





RISK MANAGEMENT REPORT FOR SMB CYBERSECURITY LEADERS 2023

Find out how security leaders are adapting to a rapidly changing risk environment.

 www.blackfog.com

 info@blackfog.com

RISK MANAGEMENT IS DIFFERENT FOR GROWING ORGANIZATIONS

Small and mid-sized businesses face unique threats in today's threat landscape. These organizations don't command the same resources as large enterprises, yet they must respond to many of the same kinds of cyberattacks.

These attacks increasingly use a sophisticated combination of social engineering, credential compromise, and technical exploits to infiltrate target networks. Organizations with less than 1000 employees often have limited options for protecting themselves in a reliable, cost-effective way.

In partnership with Sapio Research, we conducted a risk management survey of 400 security leaders throughout the United States and United Kingdom. The scope of this research was to identify how different leaders and types of organizations are responding to ongoing risk management trends.

Our findings showcase the value that third-party security services provide for smaller organizations, especially when it comes to implementing new solutions in the security tech stack. They also suggest that technologies like anti data exfiltration have an important role to play helping small to medium sized organizations achieve security performance on par with large enterprises.

Security leaders at small to mid-sized organizations are navigating an uncertain threat landscape. Finding trustworthy partners and implementing effective prevention-based security technologies can make a significant difference in their overall risk management strategy.



2023 RISK MANAGEMENT

REPORT KEY FINDINGS:



Mid-sized businesses report being exposed to the highest level of risk. 61% of respondents in organizations with 100 to 999 employees have experienced a data breach in the last 12 months. 71% of respondents believe these organizations are the most vulnerable.



Malware is the top concern that security leaders report having. 50% of respondents report that malware attacks are their top concern. Among security leaders who have experienced a successful cyberattack, 42% report that the attack was malware-based. 58% reported business downtime occurring as a result of the attack.



Security leaders are enthusiastic about the performance of IT teams. 91% of security leaders believe they are aligned with their IT teams when it comes to addressing cybersecurity challenges. 93% report being satisfied they are up-to-date on the latest innovations in the cybersecurity space.



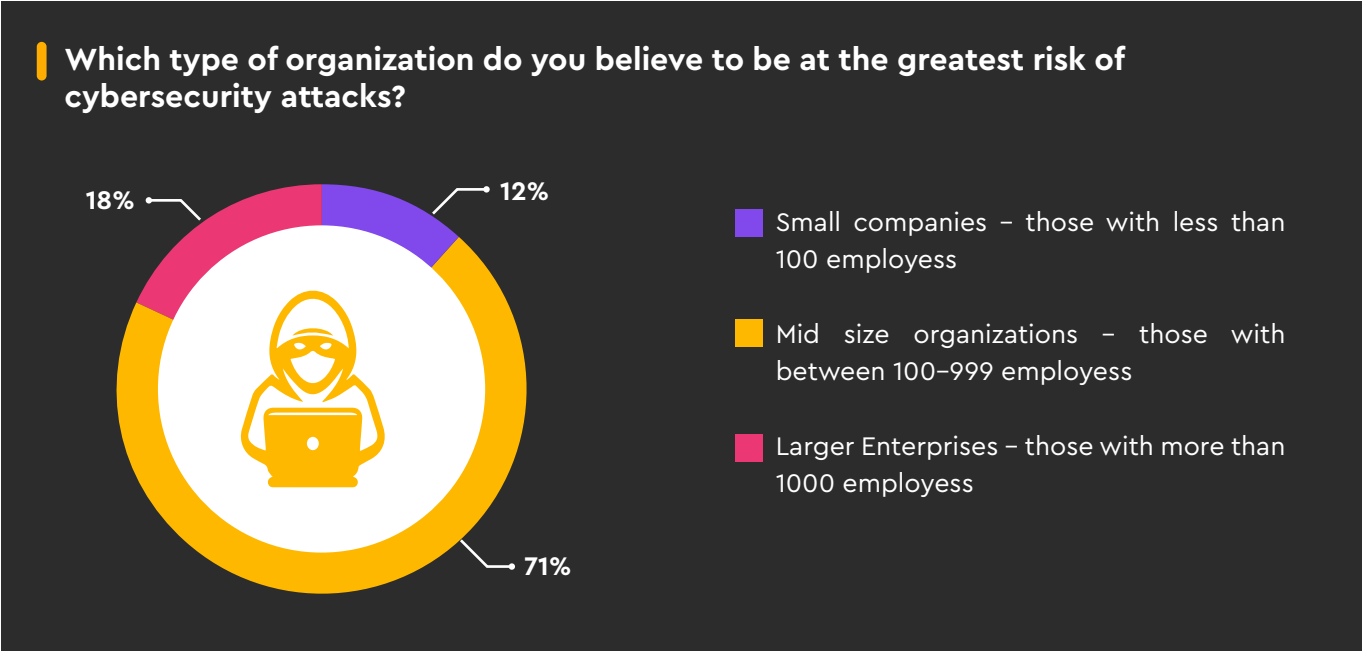
Awareness doesn't always lead to understanding. There is a disconnect between awareness of cybersecurity technologies and deep understanding of how they work. 77% of respondents report being aware of anti data exfiltration (ADX) technology, but only 42% report having in-depth understanding of it.



24/7 technical support and high security standards are vital. Organizations that rely on third-party IT service and security providers report prioritizing 24/7 technical support (41%) and high security standards (38%) above all other considerations.

MID-SIZED ORGANIZATIONS: PRIME TARGETS FOR CYBERCRIME

The majority of security leaders at mid-sized organizations feel that their companies represent the highest risk of cyberattack. These organizations command more resources than small businesses with less than 100 employees but may not have the robust security resources of an enterprise with more than 1000 employees.

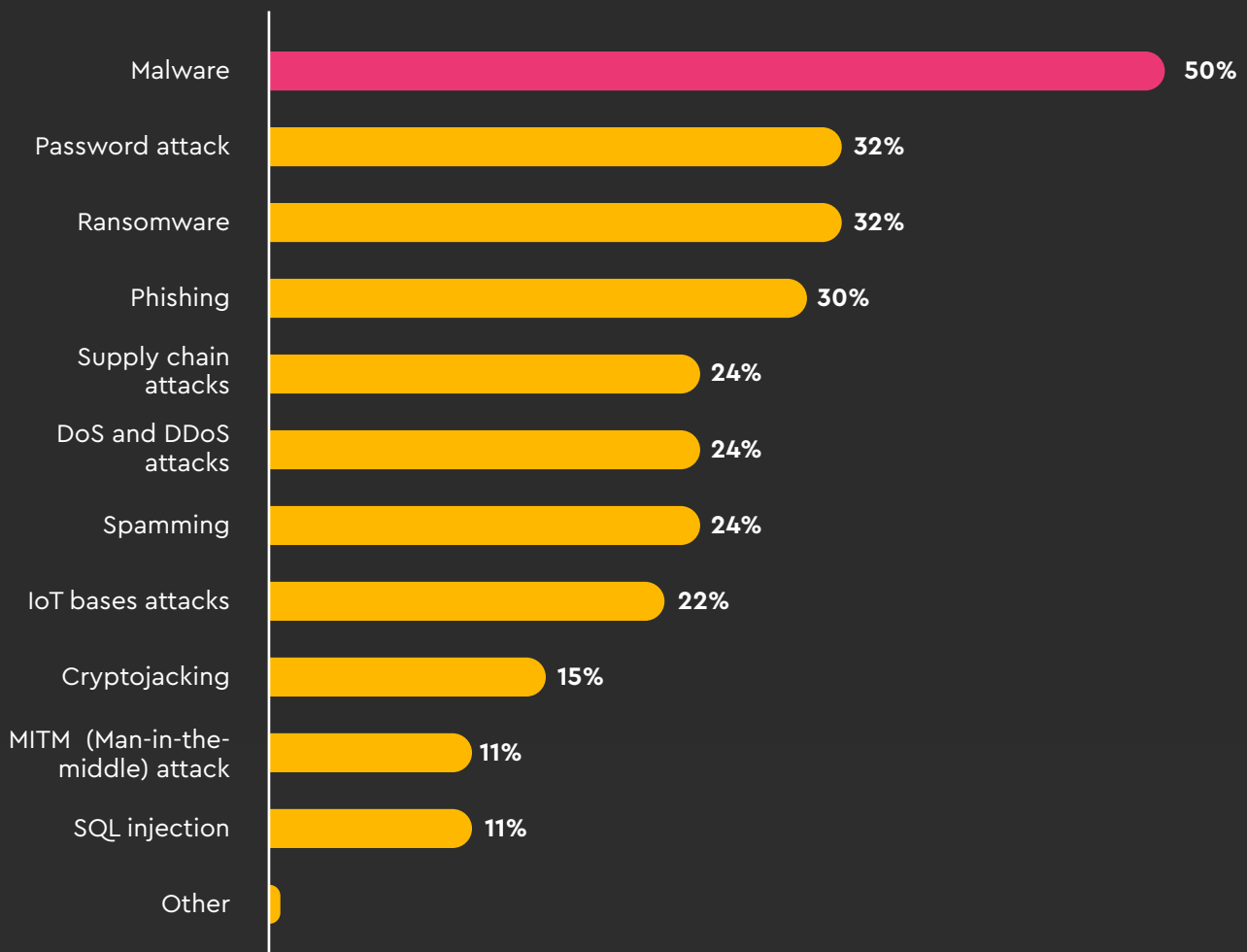


SECURITY LEADERS AGREE: MALWARE IS THE TOP PRIORITY

Malware represents the top concern security leaders at mid-sized organizations report having. For the purpose of the survey, ransomware is treated as a distinct type of threat, and corresponds to a slightly lower degree of concern, alongside credential-based attacks and phishing.

Malware is an incredibly broad threat category but keeping it distinct from ransomware helps to narrow it down to newer variants that serve different purposes. Credential-based attacks include both malicious insiders and account takeover attacks, both of which are difficult to address without a sophisticated risk management strategy.

Which cybersecurity threats are the most concerning for your organization?

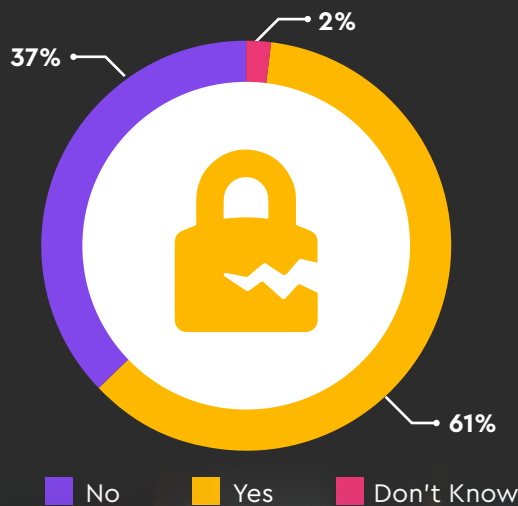


CYBERATTACKS AGAINST MID-SIZED ORGANIZATIONS REMAIN PREVALENT

61% of respondents reported that their organization experienced a data breach, malware, or ransomware attack in the previous year. Of these, 70% of attacks were reported by IT security leaders, while 45% were reported by executive leaders. There is some overlap because these roles are not mutually exclusive.

Additionally, there was a significant increase in the volume of reported attacks against larger mid-sized organizations with at least 500 employees. These represented 68% of reported cyberattacks taking place over the past twelve months.

To your knowledge, has your organization experienced a successful data breach, malware attack or ransomware attack the last 12 months?

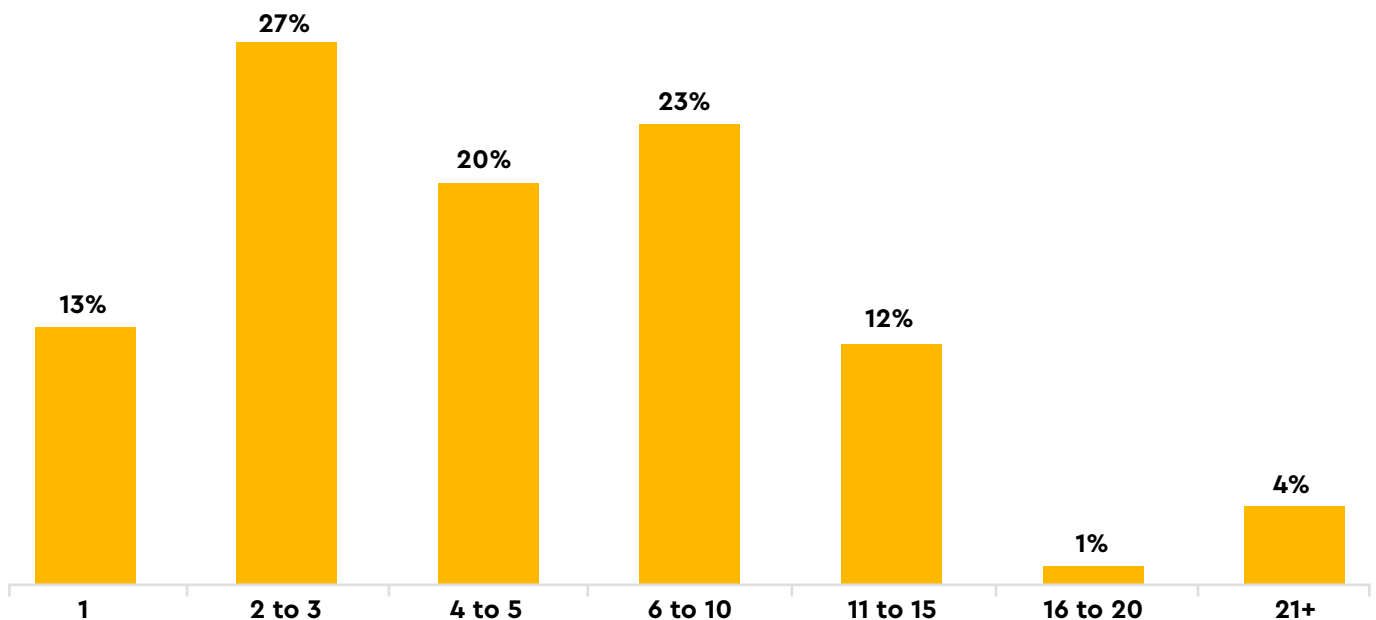


ORGANIZATIONS EXPERIENCED NEARLY FIVE SUCCESSFUL CYBERATTACKS IN THE LAST YEAR

The median number of successful cyberattacks faced by mid-sized organizations in the past year is **4.93**. The highest prevalence is actually lower, at **2-3** cyberattacks, but this is counterbalanced by statistical outliers that reported a much higher volume of incidents.

Respondents based in the United States reported a slightly higher average of cyberattack events in the past year, at **5.69**. Respondents in the United Kingdom reported a lower average, at **4.24**.

To your knowledge, how many successful cyberattacks has your organization experienced in the past 12 months?



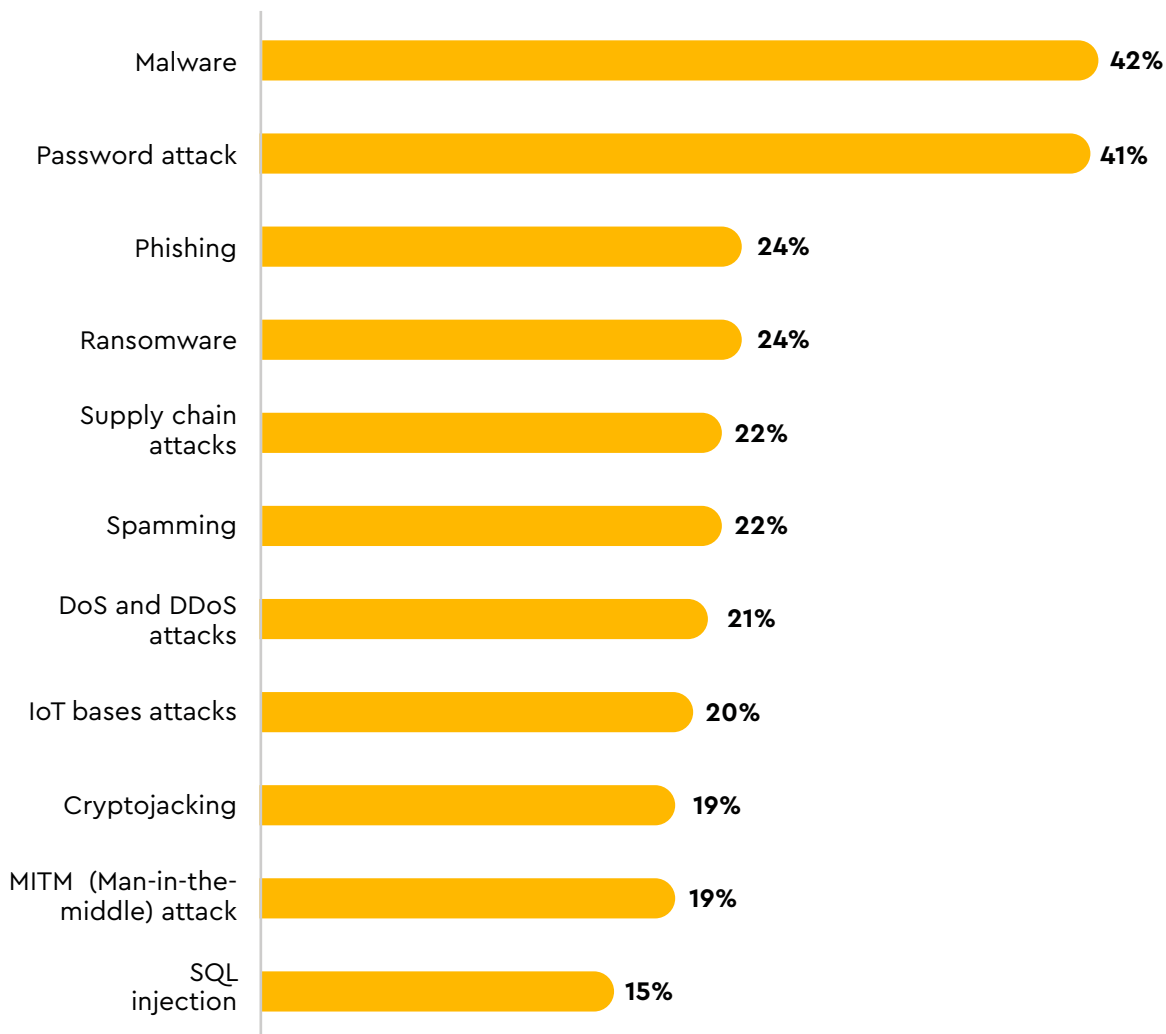
MALWARE AND CREDENTIAL-BASED ATTACKS ARE THE MOST PREVALENT TYPES OF CYBERATTACK RESPONDENTS REPORTED

Malware and password attacks respectively made up **42%** and **41%** of all reported cyberattacks, with all other attacks significantly lower in volume. Since the majority of organizations reported multiple attacks, these figures add up to more than **100%**.

Malware is slightly more prevalent in the United States than in the United Kingdom. For UK-based respondents, credential-based attacks were actually higher than reported malware attacks.

Similarly, US-based security leaders reported higher incidents of ransomware, spamming, DDoS attacks, Man-in-the-Middle attacks, and SQL injections than UK-based respondents.

What kind of cyberattacks did you experience?



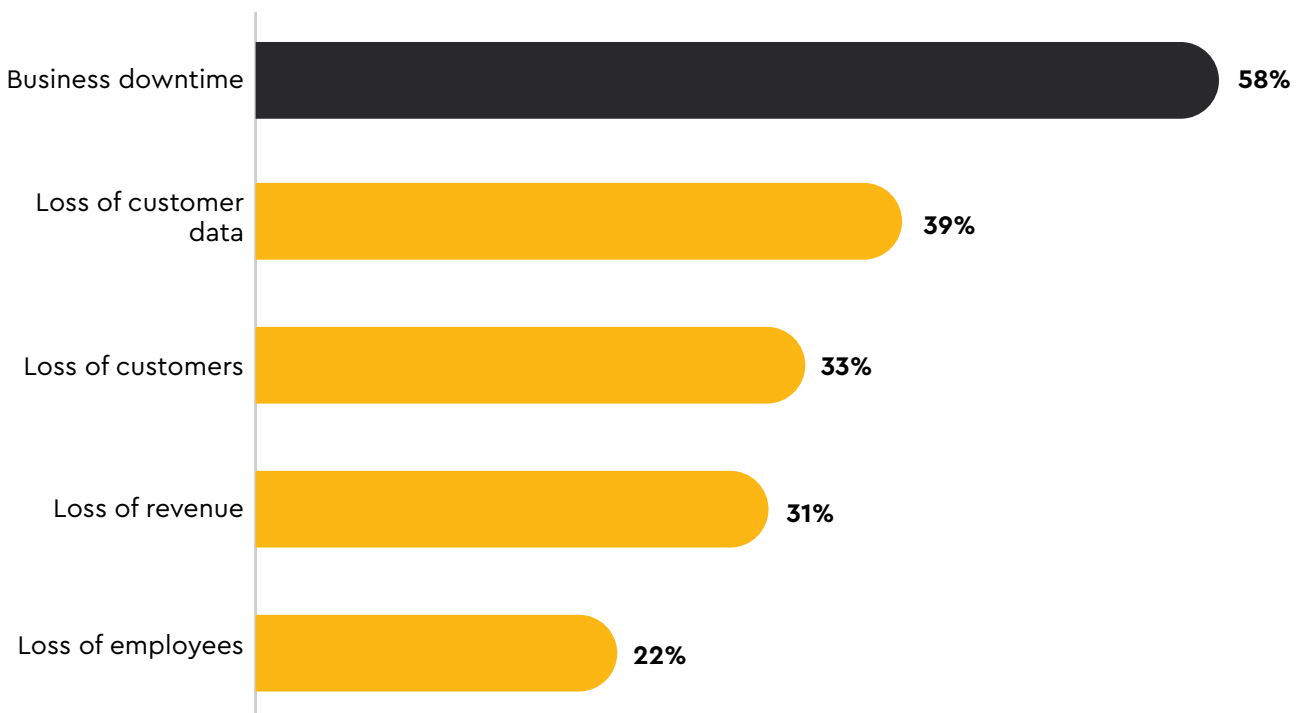
BUSINESS DOWNTIME IS THE MOST CONCERNING COST ASSOCIATED WITH CYBERATTACKS

A clear majority of respondents reported business downtime as their primary concern when it came to responding to security incidents. However, loss of customer data, loss of customers, and loss of revenue were not far behind.

Just under half of director-level respondents reported being concerned with loss of customers first, while only 25% of C-suite executives responded the same. Director-level security leaders may feel like they have greater responsibility to customer welfare than their C-level peers.

In any case, it's clear that most security professionals are generally confident they can retain customers, make back lost revenue, and even hire new employees lost due to cyberattacks. The immediate impacts of business downtime are far more disruptive for them on a day-to-day basis.

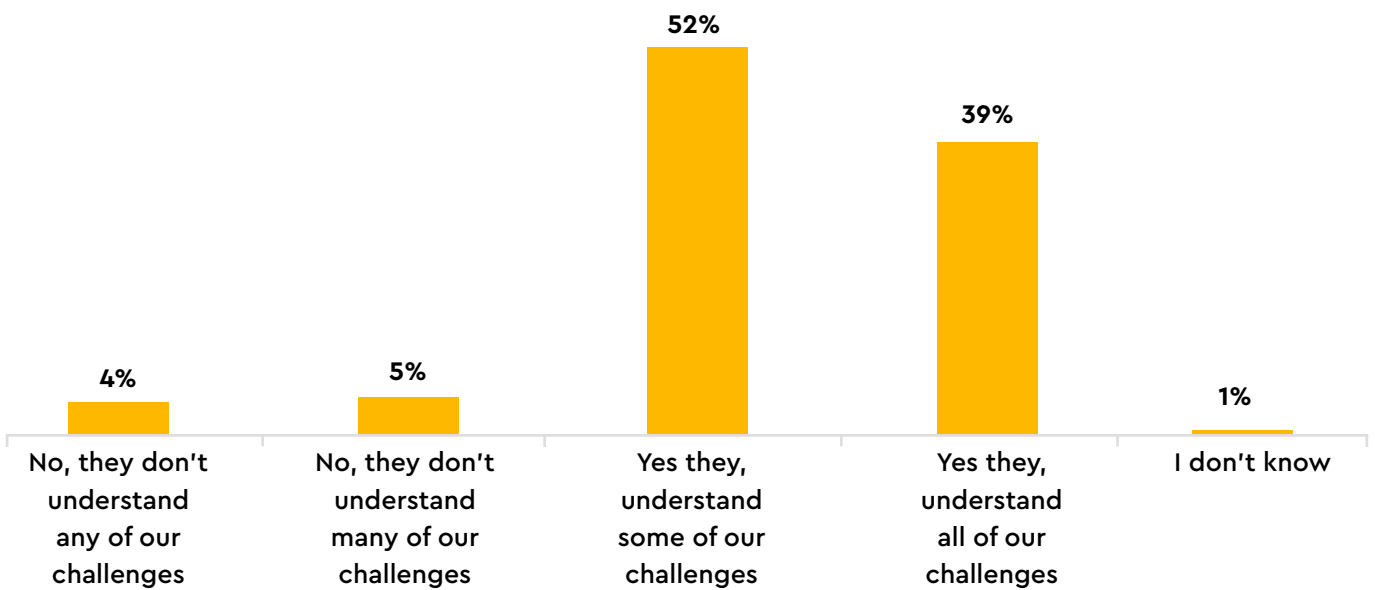
What was the impact of the cyberattack(s) on your business?



SECURITY LEADERS ARE GENERALLY HAPPY WITH IT AND CLOUD PARTNERS, BUT THERE'S ROOM FOR IMPROVEMENT

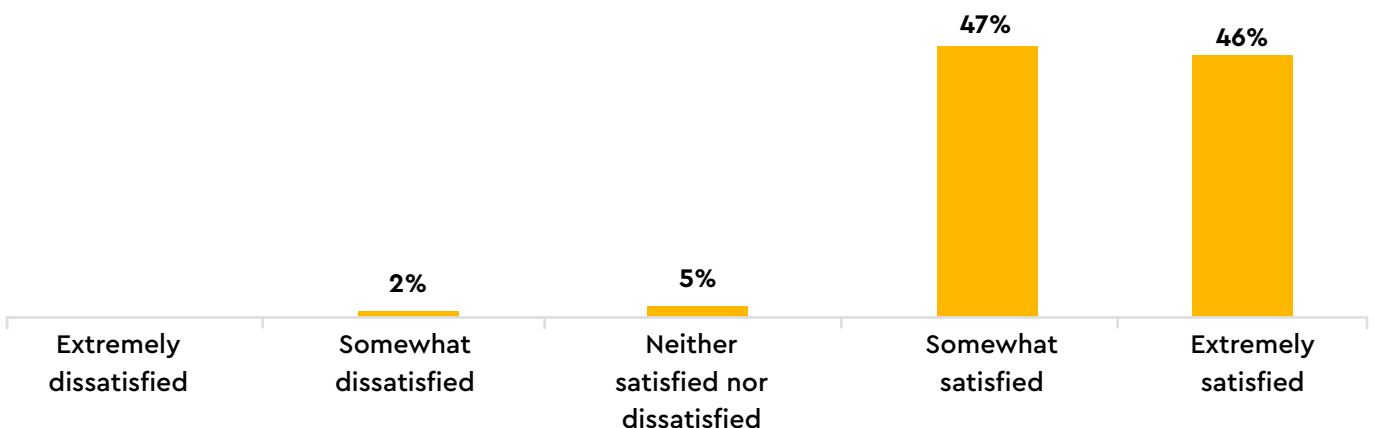
91% of respondents reported they are aligned with IT partners and cloud providers, but only 39% could confidently say their partners understand all the organization's cybersecurity challenges. That leaves a majority of respondents wishing their partners better understood the specific challenges their organization faces.

Do you think that, in general, you and your IT partner(s) or cloud provider(s) are fully aligned when it comes to your cybersecurity challenges?



Similarly, 93% of respondents are satisfied that their IT partners and cloud providers inform them of the latest cybersecurity innovations. There is a nearly equal distribution of respondents that report being "somewhat satisfied" versus "extremely satisfied". This suggests that providers can and should dedicate resources to addressing their customers' goals more comprehensively.

How satisfied are you that your IT partner(s) or cloud provider keeps you up to date with the latest innovations to manage new cyberthreats to your business?

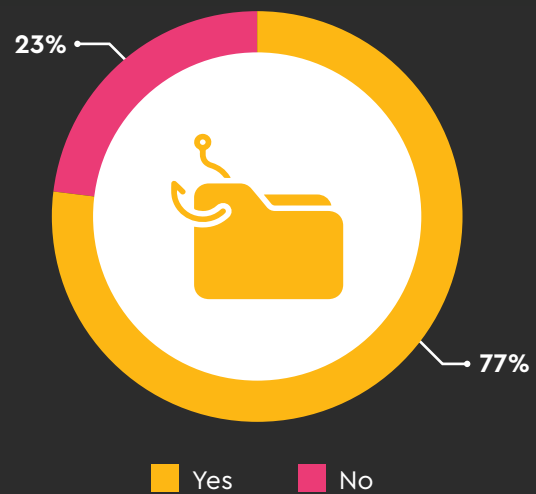


MOST SECURITY LEADERS LEARN ABOUT ANTI DATA EXFILTRATION FROM IT PROVIDERS AND EXTERNAL CONSULTANTS

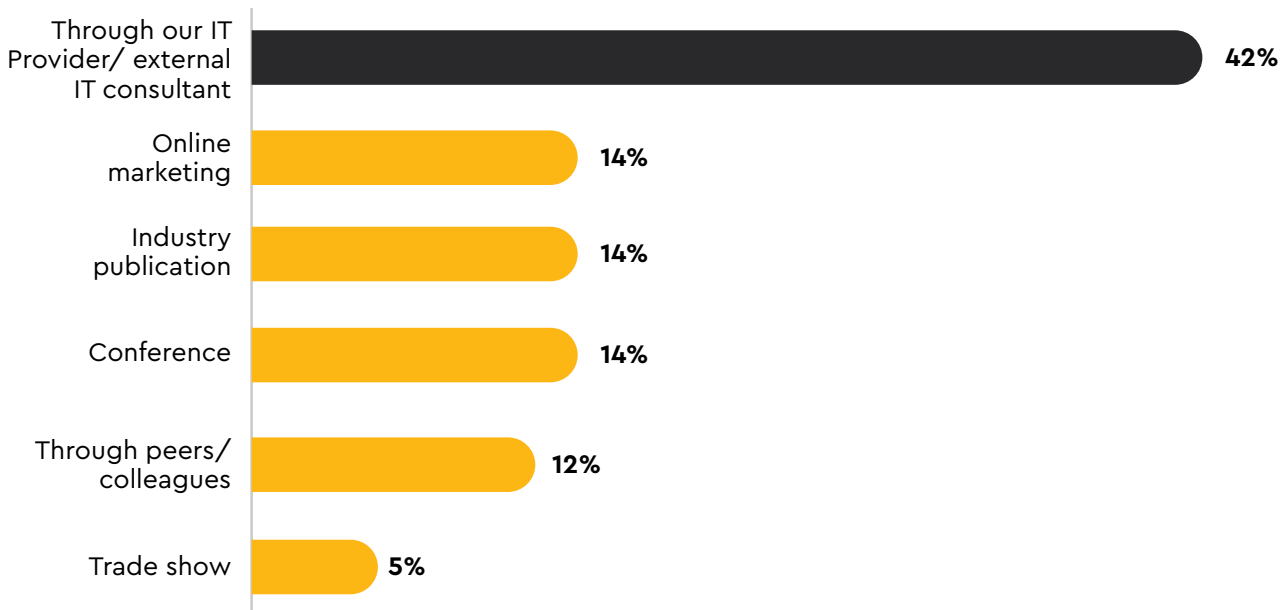
More than three-quarters of respondents reported being aware of anti-data exfiltration technology. Respondents from companies with at least 500 employees were more likely to be aware of this technology than respondents from smaller companies.

Are you aware of Anti Data Exfiltration?

42% of respondents reported learning about anti data exfiltration technology through their IT provider or another external partner. This is equal to the number of respondents who learned about this technology from online marketing, industry publications, and security conferences combined.

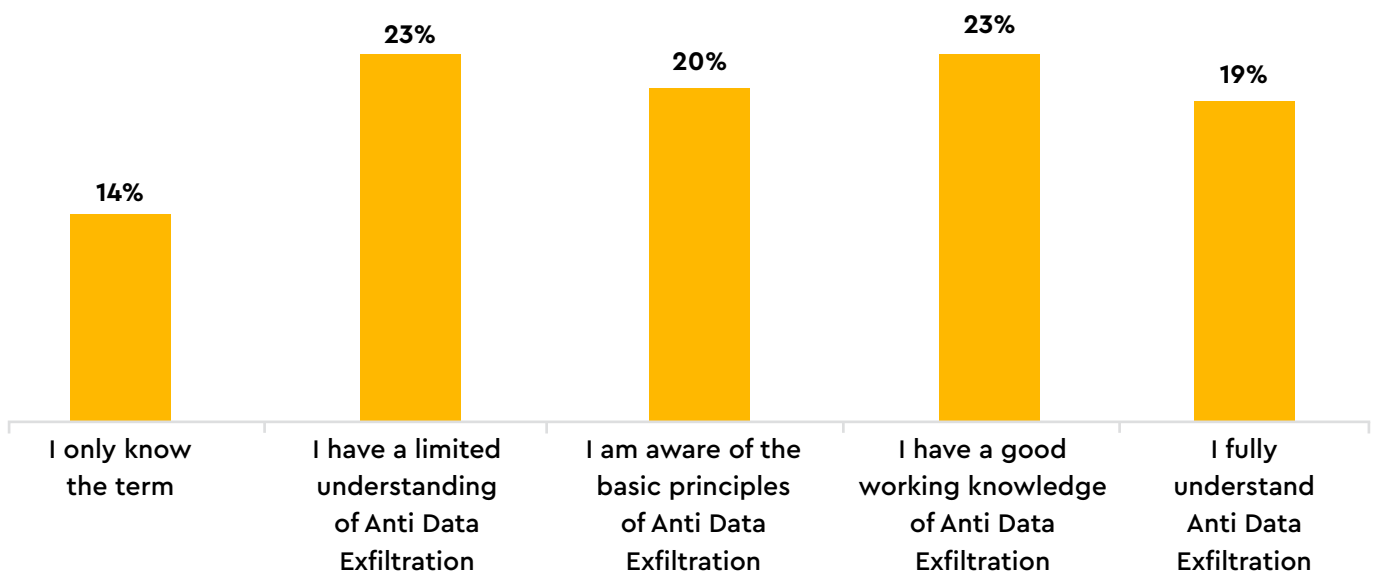


How did you first learn about Anti Data Exfiltration technology?



However, less than half of these respondents feel like they have a good understanding of anti data exfiltration technology. This number is even lower for security leaders at organizations with less than 500 employees.

To what extent do you feel that you have a good understanding of Anti Data Exfiltration?



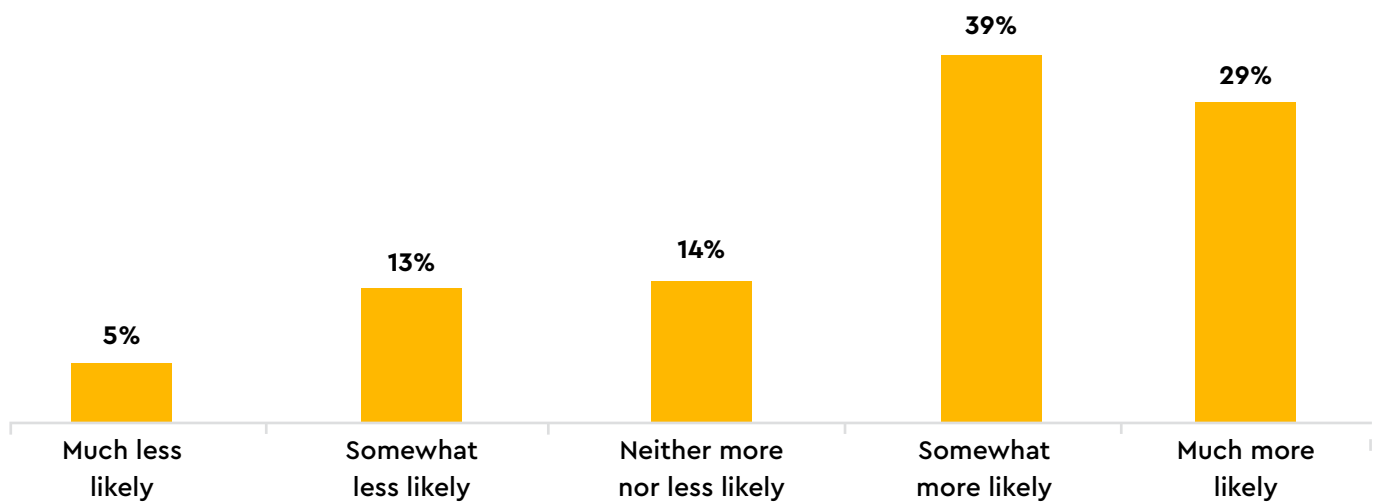
These findings suggest that IT service providers are in a unique position to provide guidance and expertise that can help mid-sized organizations deploy technologies that can have a meaningful impact on their overall security posture. At the same time, they show that IT providers have a clear incentive to showcase this kind of technology to their customers.

SECURITY LEADERS TRUST THEIR SECURITY PARTNERS AND MSPS

69% of respondents reported being likely to ask their IT provider, managed security provider, or channel partner to provide valuable advice on new cybersecurity solutions. Specifically, 29% reported being much more likely to solicit this kind of advice compared to last year, while 39% reported being somewhat more likely to do so.

Security leaders at organizations with more than 500 employees were significantly more likely to ask their IT providers for advice on new cybersecurity solutions. This reinforces the idea that security leaders place a great deal of trust in their security partner

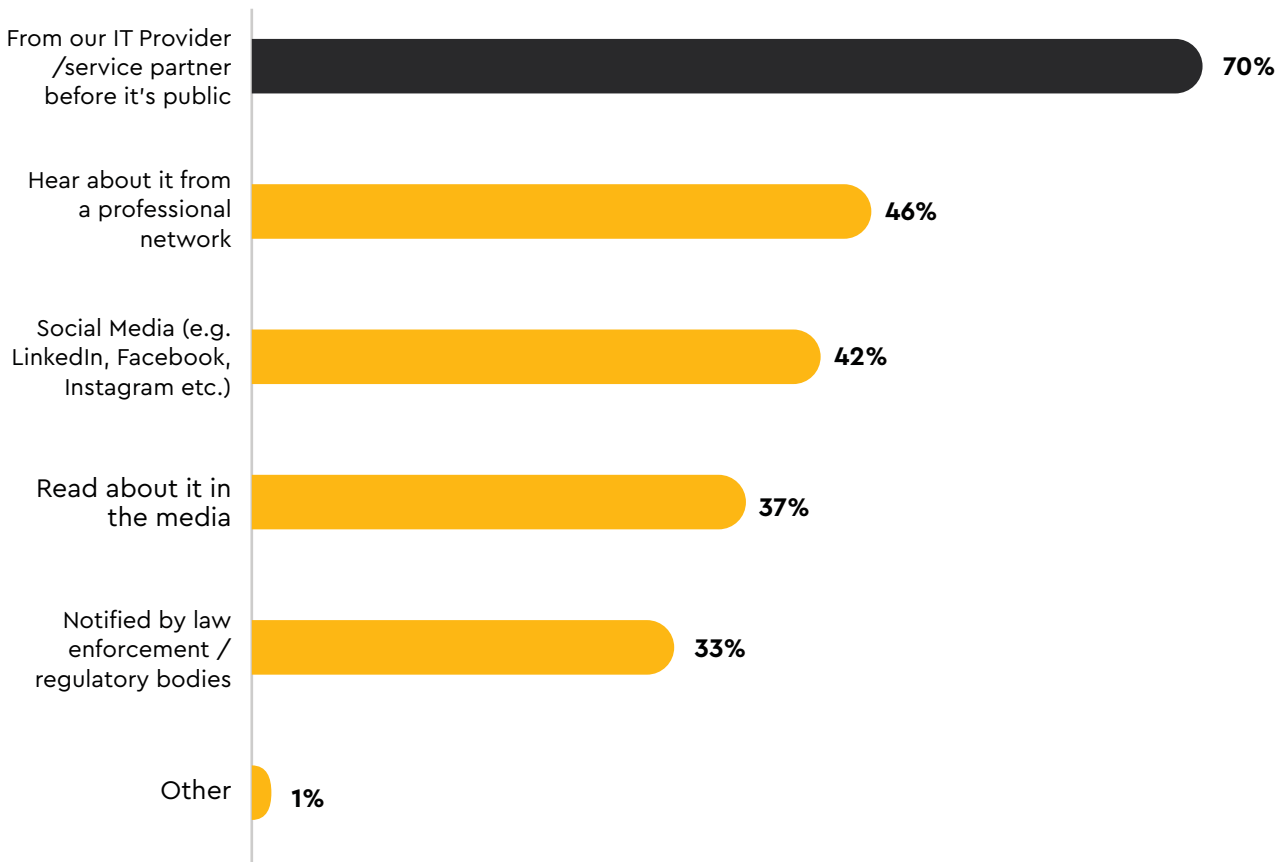
Compared with 12 months ago, to what extent are you more or less likely to ask your IT / MSP / Channel Partner / Cloud Provider for advice on new cybersecurity solutions?



IT security partners are also responsible for making leaders aware of vulnerabilities, threats, and incidents before they become public knowledge. 70% of respondents reported that they learned of threats and incidents that could impact their organization from service partners, giving them critical lead time in crafting a response.



How do you usually find out about security vulnerabilities, cyberthreats or security incidents that could affect your organization?

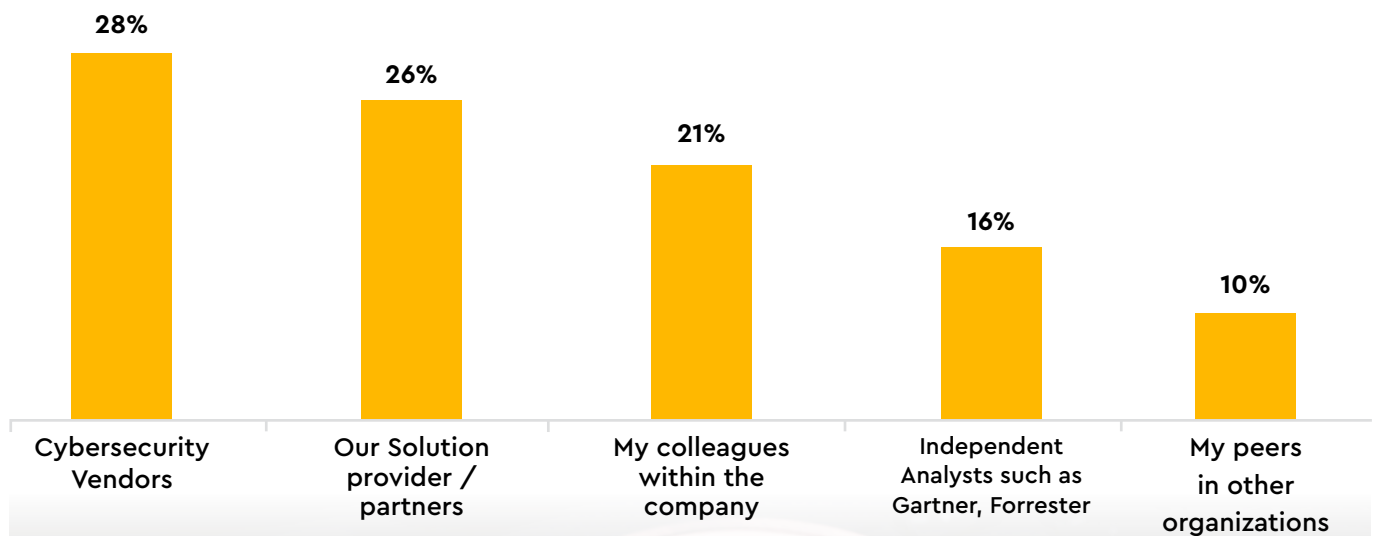


WHEN IT COMES TO SELECTING NEW SOLUTIONS, LEADERS RELY ON **CYBERSECURITY VENDORS** MORE THAN INDEPENDENT ANALYSTS AND PEERS

Respondents showed a slight preference towards cybersecurity vendors when making decisions about implementing new technologies at their organizations. This preference was even higher for IT security respondents (**40%**) compared to executive leaders (**22%**).

Interestingly, security leaders report trusting vendors more than their own colleagues within the company, independent analysts like Gartner and Forrester, and peers in other organizations. This suggests that their primary focus is on the technical capabilities of the technology in question, since this is one thing the vendor should know better than anyone else.

Thinking about how you select new security solutions within your organization, who do you most trust for advice?

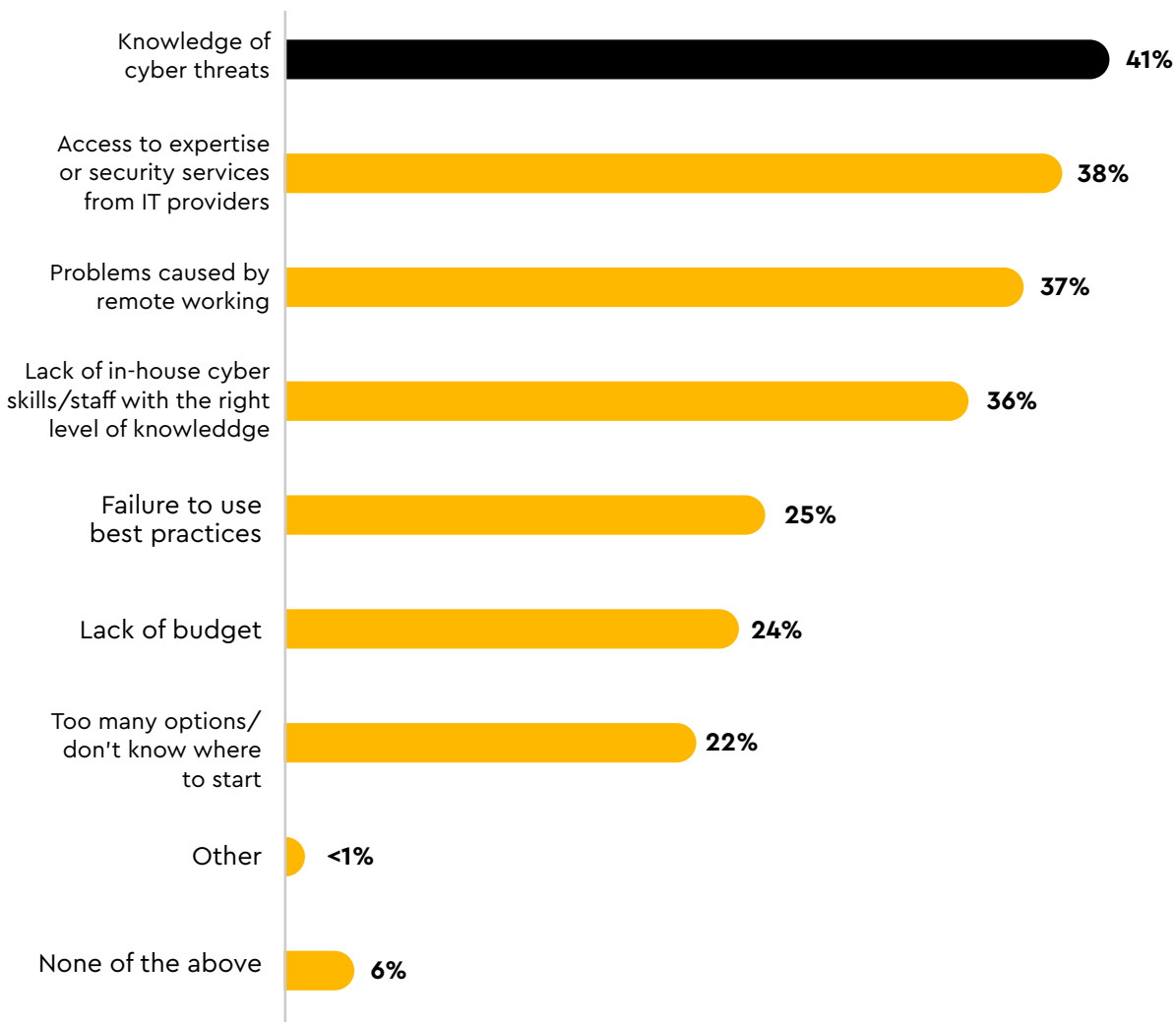


SECURITY LEADERS WITH THIRD-PARTY IT PROVIDERS ARE MORE CONFIDENT ABOUT THEIR ABILITY TO RESPOND TO INCIDENTS

Security leaders also rely on third-party IT providers to provide knowledge of emerging cybersecurity threats on a regular basis. These warnings serve an important purpose, since 41% of respondents reported that learning of emerging threats is the biggest challenge they currently face in cybersecurity.

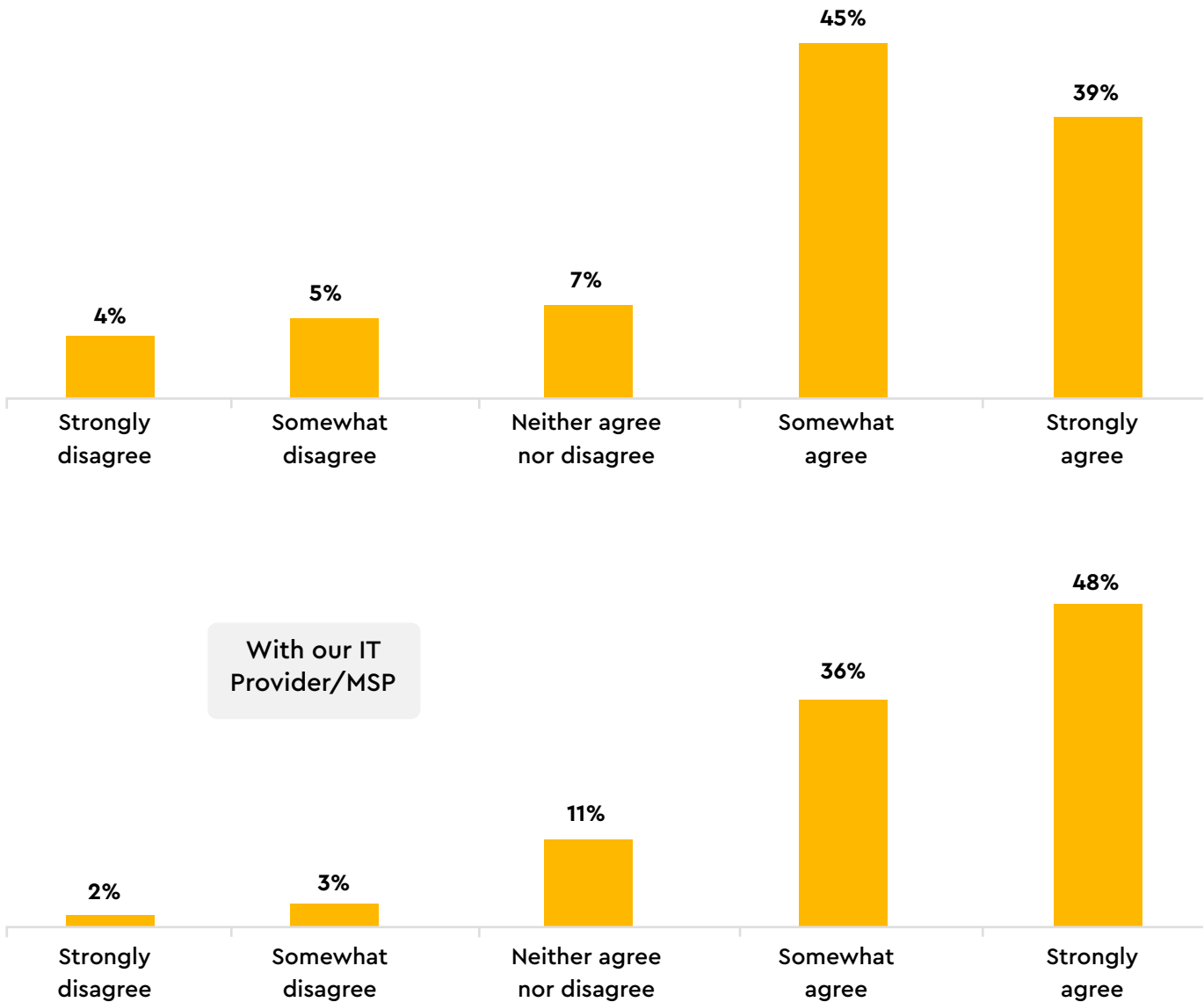
Among respondents who experienced a cyberattack in the last 12 months, access to expertise and security services from IT providers also ranked highly, at 41%. This suggests that cyberattacks stretch resources thin at underprepared organizations, and that they respond by prioritizing access to on-demand incident response capabilities.

What are the biggest challenges you currently have in protecting your business effectively from cybersecurity threats?



48% of respondents reported they would know how to manage a cybersecurity incident effectively in collaboration with their IT provider, compared to 39% who said they could manage it effectively within their organization. Both these responses were higher among respondents from the United States than those from the United Kingdom.

To what extent do you agree with the following statement: 'Should a cyber incident affect our organization, we would know the processes and have clear lines of responsibility of how to manage this effectively a) within our organization and b) with our IT provider'?



Methodology:

The results from this survey are from an online survey Sapio Research fielded on behalf of BlackFog with 400 IT decision makers in the US and UK from companies with 100-999 employees in May 2023.

CONCLUSION

On the basis of this research, we can conclude that there is a huge opportunity for solution providers and partners to build new relationships in this market, as SMBs struggle to navigate a rising tide of growing cybersecurity threats. As trusted partners, MSPs have an important responsibility to ensure their client's data is protected from extortion. Existing defensive-based approaches are no longer enough for today's polymorphic attacks which leverage data exfiltration as the main weapon of choice. Learn more about preventing data exfiltration at blackfog.com.



ABOUT BLACKFOG

Founded in 2015, BlackFog is a global cybersecurity company that has pioneered on-device anti data exfiltration (ADX) technology to protect companies from global security threats such as ransomware, spyware, malware, phishing, unauthorized data collection and profiling. Its software monitors enterprise compliance with global privacy regulations and prevents cyberattacks across all endpoints. BlackFog uses behavioral analysis to preemptively prevent hackers from exploiting vulnerabilities in enterprise security systems and data structures.

BlackFog received recognition as a Gold award winner in the Cybersecurity Excellence Awards for Best Virtual CISO Offering, as well as the Silver award for Ransomware Protection and Most Innovative Cybersecurity Company in 2023. BlackFog also won a GLOBE award in 2023 for the [State of Ransomware report](#) which recognizes outstanding contributions in securing the digital landscape.

BlackFog's preventative approach to security recognizes the limitations of existing perimeter defense techniques and neutralizes attacks before they happen at multiple points in their lifecycle. Trusted by corporations all over the world, BlackFog is redefining modern cyber security practices. For more information visit <https://www.blackfog.com>

www.blackfog.com

