IFP Insights For Professionals

Enterprise Security Research Report

Analyst Report

IFP RESEARCH

Contents

Enterprise Security
Research Report

Introduction

1

CHAPTER 1:

Introduction

Enterprise security remains a top priority for CIOs, CISOs and business leaders. A single exposed flaw or missed vulnerability can expose an entire business to a major breach and the operational, reputational and legal repercussions they bring.

Given the frantic IT decision making to support business operations and navigate the struggles of COVID-19, many firms didn't give security concerns the consideration they required, or discuss ongoing changes with IT. This resulted in hacks, downtime, business disruption and even company failures.

As the landscape of "the new normal" becomes clearer, it's time to see how IT is dealing with the current security threats.

To explore the current security landscape, we surveyed 205 IT professionals within the Insights for Professionals community to establish their priorities and concerns when it comes to enterprise security in 2022 and beyond.

Nearly

61%

of IT professionals have reported more targeted and sophisticated cyberattacks due to COVID-19

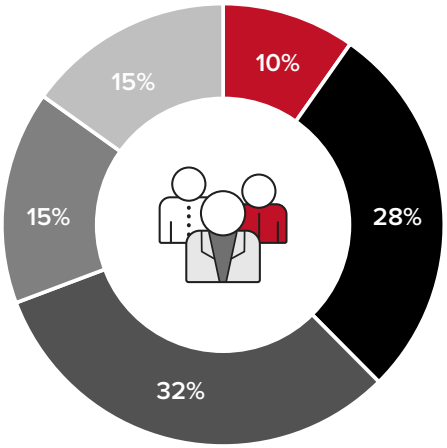
Survey demographics

Insights for Professionals surveyed 205 senior IT professionals across a range of industries of different sizes from the United States and the United Kingdom, including Technology (24%), Manufacturing (16%), Finance (13%), Information (12%), Government (8%) and more.

Company size

Our sample shows a good mix of company sizes ranging from those with 250 employees to 25,000+. The largest percentage of respondents work in large organizations with 1,000 to 4,999 employees, while the second largest (28%) work in medium-sized businesses with 500 to 999 employees.

How many employees are there in your organization?

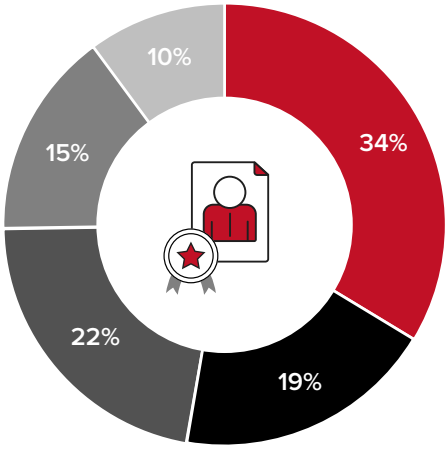


Which country are you based in?

Seniority level

By role, the largest proportion of participants are Managers (34%), followed by Directors (22%), Senior Managers (19%) and C-Suite executives (15%).

Select your authority level



This research report dives into the threat landscape, the level of attacks and how businesses are responding to them, along with the challenges that business leaders face in securing their operations.

Why is IT security so important?

Every week there are reports of major incidents among enterprises and SMBs, and new or updated methods of attack are constantly being developed to breach corporate systems. In 2021, almost all types of attack increased, with over 5 billion malware attacks and over 5 trillion intrusion attempts logged by **SonicWall alone**. This, coupled with a rapid growth in API attacks (**up 681% in 2021** according to Salt Security), indicate attackers are looking to broaden their horizons and attack businesses in areas their IT security may not be focusing on.

With the majority of attacks automated and wide-reaching, they could impact any business at any time. And with more attacks attempting to exploit new vulnerabilities, modern business security solutions always need to be up to date.

To defeat this constant stream of attacks, businesses must:

- **Be aware of the risks they face**
- **Use the latest tools to defend their IT perimeter**
- **Ensure users are trained to spot malware and other threats**
- **Use strong security and access measures across all services**
- **Have business continuity and disaster recovery plans in place**

Understanding how your peers are treating these threats and what they do to protect the business should act as a starting point to any effort to improve your IT security.

OVER 5 BILLION

malware attacks and over 5 trillion intrusion attempts were logged by SonicWall in 2021 alone.

Key findings

Here are some of the key takeaways from our report:

1. **3 in 5 firms in the US and the UK** say they're encountering more targeted and sophisticated cyberattacks, with **76%** of respondents recording up to 100 security incidents between 2021 and 2022.

2. Nearly two-thirds of IT professionals say that malware (including fileless malware) is the greatest challenge – particularly in small to medium sized companies (250-999 employees).

3. 57% of respondents say cloud security is their second most significant concern.

4. The third biggest cybersecurity challenge is phishing and social engineering, and this is most problematic for larger companies with over 5,000 employees.

5. The largest enterprises (25,000 or more) see cloud dominate as the most vulnerable endpoint, while the smallest firms (250-499) rate laptops as the biggest threat.

6. Over half of respondents say they're able to identify, respond and contain an intrusion within 24 hours.

7. Large businesses with **1,000-4,999** employees are the least responsive, with only **45%** catching intrusions within a day.

8. The biggest data protection challenge facing the IT department is the skills gap.

9. Nearly 1 in 5 respondents in the UK are underfunded and don't have enough resources to keep their systems secure.

10. Almost 60% of IT professionals say they're prepared to spend between $100,000 and $1,000,000 on IT security in the coming 12 months.

11. Nearly two-thirds of IT professionals are prioritizing cloud security solutions over the next 12 months.

12. Antivirus technology is the most popular investment among the smallest firms (250-499)

13. **Endpoint detection and response (EDR)** software is the biggest priority in the largest enterprises, with **61%** of leaders reporting a reduction in endpoint visibility due to remote/hybrid working.

Enterprise Security
Research Report

The threat landscape

2

CHAPTER 2:

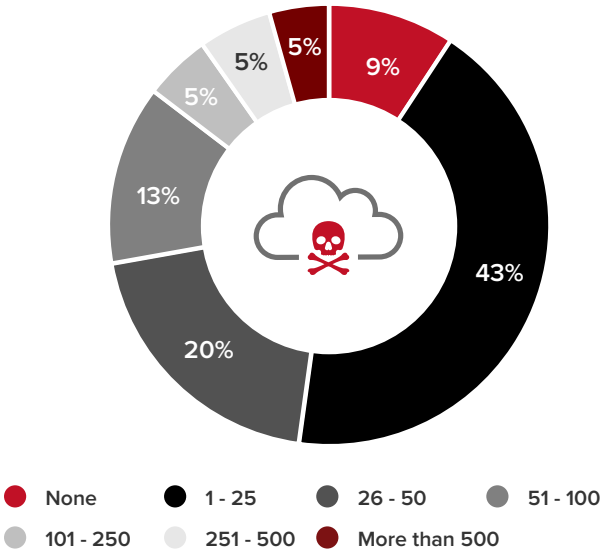
The threat landscape

The number of attacks will continue to increase in the coming years, as hacking becomes a staple of the dark digital economy and an unofficial strategy of some governments to raise money, uncover usable business information and access trade secrets.

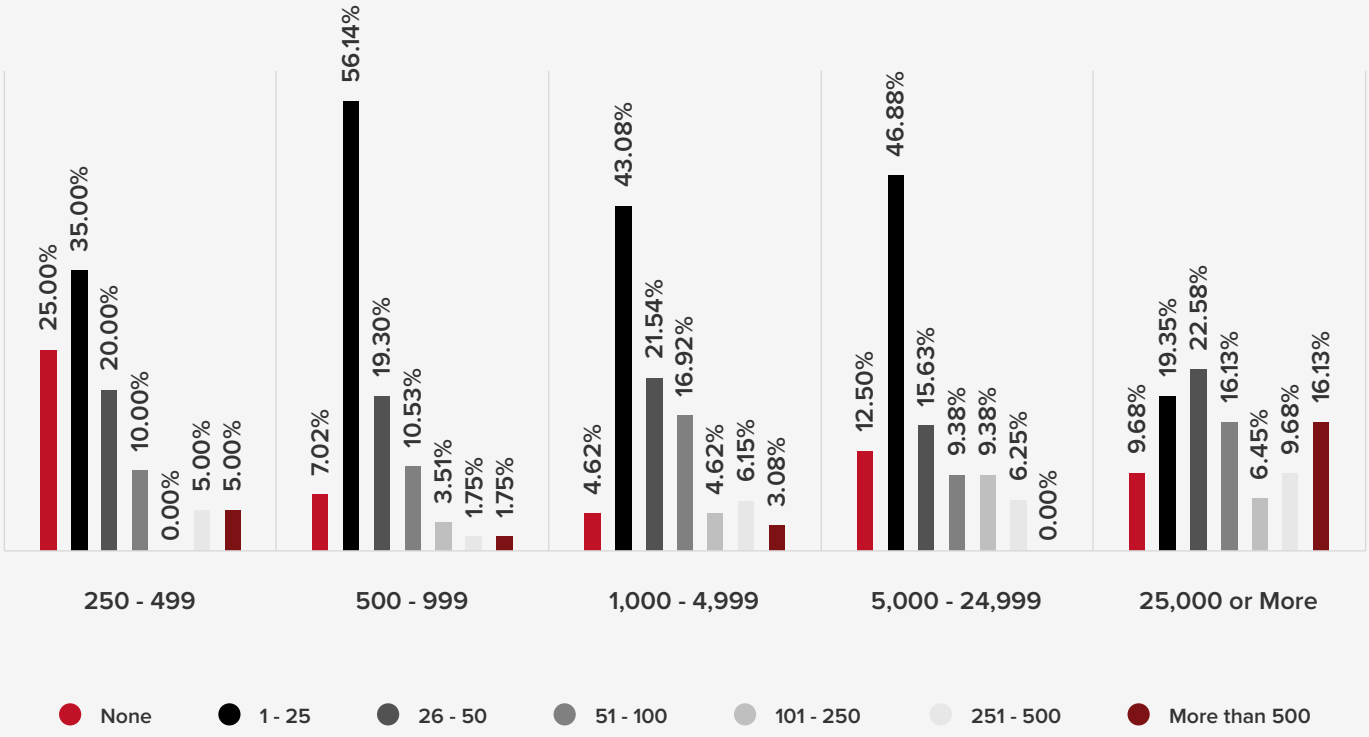
As businesses see more employees working remotely, deploy more services in the cloud and use a wider range of applications, they create complexity that increases the risk to their IT infrastructure and services.

The combination of these factors help to explain the growing reports of attacks, with nearly two-thirds (63%) of IT professionals reporting between 1 and 50 cyberattacks between 2021 and 2022, and almost 10% seeing over 251 incidents against their systems.

How many cyberattacks did you record between 2021 and 2022?



The number of cyberattacks recorded between 2021 and 2022 vs. company size



What's more, 1 in 4 (25%) of the smallest businesses (250-499 employees) in our survey reported no attacks, suggesting their IT security might not be as mature, compared to an average of 9% for all larger businesses with their likely more robust IT.

With every business a potential victim of a cyberattack, IT leaders need to ensure that the typical tools such as the latest firewalls, malware detection and virus checkers are supported by cloud-facing applications. These include cloud security posture management (CSPM) and cloud access security broker (CASB) solutions, backed up by strong compliance and governance efforts to protect the business at every step.

In the US, the **intensity of attacks** is clearer, with 20% of respondents reporting from 101 to over 500 attacks, while in the UK, only 6% reported such volumes of attack.

The cybersecurity challenges facing business

For business and IT leaders, the risks aren't solely the typical malware attack, even though this is the greatest challenge for 64% of respondents. Most are focused on delivering strong cloud security (57%) and preventing insider attacks (17%), which highlights the broad spectrum of protective services required and the tools to identify breach attempts inside and beyond the firewall.

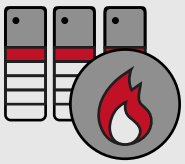
Some 51% of IT professionals are focused on phishing and social engineering attacks that target the user as the weak point in IT security. While many CIOs focus on the technical protection of the business, users must be trained to identify the threats that can come through email, messaging, deep-faked voice or video calls and other methods in increasingly sophisticated efforts to access login details or steal directly by deception from business accounts.

64.39%
Malware (including fileless malware)

57.07%
Cloud Security

51.22%
Phishing and Social Engineering

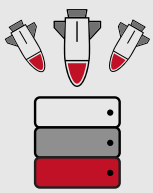
42.44%
Ransomware



26.34%
Data Loss

19.51%
Password Attacks

17.07%
End Users / Insider Threats

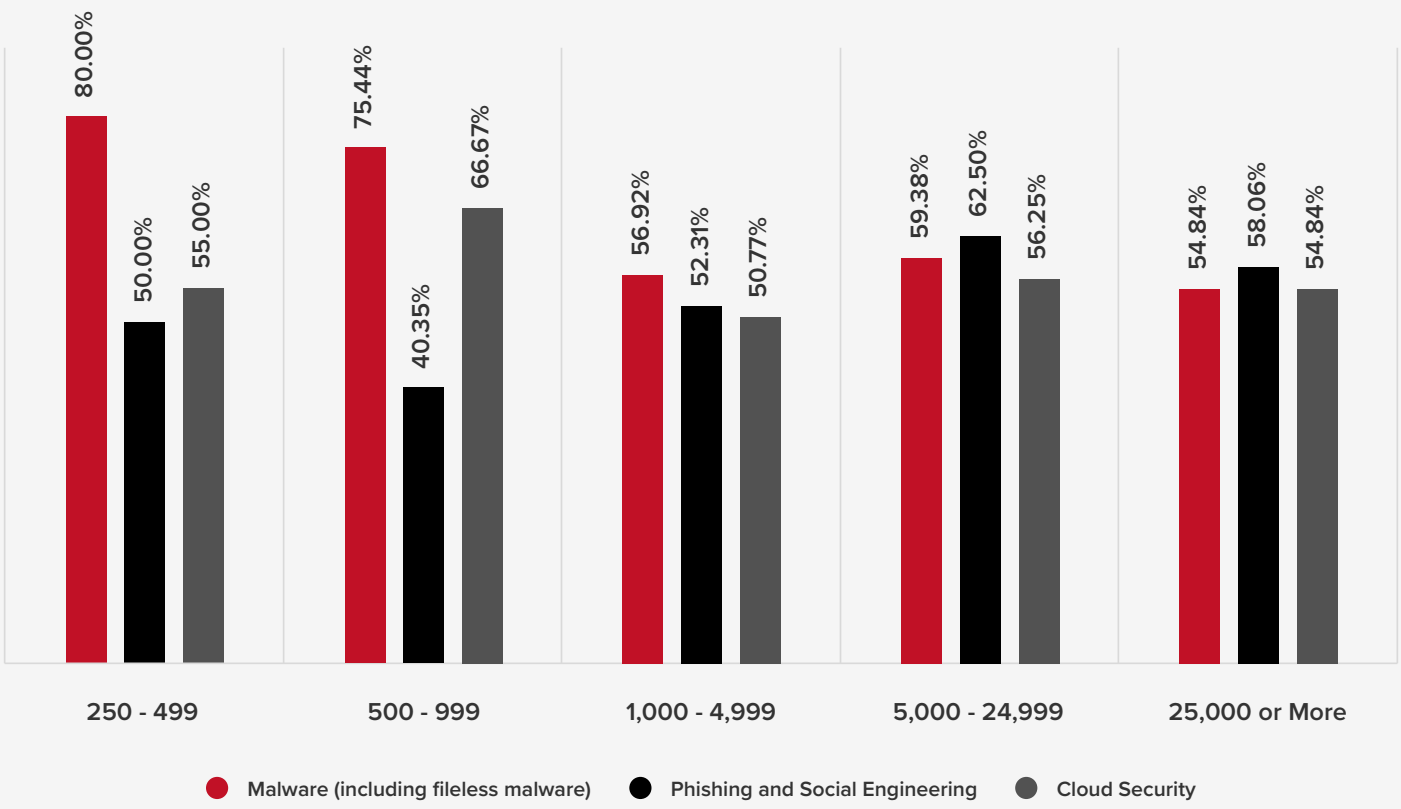


10.24%
Distributed Denial of Service (DDOS)

8.29%
SQL Injection

3.41%
Formjacking

Biggest cybersecurity challenges vs company size



When it comes to business size, small to medium sized companies (250 to 999 employees) are more concerned about malware (78%) compared to an average of 57% for larger companies, but cloud security is broadly even (averaging 57%) across all business sizes. Phishing is a greater concern for larger enterprises (over 5,000) at 60%, compared to just 40% for companies with between 500-999 workers.

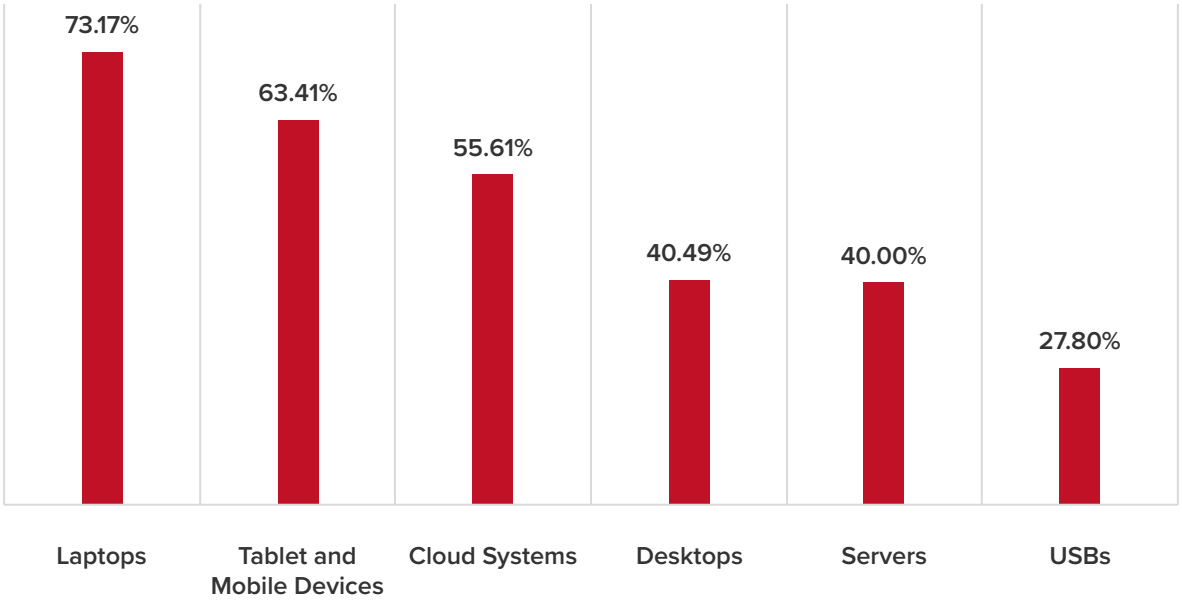
Nearly
three quarters
of IT leaders are extremely concerned about the security of their cloud-based systems, data and infrastructure.
(The State of Cloud Security)

Learn more in the "State of Cloud Security Report":

Read More

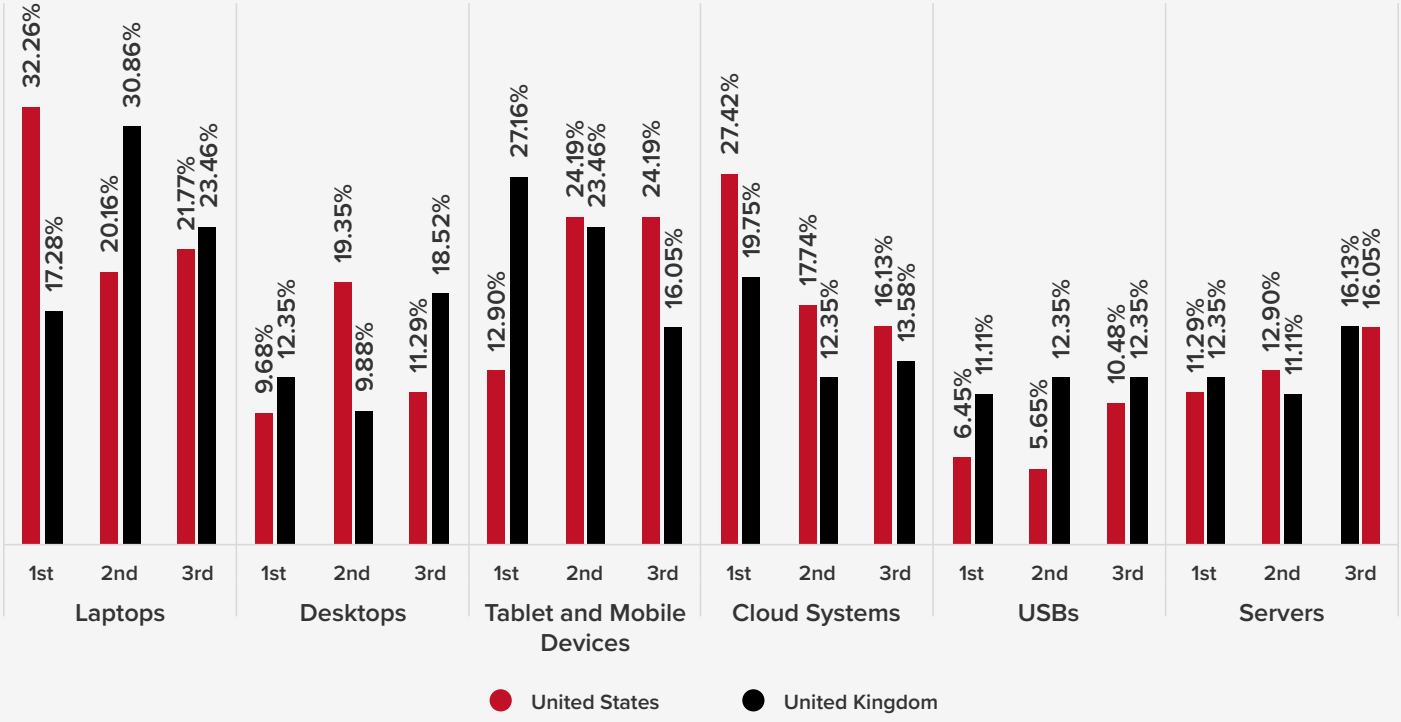
With an increasingly mobile workforce, the long-serving laptop remains the most vulnerable endpoint (73%), but beyond tablets, mobile devices and desktop computers, the more portable threat of a USB stick or device remains a threat for 28%.

Rank your most vulnerable endpoints

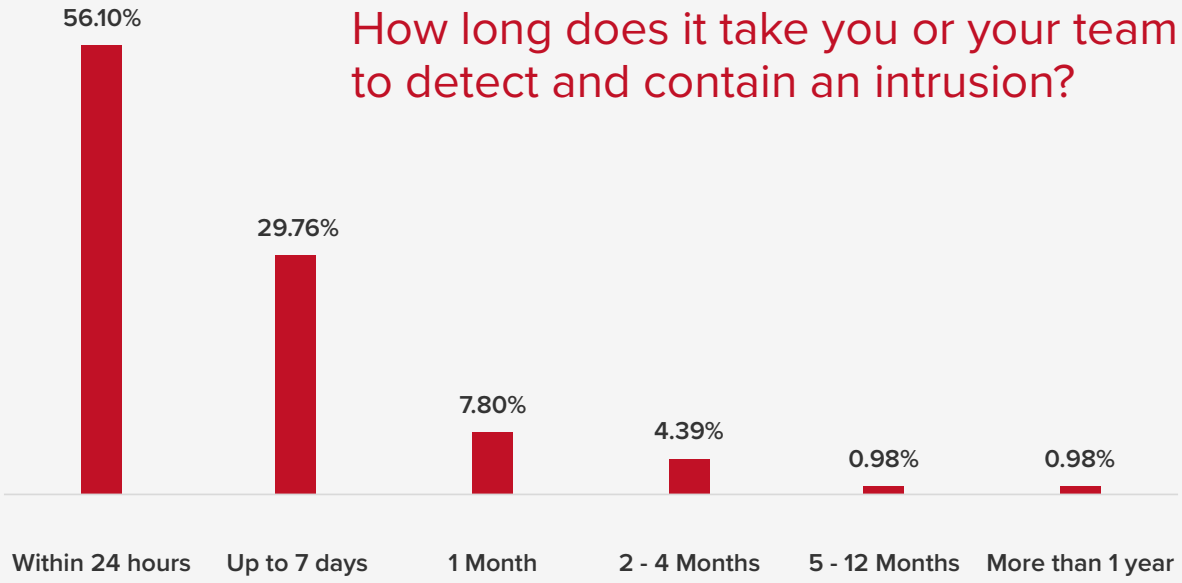


Across regions the US is more concerned about laptops (32%) while UK respondents rank tablets and mobile devices as the highest vulnerable endpoint threat (27%).

Most vulnerable endpoints vs region



How long does it take you or your team to detect and contain an intrusion?



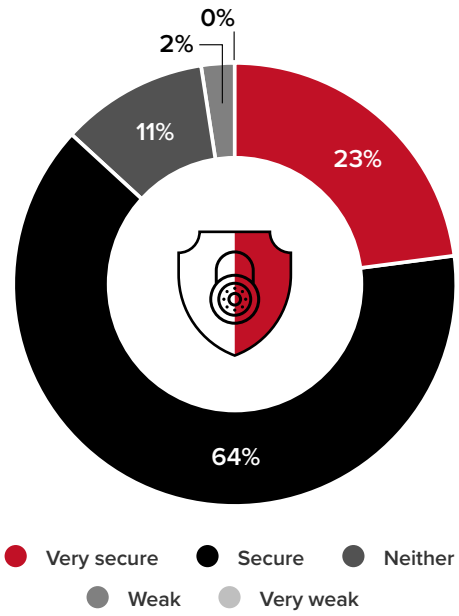
The positive aspect of this research is that 64% of IT professionals consider their cybersecurity posture secure while 23% consider their posture as very secure. However, that leaves 13% who are uncertain or less secure, with the risk and breach implications that a lower level of confidence brings.

The broader confidence is highlighted by 56% of respondents able to identify, respond and contain an incident within 24 hours. But in a landscape of increasingly automated attacks, those who take longer than a day will find their businesses likely compromised. With some companies taking up to 7 days (30%), the damage is likely done, and those who find an intrusion between 1-4 months (12%) could find serious damage done by invisible intruders.

The largest enterprises (25,000 or more) see cloud dominate as the most vulnerable endpoint at 39%.

The smallest companies (250 to 499 employees) rate laptops as the biggest threat at 35%.

On a scale of 1-5, rate your organization's overall security posture



For any business, the key to reducing the overall risk of a breach is to shorten the time to identify and mitigate any intrusion. This is achieved through software that automatically detects and alerts staff of new threats, ensuring all endpoints are secured and workers training in identifying the risks they face, backed up by live training via email and other sources to keep them alert. By organization, large businesses (1,000 to 4,999) are the least responsive with only 45% catching intrusions within 24 hours. Due to their size and organizational complexity, only the larger enterprises report any incidences (between 1.5 and 3%) where it took from 5 months to over a year to contain an intrusion.

Detecting and containing intrusions vs company size

Only

45%

of businesses with 1,000 to 4,999 employees catch intrusions within 24 hours.

Enterprise Security
Research Report

Remote/hybrid working challenges

3

CHAPTER 3:

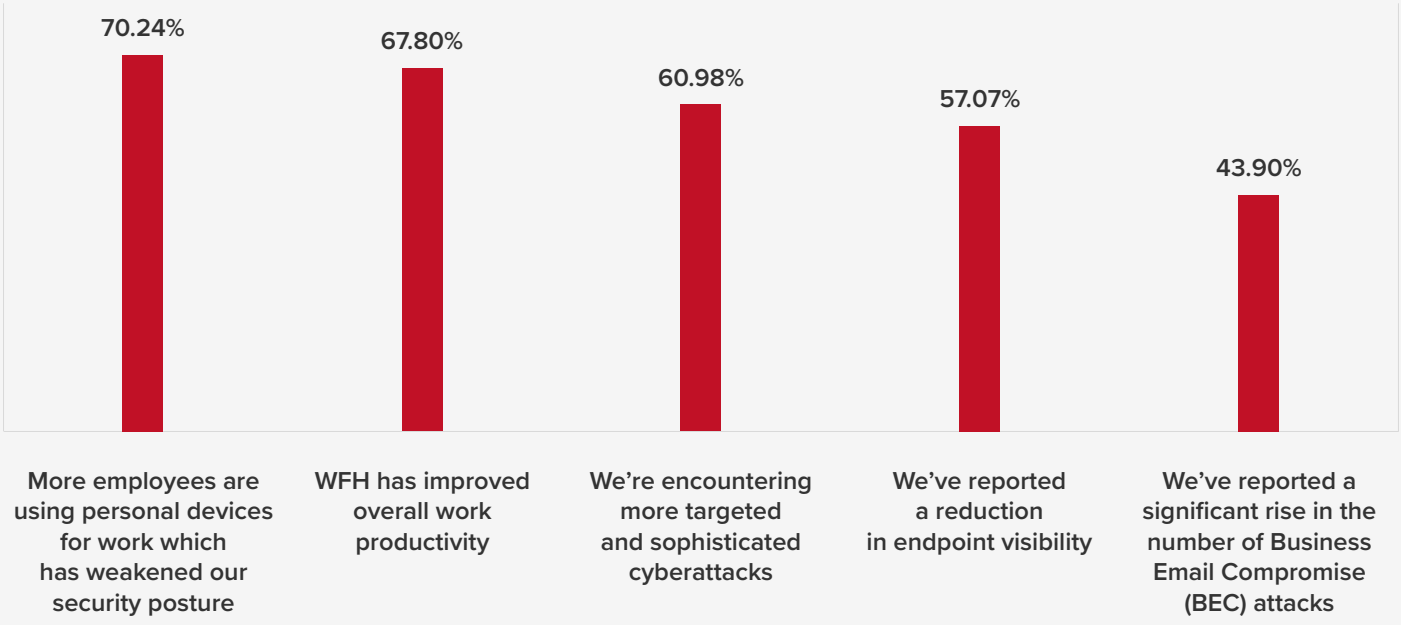
Remote/hybrid working challenges

Many businesses were increasingly prepared to offer remote working as an option before COVID-19, benefiting executives and knowledge workers. However, the pandemic created a seismic shift in working patterns, with wider ranges of roles, enabled by technology, working remotely and creating a generation of workers who enjoy the benefits of keeping out of the office.

While there were many benefits for workers, and their efforts helped keep businesses operating over the course of the pandemic, the strain on IT and a need to make fast-paced decisions created an environment that created more risk, which must be addressed today and as wider remote and hybrid working efforts are considered.

In this changing landscape, two-thirds (68%) of businesses reported an improvement in productivity. However, 70% of companies are concerned that the use of personal devices for work weakens security. Examples include reduced endpoint visibility according to 57% of respondents and a major rise in business email-based attacks, noticed by 44% of respondents.

Many organizations have embraced remote working due to COVID-19. Which of the following statements apply to you?



Around

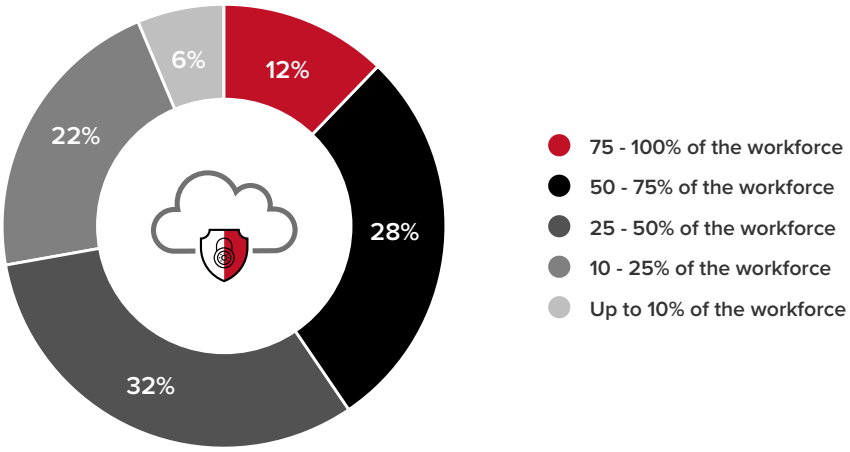
58%

of our survey respondents are prepared to spend between **$100,000** and **$1 million** on IT security in order to overcome their own security challenges.

Additional threats from remote and hybrid working styles include the risk of data being used on insecure or public storage services, such as Google Drive, Microsoft's OneDrive and others. Storing data off official servers creates a different type of business hazard. If that data is found and reported or stolen, companies are liable to GDPR consequences for the misuse of data.

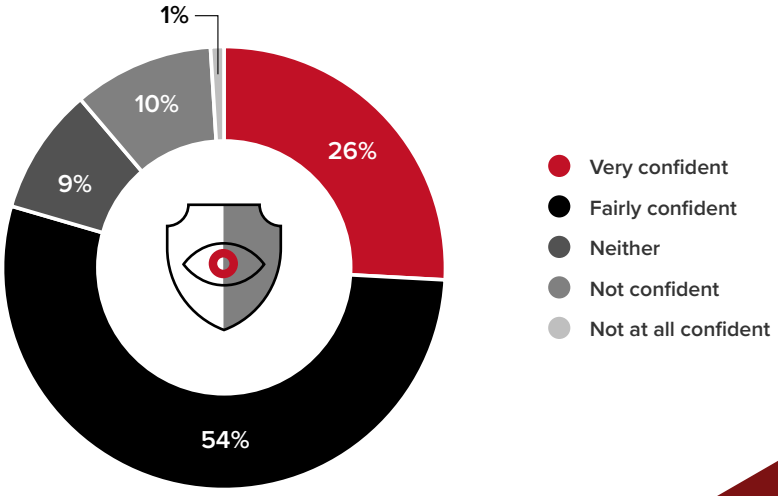
That could result in hefty fines, and with 41% of respondents identifying that over half of their workforce were using common cloud storage, there's likely a lot of insecure data that could easily be accessed, even if workers believe the storage service they're using is secure.

How many employees are using file sharing?

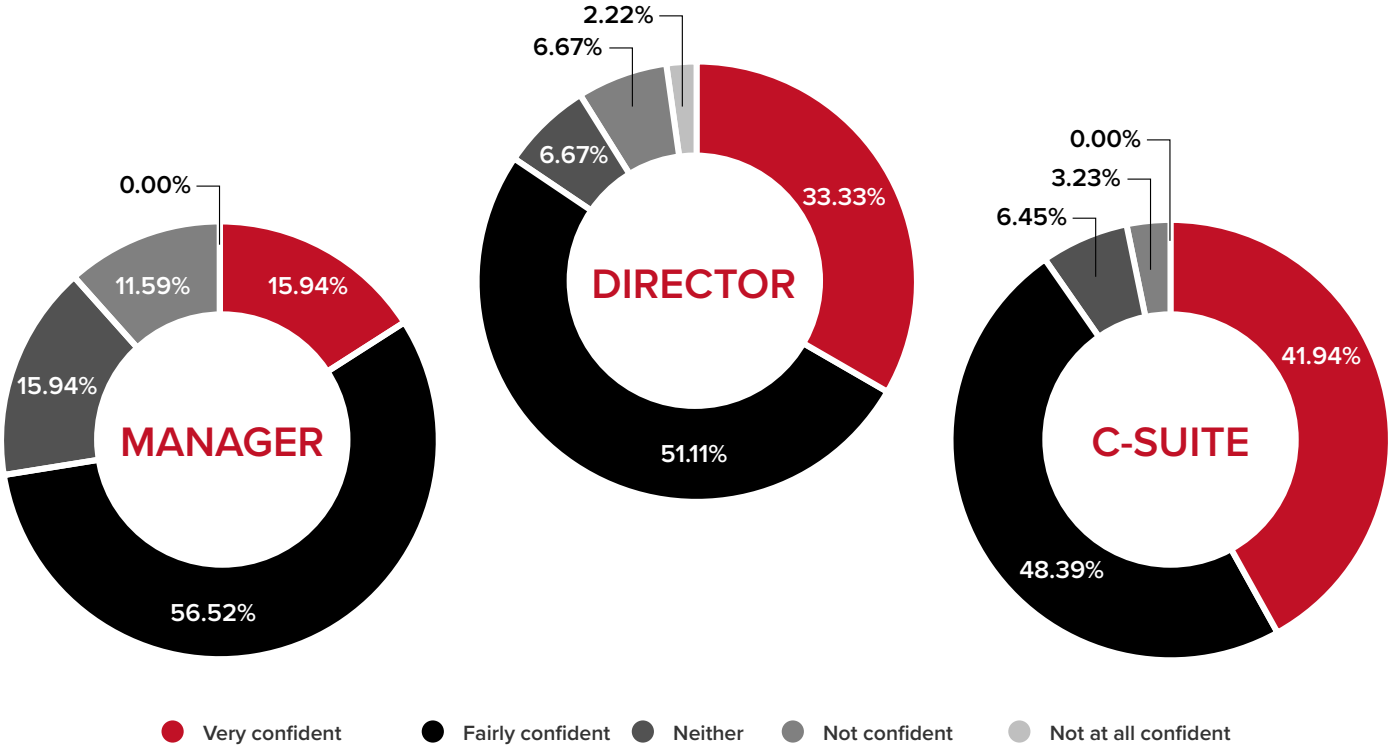


Businesses can prevent data from being stored on unsanctioned services by using Data Loss Prevention (DLP) applications and enforcing strict application usage. This is necessary as even though most respondents (80%) were fairly or very confident in their employees' security awareness, it takes just the one ill-informed, untrained or over-confident worker to create a business-wide issue. And for the 11% of respondents who were not confident in their workers' security awareness, the risk of a breach grows by the day.

How confident do you feel about your employees' level of security awareness?



From the top, 48% of C-Suite respondents are fairly confident and 42% report they're very confident, suggesting there's some work to go to harmonize the views of key roles. By role, 51% of Directors are fairly confident in their employees' level of security awareness, while almost 28% of Managers are neither confident or unconfident about their staff.



In the US, a level of enthusiasm or stronger training sees 32% of respondents indicating they're very confident, while in the UK only 16% of respondents feel that optimistic about their workers' security awareness.

Enterprise Security
Research Report

Data protection and security

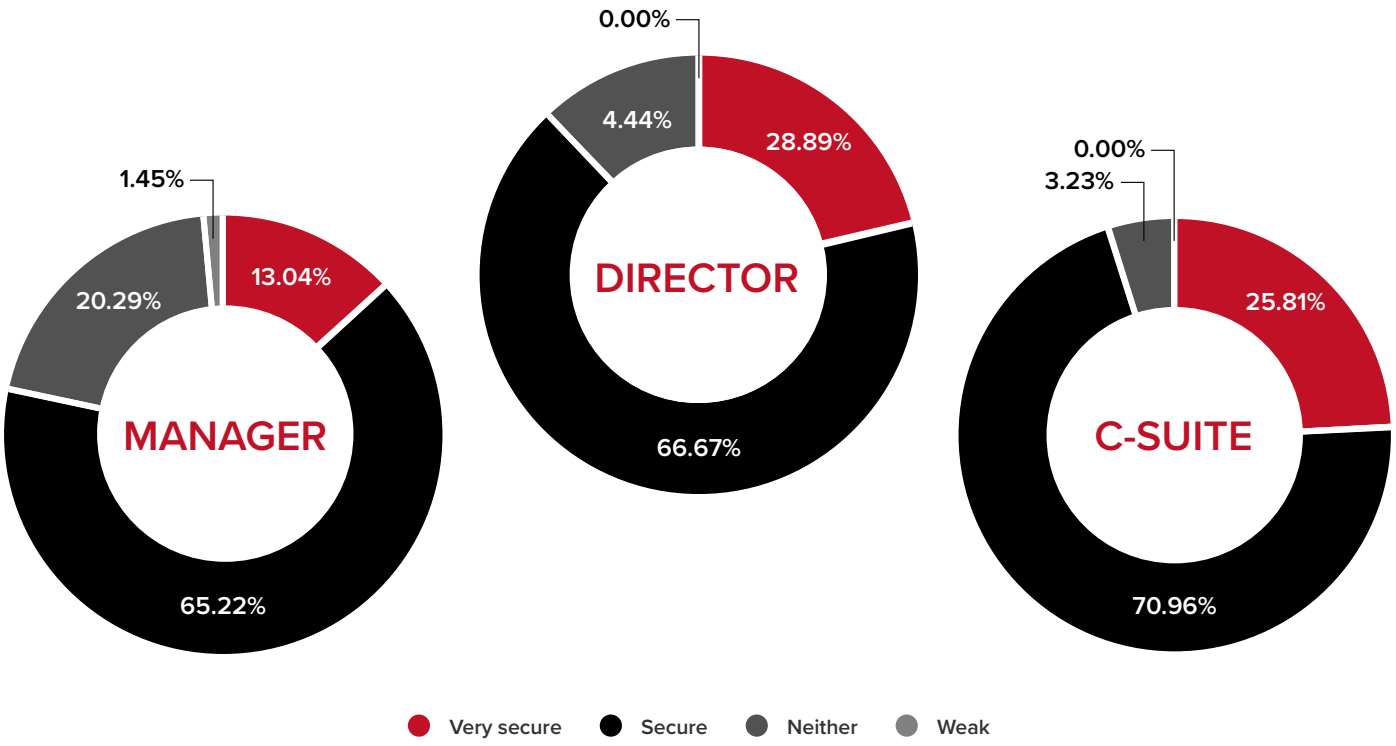
4

CHAPTER 4:

Data protection and security

Whether a company is gradually evolving and updating its IT services, or as part of any IT-led digital transformation, data protection must be at the forefront of any strategy. While the cloud may sound like a complex and technical landscape, gaining visibility into data, where it moves and what state it's stored in is key to developing a strong security posture. By role, C-Suite and Directors overwhelmingly believe their organization is secure or very secure, while only 65% of Managers believe their organization is secure with 13% in the very secure mindset.

Overall security posture vs seniority level



In the UK, only

6%

of companies rate their overall posture as weak compared to zero in the US. 17% of UK respondents think they're very secure, compared to 27% of those in the US.

Wherever a business keeps its data, be it on networked servers, within a data center or using private, public or hybrid cloud, when it comes to protecting that data, end-to-end security is required. CIOs and CISOs should be aware of the **six pillars of cloud security**, which features data protection as part of an overall protection solution with layered defenses:

1. Secure access for authenticated users and devices
2. A zero-trust approach to network security
3. Change management and compliance
4. Use of a Web Application Firewall (WAF)
5. Strong data protection
6. A continuous monitoring and improvement effort

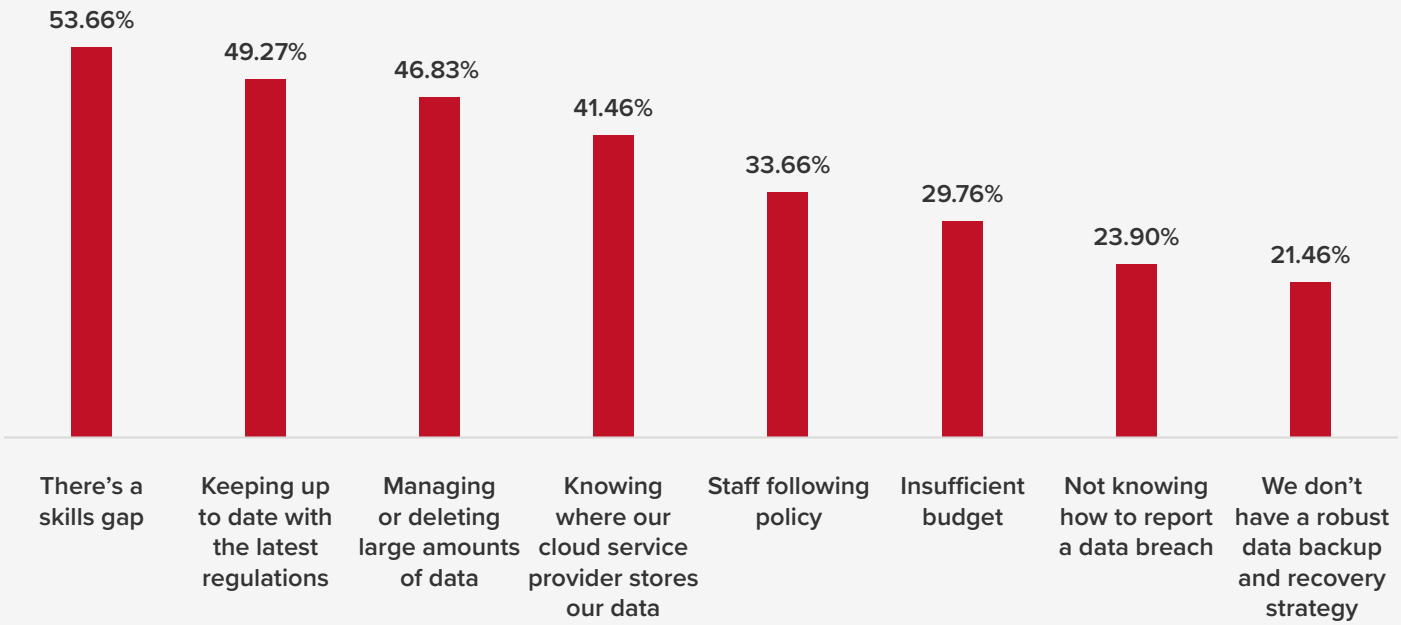
Enabling such an array of applications can be a headache for business, especially those focused on bottom line growth, or keeping the lights on in tough times. The leading pain points for IT leaders were a skills gap (54%), which can result in insufficient business knowledge to deliver a solution.

If there's any comfort in the numbers, organizations large and small struggle with this issue. While cloud partners or ISVs can deliver general or optimized security, they may not be fine-tuned to meet business needs.

The second most common data protection pain point (very similar across region and organization size) was keeping up with the latest regulations (49%). Most businesses should have an IT security office whose role includes understanding changes in regional, local and industry-specific regulations, and ensuring the business complies with them.

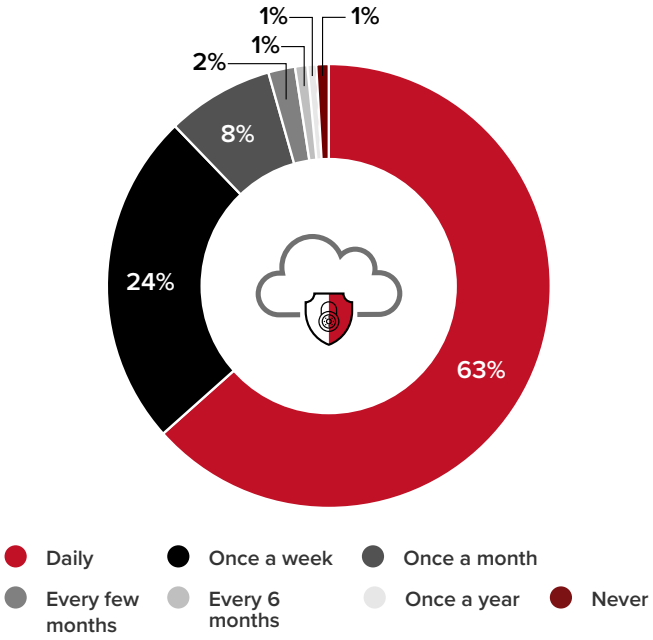
Managing and deleting large amounts of data (47%) is the third most common pain point, an issue which can be best managed by having a thorough grasp of the first two. Storing data securely and in compliance with regulations can resolve many of the issues businesses have as their data footprint grows.

What are your biggest data protection pain points?

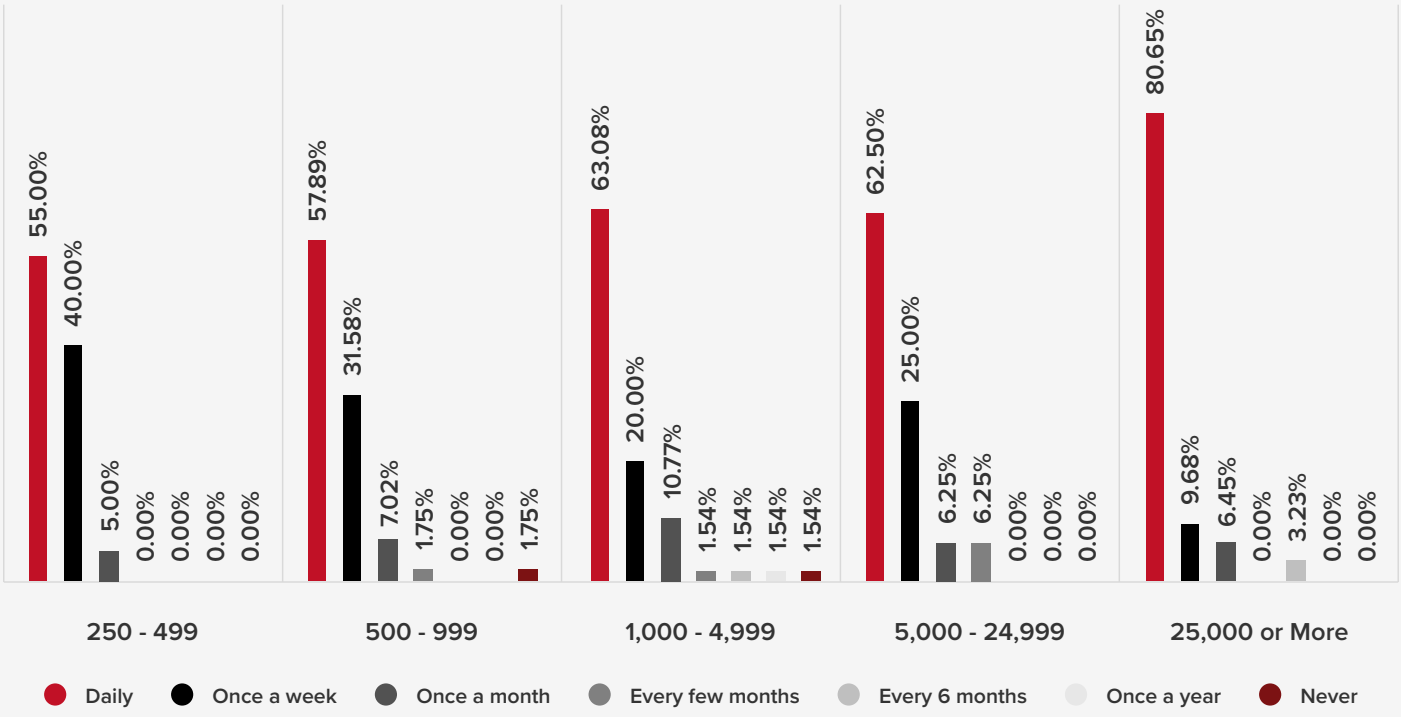


Related to that issue, it's a strong positive to see that 63% of businesses back up their data daily, with 24% of respondents doing so weekly. There's a strong curve by organization size with around 81% of large enterprise respondents backing up daily, tailing off to just 55% of the smallest firms. This approach will add business recovery efforts if there's ever a major event, and can mitigate ransomware attacks, if the company protects those backups and stores them remotely to prevent the ransomware perpetrators from accessing them.

How often do you backup your data?



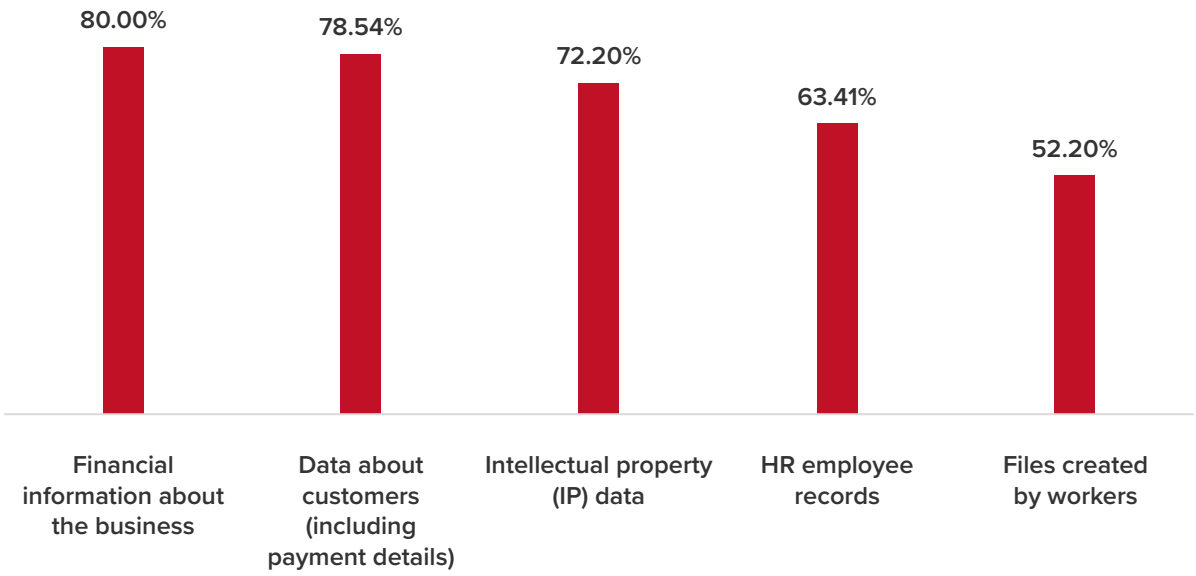
How often do you backup your data vs company size



Another key way to strengthen the business posture is through data encryption, and again, we see the majority encrypt key data types. However, if only 80% of organizations are encrypting key financial data, then 20% remain vulnerable if hacked to further financial theft or exposure to greater risk.

Strong backup and encryption procedures in line with regulations and going beyond the basics will help ensure any business remains secure, or can recover faster and with less damage compared to a business that makes only the minimum effort at data protection.

Which data do you encrypt?



Enterprise Security
Research Report

IT professionals' upcoming priorities

5

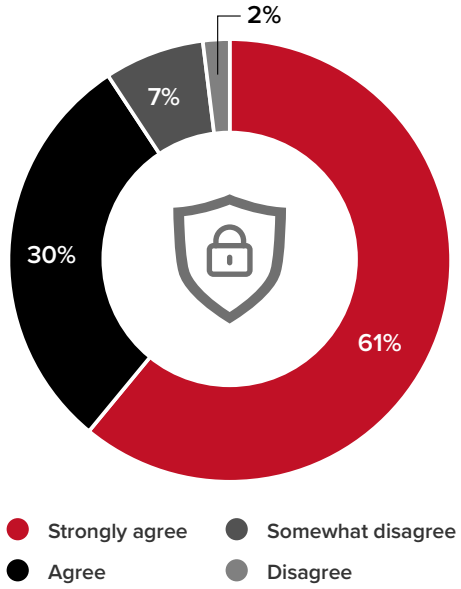
CHAPTER 5:

IT professionals' upcoming priorities

As with most areas of business, IT professionals have too much to do and insufficient staff, time or budget to achieve all of their goals. However, with IT security top of the list, it remains their priority, with 91% of professionals strongly agreeing or agreeing and heartened to hear that their boards take cybersecurity seriously.

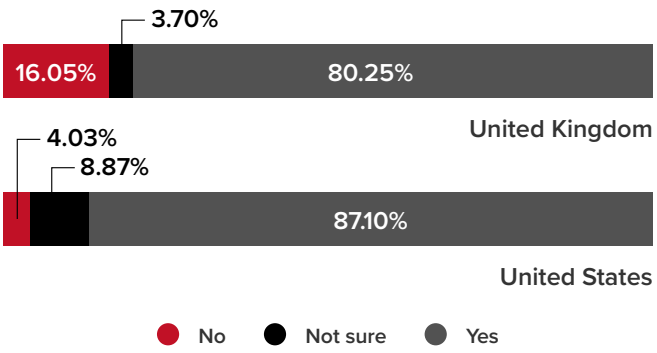
By region, only 4% of US respondents claim they lack the budget to keep systems sufficiently secure, while in the UK, 16% of respondents feel underfunded. When it comes to business size, there's a disparity between enterprises (5,000 to 24,999 employees) – with 16% reporting they're underfunded compared to just 3% of larger enterprises (25,000 or more) – and large businesses (1,000 to 4,999) at 8%.

To what degree do you agree with this statement: "My company board takes cybersecurity seriously" ?



Of the 2% that disagree the board takes the issue seriously, their challenge is to convince the board of the risks they face, demonstrate the value of a strong security posture and establish the risk of not addressing these concerns.

Do you have enough budget to keep your systems sufficiently secure vs region



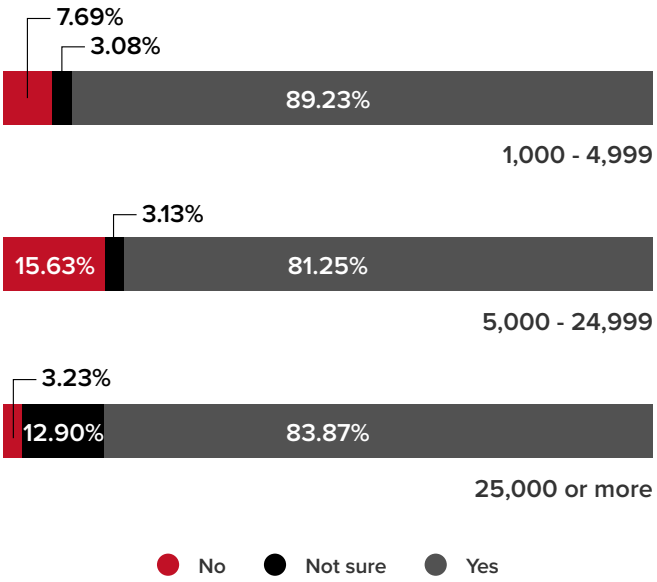
Around

16%

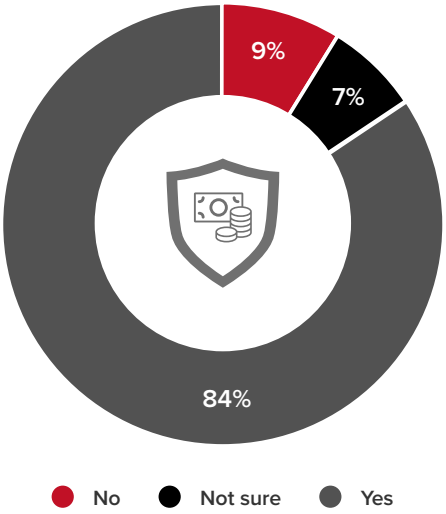
of respondents in the UK feel underfunded.

On the topic of ensuring board support, a similar level of respondents (84%) are provided the funding to adequately protect their servers. The remaining 16% should be looking at ways to improve security through direct funding, as part of wider IT solutions or adopting open source solutions that can increase security until a full strategy can be enabled.

Do you have enough budget to keep your systems sufficiently secure vs company size

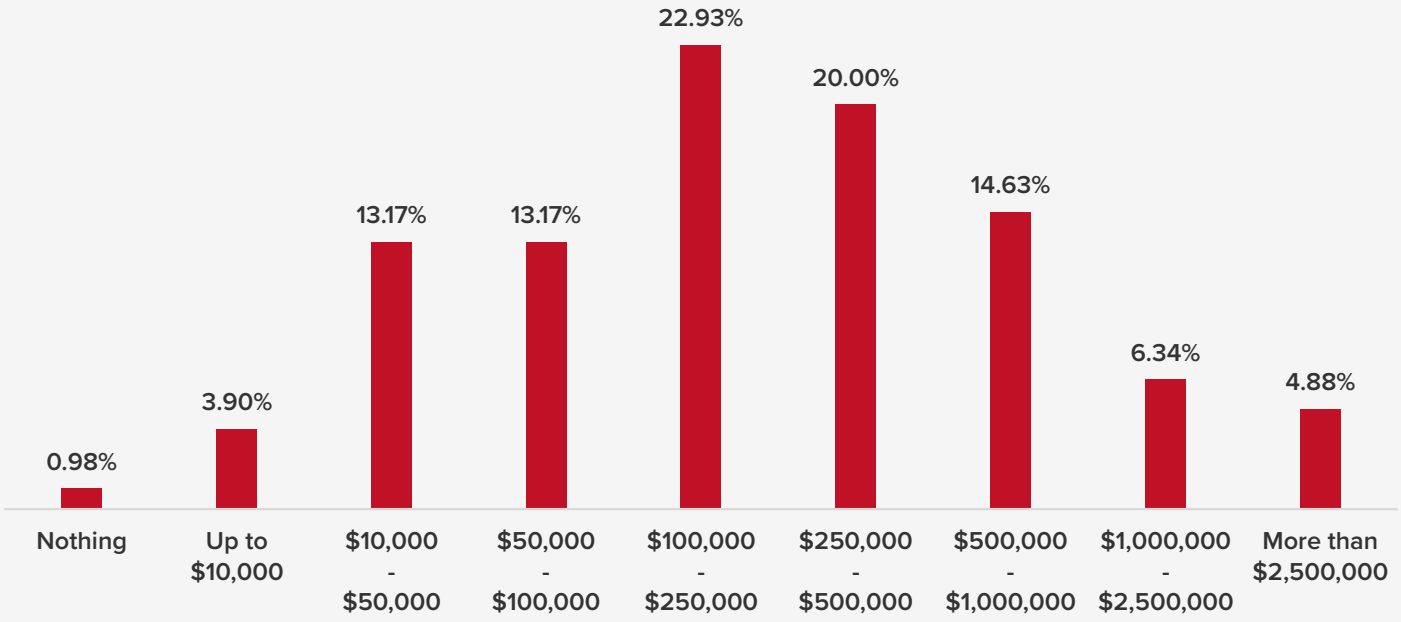


Do you have enough budget to keep your systems sufficiently secure?

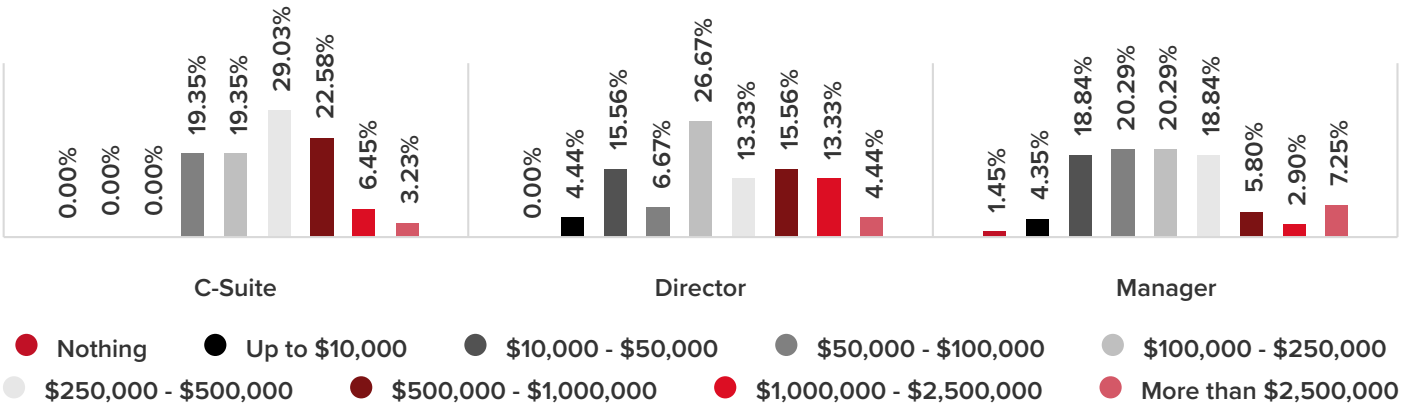


IT budgets naturally vary depending on the size and the IT focus on each company. Significantly, the 58% of respondents whose companies spend between $100,000 and $1,000,000 on IT security should act as the pacesetters for other companies who are unsure about how much they should be spending.

How much are you planning to invest on security solutions in the coming 12 months?



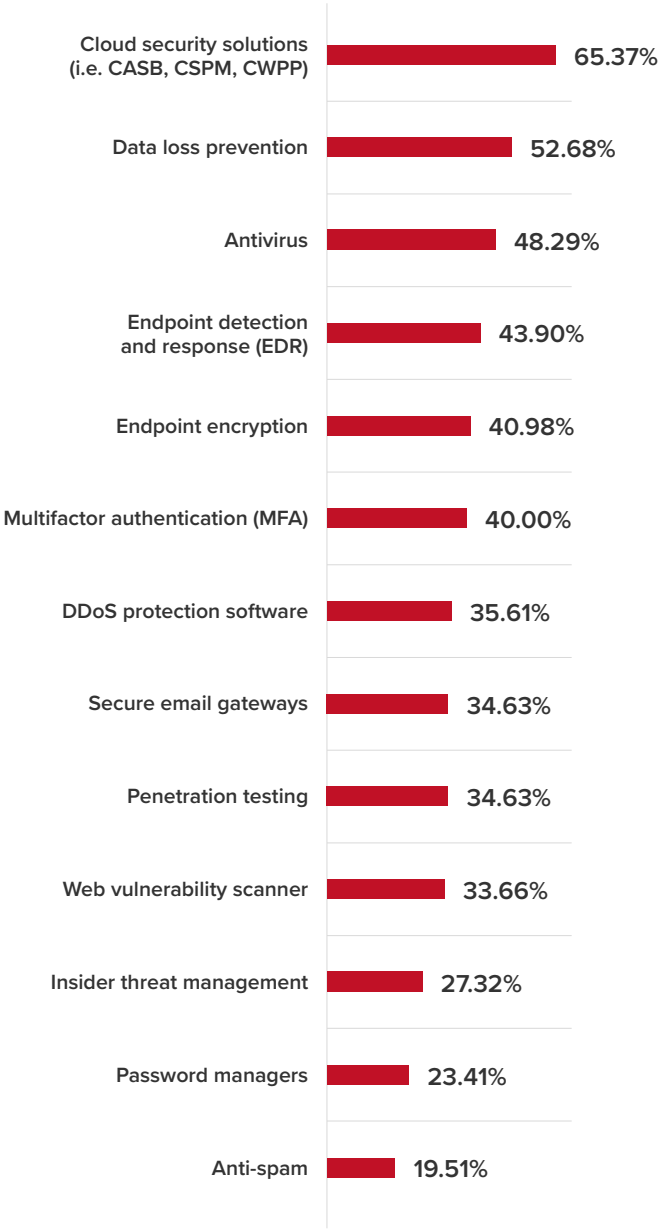
By role, budgets naturally vary. Around 52% of C-Suite executives are prepared to spend between $250,000 to $1,000,000 on new security solutions, with 40% of Directors likely to spend $100,000 - $500,000. Interestingly, two-thirds (64%) of Managers are only prepared to spend up to $250,000 on new security solutions.



Savings can be made and IT security improved as part of cloud migrations, digital transformations or rationalizations of legacy systems. IT security should never come as an afterthought to any of these projects. When it comes to areas of focus, most IT professionals are looking at **cloud-level security**, with 65% investing in cloud access security brokers, cloud security posture management and cloud workload protection platforms to secure data at any point in its journey.

Data loss prevention (53%) and antivirus solutions (48%) are the next most-popular investments, helping to prevent breaches and mitigate any damage. Following closely are endpoint detection and response (EDR) at 44%, endpoint encryption (41%) and multifactor authentication (MFA) at 40% to help secure users and devices, creating a rounded approach to protecting the business.

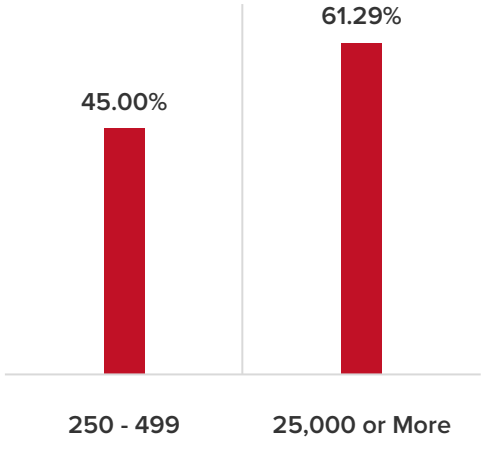
Which security solutions are you prioritizing?



By role, C-Suite respondents are mainly focused on cloud security at 32%. Nearly one-third of Managers (32%) see antivirus as their biggest priority, while Directors don't – instead they're most interested in cloud security solutions (24%), followed by endpoint encryption (13%), data loss prevention (11%) and DDoS protection (9%).

By company size, medium-sized businesses (500-999) are focused on cloud security (23%) and the smallest firms (250-499) are most focused on antivirus technology (40%). Enterprises (5,000-24,999) ranked multifactor authentication as their number one priority for investment at 19%. In the largest enterprises (25,000 or more), it's not surprising to see that endpoint detection and response (EDR) software is the biggest priority (29%) – especially considering that nearly two-thirds (61%) of business leaders reported a reduction in endpoint visibility (compared to 45% in the smallest firms).

We've reported a reduction in endpoint visibility vs company size



These tools increasingly make use of AI and automation to identify incidents and reduce the workload on the IT department, enabling them to focus on other key tasks and respond to any incident faster than ever before. While the battle against malware and hackers will never be over, well-defended businesses will find the workload more manageable than those trying to cope with legacy defensive tools.

The security battle is moving to the cloud, and businesses need to focus on remote workers using bring your own device (BYOD) as the weak points in the chain.

Growing numbers of edge-connected devices and Internet of Things (IoT) devices will also pose risks that need to be managed. Again, automation can help support thousands or millions of users, devices and data workloads, which IT will come to rely on as businesses expand and grow.

Conclusion

The findings in this report, and the general trends toward cloud, mobility and automation, highlight the risks for data privacy, security and service availability that any business must manage. They're legally obliged to protect data, and to create a digitally safe workplace for users and customers – one where IT security is a key priority with proper investment. This is the only way to reduce the risks and improve data protection across any business.

As cloud service providers have become used to the threat landscape, they already (or will) provide security features that meet business needs and work across multiple applications or services, enabling any business to have a single-dashboard view of its total threat landscape. This will make it easier for the business to monitor and control security across the organization, but will still require knowledge and investment to deliver the right solution that best supports each business and enable manageable, secure growth.

IFP Insights For Professionals

About Insights for Professionals

IFP gives you access to the latest business knowledge that's customized for you. We provide high quality, credible and relevant resources for senior professionals in one place.

An easy to access and personalized library to help you when you are researching specific topics, seeking practical advice, or simply want to stay ahead of what's happening in your industry. To do this we gather the best content from suppliers, brands and industry experts, as well as doing our own research.