
KEEPER
Cybersecurity Starts Here
2021
UK CYBERSECURITY
CENSUS REPORT

CONTENTS

FOREWORD

Over the last couple of years, cybersecurity has come of age. What many organisations saw as nothing more than an IT buzzword has evolved to become a function that is integral to ensuring business continuity.

But what is the cybersecurity landscape reality like for businesses in the UK today? How exposed are they to the growing number of destructive cyberattacks? What are their cybersecurity investment priorities like? Who is responsible for their cyber defences? And what more can be done for and by UK businesses to properly fend off cyberthreats?

To answer these questions, Keeper has, in partnership with Sapio Research, analysed the behaviour and attitudes of businesses by interviewing 1,000 senior IT decision makers across the UK.

The result is this report - Keeper's inaugural UK Cybersecurity Census - which sheds light on the cybersecurity challenges and opportunities UK businesses are facing in 2021 and beyond.

EXECUTIVE SUMMARY

Here are 5 key takeaways from our inaugural UK Cybersecurity Census:

UK businesses have never before faced a more **aggressive and relentless onslaught of cyberattacks**, resulting in significant financial losses in the event of a successful attack

The **pandemic has made UK organisations even more exposed** to cyberattacks, with existing IT policies being watered down in favour of ensuring business continuity and employee productivity

Despite understanding the critical role that the IT team plays in keeping an organisation safe, most **UK businesses are investing far too little into their IT and cybersecurity solutions**, leaving themselves incredibly vulnerable as a result

Senior IT leaders are calling for **more cybersecurity regulation**, including a minimum level of cybersecurity protections before organisations are allowed to operate and an independent regulatory body to enforce this

Senior IT leaders are under a huge amount of pressure to protect the organisations they work for, leading them to frequently ignoring their own cybersecurity advice by re-using passwords and even keeping cybersecurity breaches to themselves

SECTION 1:

CYBERATTACKS

The frequency, intensity and complexity of cyberattacks is on the rise and UK businesses are starting to feel the heat. Almost all of them (92%) have experienced a cyberattack in the last 12 months, with over two-thirds (72%) of organisations being successfully breached at least once.

The consequences of such a breach can be dire. Many organisations have had either sensitive corporate (28%) or financial (26%) information stolen from them as a result of a cyberattack. A third (34%) of UK companies have also experienced severe organisational disruptions that have resulted in them being unable to carry out business operations.

In many cases, the financial fallout of a cyberattack has the potential to cripple a company. Of those organisations having experienced theft of money as a direct result of a breach, 41% have lost over £50,000 and every twelveth (8%) has even lost over £1 million.

It is clear that UK businesses are not well prepared to deal with the barrage of cyberattacks they are exposed to every single day - and the large majority (78%) of IT professionals agree with this statement.

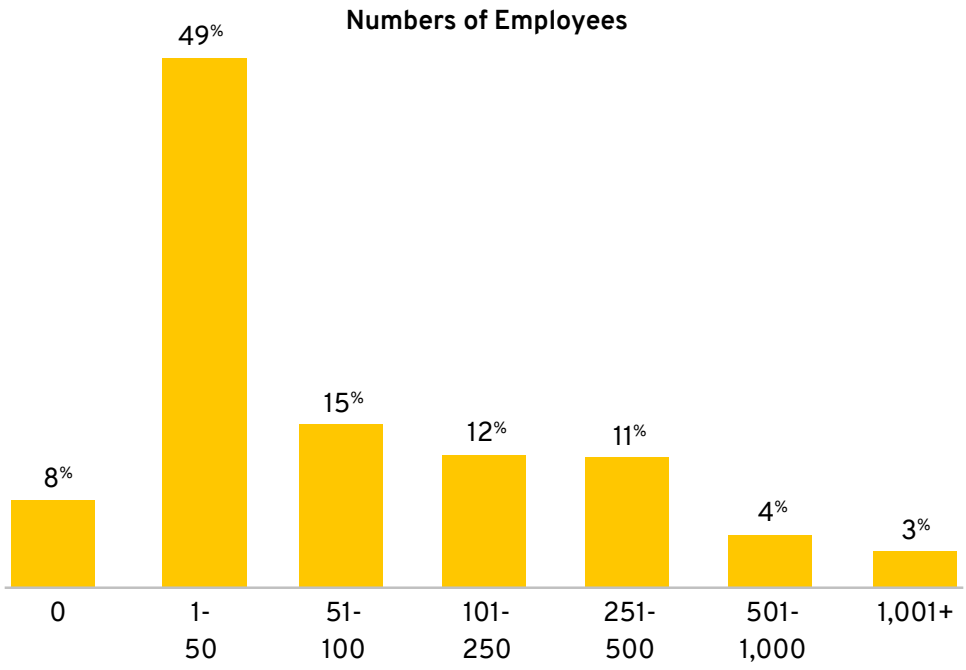
A key challenge for UK companies is a lack of cybersecurity skills. Nearly a quarter (23%) of all organisations believe that they don't have the right skills within the business to adequately protect themselves against cyberattacks.

Businesses often also take too long to react to a cyberattack, losing valuable time to limit the damage caused by cybercriminals in the process. Almost 3 in 5 (59%) organisations agree that their response time has increased over the last 12 months.

All of this paints a stark picture: Unless UK businesses dramatically increase their cybersecurity investments, they will remain easy and lucrative targets for cybercriminals.

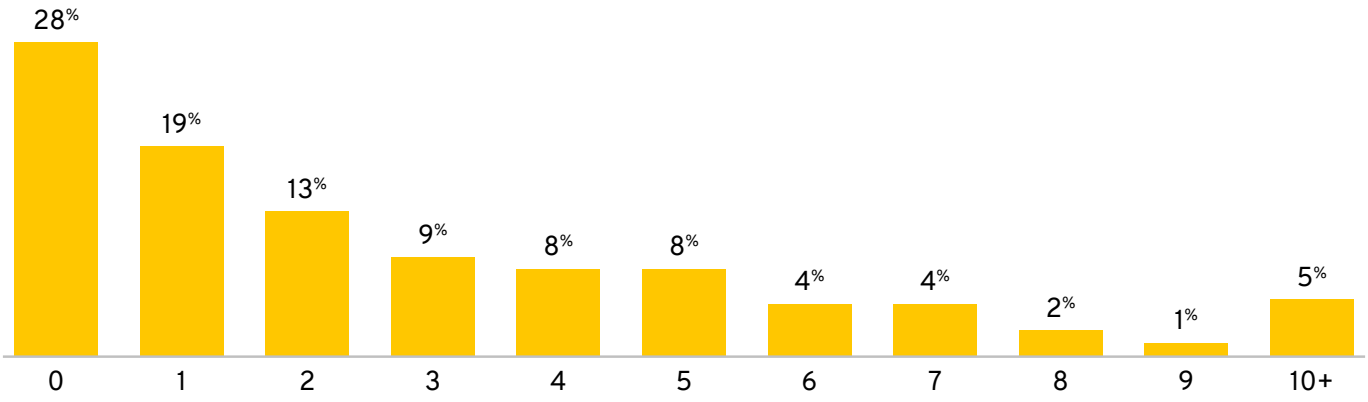
A key challenge for UK companies is a lack of cybersecurity skills.

How large are the organizations that reported at least one cyberattack in the last 12 months?



Out of these attacks, how many were successful?

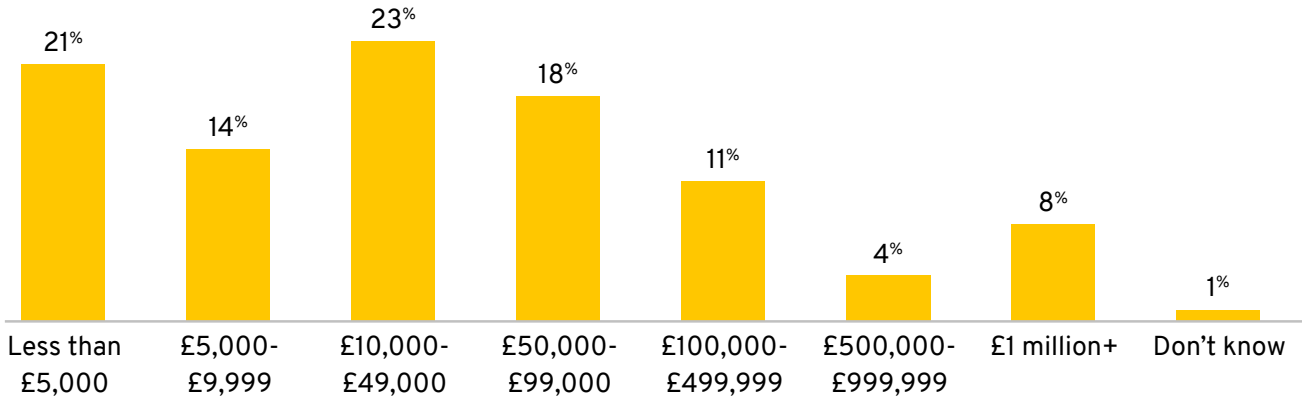
(Only asked of those that experienced a cyberattack)



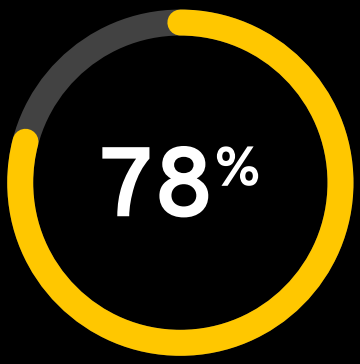
Base: 1,000

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

How much money did your organization lose as a result of a breach?

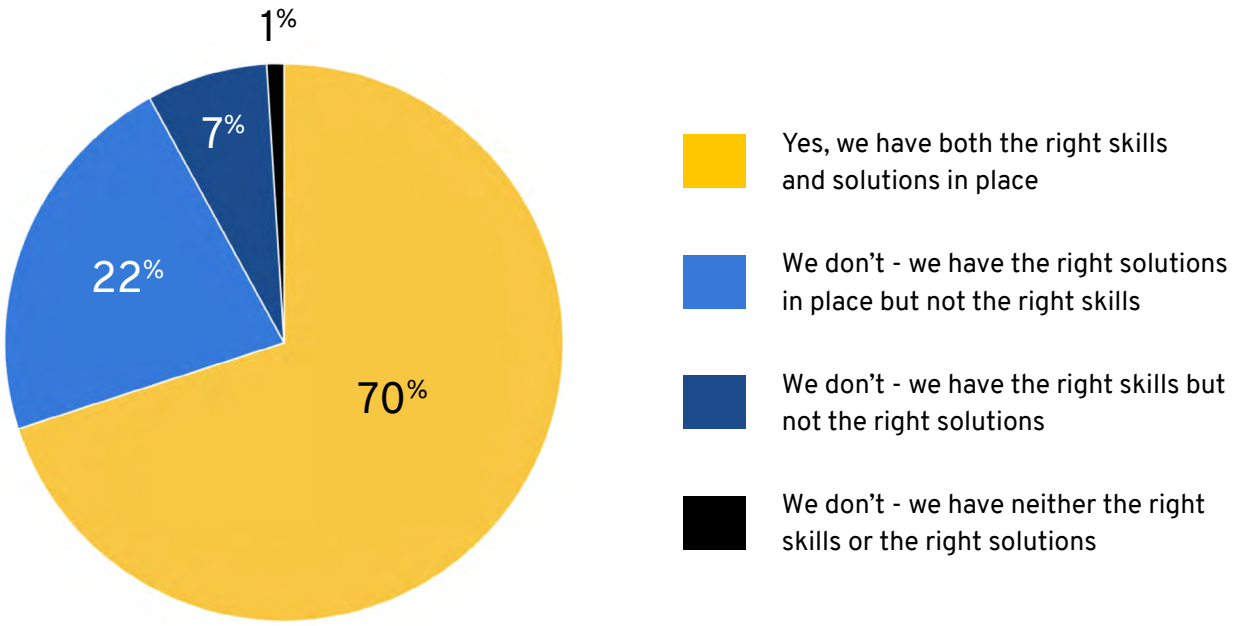


Base: 1,000

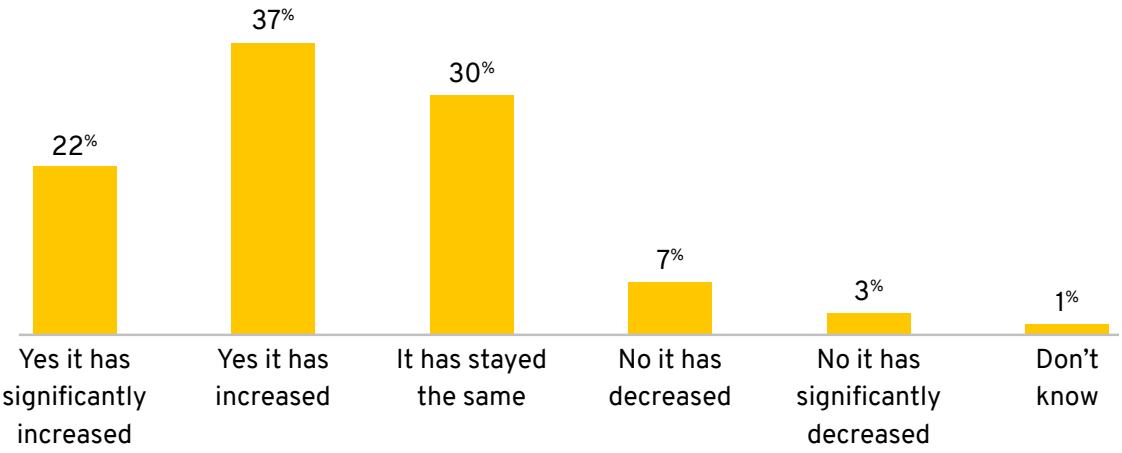


of senior IT professionals believe that businesses in the UK are generally not well prepared for cyberattacks

Do you have the right skills and cybersecurity solutions within your organisation to adequately protect yourself against cyberattacks?



Has the time taken to respond to a cyberattack increased in the past 12 months?



Base: 1,000

SECTION 2:

CYBERSECURITY INVESTMENTS

The most effective way to prevent cyberattacks from succeeding is to invest in powerful cybersecurity solutions and hire people with the right skills to manage them.

This may sound obvious but, surprisingly, for many UK organisations, IT and cybersecurity investments are still not a top priority. About a quarter of all companies (28%) don't consider IT to be one of their top 3 priorities for the next 12 months. Less than half (44%) say it is their top priority.

This is especially worrying as almost all (92%) UK organisations are aware of where the gaps or weak links in their cybersecurity defences are, but less than half (40%) are actively addressing all of them.

Looking closely at what the IT budget is being spent on, it becomes clear that, despite a certain degree of obliviousness, cybersecurity is an urgent priority for UK businesses, with 92% of them allocating at least 10% of their IT budget to cybersecurity solutions.

But investing in cybersecurity solutions alone is not enough. UK businesses also need to ensure they have the right people with the right skills within their organisations. Currently, this isn't the case, with 61% of UK companies experiencing a cybersecurity skills shortage.

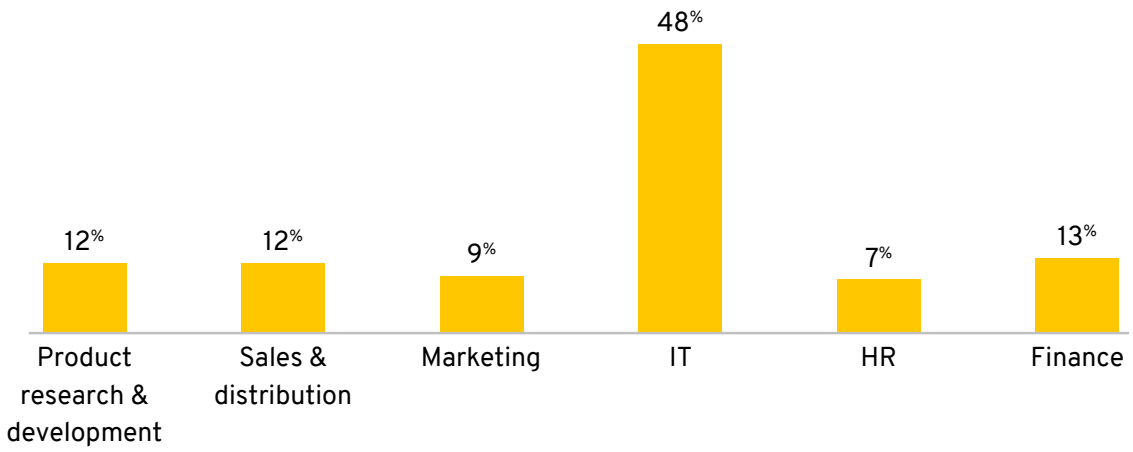
On top of that, businesses need to invest in educating their wider workforce around the cybersecurity dangers they are exposed to, and the active role they can play in keeping the company safe. After all, employees are often an organisation's first line of defence.

Four in five IT professionals (79%) agree that more needs to be done to educate employees on the importance of following cybersecurity best practices, and the consequences of not doing so. Poor password hygiene is a particular risk to organisations, with 58% of IT professionals agreeing that employees do not understand what the full consequences of this are.

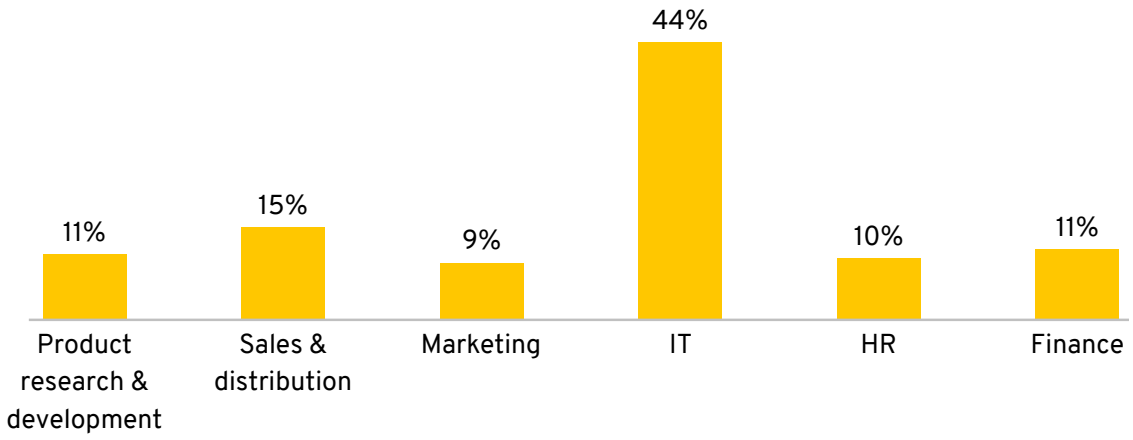
Ultimately, many components make up an organisation's cybersecurity defences. But, despite this complexity, if a cyberattack is successful, most organisations want a single culprit to hold accountable. And this person often sits at the very top of the business.

Poor password hygiene is a particular risk to organisations.

What have your investment priorities as a business been over the past 12 months? (#1 Priority)

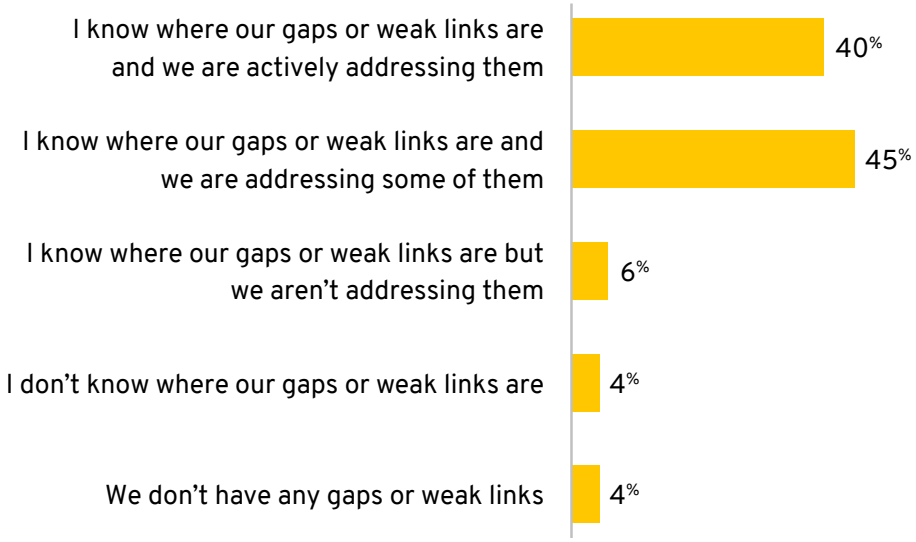


What are your investment priorities as a business now and over the next 12 months? (#1 Priority)

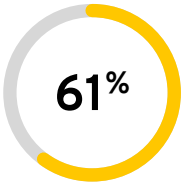


Base: 1,000

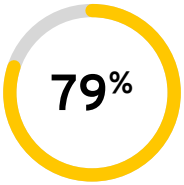
Do you know where the gaps or weak links in your cybersecurity defences are? And are you addressing them?



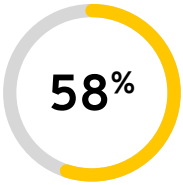
How much do you agree or disagree with the following statements:



Agree - there is a skills shortage among UK IT workers and this is impacting cybersecurity in my organisation



Agree - more needs to be done to educate employees on the importance of following cybersecurity best practices and the consequences of not doing so



Agree - employees at my company do not understand the implications of poor password hygiene

Base: 1,000

SECTION 3:

CYBERSECURITY OWNERSHIP

Senior IT leaders across the UK have never been under more pressure. They are expected to continue protecting their organisations - often with limited resources - while the world around them is rapidly changing.

Almost half (47%) of IT leaders are most worried about cyberattacks becoming increasingly sophisticated, while another quarter (27%) say that the frequency of these attacks is their biggest concern. Add the common lack of critical cybersecurity resources to the mix and it becomes clear that IT decision makers are fighting an almighty battle.

Internal company pressures are another factor to consider here. For a lot of IT leaders, their head is on the line. While many organisations haven't necessarily appointed a single person in charge of cybersecurity, a third (31%) believe that CTOs will have to bear the brunt of the blame in the case of a successful cyberattack.

With that in mind, it might be somewhat understandable - while still concerning - that senior IT decision makers are not always leading by example.

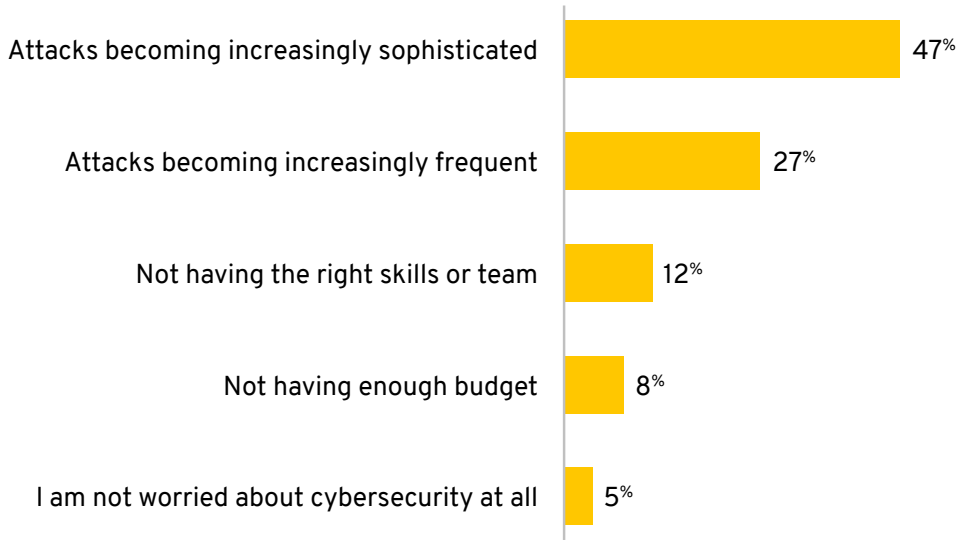
One third (34%) of IT professionals admit to using the same password more than once at work and 32% are using weak default login credentials such as 'password' or 'admin' to protect their data.

Perhaps most shockingly, more than a third (36%) admit to having kept a cyberattack to themselves. The ramifications of this are severe.

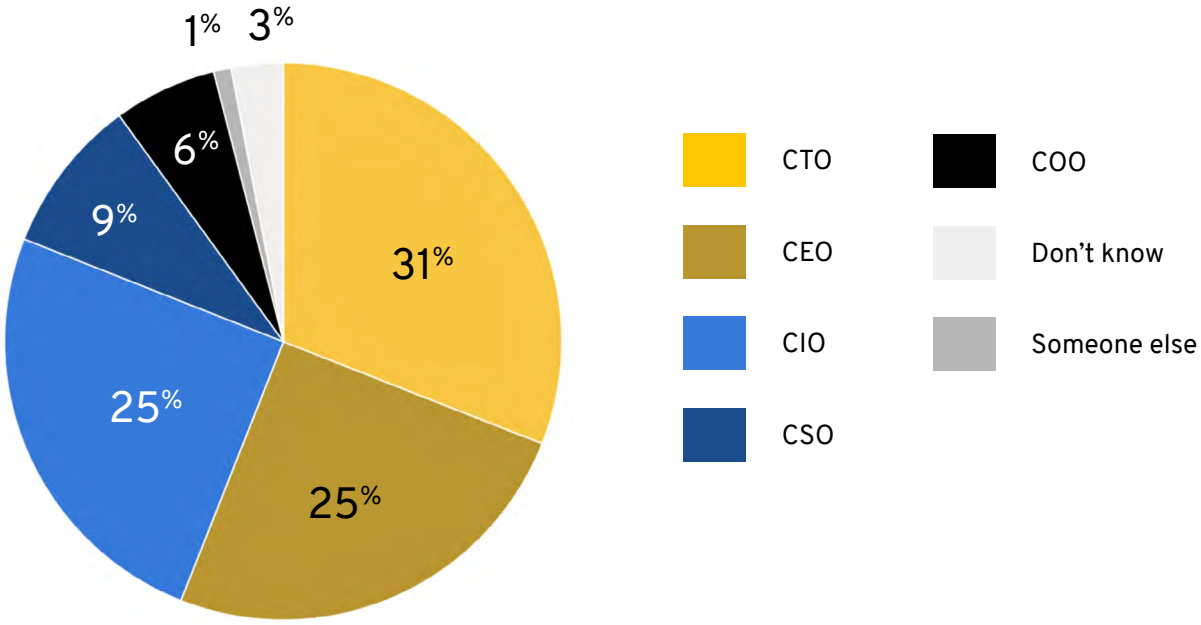
It therefore comes as no surprise then that three quarters (76%) of senior IT leaders agree that there should be a member of the Board specifically dedicated to the cyber-welfare of the business. This would help clarify ownership and put a clear person at the top in charge of all cybersecurity matters across the company.

34% of IT professionals admit to using the same password more than once at work.

What is your biggest cybersecurity worry?

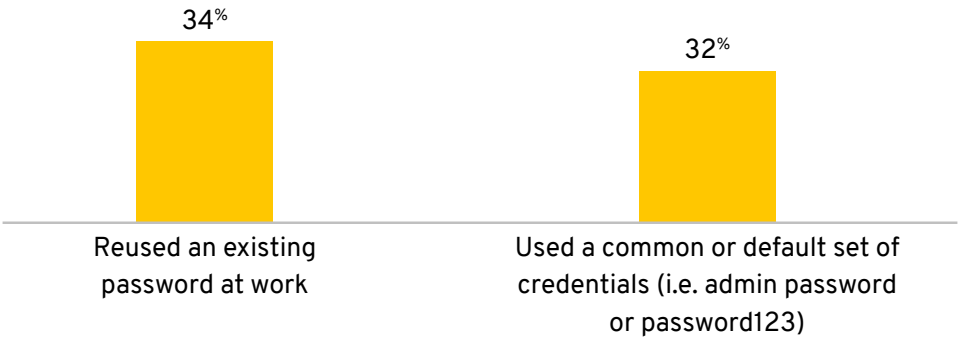


Who is ultimately being held responsible internally if a cyberattack is successful?

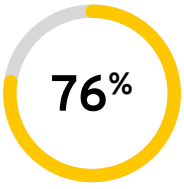


Base: 1,000

Which of these have you done at least once in the last 12 months? Select all that apply.

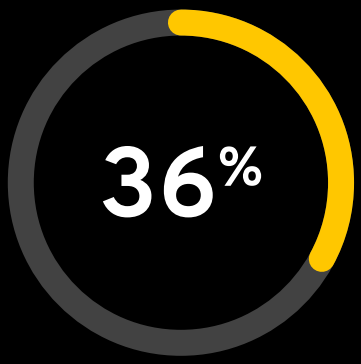


How much do you agree or disagree with the following statement:



Agree - there should be a member of the Board specifically dedicated to the cyber-welfare of the business

Base: 1,000



Have kept a cybersecurity attack or breach affecting their organisation to themselves

SECTION 4:

CYBERSECURITY DURING THE PANDEMIC

The pandemic has dramatically affected and altered the foundations of almost every UK business. Many were forced to shift to remote work practically overnight.

This has posed particular challenges for IT departments in charge of the technical aspects of that migration, while simultaneously having to ensure companies continue to be adequately protected against cyberattacks.

Business continuity has been the top priority, sometimes at the expense of existing cybersecurity protocols.

As a result, two thirds (66%) of UK organisations have relaxed their cybersecurity policies over the past 12 months so staff can work remotely or in order not to stifle productivity. Despite this, nearly a quarter (22%) of UK businesses still have not updated their cybersecurity policies to reflect this new reality.

Senior IT leaders are very aware of the challenges this poses to them and their teams, and that they need to double down on their cybersecurity efforts. In fact, most of them (79%) believe cybersecurity will become more important as they navigate the next 12 months.

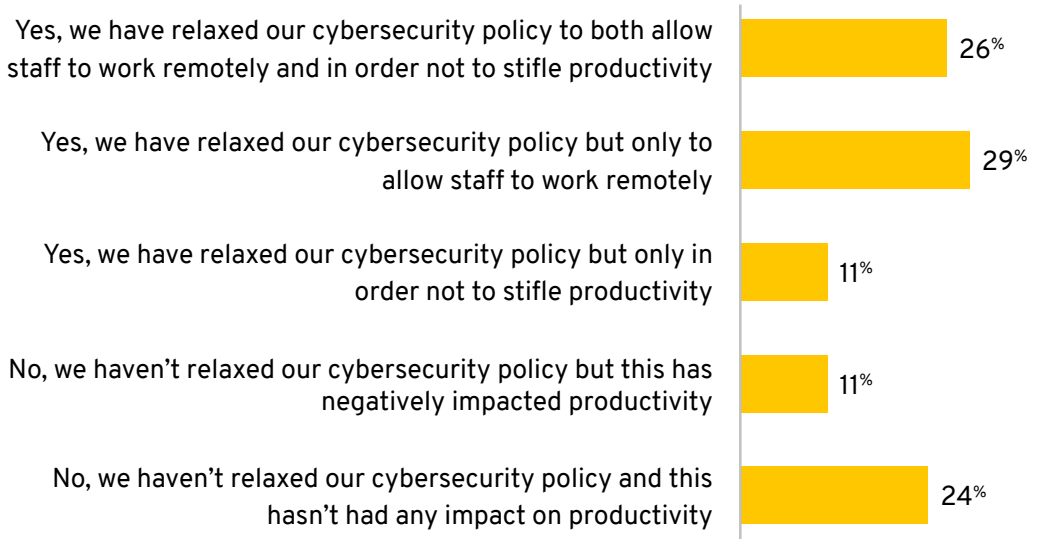
For three quarters (76%) of UK businesses this added layer of focus towards cybersecurity is a direct result of the conditions caused by the pandemic. Particularly given one in five (18%) organisations consider employees continuing to work remotely to be their largest cybersecurity vulnerability in 2021.

Yet this does reflect a general attitude towards the most pressing issues for organisations this year. 95% of UK businesses are worried about cybersecurity, but more clearly still needs to be done to ensure organisations act on this worry. IT leaders believe companies should face increased external pressure to ensure they do so.

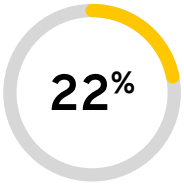
The pandemic has dramatically affected and altered the foundations of almost every UK business. Many were forced to shift to remote work practically overnight.

Have you relaxed your cybersecurity policy over the last 12 months to allow staff to work remotely and/or not to stifle productivity?

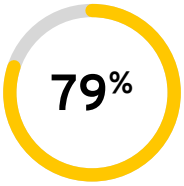
65% have relaxed their cybersecurity policies



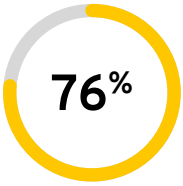
How much do you agree or disagree with the following statements:



Agree - companies have not updated their cybersecurity policy since shifting to remote working

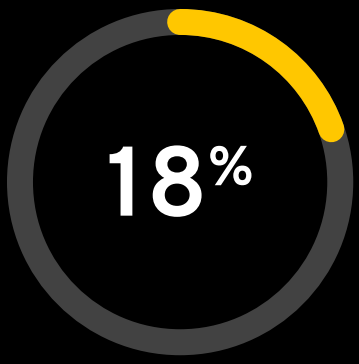


Agree - cybersecurity will become more important for my business in the next 12 months



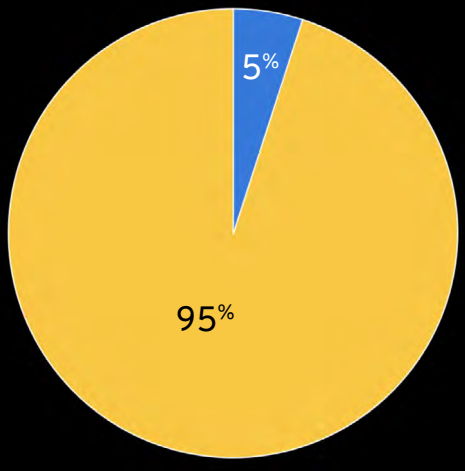
Agree - the conditions caused by Covid-19 have made my company take cybersecurity more seriously

Base: 1,000



of organisations consider employees continuing to work remotely to be their largest cybersecurity vulnerability in 2021

Are you worried about cybersecurity at all?



Are worried in some form

Not worried about cybersecurity at all

Base: 1,000

SECTION 5:

CYBERSECURITY LEGISLATION & POLICY

Not all UK businesses conform to one way of protecting their online security. Different areas are prioritised, and the gaps are present in different places.

But while every organisation has a slightly different view of how they should go about properly protecting themselves against cyberattacks, senior IT decision makers do largely agree on one thing: there should be more external pressure on companies to ensure their cyberdefences are up to scratch.

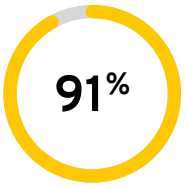
Almost all (91%) IT leaders think businesses should be legally required to have basic cybersecurity protections in place before being allowed to operate and trade.

Additionally, four in five (82%) believe that new employees should be required to complete a basic level of cybersecurity training before they start a role at the company.

Senior IT professionals further feel that there should be a degree of public accountability for businesses to ensure they keep investing in cybersecurity. In fact, a large majority (87%) think that the creation of a regulatory body - an 'Ofcom for cybersecurity' - would be an effective way to hold businesses accountable and reduce cyberattacks in the UK.

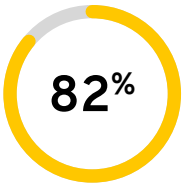
Senior IT decision makers do largely agree on one thing: there should be more external pressure on companies to ensure their cyberdefences are up to scratch.

Do you agree that businesses should be legally required to have basic cybersecurity protections in place before being allowed to operate or trade?



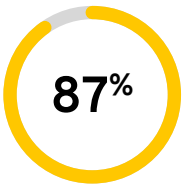
Yes, agree

How much do you agree or disagree with the following statement:



Agree - all employees should be required to complete a basic level of cybersecurity training before they start

Do you agree that an independent body - an 'Ofcom for cybersecurity' - would be an effective way to hold businesses accountable and reduce cyberattacks in the UK'?



Yes, agree

Base: 1,000

CONCLUSION

Cybersecurity is clearly a major concern for UK businesses. But, as this report has shown, there is no such thing as just one singular cybersecurity challenge.

Companies are struggling to put the right solutions in place to cope with the onslaught of cyberattacks that they are exposed to on a daily basis, often with costly consequences.

While there is a desire to boost cybersecurity efforts, companies are still reluctant to put their money where their mouth is and make IT an investment priority.

There is also a clear lack of ownership around who makes cybersecurity decisions - and who is ultimately responsible in case there is a successful breach.

The global pandemic has added a further level of complexity to the situation, with the widespread shift to hybrid work making it even more difficult to have adequate cybersecurity defences in place.

And there is a growing call for further regulation, forcing companies to wise up and address some of the dangerous cybersecurity gaps that exist within, but also between, organisations.

Yet with all of these challenges also come opportunities. There is a clear path for UK businesses towards a more mature, effective and robust cybersecurity future. Ultimately, a clear dissonance exists between awareness and actions taken to address the problem. The next 12 months will show how much progress UK businesses are willing to make to close this vast cybersecurity gap.

RESEARCH METHODOLOGY

The survey results are taken from interviews with 1,000 senior IT decision makers in the UK. The interviews were conducted online by Sapio Research in April and May 2021.

ABOUT KEEPER SECURITY

Keeper is transforming the way organisations and individuals protect their passwords and sensitive digital assets to significantly reduce cybertheft and data breaches. Keeper is the leading provider of zero-trust, zero-knowledge security and encryption software covering password management, dark web monitoring, digital file storage and advanced reporting and alerts. Keeper protects any-sized business across every major industry sector by providing visibility and control over its password security and dark web threats. To learn more visit **keeper.io/uk-census**.

Get Protected