, resulting from poor cyber hygiene. A successful attack can have serious consequences that impact the business and its customers. For SMEs that run almost exclusively on third-party apps, it could even mean going out of business.

Supply chain risks

77% of SMEs are part of a supply chain. Yet few businesses evaluate their suppliers' cybersecurity controls and strategies during the tender process.

This is a problem because supply chains have become a popular target for cybercriminals. As demonstrated by high-profile incidents like the SolarWinds attack of 2020, all it takes is one weak link in the chain to put you and other connected businesses at risk.

DID YOU KNOW?

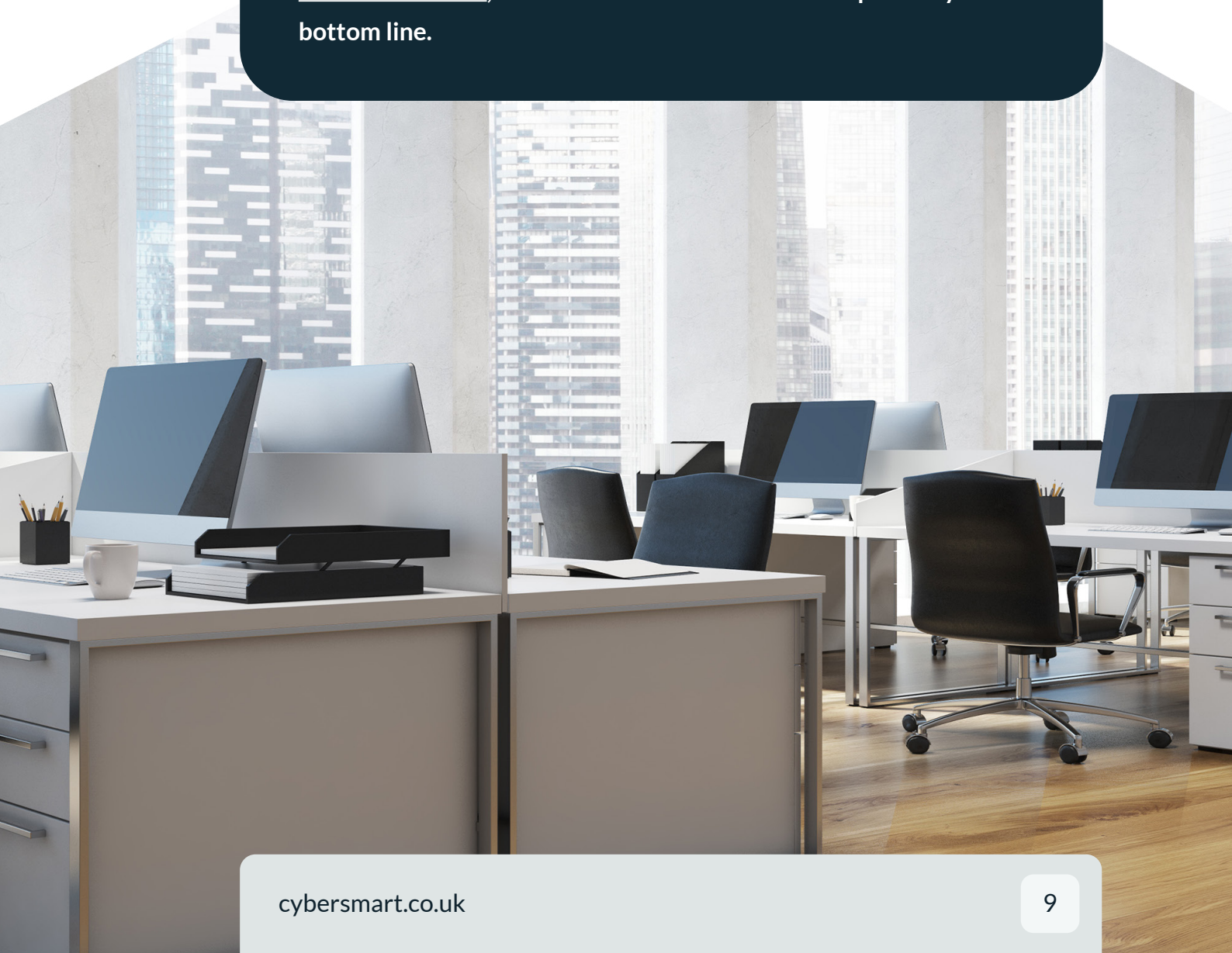
Only 13% of businesses assess supplier risks posed by their immediate suppliers

GOV UK

How much does a Cybersecurity breach cost?

According to the latest government statistics, the average cyberattack costs UK SMEs £4,200. This figure includes costs associated with recovering stolen or encrypted data and lost revenue due to prolonged disruption.

However, this estimate doesn't factor in potential financial penalties or the reputational damage that may follow an attack. 19% of consumers won't shop with an e-commerce store that's suffered a breach, and this can have a noticeable impact on your bottom line.



COMMON CYBER THREATS

The 4 biggest cyber threats to SMEs

#1 Phishing

A popular form of social engineering, phishing attacks trick people into handing over information or installing malicious software on their computers. Scammers achieve this by creating panic or impersonating a person or business the victim recognises.

Examples of Phishing

Your computer is at risk! Click the link below to install the latest security update.

Hi, I need to complete a wire transfer but I'm in an all-day meeting. Can you please send £5,000 to account number xxxx, please?

#2 Hacking

Hacking describes a range of attacks in which a hacker breaks into your computer network to access your data and systems. Hackers typically gain access through malicious software, like spyware, or via a brute force attack, like credential stuffing.

In a credential stuffing attack, the perpetrator uses stolen account information – typically a list of usernames and passwords purchased off the dark web or obtained in a previous breach – to access other accounts belonging to the victim. Some hackers use automated bots to test username and password combinations until they get a match. Credential stuffing leaves little to no trace and is highly effective because many people use the same password on multiple accounts.

#3 Ransomware

Ransomware is a type of malicious software that infects the victim's computer, typically though an email attachment or link. One of the most common and effective attack vectors, ransomware encrypts the victim's files or threatens to release confidential information unless the victim pays a ransom – usually in the form of cryptocurrency, which is harder to track.

What makes ransomware particularly nasty is that there's no guarantee the hacker will keep their word once the victim pays up. In recent years, cases of double extortion attacks – in which the perpetrator launches a second strike immediately after the first – have risen considerably. Aside from the financial repercussions, ransomware attacks can erode trust and seriously damage your brand.

> **The share of breaches caused by ransomware grew 41% in the last year and took 49 days longer than average to identify and contain.**
>
> IBM COST OF A DATA BREACH 2022 REPORT

#4 Distributed denial of service

Also known as distributed network attacks, a distributed denial of service (DDoS) attack barrages your network resources, such as web servers, with multiple requests. Because network resources have limited capacity, and the channels that connect them have finite bandwidth, DDoS attacks prevent your website from functioning correctly. This results in frustrated customers and lost revenue.

WHAT TO PROTECT AND HOW TO PROTECT IT

Key areas to focus your cybersecurity investment

Network

Your network is the gateway to your business. It's the channel that connects the disparate endpoints in the hybrid workplace, ensuring people can work effectively, no matter where in the world they are.

Once a hacker gets past your network, they have access to everything – from sensitive company and customer data to intellectual property.

How to protect your network

- Install a network firewall to filter network traffic
- Use a virtual private network (VPN) to encrypt network traffic
- Segment your network to remove single points of failure vulnerabilities
- Regularly update your router's firmware

Databases

Whether you store data locally, on the cloud, or on a combination of the two, securing your databases helps to prevent breaches. Company and customer data is an enticing target for cybercriminals, with stolen data worth millions on the dark web. Recovering or replacing stolen data isn't the only issue. Data breaches can result in hefty fines and harm your reputation.

How to protect your data

- Encrypt your data
- Install identity management software to verify access requests and ensure users can only access the data they need
- Monitor and update applications to patch vulnerabilities
- Use secure passwords and multi-factor authentication
- Configure your cloud properly – don't assume the default setup is correct!

Documents

Hackers aren't necessarily the biggest threat to your documents. Human error is the main cause of data loss, according to experts. For example, accidental deletion or file corruption. Whatever the reason, it takes time and resources to recover or recreate lost documents that could be better spent elsewhere.

How to protect your documents

- Backup your documents regularly using the 3-2-1 rule
- Set permissions to prevent accidental deletion
- Password protect sensitive documents

Employee devices

Hybrid working allows employees to work effectively from anywhere. In the office, at home, during the morning commute. All they need is a device, a stable internet connection, and access to the company network. However, this freedom and flexibility adds an extra layer of complexity for IT teams.

The most rigorous cybersecurity policy in the world can't stop an absent-minded employee from leaving their laptop on a busy commuter train. If the device falls into the wrong hands, it can leave your business open to attack.

How to protect your devices

- Use secure passwords and multi-factor authentication to prevent unauthorised device and account access
- Regularly update your antivirus software to protect against common cyber threats
- Enable remote data wiping so administrators can delete sensitive data from lost or stolen devices
- Install full-disk decryption on company devices so hackers can't access the hard drive without the password
- Run cybersecurity awareness training to instil best practices in your team

HOW TO KEEP CYBERSECURITY COSTS IN CHECK

3 tips to maximise your cybersecurity budget

- Evaluate cybersecurity solutions thoroughly before buying
- Consolidate your tools
- Get Cyber Essentials certified

#1 Evaluate cybersecurity solutions thoroughly before buying

Investing in the best cybersecurity solutions doesn't mean you're bulletproof. Everything from the assets you want to protect to the size of your business and the industry you work in will determine the best solution for you.

Before committing to a solution based on the elevator pitch, look deeper at the:

- Features it offers
- Management and maintenance requirements
- Monthly costs
- Support services

For example, investing in a cutting-edge, automated solution will be a waste of money if you don't have the internal expertise to configure the software properly or keep on top of updates.

#2 Consolidate your tools

More isn't always better when it comes to cybersecurity. Research from the Ponemon Institute found that enterprises with over 50 cybersecurity tools are less able to detect and respond to attacks than those with fewer solutions.

It's simple, more tools means more complexity. Multiple providers. Multiple invoices. Multiple onboarding and training sessions for each tool. Additionally, using multiple cybersecurity tools increases the number of potential weaknesses in your security framework, as you'll need to manage and update each solution separately.

There's a financial cost to using multiple tools, too. Although different solutions have different capabilities, some features will inevitably overlap. This essentially means you end up paying for the same service twice.

It's impossible to find a single solution that has all the features you require. But consolidating your cybersecurity framework into as few tools as possible will help to reduce costs without compromising your business.

#3 Get Cyber Essentials certified

Effective cybersecurity is about creating a solid baseline that protects your SME against the most common threats – not creating an action plan for every eventuality. That's what the government's Cyber Essentials scheme aims to do.

Cyber Essentials provides stronger security without the cost of hiring internal experts. It's built around five simple technical controls:

1. Use a firewall to secure your internet connection
2. Choose the most secure settings for your devices and software
3. Control who has access to your data and services
4. Protect yourself from viruses and other malware
5. Keep your devices and software up to date

Simply being certified can reduce cyber risks by up to 98.5%. In most industries, Cyber Essentials is entirely optional. However, it's mandatory for companies bidding on government contracts in the UK.

How much should you put in your cybersecurity budget?

Unfortunately, there's no universal answer to this question.

The size of your cybersecurity budget will ultimately depend on multiple risk factors, including the size of your business and your industry. For example, businesses that operate in the healthcare and financial services sectors must adhere to HIPAA and PCI-DDS regulations respectively, which inevitably affects cost.

According to a 2020 Deloitte survey, US businesses spend roughly 11% of their IT budgets on cybersecurity. However, SMEs have fewer resources at their disposals than enterprises. So, it's better to think about your cybersecurity budget in terms of potential ROI rather than a percentage of your budget. That is, how much you stand to lose if you were the victim of a cyberattack vs the cost of protecting your business.

Active Protect from CyberSmart

No business is immune to cybercrime. While hackers are more likely to target global brands and multinational corporations than an SME with five employees, opportunistic criminals won't pass up an opportunity when they see one.

The challenge for SMEs is that off-the-peg cybersecurity options are built with large businesses in mind, making them expensive and complicated to manage. That's why we developed Active Protect.

Active Protect secures every employee device that touches your data. It monitors your network 24/7 to identify active threats, providing easy-to-understand recommendations to help you fix vulnerabilities – without the need for expensive software or an in-house team.

In addition, we provide support and training to give you the confidence to take control of your cybersecurity.

Learn more about Active Protect