vade

# The Time for MSPs Is Now:

## SMB Cybersecurity Landscape Report 2022

# TABLE OF CONTENTS


**FOREWORD** 3

**INTRODUCTION** 4

**KEY FINDINGS** 5

**CYBERSECURITY IS INTEGRAL TO THE MODERN-DAY ORGANIZATION** 6

Beyond the IT department boundary 6
Sophistication of attacks the key driver 7

**ALL ROADS POINT TO MSPS** 8

The rise and rise of providers 8
The time of the MSP is now 10

**THE EVER-CHANGING THREAT LANDSCAPE** 11

Cybersecurity attacks are on the rise 11
Email Security: Overshadowed or Misunderstood? 13

**CONCLUSION** 14

**METHODOLOGY** 15

# FOREWORD

For better or worse, the world has changed. Nowhere is this more apparent than in the workplace. From empty office space to distributed teams with privileged access and limited supervision, the security perimeter has contracted, if not disappeared entirely.

Small-to-medium-sized businesses (SMBs) have come to terms with the risks their organizations face. In this survey of 500 IT decision makers, 67% say that cybersecurity is the top priority. Some have had this realization only after suffering from a devastating breach. Other, more fortunate organizations, recognized the pending storm and determined to prepare themselves for the real possibility that one day their organization would be attacked.

What both have in common is the need for additional budget, people resources, and cybersecurity expertise. The answer is managed service providers (MSPs), who have in recent years pivoted from offering break-fix services and reselling hardware and software to managing systems and infrastructure, and, in some cases, all IT functions. MSPs who foresaw the cybersecurity opportunity moved into the space and readied themselves to serve as trusted advisors and skilled technologists for SMBs in need of cybersecurity services.

Together, SMBs and MSPs are working together to secure businesses from a relentless onslaught of cyberattacks from threat actors around the world. Through social engineering, email, and remote attacks, hackers have given SMBs a reason to make cybersecurity their top priority and MSPs the top choice for achieving their goals.

# INTRODUCTION

Cybersecurity is no longer IT's problem. It is everyone's problem. Organizations of all sizes in the US have learned this the hard way. Others are only now beginning to recognize cybersecurity's role in the overall health, reputation, and longevity of a company. Cybersecurity is now near the top of many organizations' priorities, and front and center to many strategies.

However, as attention to cybersecurity increases across organizations, so do the associated challenges. Every passing month brings more headlines about major attacks, while the rise in remote working adds an extra layer of complexity to security teams as they aim to secure a distributed workforce. A shortage of cybersecurity experts only compounds the issues facing IT decision makers.

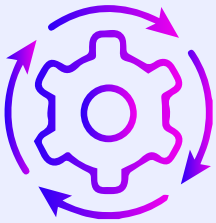
Many, if not most, organizations will look for external support to help plug the gaps in their cybersecurity defenses. Managed service providers (MSPs) are the answer. MSPs already support IT teams in many other areas, such as cloud packages and as-a-Service offerings, so it only makes sense for organizations to lean on their trusted advisors when it comes to cybersecurity. Key to success in this pairing are MSPs who are equipped, both technically and strategically, to provide cybersecurity services and SMBs that are willing to follow their lead.

This white paper, based upon independent research with 500 US IT decision makers (ITDMs) across organizations with 10-1,000+ employees, will explore:

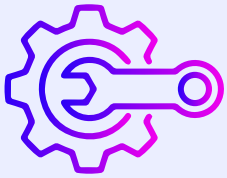
- The importance of cybersecurity, and the key reasons behind this drive
- How MSPs are primed to take advantage
- Why decision makers need to spread their focus across all areas of cybersecurity

# KEY FINDINGS

**91%**
say **cybersecurity will increase** in importance over the **next two years**



**92%**
of **US organizations outsource** at least **some** of their **IT operations to an MSP** currently



**91%**
are **currently using** an **MSP for cybersecurity**

**79%** agree the **number of cyberattacks** their **organization** has experienced has **increased over the past 12 months**

**87%** agree their **organization** could take the **threat from email security more seriously**

# CYBERSECURITY IS INTEGRAL TO TODAY'S ORGANIZATIONS

## Beyond the IT department boundary

For US organizations, there has never been as much focus on cybersecurity as there is now, and that focus will only become clearer in the coming years. Ninety-one percent of surveyed IT and business decision makers say cybersecurity will increase in importance for their organization over the next two years, and 54% report this increase will be dramatic.

Traditionally, cybersecurity has been a topic limited to the IT department. In fact, when asked to rank which IT priorities are of the greatest importance, cybersecurity comes out on top (67%), with IT sustainability (43%) and digital transformation (33%) ranked second and third. While the top priority for all, larger organizations are placing a greater focus on cybersecurity (83%) than their smaller counterparts (55%).

The importance of cybersecurity is felt across the organization, with 93% agreeing that cybersecurity will become integral to every part of their organization. Given this, it's hard not to see IT departments playing a major role in helping to shape organizational strategies going forward.

With the spotlight on cybersecurity increasing, it's promising to see that organizations are supporting this trend with greater investment. The vast majority of organizations say that they both invested more in the past 12 months (87%) and will continue to do so over the next 12 months (88%). It's clear that organizations recognize the substantial cyber threat they are under and are willing to increase their budgets as a result.

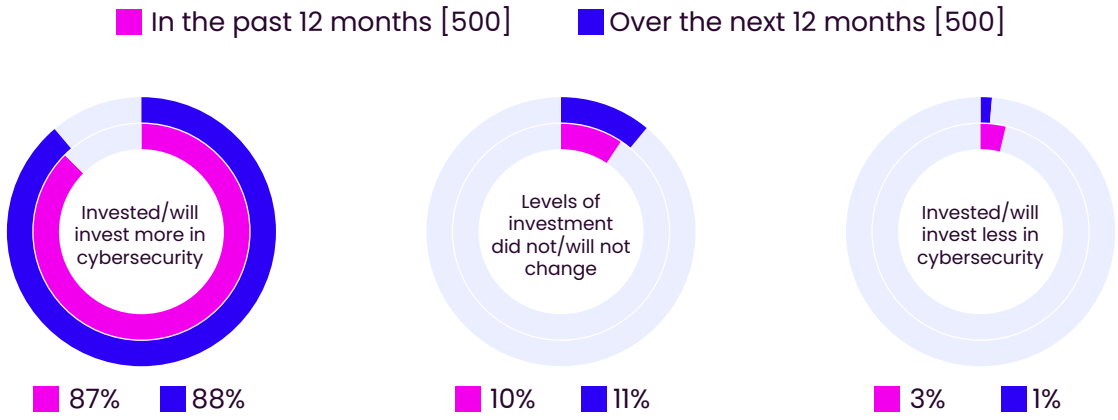



Figure 1. To what extent did the level of your organization's investment into cybersecurity change in the past 12 months, and how will it change over the next 12 months? [Bases in chart], not showing all answer options

## Sophistication of attacks the key driver

Ensuring organizations are protected against the rising cyber threat is evidently a top priority for organizations in the US. Therefore, it's important to understand the drivers behind the ongoing investment in the area.

With every passing year, cyberattacks are becoming more complex—hackers are constantly looking at new ways to slip through defenses. Decision makers recognize this, citing it as the greatest reason behind their focus on cybersecurity (63%), along with the rise in remote/hybrid work environments (53%), and breaches/cyberattacks (53%). Despite the attention placed on cybersecurity, decision makers will need as much help as they can get as they grasp with the ever-growing sophistication of cyberattacks.

Intriguingly, the general trend indicates that enterprises (1,000 or more employees) are more likely than smaller companies (10-249 employees) to cite the different reasons for why cybersecurity is increasing in importance. With the consequences of a successful attack likely greater for enterprises, it's perhaps not a surprise they place more focus on cybersecurity.

Now that US organizations are taking the threat more seriously than ever before, the next step will be to ensure their defenses are secure as they deal with the increased sophistication of hackers. Essentially, organizations are in demand for support.

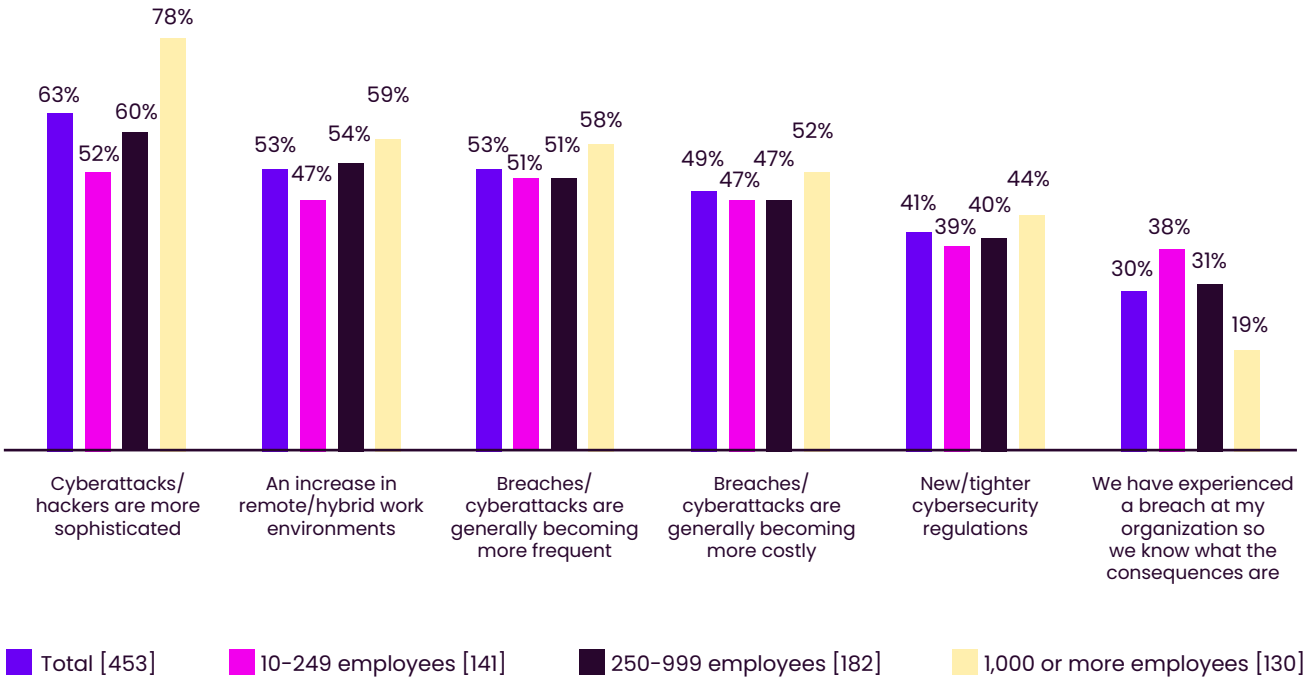



Figure 2: Which of the following reasons help explain why cybersecurity is increasing in importance to your organization? [Bases in chart], asked to respondents who predict cybersecurity will increase in importance to their organization over the next two years, split by organization size, not showing all answer options

# ALL ROADS POINT TO MSPS

## The rise of providers

MSPs play a huge role for organizations currently, with the vast majority of decision makers (92%) reporting that at least some of their IT operations are outsourced to an MSP. This reliance only increases for smaller companies (10-249 employees), where 97% say they outsource to an MSP. The general trend is only set to continue, with 92% of all organizations reporting this will be the case in two years' time.

It's clear from this that MSPs are a critical function today; organizations of all sizes would likely be in a more difficult position without them.

MSPs provide a range of services to organizations. Chief among the most valuable are managed cybersecurity services (50%), managed cloud services (45%), and managed software-as-service (43%). Given the fact cybersecurity is a top priority in IT departments and across the wider organization, it's perhaps no surprise that organizations are looking to external resources to ensure they are best protected against the growing threat.

The growing importance of cybersecurity is not the sole explanation for why businesses look to others for their security needs. As more focus is placed on the topic, organizations are experiencing challenges or obstacles in the way. The greatest challenges reported among IT and business decision makers is managing software vulnerabilities (45%), followed by securing a remote/hybrid work environment (41%), and facing a cybersecurity talent shortage on the market (40%).

Chief among the most valuable managed services are:

**50%** 

**managed cybersecurity services**

**45%** 

**managed cloud services**

**43%** 

**managed software-as-service**

Perhaps understandably, organizations of different sizes experience these challenges to differing degrees. Smaller organizations, for example, are far more likely to say the lack of in-house cybersecurity skills is a challenge (37%) than larger organizations (25%). Given the fact smaller organizations are limited in the resources available to them, it would make sense that this challenge hits home harder for these companies—enforcing the need to seek expertise elsewhere.

| | Total [500] | 10-249 employees [150] | 250-999 employees [200] | 1,000 or more employees [150] |
|---|---|---|---|---|
| Managing software vulnerabilities | 45% | 39% | 42% | 55% |
| Securing a remote/hybrid work environment | 41% | 36% | 37% | 53% |
| Cybersecurity talent shortage in the market | 40% | 37% | 41% | 43% |
| Educating employees about the importance of cybersecurity | 39% | 33% | 36% | 51% |
| Dealing with phishing attacks | 39% | 37% | 43% | 36% |
| Dealing with ransomware attacks | 34% | 32% | 38% | 29% |
| Lack of in-house cybersecurity skills | 32% | 37% | 35% | 25% |
| Implementing BYOD (bring your own device) policies | 27% | 33% | 27% | 19% |
| Budget constraints | 25% | 27% | 23% | 27% |
| My organization is not facing any challenges related to cybersecurity | 1% | 2% | 0% | 3% |

Figure 3: What are the greatest challenges your organization is facing when it comes to cybersecurity at the moment? [Bases in chart], split by organization size, not showing all answer options

Remote work is here to stay, and IT decision makers face increasing challenges to secure their workforce. In fact, 85% agree that remote workers and the complexity surrounding their devices makes their organization more vulnerable.

Exacerbating this problem is the fact that almost two thirds (63%) suggest that their organization lacks the skillset in house to understand or deal with security incidents. The dwindling supply of cybersecurity talent shows the full extent of the problem.

## The time for MSPs is now

MSPs are a critical resource for the modern-day organization, particularly so for smaller companies. When it comes to cybersecurity, MSPs are a lifesaver. Cybersecurity is a highly sought-after service, with the overwhelming majority of organizations (96%) either currently outsourcing at least some of their needs to MSPs or planning to in the future.

Indeed, the results paint a picture that there is a heavy reliance on MSPs for cybersecurity. Therefore, it's imperative for providers to ensure their services match requirements and meet demand, with opportunity aplenty.

When it comes to individual cybersecurity services, decision makers note that threat monitoring and intrusion detection is the most important service (43%), followed by cybersecurity consulting (37%), and firewall management (36%). Despite this, nearly all services listed are regarded within their top three most important by nearly three-in-ten decision makers, revealing that MSPs must be able to cover many different bases when it comes to cybersecurity—what will work for one organization will likely not work for another.

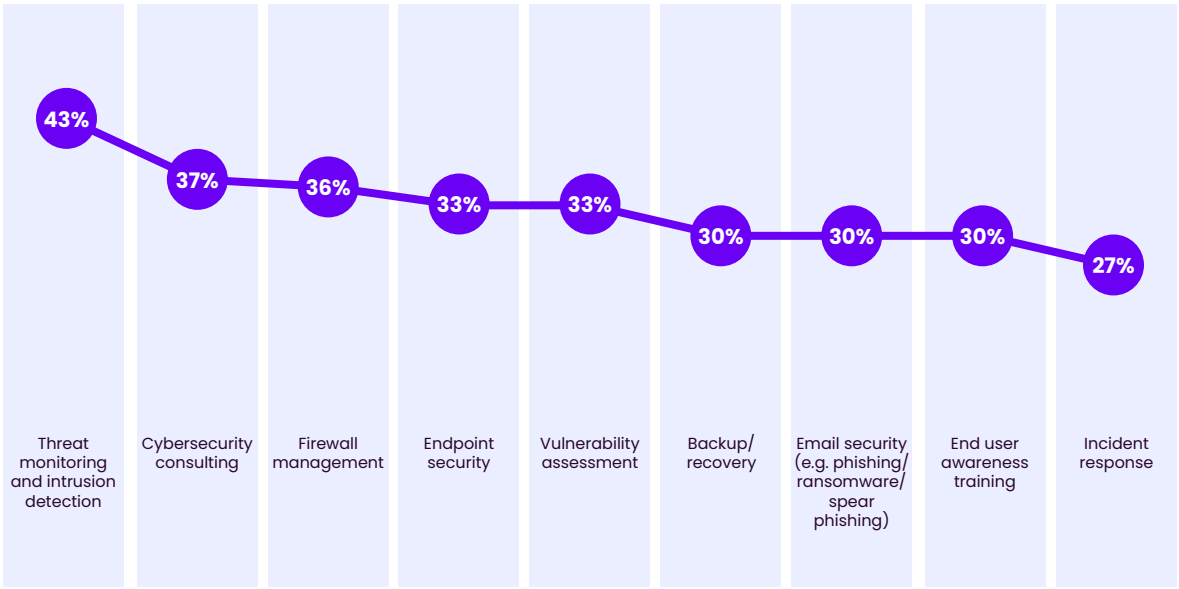



Figure 4: Which of the following managed cybersecurity services are/will be most important to your organization? Combination of responses ranked first, second and third [479], shown to respondents who use or plan to use an MSP for their cybersecurity needs

What is especially prevalent here is that cybersecurity consulting is ranked as the second most important service within the topic area.

Building upon this, when asked why their organization outsources or will outsource their IT operations, the top three reasons cited by decision makers are access to latest technology upgrades/solutions (66%), access to advanced cybersecurity solutions (63%), and access to technical expertise (62%).

Clearly, MSPs must be willing to not only provide organizations access to advanced solutions, but also expert advice. In the context of a cybersecurity talent pool shortage, and a lack of in-house skills for smaller organizations, MSPs are viewed as specialists. Those who can be strategic partners to their clients will fare best and stand out among competitor MSPs.

# THE EVER-CHANGING THREAT LANDSCAPE

## Cybersecurity attacks are on the rise

Given the priority placed upon cybersecurity, it's no surprise that all (100%) US decision makers believe safeguarding and protecting their organizations against cybersecurity attacks is important. Cybersecurity is no longer a secondary priority—all organizations now understand the risks they face.

Understandably, the greater protection in place, the better organizations are prepared against attacks and any subsequent data breaches. This is especially prevalent given that almost four-fifths (79%) agree that the number of cyberattacks they've experienced has increased over the past 12 months. Putting further numbers to this, organizations within the US report they have suffered on average eight cyberattacks over the same time period.

Decision makers must now realize that attacks can come in any shape or form. While organizations are most likely to have suffered from malware (40%), password cracking attacks (35%), or phishing (34%), a different picture emerges depending on the size of the company.

**79%** agree that the number of cyberattacks they've experienced has increased over the past 12 months

| | Total [500] | 10-249 employees [150] | 250-999 employees [200] | 1,000 or more employees [150] |
|---|---|---|---|---|
| Malware | **40%** | **33%** | **40%** | **48%** |
| Password cracking attack | **35%** | **41%** | **37%** | **25%** |
| Phishing | **34%** | **23%** | **34%** | **45%** |
| Compromised account | **30%** | **33%** | **25%** | **33%** |
| Distributed denial of service (DDoS) attack | **30%** | **35%** | **30%** | **23%** |
| Spear phishing (business email compromise) | **29%** | **34%** | **28%** | **24%** |
| Ransomware | **25%** | **25%** | **27%** | **25%** |
| Zero-day exploit attack | **24%** | **35%** | **25%** | **11%** |
| IoT based attack | **23%** | **26%** | **28%** | **15%** |
| Man-in-the-middle (MITM) attack | **23%** | **31%** | **27%** | **10%** |

Figure 5: What type(s) of cyberattack has your organization suffered? [Bases in chart], split by organization size, not showing all answer options

Demonstrating this, small businesses are far more likely (35%) than enterprise-size organizations (11%) to say they have experienced a zero-day exploit attack. On the other hand, the data indicates that cyberattacks are more likely to target larger organizations with malware (48%) and phishing (45%) attacks.

Despite the inherent differences based upon the organization's size, there's a clear need for organizations to increase their understanding of all attacks, rather than placing greater emphasis on only one or two types.

Of course, not every cyberattack is successful and results in a data breach. However, decision makers still report that they have, on average, suffered at least three data breaches over the past 12 months. Those who have suffered a data breach report a wider range of impacts, most notably a loss of sensitive data (50%), operational downtime (49%), and financial losses (43%). With nearly all respondents (99%) reporting they have suffered as a result of the breaches, it shows that the impacts are damaging and an extreme burden to organizations.

Over the **past 12 months**, organizations have, on average, suffered at least **three data breaches**.

Given the context of the number of attacks, it's surprising to learn that decision makers have a high level of confidence (94%) in their organization's ability to completely defend themselves against all types of attacks, with over half (51%) saying they are completely confident. While surface level confidence appears high, a lot of improvement is needed for defenses to be as robust as possible. Indeed, 68% agree that their organization's security solutions are not as advanced as they could be, leaving them susceptible to attacks. Add in the fact there is a cybersecurity talent skills shortage, and it's clear that organizations of all sizes need extra support here.

As discussed, there is already a heavy reliance on MSPs for all types of IT services, including cybersecurity. Therefore, MSPs appear primed to take advantage of the current situation. Organizations clearly look to providers for expert advice and guidance for the right tools and solutions. The role of the provider is to ultimately reduce the pressure on IT decision makers and make their lives easier. Given this, MSPs need to ensure they are recommending tools that are easy to use, reducing the complexity so ITDMs have confidence in their cybersecurity defenses.

# **69%** say a serious breach has bypassed their current email security

## Email security: Overshadowed or misunderstood?

Email is a fundamental feature in every organization, making it an easy and popular target for would be threat actors. Therefore, it's important to understand how seriously organizations take email security and explore the solutions currently in place.

The vast majority of decision makers (95%) say they are confident their current email security solution can protect them from a data breach. However, this bullishness would appear somewhat misplaced, especially with nearly seven-in-ten (69%) saying a serious breach has bypassed their current email security.

With so many reporting threats have sidestepped their defenses, it's concerning that a high number (87%) of decision makers say their organizations could do more to take the threat from emails security more seriously. This raises an important question: What solutions are organizations relying on for their email security?

Nearly four-fifths (77%) report their organization uses the in-built security features provided by their email provider (e.g., Microsoft 365, G-suite etc.). Inversely, just under a quarter (23%) say they use a third-party email security solution. Intriguingly, smaller organizations are more likely (26%) than their enterprise level counterparts (19%) to use third-party solutions.

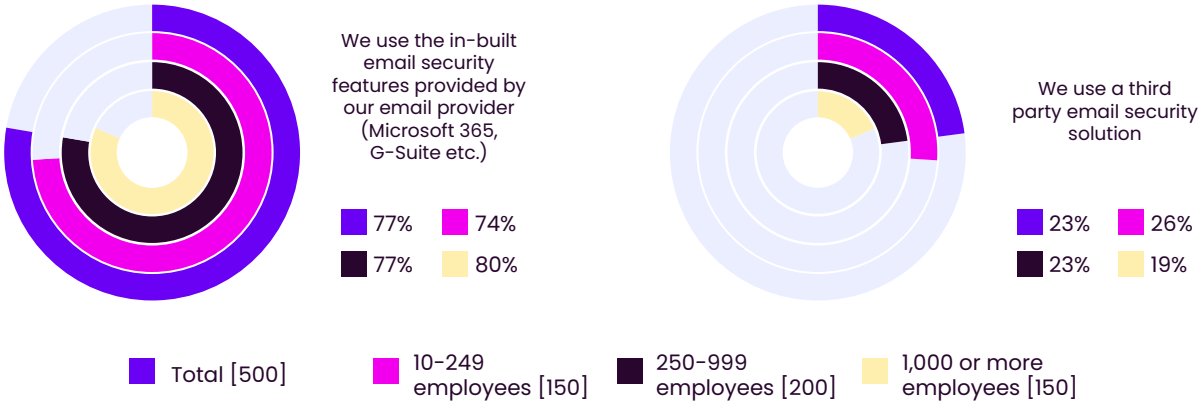



Figure 6: Which of the following statements reflects your organization's current approach to email security? [Bases in chart], split by organization size, not showing all answer options

With the vast majority (80%) agreeing that in-built security features from their email providers are not always secure and robust enough to protect against threats, it's likely that current approaches are leading to increased vulnerability.

Put together, the data suggests that email security is currently a source of weakness. Encouragingly, however, there is an appetite among organizations to ensure improvements are made. Many will look to their IT provider for help and guidance, a notion supported by the fact 92% say they would be willing to listen to email security suggestions made by an MSP.

Although on a high level, decision makers appear confident in their current cybersecurity defenses, a scratch below the surface indicates improvements are needed, especially with regards to email security. Seeking expert advice, MSPs can play a crucial role in ensuring any complacency is guarded against.

# CONCLUSION

Cybersecurity was once relegated to the IT security department. That's no longer the case. It's now integral to the whole organization. The increasing number of cyberattacks, combined with growing sophistication in attacks, is behind this change and has sharpened the minds of key decision makers and stakeholders.

However, the rise in importance places the spotlight on key challenges and obstacles being faced in the industry. Organizations note that a rise in remote working increases their vulnerability—a vulnerability that is only made worse by the lack of cybersecurity talent in the market.

While cybersecurity confidence is high, a dip below the surface shows that organizations have weaknesses to plug, with some areas of cybersecurity such as email security given less focus than others and providing a window of opportunity for threat actors.

It makes sense therefore that the vast majority of US organizations of all sizes are turning to MSPs for their cybersecurity needs. MSPs are an invaluable resource as they tighten the defenses of organizations. While MSPs need to ensure they're providing tools that safeguard security defenses, perhaps their key attribute is their expertise. The ability to offer the right tool to the right customer and understand their needs will go a long way to capitalize on the numerous opportunities offered to them.

# RESEARCH SCOPE AND METHODOLOGY:

Vade commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this whitepaper is based. A total of 500 IT, IT security and business decision makers from the US were interviewed in May and June 2022. Respondents were from organizations of different sizes, including 10-249 employees (150), 250-999 employees (200) and 1,000 employees (150). Respondents were from all public and private sectors.

Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Unless otherwise indicated the results discussed are based on the total sample.

## About Vade:

Vade is a global cybersecurity company specializing in the development of threat detection and response technology with artificial intelligence. Vade's products and solutions protect consumers, businesses, and organizations from email-borne cyberattacks, including malware/ransomware, spear phishing/business email compromise, and phishing.

Founded in 2009, Vade protects more than 1 billion corporate and consumer mailboxes and serves the ISP, SMB, and MSP markets with award-winning products and solutions that help increase cybersecurity and maximize IT efficiency.

## About Vanson Bourne:

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com



Follow us on Twitter and LinkedIn

Subscribe to our blog: www.vadesecure.com/en/blog