KEEPER
Cybersecurity Starts Here®

2022

# UK Cybersecurity Census Report

# Foreword

Cybersecurity is now recognised as a key priority for UK businesses. However, cybersecurity threats are evolving as risks, and the responses necessary to mitigate them, change rapidly. Staying a step ahead of bad actors is a continuous challenge and businesses—despite their intentions to do so—aren't always keeping pace.

To solve this problem, IT leaders must understand why. They need answers to questions such as, how is cybersecurity transforming? How are cyberattacks harming businesses? Where must investment in preventative training and tools be focused? Is cybersecurity being prioritised by leadership? And how does cybersecurity fit within organisational culture?

In partnership with Sapio Research, Keeper Security analysed the behaviours and attitudes of 512 IT decision makers in the UK to answer these questions and more. This report, Keeper's second annual UK Cybersecurity Census, maps the transforming landscape of cybersecurity based on these expert insights.

It provides leaders with a forensic assessment of the threats their businesses face, and details the urgent strategies necessary to overcome them.

# Executive Summary

Four key takeaways from Keeper's second annual UK Cybersecurity Census

### Almost half of IT leaders expect the number of cyberattacks, and the number of successful attacks, to increase

Cyberattacks are severely impacting businesses of all sizes and sectors across the UK. In their wake, companies are suffering severe organisational, financial, and reputational damage. IT leaders expect this onslaught to intensify over the next year. Despite this, preparation is lacking, with only a minority of organisations feeling ready to face the threat of cyberattacks. Businesses must take urgent action to protect themselves, their finances, their reputations and their employees.

### Over one-third of IT leaders lack a management platform for IT security

Despite awareness of the threats cyberattacks pose, IT leaders don't have the right tools at their disposal to defend against them. The rise of hybrid and remote work is only widening the gap between what's necessary to secure organisations, and what's available. Security around cloud and SaaS apps, as well as remote access tools, are particular areas where current tech stacks are falling short and leaving businesses exposed.

### One third of C-suite highlighted remote and hybrid work as a concern in their organisations to maintain security

The vast majority of the C-suite recognises that cybersecurity is an essential priority for their business. While this recognition is translating into healthy budgets for IT leaders, the speed at which threats are evolving may be outpacing their ability to respond. In particular, leaders are struggling to source the skilled workforce they need to keep their organisations safe. With economic uncertainty only growing, IT and broader business leaders must remain focused and committed to ensuring they have the necessary cybersecurity solutions, strategies and skill sets.

### Over half of IT leaders have been aware of a cyberattack and kept it to themselves. Lack of transparency into cyberattacks could fuel a culture of mistrust

When it comes to reporting cyberattacks to any relevant authority, there's a concerning lack of transparency. And despite training and concerns about rising threats, understanding of key cybersecurity concepts like zero-trust and zero-knowledge—by both IT leaders and the broader employee base—is limited. Organisations must invest in educating and upskilling their teams. Alongside solutions that can keep essential data protected, IT leaders must cultivate a culture of transparency and accountability so that cyber threats are fully understood by the business, and adequately responded to.

SECTION 1

# Cyberattacks

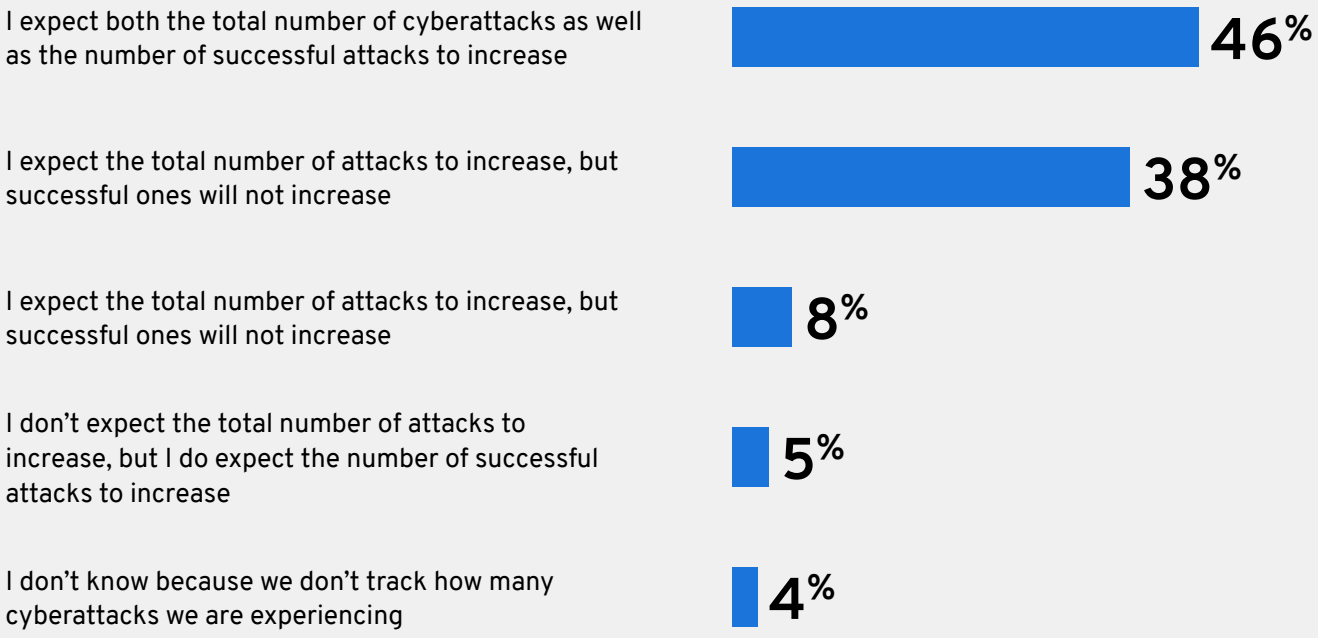
## Cyberattacks Present a Growing Threat

UK businesses face an onslaught of cyberattacks each year, with significant impact on their organisations.

The average business experiences 44 cyberattacks per year—more than three every month. Almost one in five (17%) is subjected to more than 500 attacks in a single year—that's roughly two cyberattacks every working day.

Of those, the average business faces around two successful cyberattacks each year. However, IT leaders fear the frequency of these attacks will intensify. Almost half (46%) expect both the total number of attacks and number of successful attacks to increase over the next year.

**How IT leaders expect the number of cyberattacks (successful and total) to change over the next 12 months**

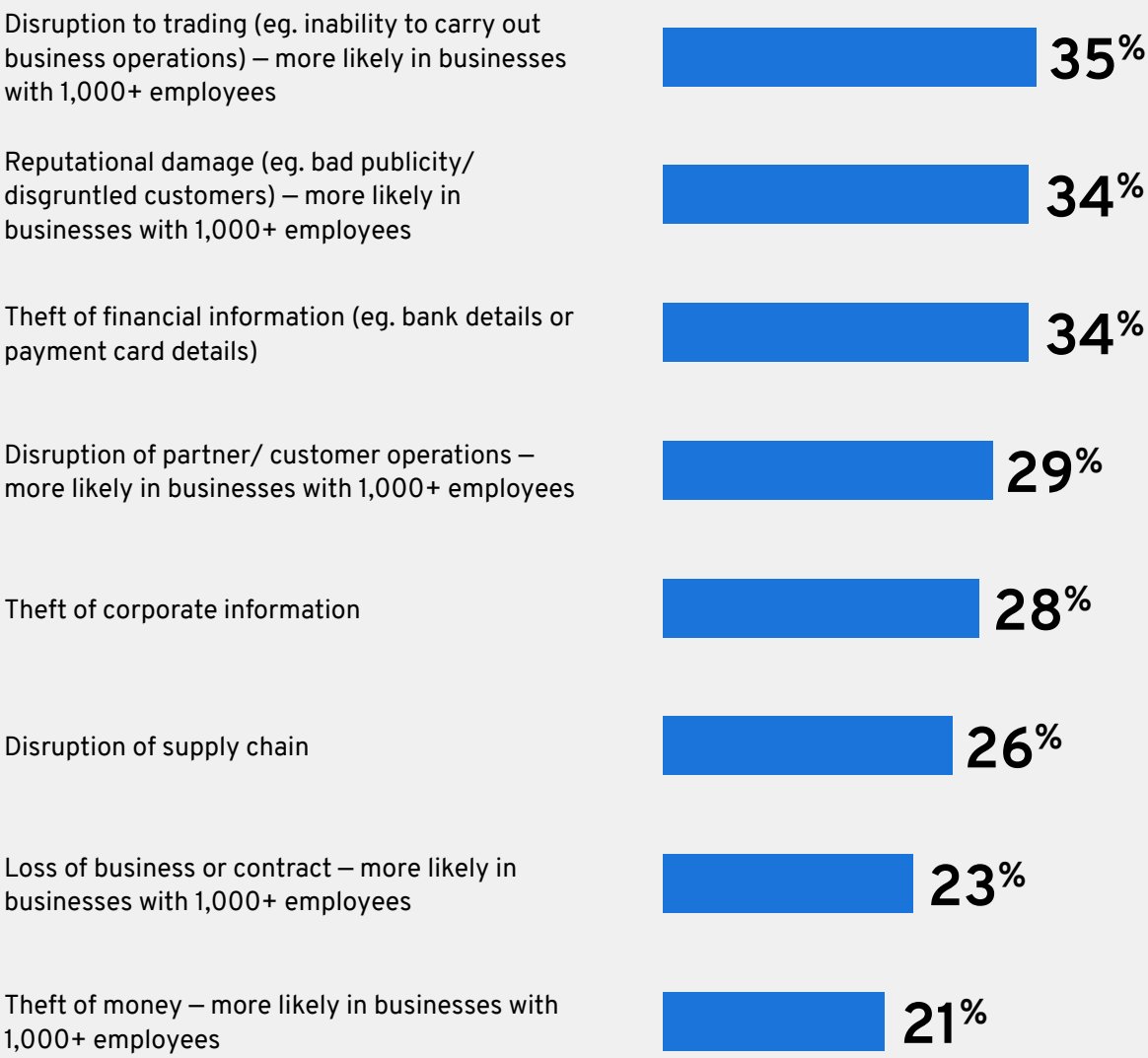


## Cyberattacks are Causing Significant Harm to Businesses

Successful cyberattacks have the potential to seriously damage businesses, bringing them to a standstill. Over one third (35%) of victims of a cyberattack report disruption to trading such as the ability to carry out business operations.

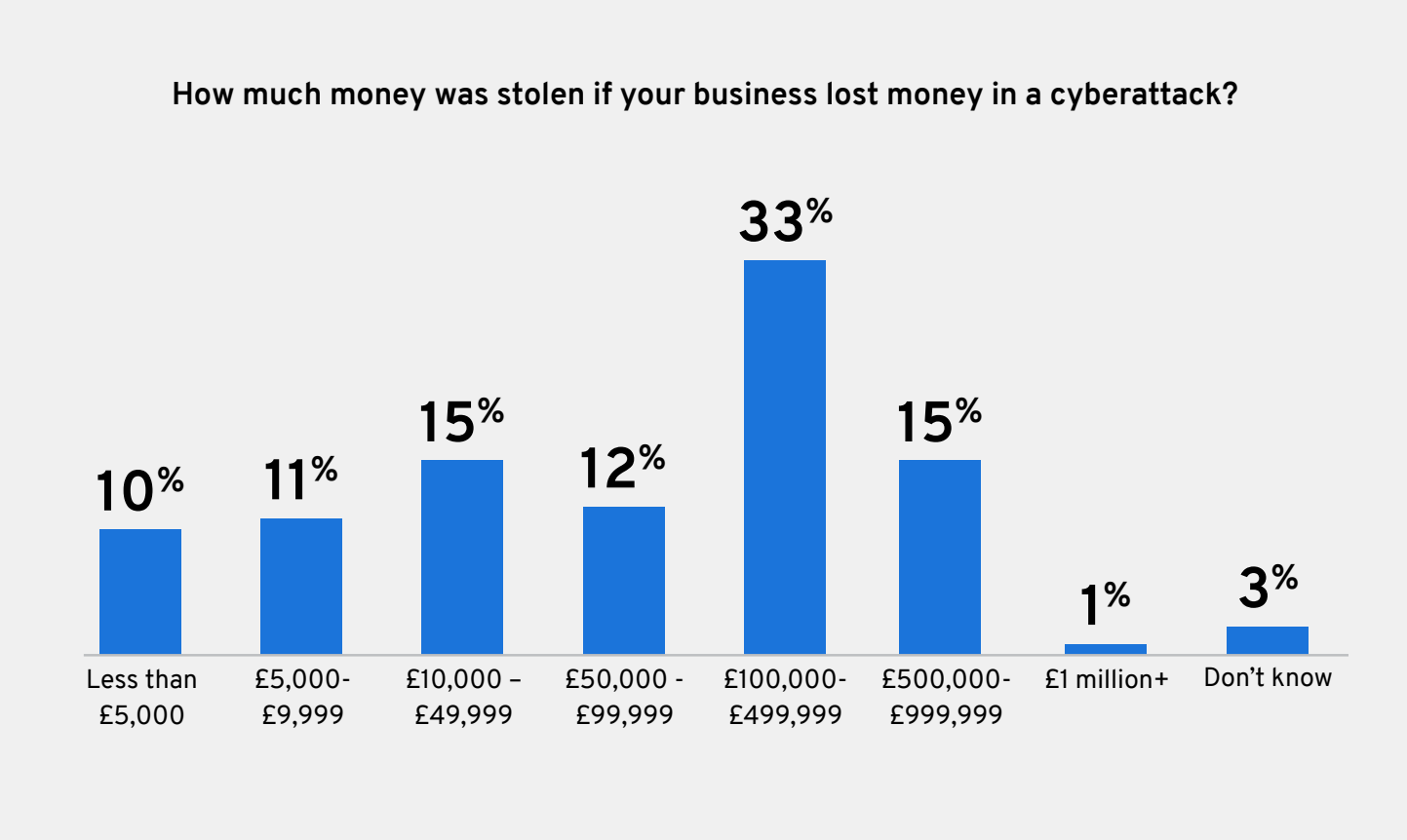
### Which of these has happened to your business as a result of a successful cyberattack?



Cyberattacks affect businesses of all sizes. For example, 31% of organisations with over 1,000 employees, and those with fewer than 1,000 employees, experienced theft of financial information from a successful cyberattack. Likewise, 22% and 21% respectively experienced theft of money.

The financial disruption caused by these attacks is significant, at over £100,000 on average. For 16% of organisations, it was more than £500,000.




Considering the current macroeconomic uncertainty in the UK, and the fact that the average **UK SME's makes just £11,000** in profit per year, such losses can be terminal.

Yet the impact of cyberattacks is not only monetary. Over one third (34%) experienced reputational damage in an attack, and 29% highlighted disruption to partner operations. In short, cyberattacks can cause lasting damage to business perception, client trust and the smooth running of future partnerships.

## Organisations Aren't Fully Prepared for Attacks

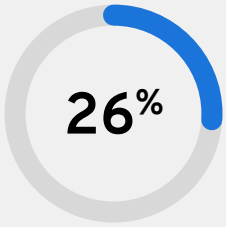
While organisations recognise (and have experienced) the harm of cyberattacks, worryingly only 26% consider their business very prepared to defend against them.

Meanwhile, the time to address attacks is increasing. The majority of respondents (61%) say it is taking longer to respond to attacks, and only 10% say responses are getting faster.

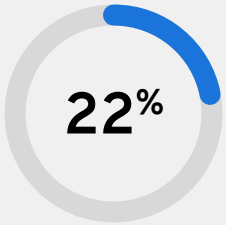
### Darren Guccione, CEO and Co-Founder, Keeper Security

"This research demonstrates that cyberattacks present a profound threat. Preventative measures, in the form of investment, education, and cultural shifts, will be essential for businesses to drive resilience and protect their organisations from cybercriminals."

**How prepared to fend off cyberattacks is your business? How prepared do you think other UK businesses are?**




Very well prepared (my business)




Very well prepared (UK businesses generally)

SECTION 2

# Cybersecurity Investment and Tools

Shortfalls in cybersecurity investment are leaving businesses exposed to threats. Visibility of users, password strength, identities and permissions are baseline necessities regardless of business size or sector—but they aren't being met.

## Leaders Admit Their Tech Stacks Lack Essential Tools

Over one-third of respondents (35%) lack a management platform for IT secrets, such as API keys, database passwords and credentials. Almost nine in ten (87%) also highlight concerns about the dangers of hard-coded credentials.

Meanwhile, 29% lack a remote connection management solution to secure remote access to IT infrastructures.

**With 38% of workers either working exclusively from home or both home and office**[2], this highlights a concerning security gap in this era of hybrid work. As more devices, networks, operating systems and authentication schemes are used in a hybrid environment, the security risks spiral. IT leaders are struggling to keep up with the rapid shifts in how the world works and the subsequent impact these shifts are having on their security.

**29%**

Lack a remote connection management solution to secure remote access to IT infrastructures.

## Security Investment is Planned, but Immediate Action is Needed

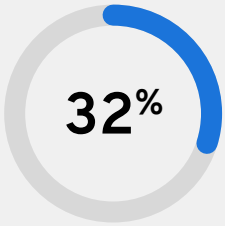
The data shows a pattern of IT leaders acknowledging that their current security measures have identifiable weak points.

Passwords and credentials are a particular area that requires urgent investment, with less than half (48%) of respondents providing employees with guidance and best practices governing passwords and access management.

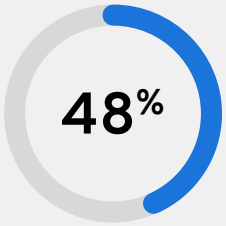
While this should be a minimum best practice, around one third (32%) state they leave it entirely to employees to set their own passwords, and employees often share login credentials—peaking at 37% among organisations with fewer than 1,000 employees. This laissez-faire approach to access management makes it clear that more must be done to keep organisations and their employees protected.

Meanwhile, only 21% state that they have a highly sophisticated framework to govern access to their systems.

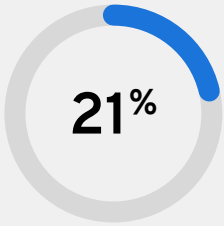
**What is your organisation's maturity with regards to visibility and control over identity security across on-premises and cloud systems?**




**Low maturity**
We leave it to employees to set their own passwords, and access is often shared




**Average maturity**
We provide guidance and best practices governing passwords and access management




**High maturity**
We offer a highly sophisticated framework to govern access to our system

**Which of the following investments are you planning to make around cybersecurity within your organisation over the next year?**


Despite these issues presenting a clear threat to businesses, less than half of respondents state they have plans to invest in password management, security awareness training, or infrastructure secrets management.

Cybersecurity is complex, with many moving parts and shifting priorities to manage, and the research shows that organisations could be doing more.

IT leaders are conscious that their defences are limited and are voicing concerns as to where those weaknesses can be found. And while many organisations are considering future investments, they face being outmatched by rising external threats and demands created by existing gaps.

Analysing how cybersecurity ranks in terms of leadership priorities can help demonstrate the resources necessary to meet those changing demands.

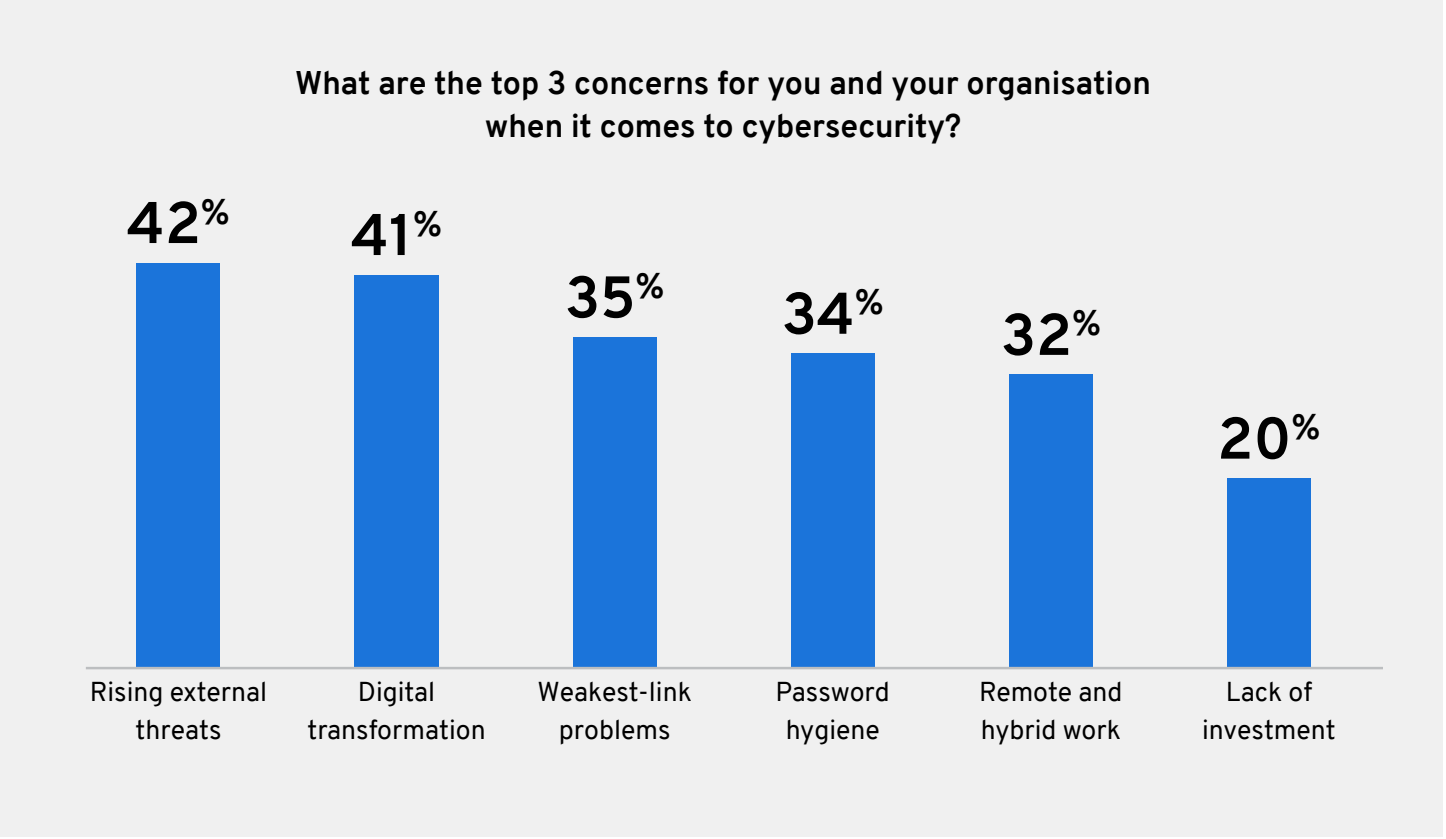
SECTION 3

# Cybersecurity Leadership

Protecting businesses from cyberattacks in the face of growing threats is no small task. IT leaders are under immense pressure from stakeholders, particularly as cybersecurity concerns compete with wider digital transformation and hybrid working priorities.

## Cybersecurity is a Key Concern for the C-suite

As more employees work remotely, businesses must rethink their investments to maintain security. In fact, 32% of organisations highlighted remote and hybrid work as a concern—reaching an even higher point of 38% of organisations with over 1,000 employees.



However, rising external threats present the top concern for IT leaders overall—reinforcing the findings in Section 1 that cybersecurity challenges are increasing.

Positively, just 20% state that a lack of investment is a concern. This is likely because the wider C-suite recognises cybersecurity is vital.

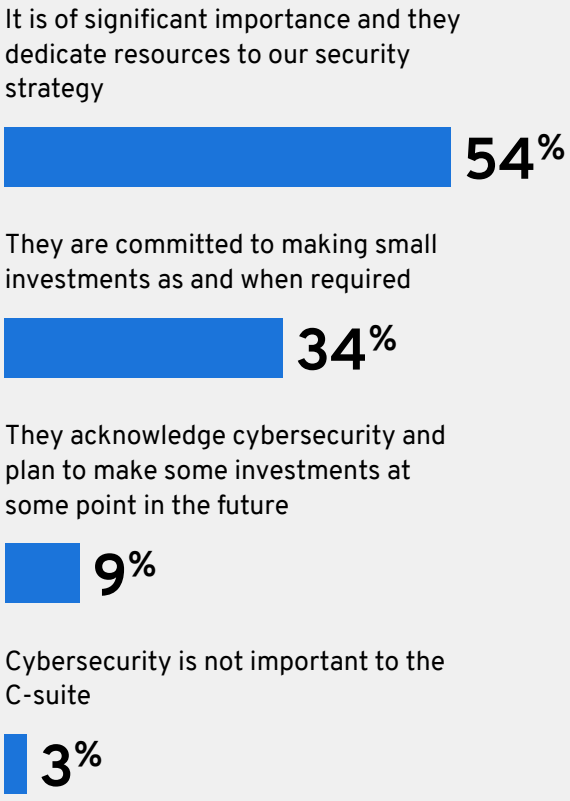
Just 3% of respondents said that cybersecurity is not important to senior leaders at their organisation. In contrast, 54% say the opposite.

## How Leadership Is Shaping Cybersecurity within Organisations

While business leaders recognise the importance of cybersecurity, they are yet to source the necessary talent to keep their organisations secure.

Only 11% state they already have the right personnel in place, while 74% have made new hires in cybersecurity over the past year. The lack of cybersecurity expertise available in the organisations surveyed reflects a broader skills shortage across the country—a key risk to the macro security of businesses.

**What best describes the C-suite's commitment to your organisation's overall security posture?**

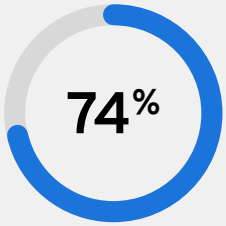



## The UK's cybersecurity skills gap

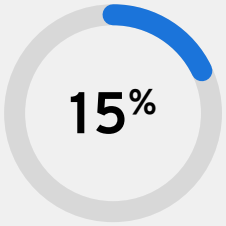
The Department for Digital, Culture, Media & Sport found that across the UK, around **51% of businesses**[3] have a basic talent gap in cybersecurity—lacking the skills to carry out simple tasks like setting up configured firewalls and securely storing or transferring personal data. Meanwhile, 33% have a more advanced skills gap (in areas such as penetration testing, and security architecture), and 37% have an internal skills gap in incident response and recovery.

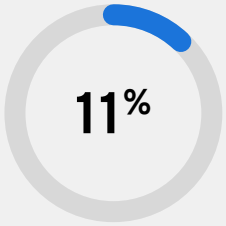
**Have you made any new personnel appointments to your organisation in the past 12 months to bolster your cybersecurity expertise?**




Yes, we have made investments in the cybersecurity personnel within the organisation




No, but we have plans to hire a cybersecurity specialist in the future




No, we have the right personal in place already

When it comes to cybersecurity solutions, half (50%) have increased spend on cybersecurity software. Just 7% state they haven't made any changes to their tech stacks in the past year—demonstrating a broad commitment across UK businesses to continue iterating and evolving their security tech stacks.

While incoming economic headwinds could present challenges to all businesses in the next year, current cybersecurity budgets remain healthy and 68% of respondents even expect their cybersecurity budgets to increase.

In the following section, however, it will become clear that fiscal commitments are just one part of the cybersecurity picture. Cultural attitudes to cybersecurity present an emerging challenge.

### Craig Lurey, CTO and Co-Founder, Keeper Security

"Cybersecurity is now firmly recognised as a foundational priority for senior business leaders. In the coming year, we need to see that positive sentiment translated into not only budgets, but a solid base of skills and solutions which will keep UK companies secure in the face of ever-changing threats."

SECTION 4

# Cybersecurity in Company Culture

## Lack of Transparency into Cyberattacks Could Fuel Culture of Mistrust

Despite budgetary commitments and a clear prioritisation of cybersecurity from the C-suite, IT leaders themselves admit a concerning lack of transparency in cyber incident reporting within their organisations.

Over half (55%) have kept a cyberattack to themself (and so suggesting they didn't report it to any relevant authority'). This figure must act as a wake-up call to businesses and IT leaders alike.

Within a business, IT leaders must be able to share news of cyberattacks. A shortfall in trust in the organisation or fear of reprisal may be fuelling a lack of accountability. Yet if attacks aren't reported, businesses will fail to respond to them. The scale of threats becomes unclear and ultimately the business becomes less secure.

**55%**

of IT leaders have been aware of a cyberattack and kept it to themselves (and so suggesting they did not report it to any relevant authority)

Meanwhile the vast majority (80%) of IT professionals are concerned about a breach from within their organisation, suggesting more must be done to educate teams and ensure everyone is following cybersecurity best practices.

**Has your company ever experienced a breach from within your organisation, and is it something that worries you?**

Yes, I have experienced a breach from within my organisation, so it is something I am concerned about

49%

Yes, I am concerned about the threat of a breach occurring from within my organisation, but I am yet to experience it

30%

No, I haven't experienced a breach from within my organisation, and it's not something that I am concerned with

20%

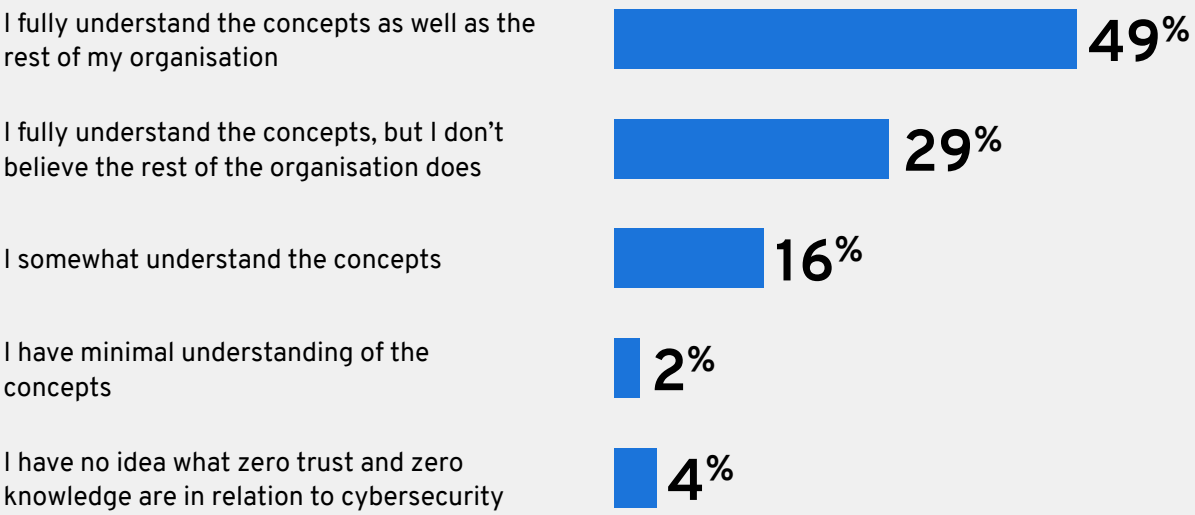
 

## More Robust Cybersecurity Education, Training and Planning Are Needed

Despite the complexity of the cybersecurity landscape in terms of vendors and technologies, most (90%) find it manageable or easy to build a cybersecurity roadmap. Just 10% find the process confusing or impossible.

However, while IT professionals themselves feel able to build roadmaps, there are clear gaps when it comes to understanding key concepts in security—both among IT teams and the wider business. More education is needed.

### Do you understand the concept of zero trust and zero knowledge in relation to cybersecurity?




## What are Zero trust and Zero knowledge in Cybersecurity?

- **Zero trust** assumes that all users and devices could potentially be compromised and everyone, human or machine, must be verified before they can access a network.
- **Zero knowledge** is a security model that utilises a unique client-side encryption and data segregation framework that helps support zero trust by protecting against data breaches.

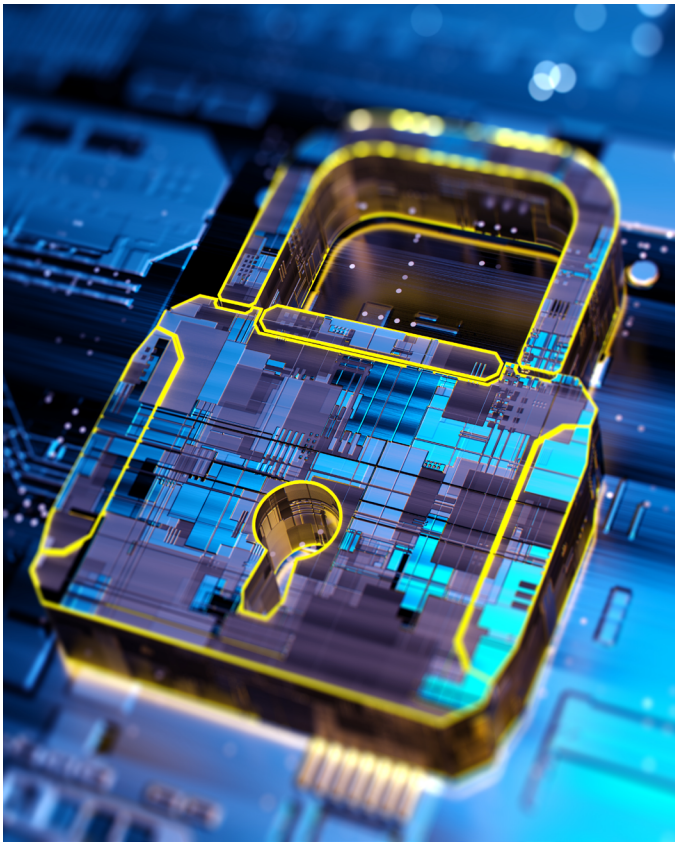
If the zero trust tagline is “Trust no one,” the zero-knowledge tagline is, “We know nothing, and we can’t access your data.”

Organisations should also explore how they can use learnings from third-party sources to build a robust cybersecurity culture. Half (50%) of IT leaders cite industry analysts like Gartner and Forrester as their most trusted source of cybersecurity guidance, while 22% highlight peer groups.

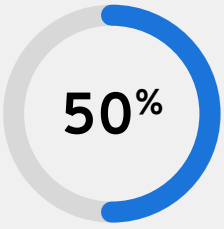
Tapping into that expertise and creating learning groups to delve into findings could be one way to start building cybersecurity into an organisation’s culture.

As cybersecurity threats rise, IT leaders must lead by example.

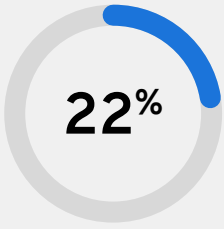
Being open with other leaders about attacks is a first step. An open dialogue on these issues is essential to recognising the scale of the cybersecurity challenges organisations face. Only with that recognition can resources be devoted to education and truly embedding a cybersecurity mindset into an organisation’s culture.



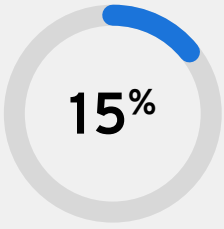
**Who do you trust the most for cybersecurity guidance?**



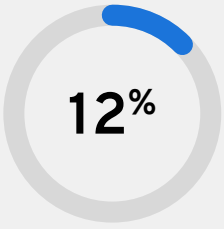

Industry analysts




Peer groups




Media




Vendor white papers

# Conclusion

Businesses across the UK are making cybersecurity a priority. However, despite efforts and investments, clear gaps remain. Our research shows that there have been small steps, but no giant leaps.

The volume and pace at which threats are hitting businesses is increasing, and leadership can't afford to wait. If they do, the financial, reputational and organisational penalties will be severe.

Likewise, as work has transformed dramatically over the past two years—with hybrid and remote working normalised—companies need to rethink how they are building cybersecurity resilience.

As we enter a new moment of economic uncertainty, we must not lose focus. The pace of cyberattacks is not going to decrease, even if the budgets to address them come under pressure. Preventative measures are always less costly in the long-run. Deploying defensive solutions that protect against attacks and their impacts is essential.

Yet for UK businesses to become truly secure, perhaps the biggest change that must be made is cultural. The majority of IT leaders admitted to keeping a cyberattack they were aware of to themselves (and so suggesting they did not report it to any relevant authority). This figure should shock business leaders. Without a culture of trust, accountability and responsiveness, cyber criminals will thrive.

As we move forward, businesses and IT leaders need to not only voice commitments to cybersecurity but act on them. They need to acknowledge how our workplaces have evolved and respond to new ways of working with revised tech stacks.

Most importantly of all, they must make cybersecurity a pillar of organisational culture. Cybersecurity needs to be understood as a pillar of every good business, but understanding, accountability, education and progress must start at the top.

[1] Statista, 'UK average SME profit by size 2021', (2022)
[2] Office for National Statistics 'Is hybrid working here to stay?', (2022)
[3] Department for Digital, Culture, Media & Sport, 'Cyber security skills in the UK labour market 2022: findings report' (2022)