CyberSmart

CyberSmart

SME cost of living crisis report

How the cost of living crisis is affecting UK SMEs

Economic storm clouds have been gathered overhead for some time now. With interest rates at 15-year highs, inflation running rampant, and the cost of just about everything mounting, every business – from FTSE 100 monoliths to local micro firms – is being forced to make difficult choices.

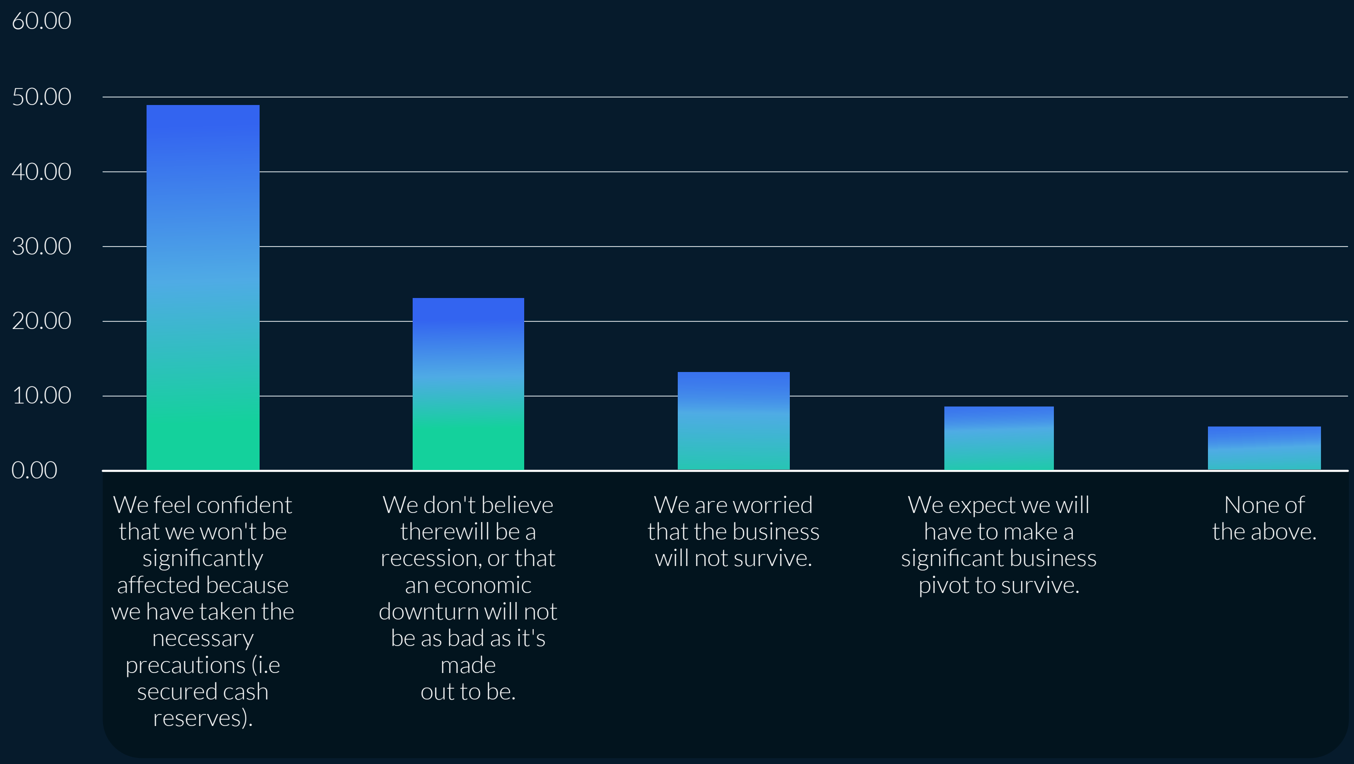
But how are the UK's small businesses weathering the storm? What's the impact on their people? And what does the cost of living crisis mean for their cybersecurity? To get the answers to these questions and more we tasked **Censuswide** with surveying 1,000 UK SMEs.

How are SMEs weathering economic uncertainty?

It's no secret that an economic downturn often disproportionately affects SMEs. During the 2008 recession, UK small businesses reported a **54% drop in demand** (its lowest point since 1991) with many firms simply folding under huge pressure.

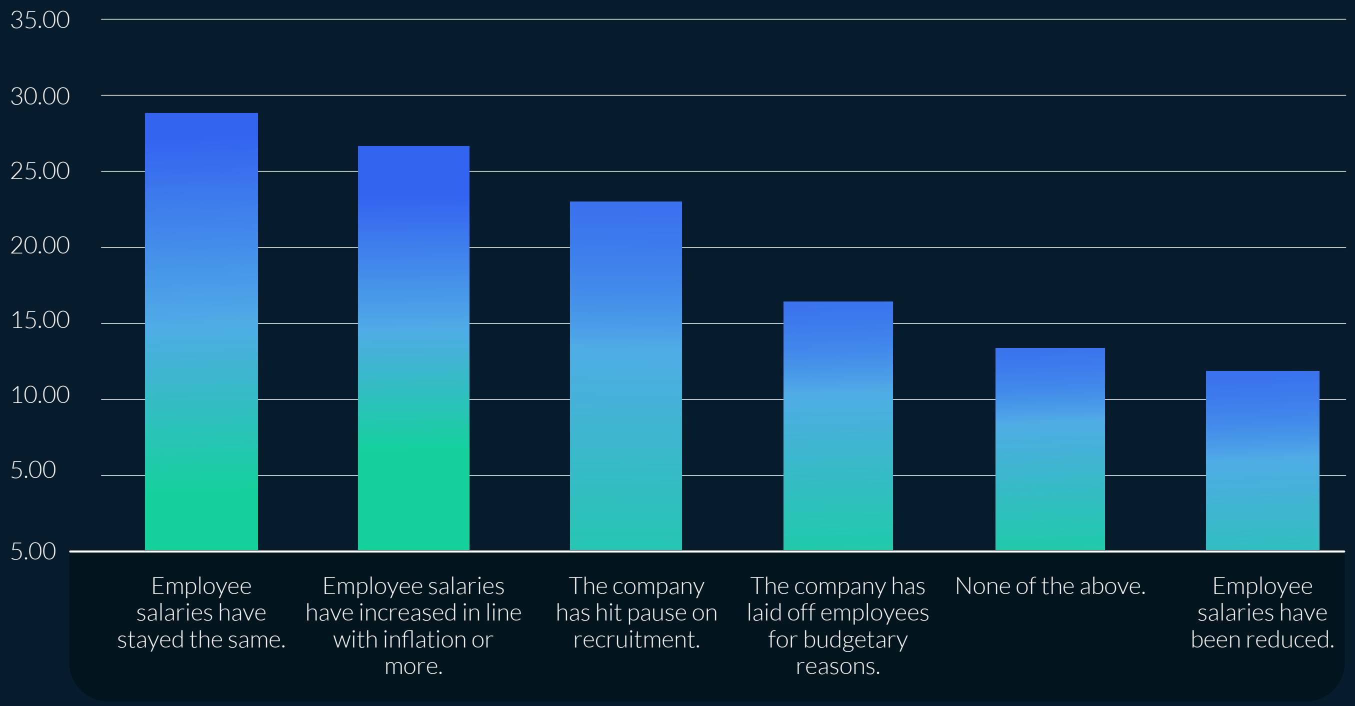
We might currently be some way from the apocalyptic scenes of 2008, but it's clear SMEs are facing some of the same financial pressures. Although 50% of SMEs feel confident they won't be significantly affected by economic uncertainty, a substantial proportion of respondents are fretting about the future. Over 1 in 5 (21%) small businesses are either worried about the survival of their business (12%) or expect to make a significant pivot to survive (9%).

Q4. Which of the following best applies to the general sentiment within the business towards the current economic uncertainty/cost-of-living crisis?



In light of this economic uncertainty, small businesses are being forced to make difficult choices. Almost 1 in 3 employers (29%) admit that employee salaries have stayed the same: in effect, resulting in a decline of real wages to accommodate for inflation. A further 11% have even gone so far as to reduce salaries. What's more, nearly a quarter (24%) of SMEs have hit pause on recruitment, while 16% have laid off employees for budgetary reasons.

Q9. In the context of the current economic uncertainty/cost of living crisis, do any of the following statements apply to your workforce? (Tick all that apply)



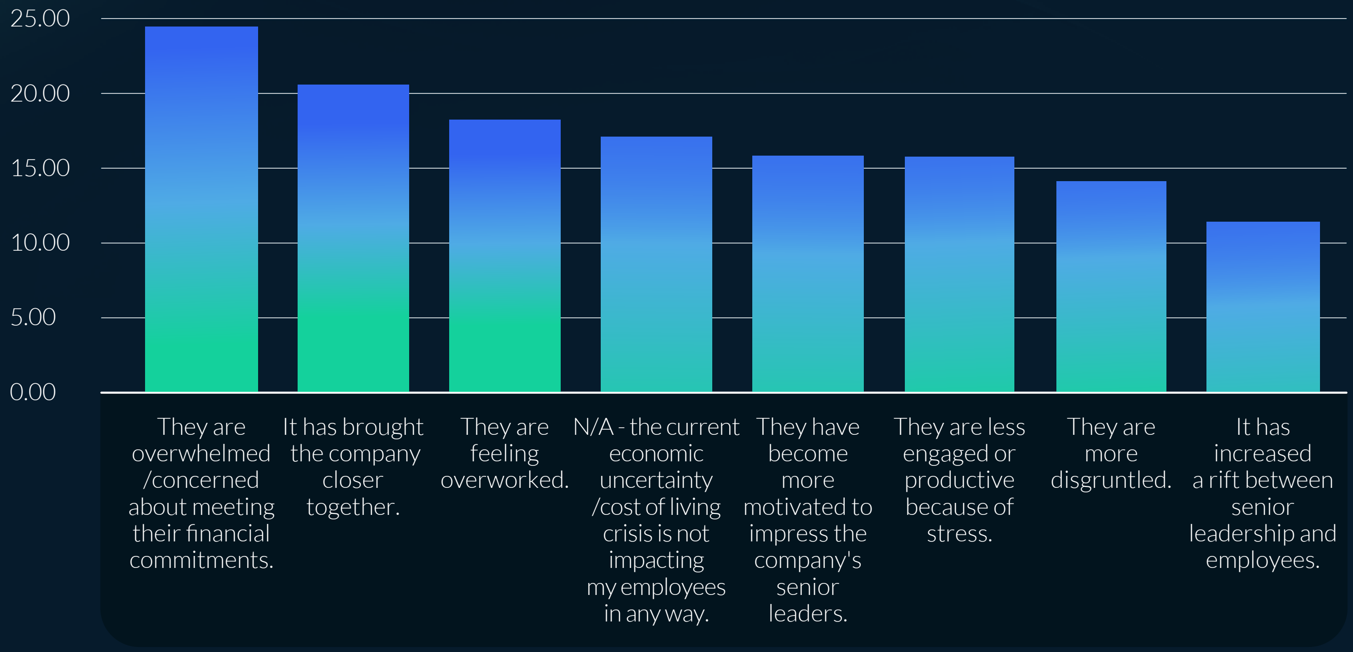
These budgetary limitations are having a huge impact on SMEs' employees and cybersecurity, more on which in our next section.

What's the impact of reduced budgets on SME's staff?

Anyone who has worked in a small business during a recession will tell you that it's often a stressful time, with work life coloured by financial worries, stretched teams and fears of redundancy.

Therefore, it's perhaps unsurprising to find that our survey results bear this out. 1 in 4 employers (24%) are finding that their staff are overwhelmed or concerned about meeting their financial commitments, while nearly a fifth (18%) are feeling overworked.

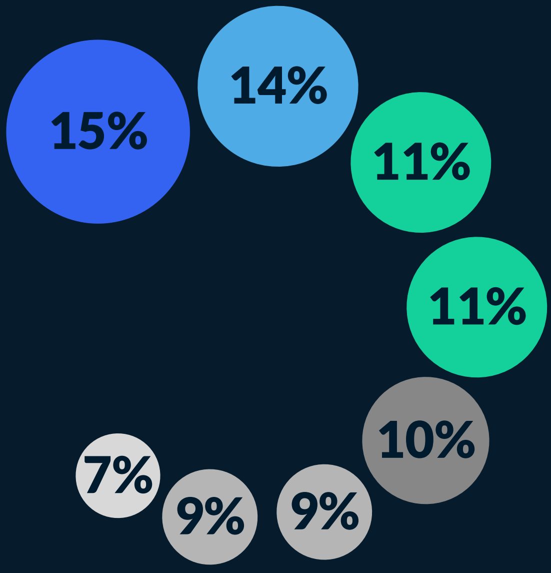
Q9a. How, if at all, is the current economic uncertainty/cost of living crisis impacting your employees? (Tick all that apply)



What's more, this could be having an impact on UK business's already slow productivity growth. 16% of SMEs believe that staff are less engaged or productive due to stress. Meanwhile, 14% think they are more disgruntled and 11% have noticed an increased rift between senior leadership and employees (more on this in the next section).

So far, nothing particularly surprising. However, what is surprising is the lengths some senior leaders within SMEs would countenance to ensure the survival of their business.

Lengths SME senior leaders would go to ensure the survival of their business



15%	would commit accounting fraud and lie to bankers/investors to secure funding or commit tax fraud/evasion
14%	would cut employee salaries and/or benefits
11%	would leverage proprietary information from partners/clients such as selling off the data
11%	would neglect compliance requirements due to the additional costs they incur.
10%	would engage in cybercriminal activity such as hitting a rival company with a cyberattack
9%	would mortgage their house
9%	would leave fake online reviews about the company and/or about competitors
7%	would engage in bribery

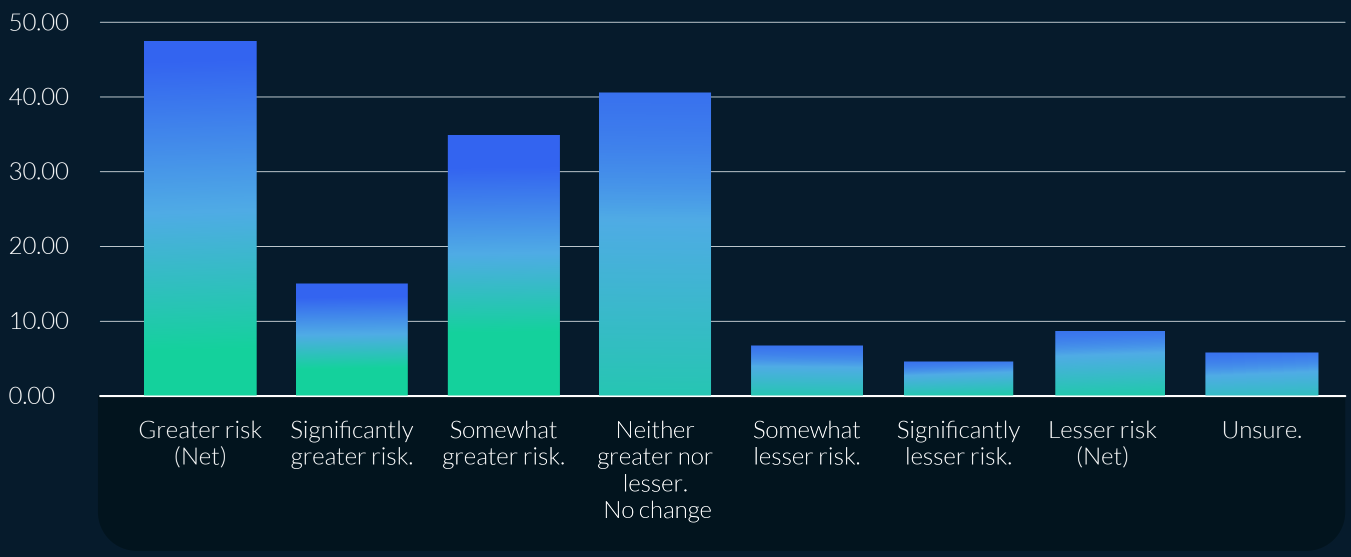
Of course, these findings should be taken with a healthy dose of salt. The scenarios presented do represent the extreme end of the spectrum. Nevertheless, the fact that a small minority of senior leaders would even consider taking such drastic measures reveals something about the state of worry within some small businesses.

How is the cost of living affecting SMEs' cybersecurity?

It's one of the immutable laws of modern economies that fiscal strife tends to be followed by an increase in cybercrime. The most infamous example of this is the 2008 recession, which saw a **40% increase in cyberattacks at its height**.

Unsurprisingly this appears to be something SME leaders are aware of. Nearly half of UK SMEs (47%) believe they are at greater risk of a cyberattack since the onset of the cost-of-living crisis.

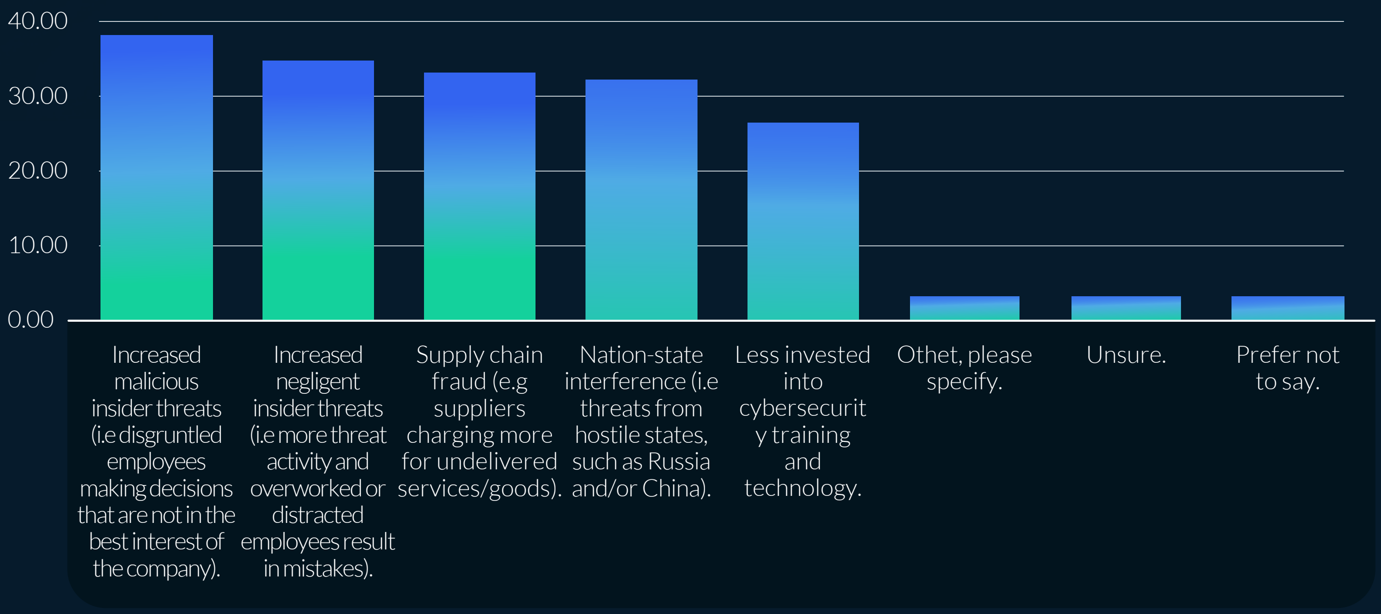
Q5. Do you believe your company is at greater or lesser risk of a cyber attack since the economic uncertainty/cost of living crisis?



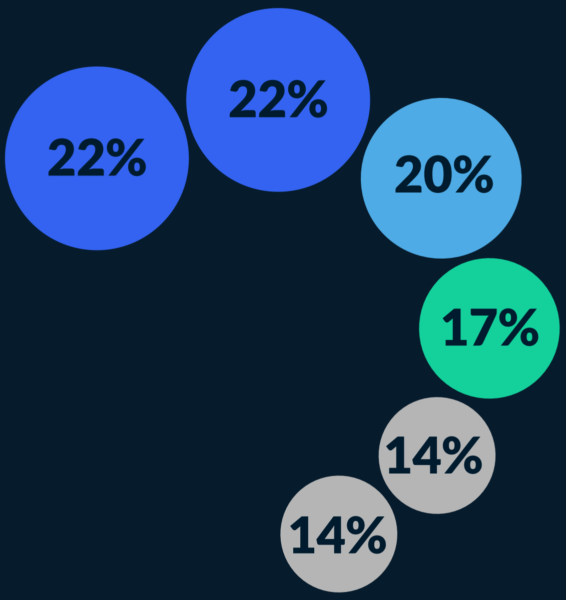
However, what is remarkable is why SMEs believe the risk has increased. SME leaders do attribute some of this rise to external forces, with 32% blaming higher rates of **supply chain fraud** and 31% expressing concern about nation-state interference from hostile countries such as Russia and China. But nestled in amongst the factors we'd expect to see small businesses worried about, is a growing concern about insider threats.

38% of respondents believe the rise is due to increased malicious insider threats. For example, disgruntled employees making decisions that are not in the best interest of the company. And 35% put the increase down to negligent insider threats such as overworked or distracted employees making mistakes.

Q5a. Why do you believe you are at greater risk of a cyber attack? (Tick all that apply)



Incredibly, some employers expect their employees might engage in the following activities:



22% believe employees will take on a second or third job during contractual hours

22% believe employees will be more likely to make mistakes such as clicking on a phishing link

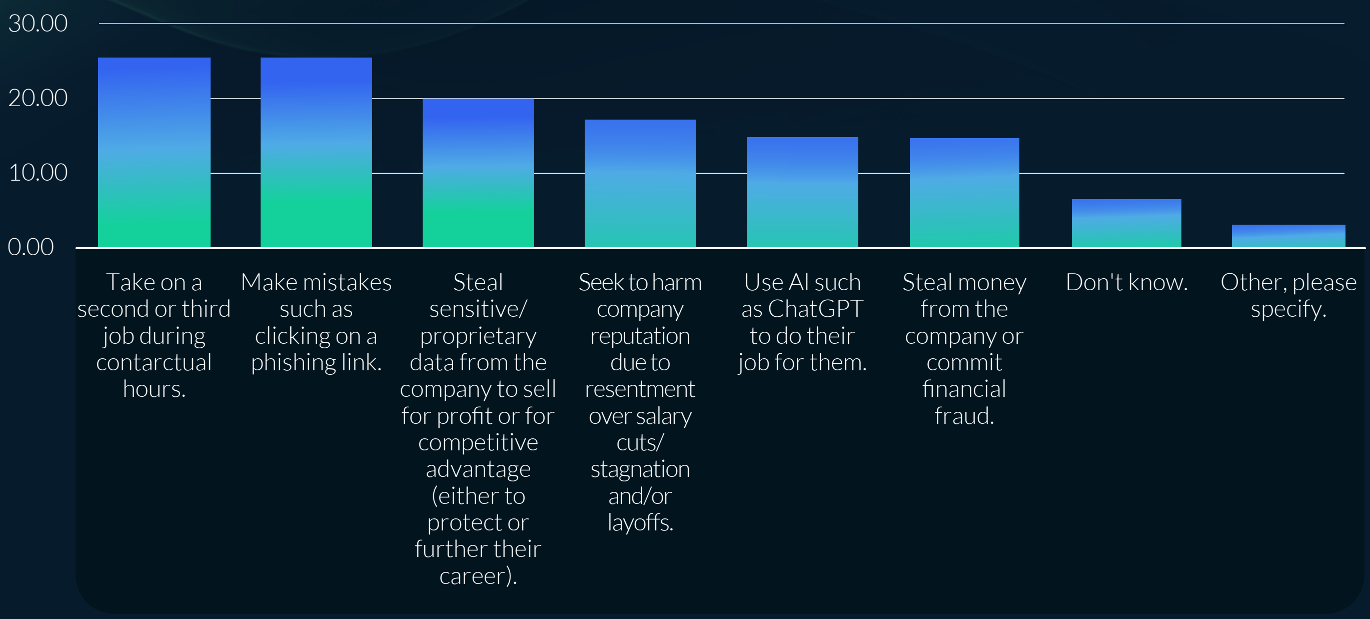
20% believe employees will steal sensitive or proprietary data from the company to sell for profit or a competitive advantage

17% believe employees will seek to harm the company's reputation due to resentment over salary cuts/stagnation and/or layoffs

14% believe employees will use AI such as ChatGPT to do their job for them

14% believe employees will steal money from the company or commit financial fraud

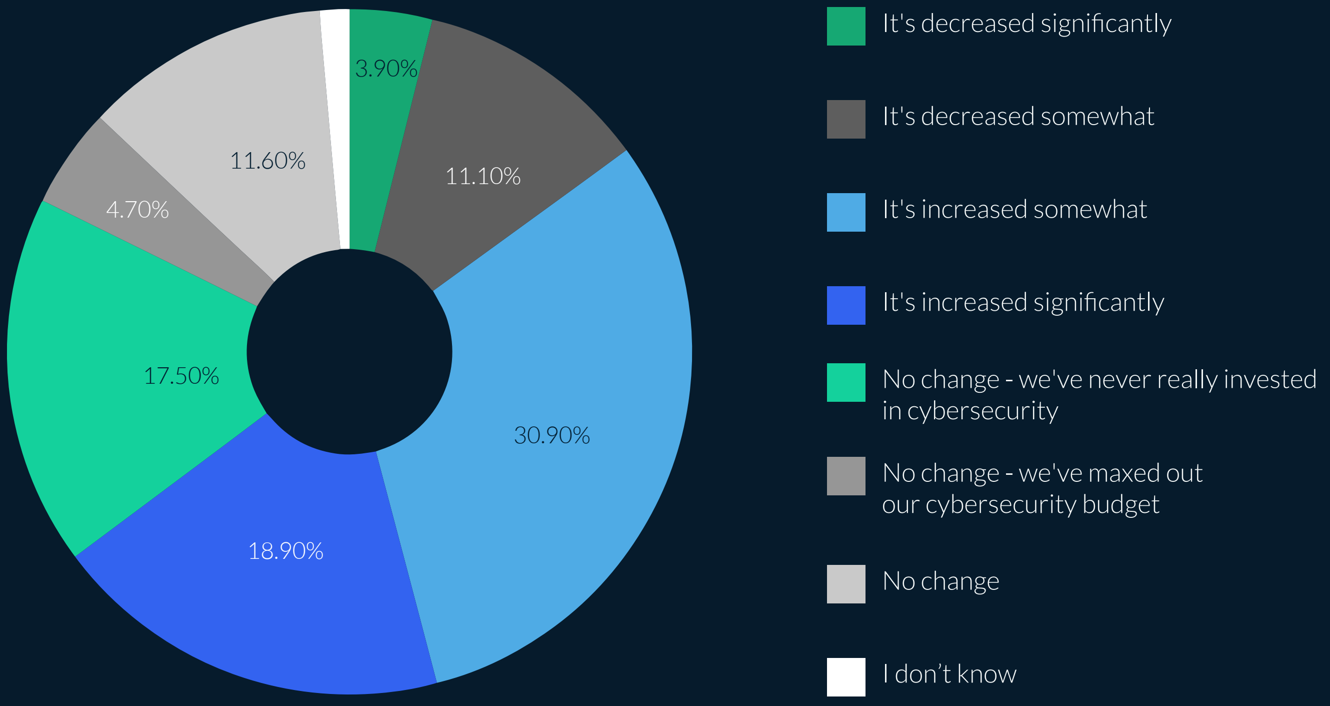
Q10. What harmful/malicious activities, if any, do you think your employees are likely to engage in if they are feeling unhappy? (Tick any that apply)



It's clear that SMEs are concerned about how the cost of living crisis is impacting their cybersecurity. With that in mind, how are current conditions affecting SMEs' investment in cybersecurity?

What is the current state of SMEs' cybersecurity investments?

Q6. How has your companys investment in cybersecurity changed since the economic uncertainty?

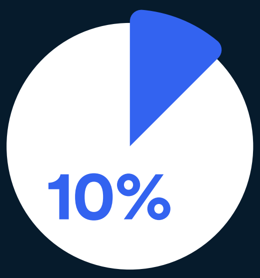


Unfortunately, this comes with a very large caveat: the number of SMEs who have decreased spending or weren't investing in their security in the first place. A third of the small businesses surveyed have either decreased cybersecurity investment or admitted to never really investing in it.

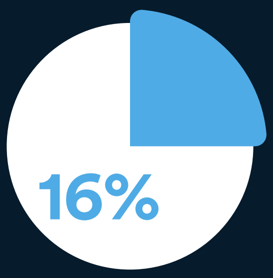
Why?

Small businesses have to be cost-conscious. Careful budgeting and knowing when to invest is key to an SME's survival. And this means many small business leaders won't invest unless they're sure the payoff is worthwhile.

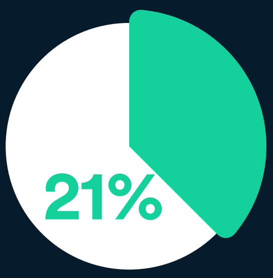
Unfortunately, it appears some SMEs still feel that cybersecurity isn't a priority, with 42% stating that they don't believe investing in cybersecurity is worth it. Among the reasons for non-investment given:



don't believe it's a priority

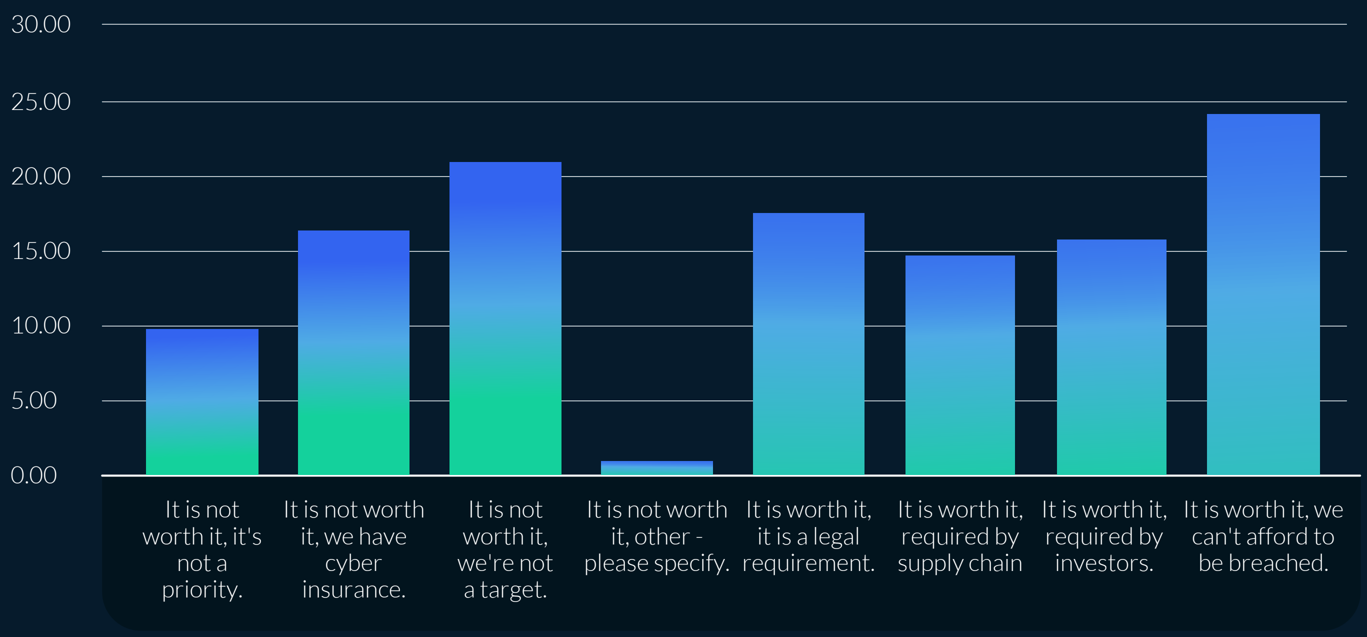


claim it's because they have cyber insurance



don't believe they are a target

Q7. For what reasons, if any, do you think it is worth or not worth investing in cybersecurity? (Tick all that apply)

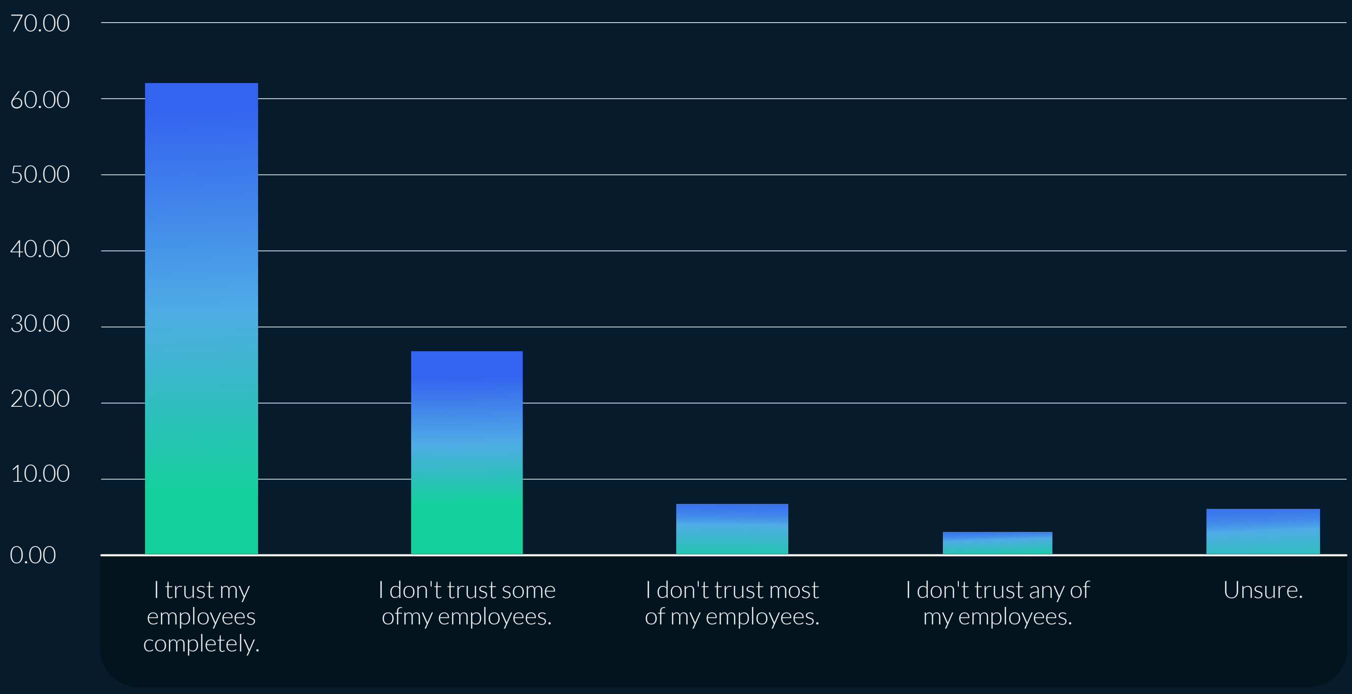


Even among those small businesses that do invest in cybersecurity, it appears that this is being driven by external pressures. 18% of those surveyed cited legal requirements as the reason for investment, 16% pressure from investors, and 15% supply chain obligations. Meanwhile, 25% recognised they couldn't afford to be breached.

Is a lack of cybersecurity investment in training and other security measures the reason behind distrust toward employees?

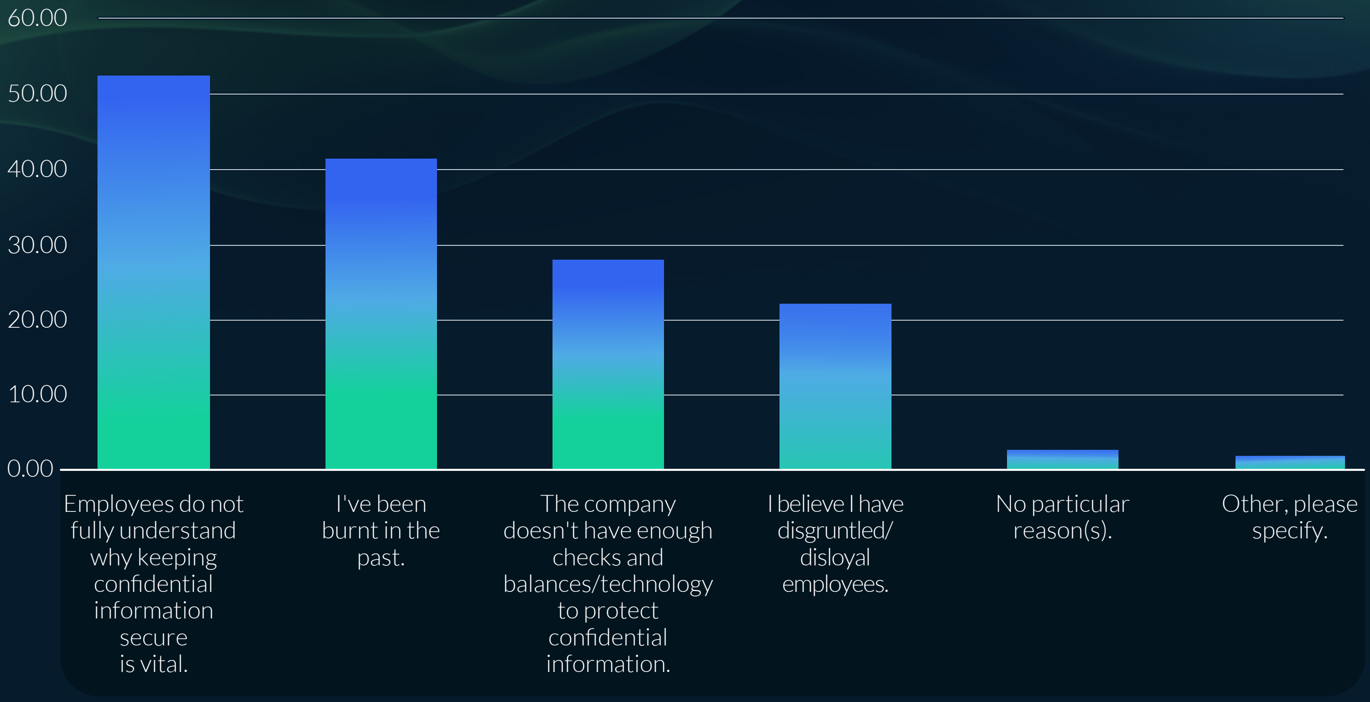
As discussed earlier, many SME leaders seem to be particularly worried about the actions of employees during the financial downturn. And this extends to cybersecurity. A third of SME leaders do not trust some, most or all employees with confidential information.

Q1. To what extent do you trust your employees with confidential information?



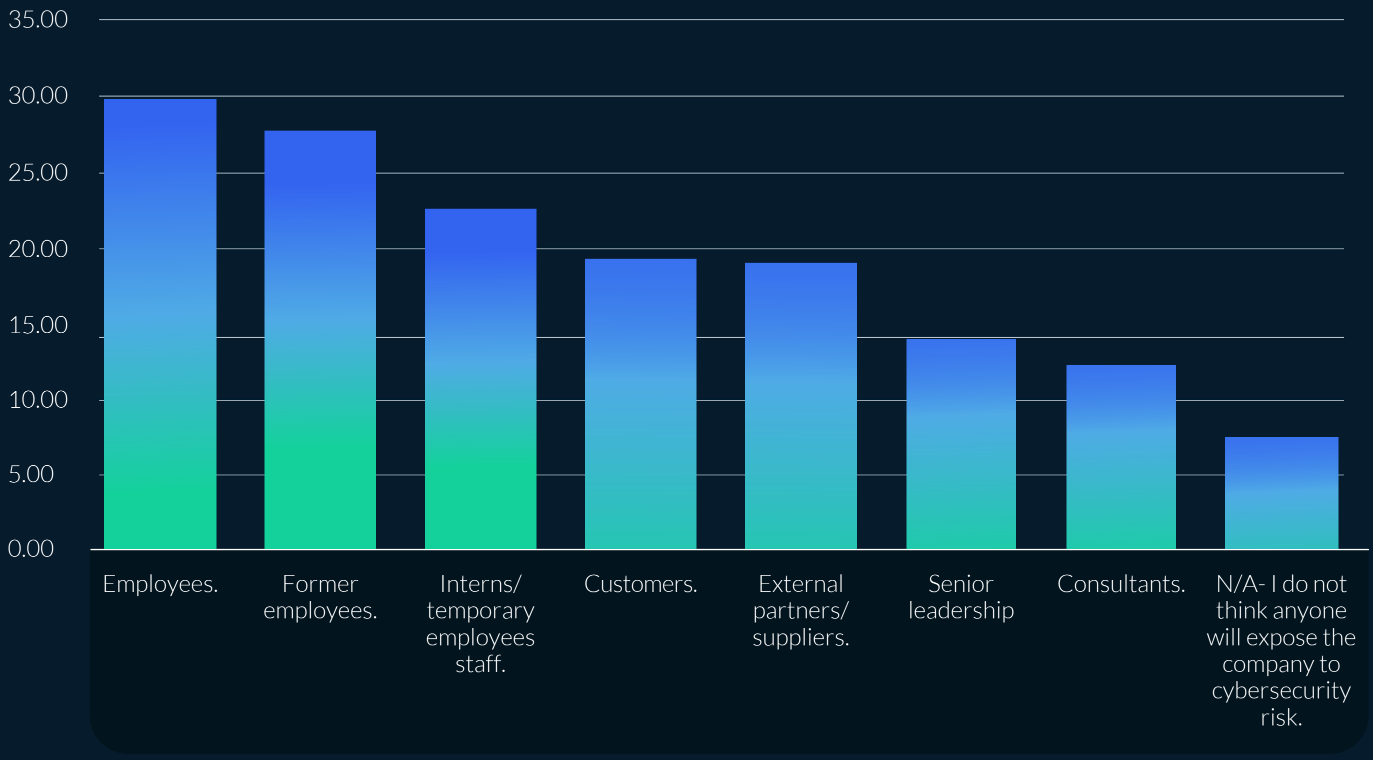
However, what makes this really interesting is why. For 80% of respondents, this is because employees do not fully understand why it is important to keep confidential information secure (51%). A further 29% admit this is because the company does not have enough checks and balances, nor the technology to protect confidential information. In addition, 40% profess that their wariness is attributed to having been burnt in the past and 23% believe they have disgruntled or disloyal employees.

Q1a. Why do you not trust some or most of your employees? (Tick all that apply)



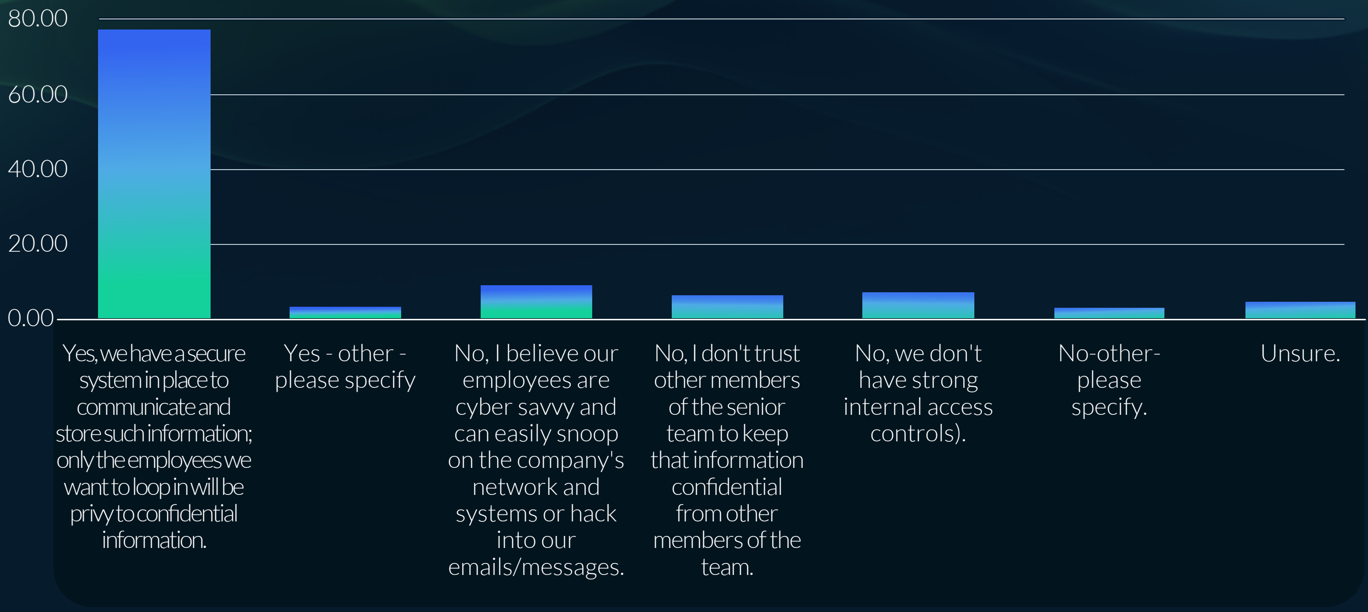
In fact, employees were ranked as the most likely to expose the company to the greatest cybersecurity risk by 30% of SME senior leaders. This was followed closely by former employees (28%), and interns or temporary staff (23%).

Q3. Who, if anyone, do you think is most likely to expose the company to the greatest cybersecurity risk? (Tick up to three)



Of the 620 SME leaders who claimed to trust their employees completely, a quarter still believed that staff posed the greatest security risk. Although, interestingly, as many as 76% of all respondents believe they, along with other members of the senior leadership team, can keep high-level meetings or confidential information private from employees.

Q2. Do you think you and other members of the senior leadership team can keep high-level meetings or confidential information private from employees? (Tick all that apply)



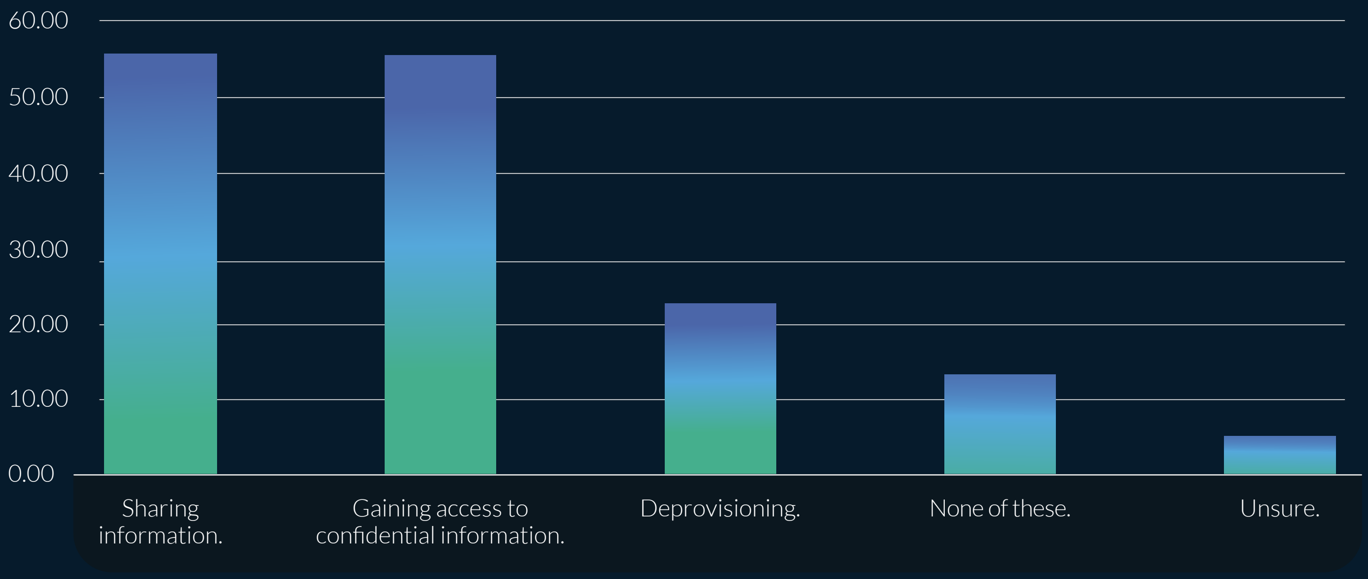
Fun Fact

7% of senior leaders and decision-makers within the UK believe their employees are cyber savvy and can easily snoop on the company's network and systems or hack into the company's emails/messages.

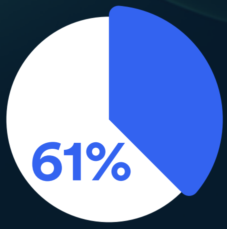
Policy problems?

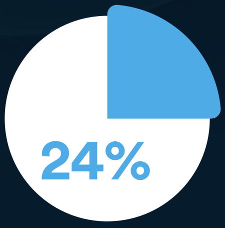
Despite senior leaders' confidence in their processes, when we dig a little further into companies' security policies this appears misplaced. Only 55% and 54% of SMEs have clear policies and procedures for sharing information and gaining access to confidential information, respectively.

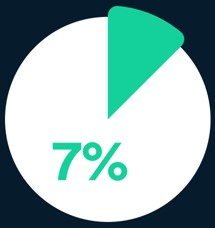
Q8. Which of the following, if any, does the company have a clear set of policies/procedures for? (Tick all that apply)



What's more, just 22% have policies and procedures for offboarding former employees, while 13% have no policies at all.







Of the **76% of respondents** who claimed to have a secure system in place to communicate and store confidential information, keeping it private from employees, only **60%** and **61%** have clear policies for sharing information or gaining access to confidential information, respectively. Moreover, only **24%** have clear policies and procedures for de-provisioning/offboarding and **7%** have none of these policies.

Of the **278 people** who said former employees were one of the greatest cybersecurity risks, only **24%** had clear policies and procedures for de-provisioning/offboarding.

How should SMEs approach the cost of living crisis?

It's clear from our research that economic hardship is impacting SMEs' ability to protect themselves. But what can small businesses do about it? Budgets are budgets, right? And senior leaders are unlikely to suddenly find large reserves of cash for investment.

Although all of the above is true, it's also true that investing in your cybersecurity doesn't have to cost the earth. Instead, it's about being smart with your investment. With the right approach, you can have complete cyber confidence without breaking the bank.

Prioritise your investments

When it comes to cybersecurity investment, there are a few areas that are 'must haves'. Without these things being nailed down, you risk opening up your business to a breach. So, in no particular order, ensure you've got the following covered.

1. Network

A network is the gateway to your business. In a positive sense, it's what allows your business to embrace hybrid working. However, it also comes with risks. If a hacker gains access to your network, they've got everything – from confidential information 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

2. Your staff

This might sound like a slightly odd one, given the findings revealed in the survey. Nevertheless, your staff are the last line of defence for your business and your biggest cybersecurity asset.

But they need to be equipped with the tools to help them counter potential attacks.

How to invest in your staff

- ✓ Have clear policies and procedures for cybersecurity and data protection, usually if people are clear on what they need to do, they'll do it
- ✓ Consider investing in basic cybersecurity training for staff. It doesn't have to be extensive or expensive. A good grounding in the basics will stand your people in good stead

3. Databases

Wherever you store your data, secure databases make for a secure business. Cybercriminals love company and customer data, which often fetches a pretty penny on the dark web and is relatively easy to steal.

And it's not just the hassle of recovery you need to worry about, data breaches can lead to fines from the Information Commissioner's Office.

How to protect your data

- Encrypt all data
- Install identity management software to verify access requests and ensure users can only access the data they need
- Set up automatic updates for all applications to patch vulnerabilities
- Use secure passwords and multi-factor authentication
- Ensure the cloud is configured in the best way for your business

4. Employee devices

It's a well-worn cliche by this point, but hybrid working really has revolutionised the way we work. Employees can now work from just about anywhere. However, this newfound freedom does bring with it some cybersecurity risks.

The most rigorous cybersecurity policy in the world can't stop an absent-minded employee from leaving their laptop on a busy commuter train or accidentally using an unsecured network on their lunch break. And these risks can open your business 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 encryption 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

5. Backups

The rationale behind backups is pretty simple: sometimes, bad things happen and, when they do, you want to be sure your most valuable assets are safe. In this case, we're talking about data, whether that's personal data, customer data, or important files.

Losing and recovering important data can be a time-consuming and costly business, but keeping data safe needn't be.

CyberSmart

How to protect your data

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

More tips

Want more tips on how to maximise your cybersecurity budget? Check out our guide to protecting your business on a budget.

Finally, consider your current cybersecurity tools. More isn't always better when it comes to protecting your business. More tools means more complexity, more applications to update, more bills to pay, and potentially more gaps in your defences.

In fact, it could even be detrimental. Research from the Ponemon Institute reveals that enterprises with over 50 cybersecurity tools are less able to detect and respond to attacks than those with fewer solutions.

We're not suggesting you should go uber-minimalist with your cybersecurity. Nor are you likely to find a tool that does absolutely everything. However, it's worth figuring out what you need and what can be dispensed with. And, wherever possible, use tools that consolidate several things.

A tool like CyberSmart is a great example of this. It's an all-in-one cybersecurity monitoring, optimisation, training and insurance solution proven to defend against the unexpected. And, while it can't do everything (you'll still need an anti-virus) it does provide your business with complete cyber confidence.