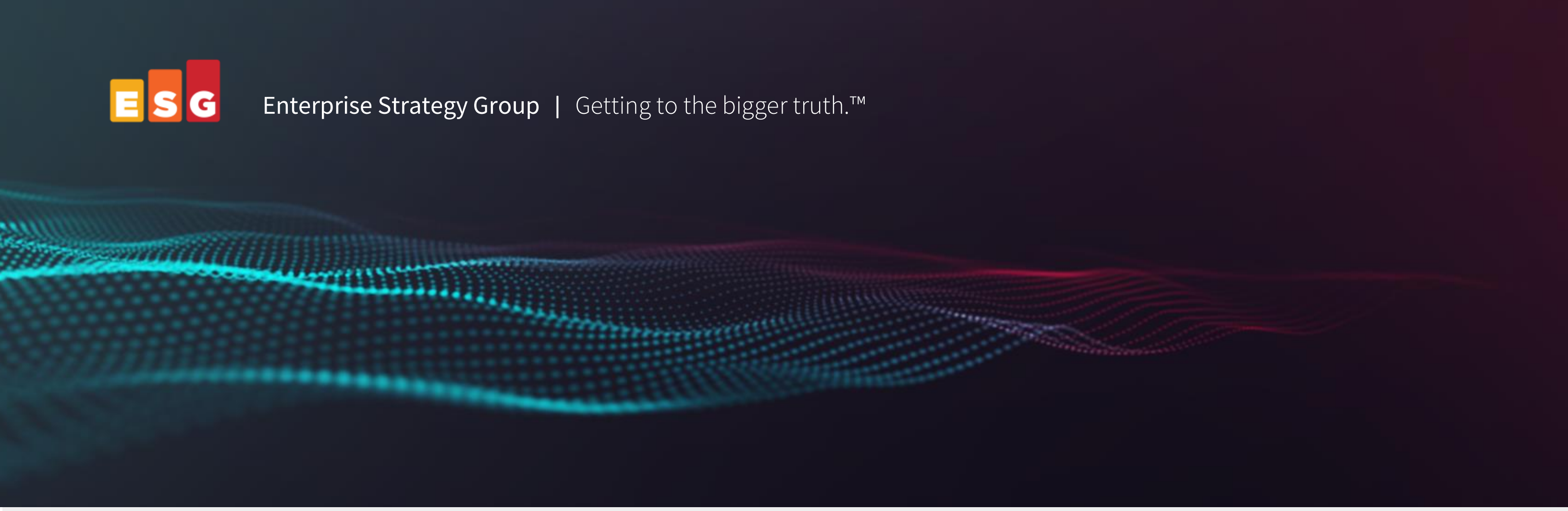


Enterprise Strategy Group | Getting to the bigger truth.™

ESG RESEARCH INSIGHTS PAPER

The Evolving Cybersecurity Threat for SMBs and How MSPs Can Mitigate the Risk

By Bob Laliberte, ESG Senior Analyst; and Adam DeMattia, Director of Custom Research

April 2020

This ESG Research Insights Paper was commissioned by Sharp and is distributed under license from ESG.

The Existential Threat to Small Midmarket Business

Organizations of all sizes are transforming to better serve their customers in a digital economy. For most this involves distributing applications to public clouds to increase agility and leveraging data more effectively to provide a differentiated experience. Indeed, public cloud services have leveled the playing field for the midmarket by providing access to enterprise-grade solutions on a pay-as-you-go basis, enabling these organizations to compete against larger companies. Unfortunately, this has also created more complex IT environments and can place these organizations at risk for cyberattacks. And the risk is real—organizations that suffer cyberattacks are at risk of going out of business. Universally, organizations of all sizes recognize the need to invest in better solutions to protect their organizations from attacks. This is even more critical for small midmarket organizations that lack the resources of larger enterprise organizations. But who can these organization turn to for help?

ESG recently performed research to identify the challenges small midmarket organizations were experiencing, the numbers of dedicated security resources they have, the amount of security events they experience per year, and how they are prioritizing spending to support cybersecurity and other managed services. Additionally, ESG sought to determine the impact MSPs have on small midmarket environments. The research consisted of a survey of 250 IT/information security decision makers responsible for and/or knowledgeable about their organization's networking infrastructure and security controls who are employed at organizations with 20 to 500 employees. Respondents were based in North America (US and Canada). Organizations represented in the sample included a broad cross-section of industries, such as technology, manufacturing, education, and business services, among others.

High Level Findings

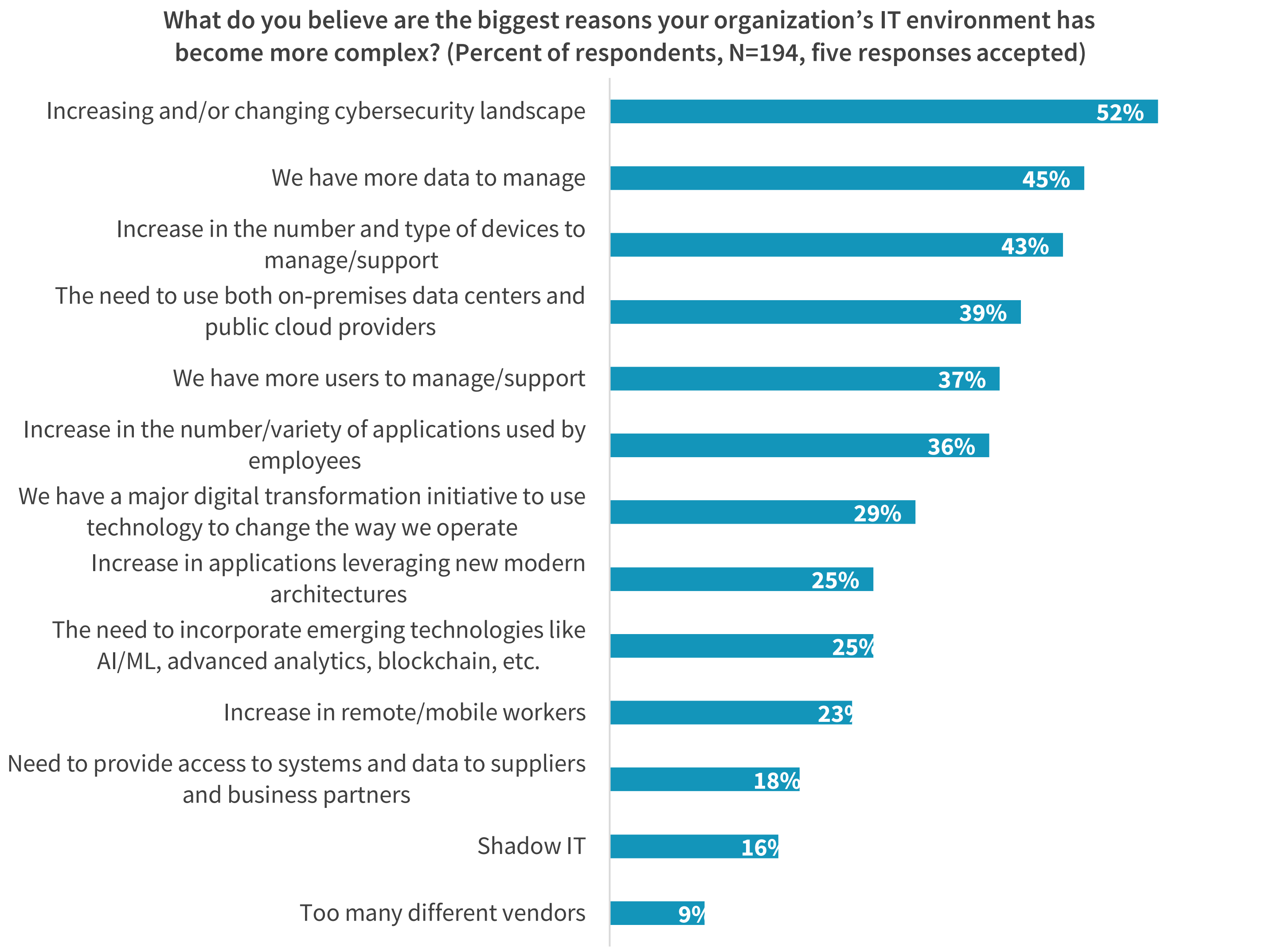
85% of small and medium businesses surveyed said they have at most one dedicated security professional on their team.

The cybersecurity landscape is driving increased complexity and small midmarket firms are not resourced to adequately defend the company, as evidenced by the fact that almost half of the respondents reported multiple security incidents over the last year. These events place the business at risk and will require organizations to invest in additional security services. Fortunately, according to respondents, MSPs can help organizations improve their security posture, as well as other areas, and are able to handle increasingly difficult tasks with greater efficiency.

Cybersecurity Is Driving Complexity at Midmarket Organizations

As the IT pendulum swings from consolidated to distributed applications, data growth continues unabated, and new security threats emerge daily, midmarket organizations are faced with an increasingly complex IT environment. ESG research highlights this fact as 77% of the small and midmarket organizations surveyed report that their IT environments have become more complex over the last two years. More importantly, when asked about the biggest reasons for their IT environment becoming more complex, the number one response was an increasing and/or changing cybersecurity landscape (see Figure 1).

Figure 1. Reasons for IT Complexity

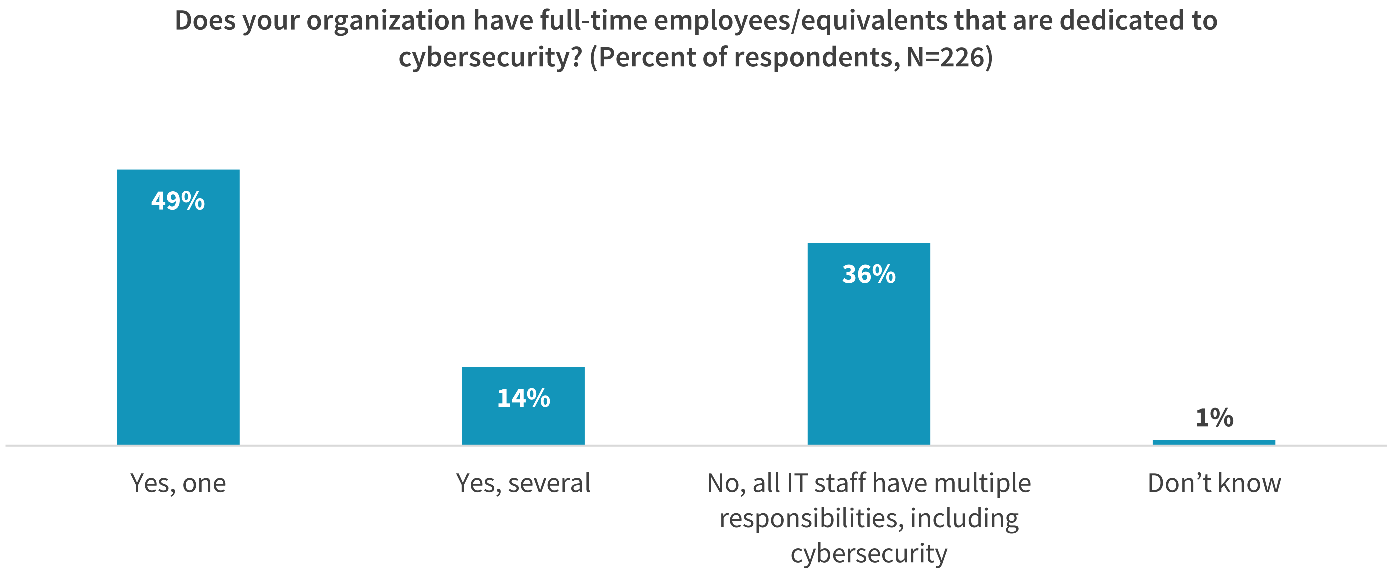


Source: Enterprise Strategy Group

In addition to cybersecurity, these organizations must deal with growing amounts of data to manage and an increase in the number and types of devices to manage or support. In many cases, this increase could be a result of bring-your-own-device (BYOD) initiatives, where employees may be using a wide range of devices, which can also create their own security issues. Also, with these organizations distributing applications to the cloud, having to manage and support both on-premises IT equipment and potentially multiple public cloud environments creates complexity and introduces risk.

It is interesting to note that even though cybersecurity issues are the leading cause of complexity, the vast majority (85%) of surveyed organizations either do not have resources dedicated to security, or only have one (see Figure 2). It should be noted, however, that younger, digital-native organizations (defined as businesses that are less than 10 years old) are much more likely to have a dedicated cybersecurity resource than older organizations (65% versus 40%).

Figure 2. Full Time Employees Dedicated to Cybersecurity

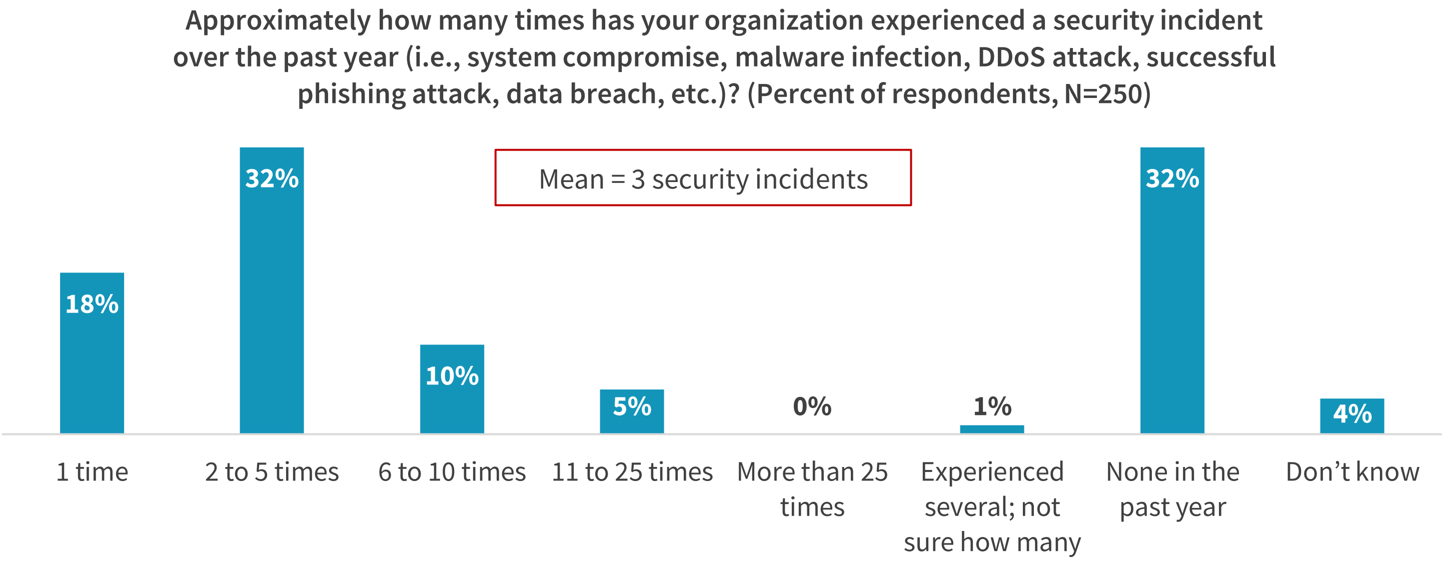


Source: Enterprise Strategy Group

Cybersecurity Events Can Impact the Business

Given the increased complexity and lack of resources, it shouldn't come as a surprise that these organizations are at risk for cyberattacks. In fact, according to ESG research, nearly half of these organizations (48%) have suffered multiple serious security incidents in the past year, with the mean being three incidents, and another 18% reporting one incident.

Figure 3. Number of Serious Security Incidents in the Past Year

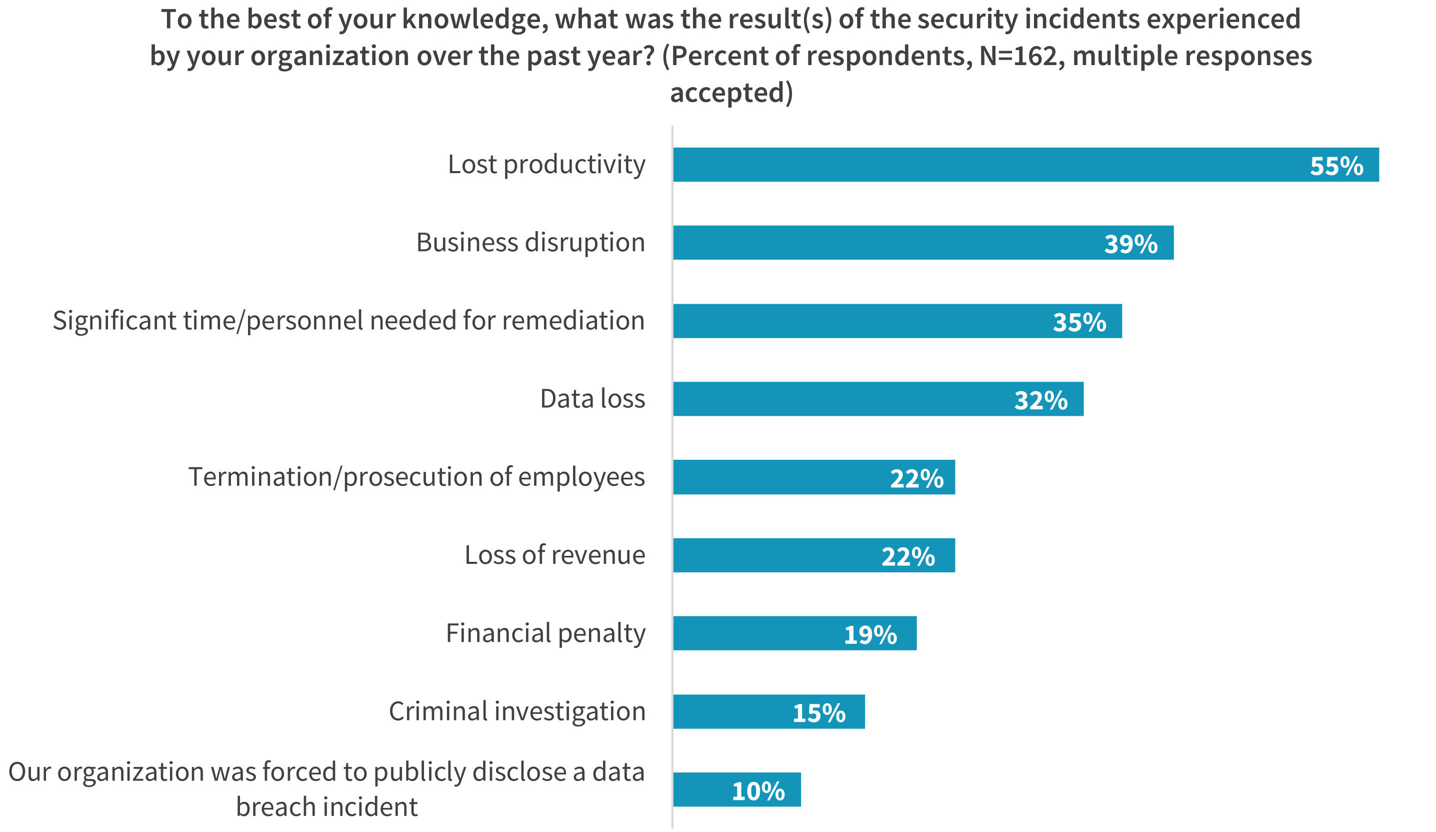


Source: Enterprise Strategy Group

While 32% of organizations reported no security incidents in the last year, it should be noted that organizations that experienced a security incident are three times more likely to say IT has become more complex, creating a direct link from complexity to security incidents.

It will be critical for organizations to better protect themselves from these security incidents to ensure continued operations. This is especially true given the impact these events can have on the business. Respondents from the survey indicate that any one security incident has a 23% chance of putting their organization out of business. Given the number of incidents that occur every year, it is possible that allowing these security incidents to occur unchecked could result in the business failing. Even if the business can remain open, these incidents have additional ramifications. When asked about how these security incidents impacted the business, more than half (55%) of organizations cited lost productivity (see Figure 4). Other top impacts include disruption to business, the amount of time required to remediate the situation, and the loss of data.

Figure 4. Impact of Security Incidents on the Business



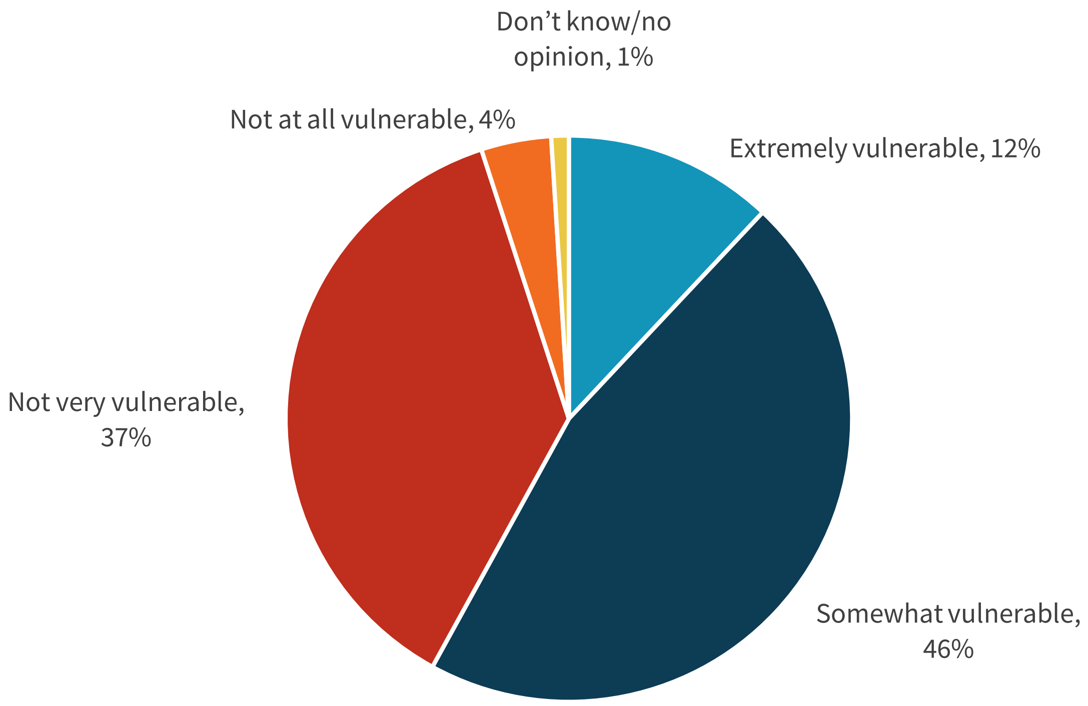
Source: Enterprise Strategy Group

Are Organizations Doing Enough?

With the lack of dedicated resources and the number of incidents that have occurred, the question is are these organizations doing enough to protect their IT infrastructure and business? The research also asked how vulnerable these organizations were to a future cybersecurity attack. Not surprisingly, 58% of organizations responding believe they are either extremely or somewhat vulnerable to a cybersecurity attack or breach (see Figure 5). However, the reality is that with an everchanging and evolving threat landscape, virtually every organization is vulnerable. In fact, those organizations that feel they are least vulnerable may be not informed enough, or just chose to answer this question in an aspirational manner.

Figure 5. Vulnerability to Cyberattacks

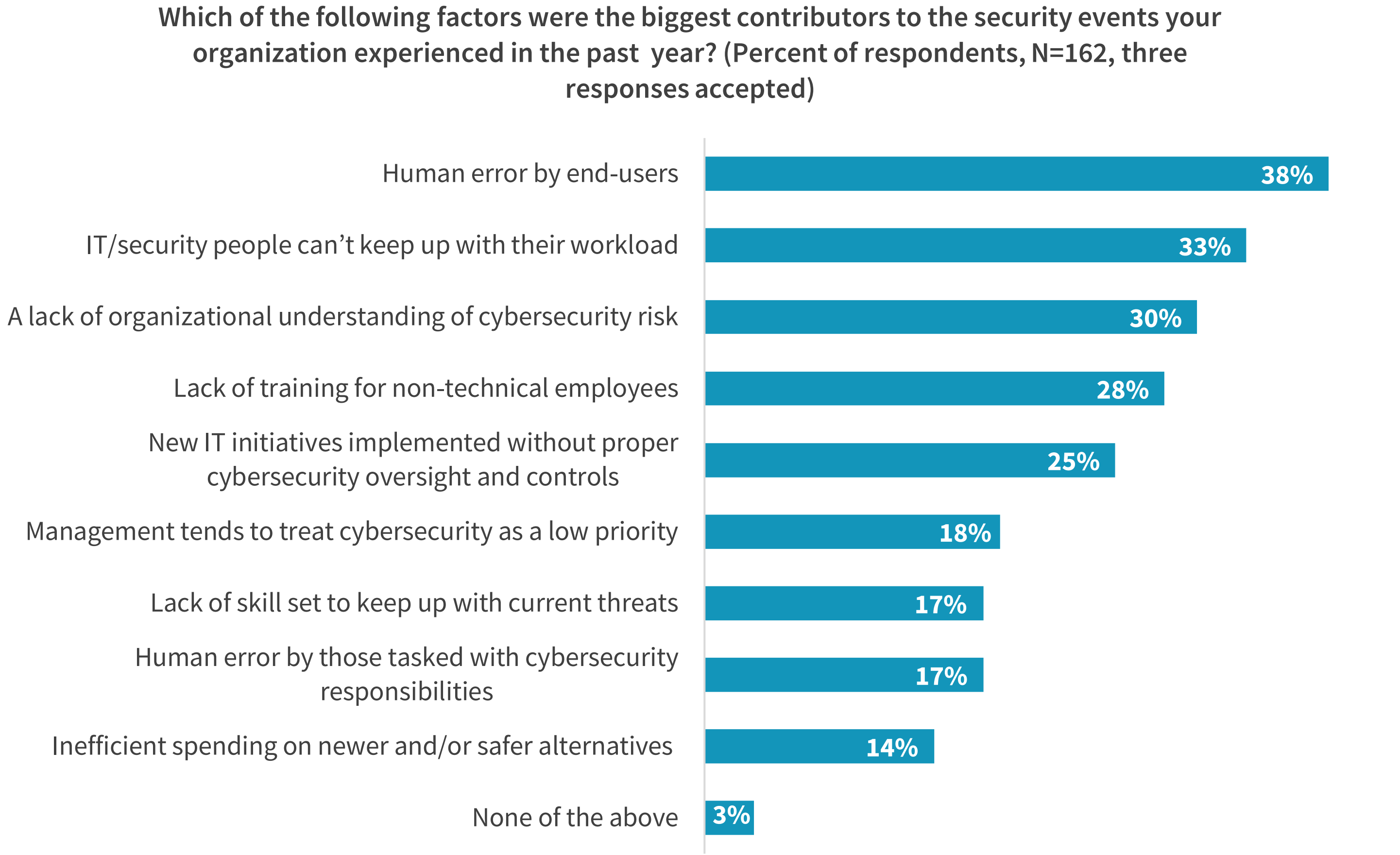
In your opinion, how vulnerable is your organization to a significant cyberattack or data breach? (Percent of respondents, N=250)



Source: Enterprise Strategy Group

The research also wanted to understand what factors contributed to these security incidents occurring. The top three most commonly reported factors were human error by end-users, the inability of IT resources to keep up with their workloads, and a lack of organizational understanding of cybersecurity risk (see Figure 6). It is this last response that may contribute to organizations not feeling vulnerable. However, even if you are not aware of the risk, it is still very real, and it is imperative for organizations to be informed. In addition to those three factors, organizations reported a lack of training and new IT initiatives that were implemented without proper cybersecurity oversight and control. As organizations digitally transform to become more agile and responsive to their customers, it is important that business ensures that any new IT initiatives are fully vetted and approved by those responsible for cybersecurity.

Figure 6. Vulnerability to Cyberattacks

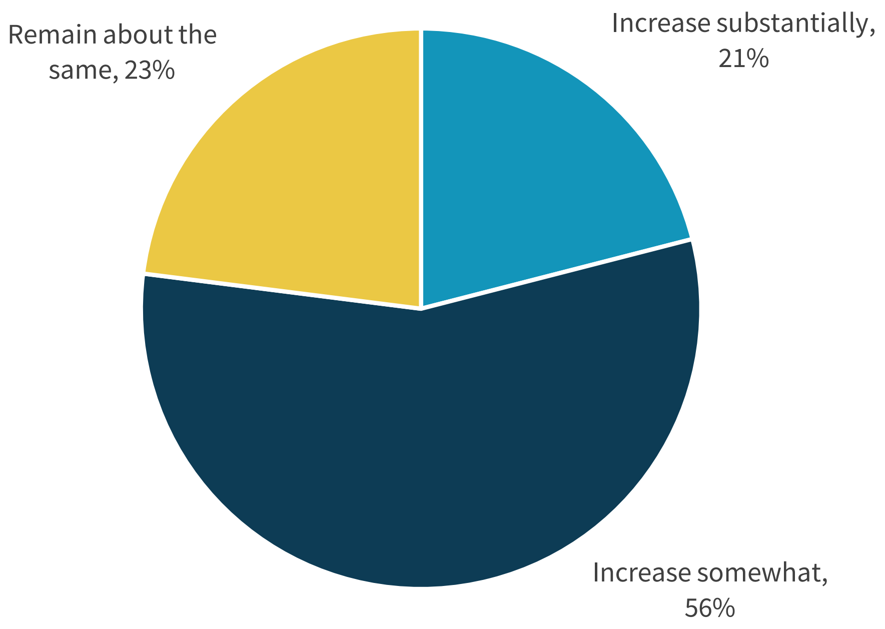


Source: Enterprise Strategy Group

Further proof that organizations are feeling vulnerable is the fact that more than three-quarters (77%) of them are planning to either substantially or somewhat increase their cybersecurity spending in the next 12 months and the remainder will spend the same amount as last year (see Figure 7). Given the importance to the business, it is worth noting that no one responded that they were decreasing their spend on cybersecurity.

Figure 7. Increased Spending on Cybersecurity

Relative to other areas of technology, how do you expect your organization's cybersecurity spending to change – if at all – over the next 12 months? (Percent of respondents, N=250)



Source: Enterprise Strategy Group

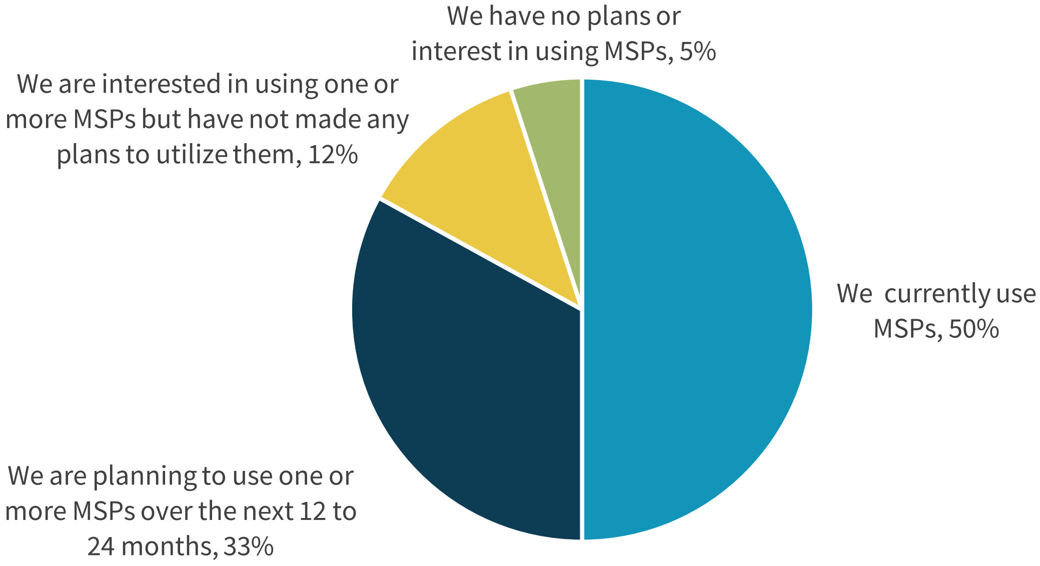
Will these increases in the security budget be enough? When asked what was hindering the adoption of additional security services, close to two-thirds (62%) reported that a limited budget was one of the top hindrances, the most common response. Also in the top three reasons was the fact that their (already limited) staff is not familiar with the technology. Given these challenges, it is unlikely these organizations will be able to hire additional dedicated resources, but rather will need to look outside their walls to find services or resources to help them securely navigate new technology deployments.

Working with MSPs Can Reduce the Security Risk

Many of these small midmarket businesses with limited resources and increasing complexity are leveraging managed service providers or MSPs to help. ESG research asked respondents about their use of MSPs. The overwhelming response was that 95% of the survey respondents were using, planning to use, or interested in using MSPs (see Figure 8). Again, the data indicated that younger companies were more likely to leverage the services of an MSP (61%) than older companies (44%).

Figure 8. Use of MSPs

Which of the following statements best describes your organization's use of managed service providers (MSPs)? (Percent of respondents, N=250)

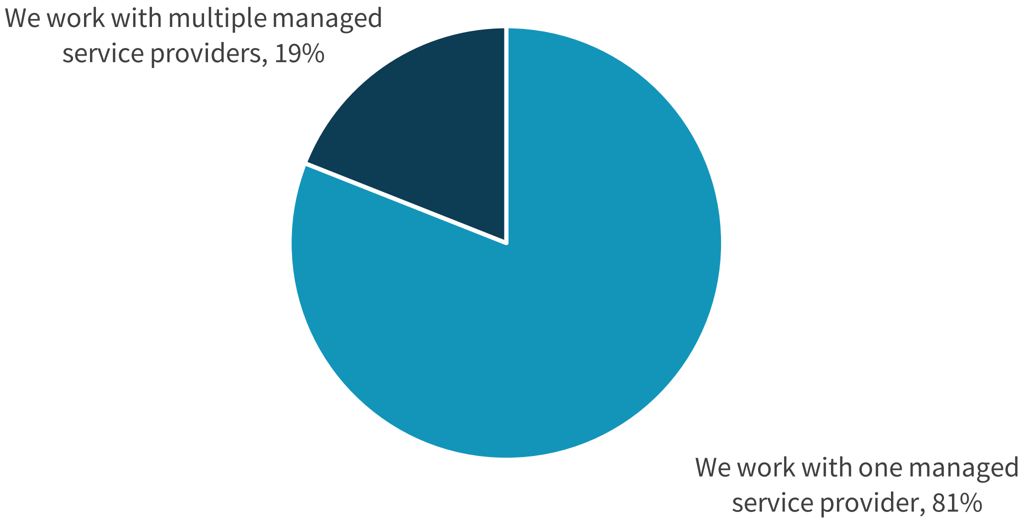


Source: Enterprise Strategy Group

The next logical question then is how many MSPs do these organizations conduct business with? Do they consider them to be one of many vendors they transact business with or are they looking for more strategic relationships? Given that more than three-quarters (81%) of organizations using MSPs work with only one, and that 42% of those organizations that work with more than one MSP are only interested in working with one, it would be reasonable to conclude that these organizations want the MSP to be a strategic partner and not just another vendor.

Figure 9. Number of MSPs Organizations Work With

You indicated your organization currently uses MSPs. Approximately how many MSPs does your organization currently work with? (Percent of respondents, N=125)

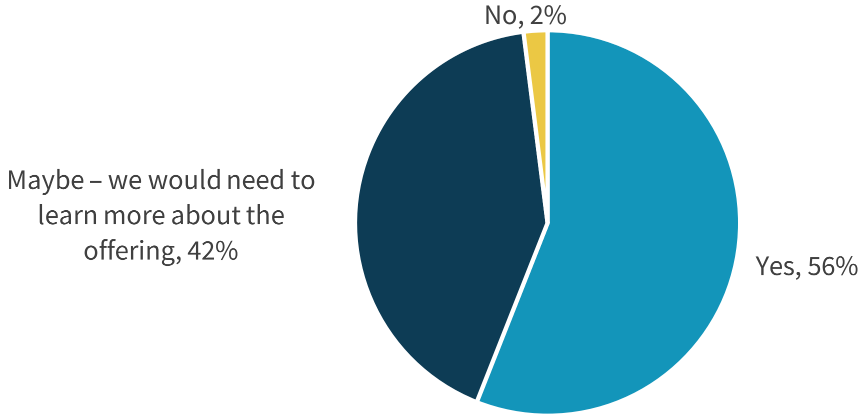


Source: Enterprise Strategy Group

As a result, the majority (56%) of these organizations are interested in working with an MSP that offers end-to-end solutions such as an "office-as-a-service" (see Figure 10). Furthermore, another 42% of respondents would be interested in an offering like this but would need to hear more about it. This is yet another proof point that these organizations would like to have a strategic partner to work with and not multiple different vendors.

Figure 10. Interest in End-to-end Solutions from MSPs

Would your organization have serious interest in evaluating a single "office-as-a-service" managed service that spans multiple disciplines within the next 12-18 months? (Percent of respondents, N=111)

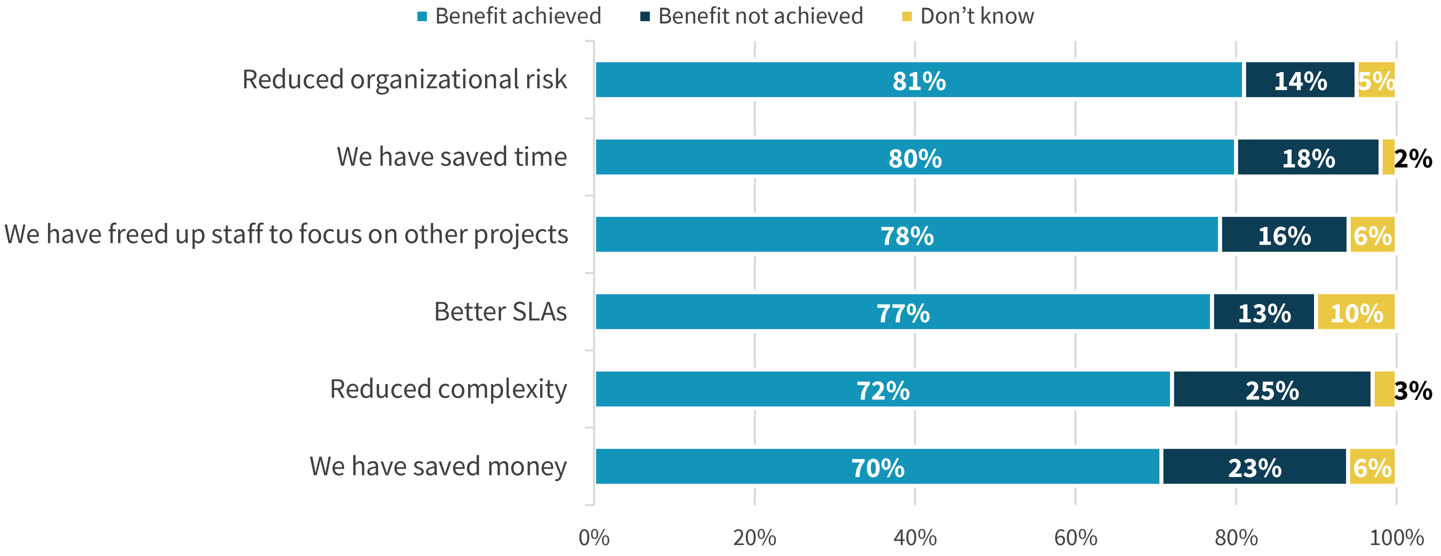


Source: Enterprise Strategy Group

There is a reason so many of these organizations are working with MSPs, and it's that they are delivering benefits to those businesses. According to the research, the most commonly reported benefit organizations have achieved from working with their MSP is that the MSP has reduced their operational risk (reported by more than eight out of ten [81%] respondents) (see Figure 11).

Figure 11. Benefits of Working with MSPs

Which of the following benefits has your organization achieved as a result of engaging its MSP(s)? (Percent of respondents, N=125)

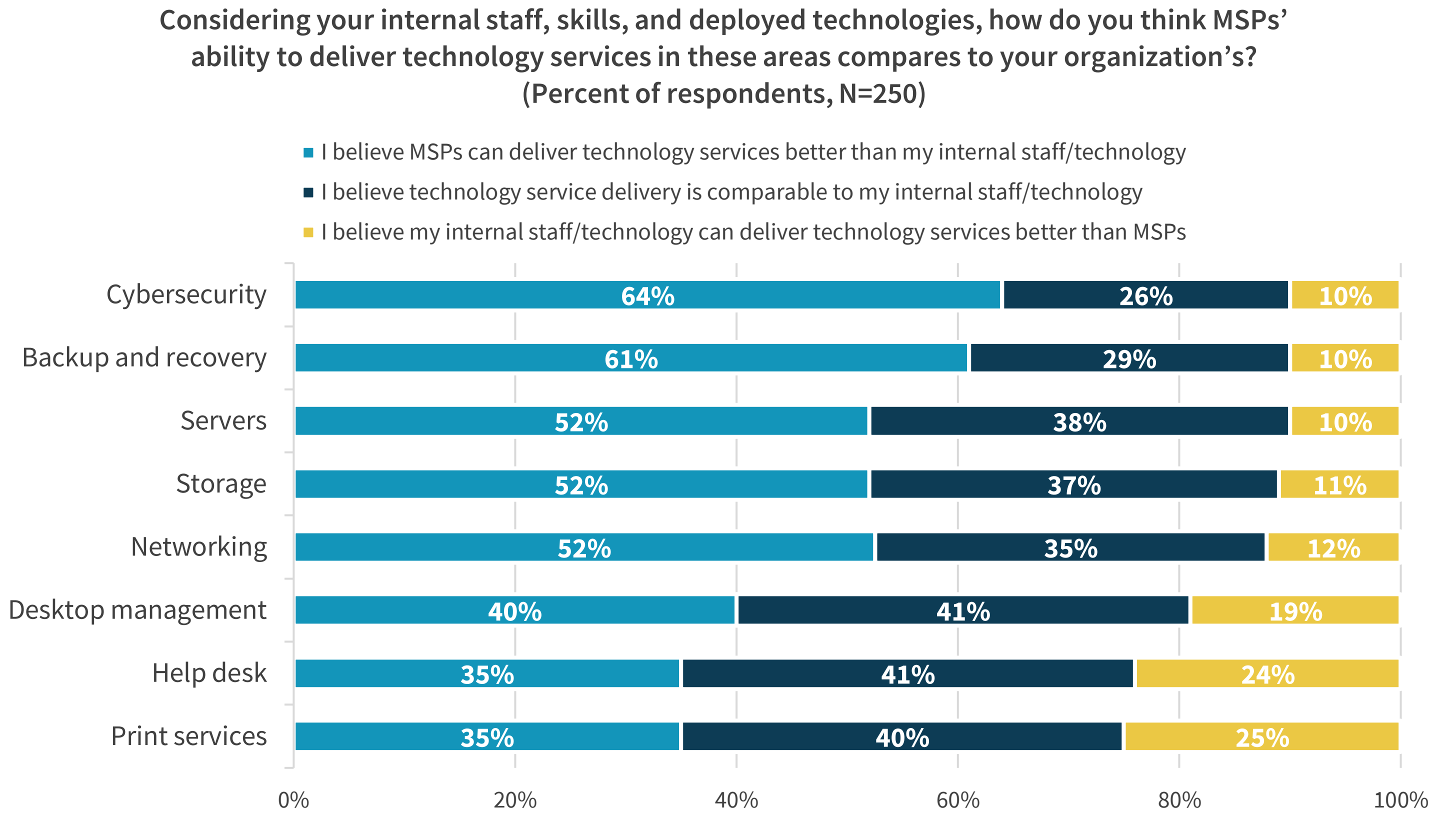


Source: Enterprise Strategy Group

Other benefits of working with MSPs include the abilities to save time, enable existing staff to work on other projects, achieve better SLAs, and reduce complexity. Lastly, many also reported they were able to save money. Given the previously reported budget issues holding back security initiatives, this appears to be a natural fit.

ESG research asked these organizations who would be better prepared to deliver a number of different IT services as compared to their internal staff. Figure 12 illustrates the results. It should be noted that 90% of organizations thought that MSPs could do as well as or better than their internal staff when it came to cybersecurity, with almost two-thirds (64%) believing that MSPs can deliver security services better than internal resources.

Figure 12. Organizations Believe MSPs Are Better for Security



Considering your internal staff, skills, and deployed technologies, how do you think MSPs' ability to deliver technology services in these areas compares to your organization's? (Percent of respondents, N=250)

Source: Enterprise Strategy Group

The Bigger Truth

The reality is that all companies that rely on IT to run their business are facing a complex and ever-changing cybersecurity threat landscape, yet based on the research collected, few small midmarket companies are well equipped to deal with it. The lack of dedicated resources, IT budgets, and skills to deploy and operate the security solutions poses real problems. With so many organizations dealing with multiple security incidents per year, it will be imperative to find a solution to mitigate risk or potentially go out of business.

This is where MSPs can play a significant role. The research indicates that MSPs with the appropriate security skills and services can deliver meaningful results. In fact, organizations are 6.4x more likely to believe MSPs are better at delivering cybersecurity services than their own staff. And furthermore, if the right MSP is selected, there are a number of additional IT services it could deliver to provide additional value. Given that most organizations in the survey would prefer to work with a single MSP, organizations need to approach the selection process not as one-off vendor selections but as a search for strategic partners that can help mitigate risk and enable employees to focus on the business.

Appendix: Research Methodology and Respondent Demographics

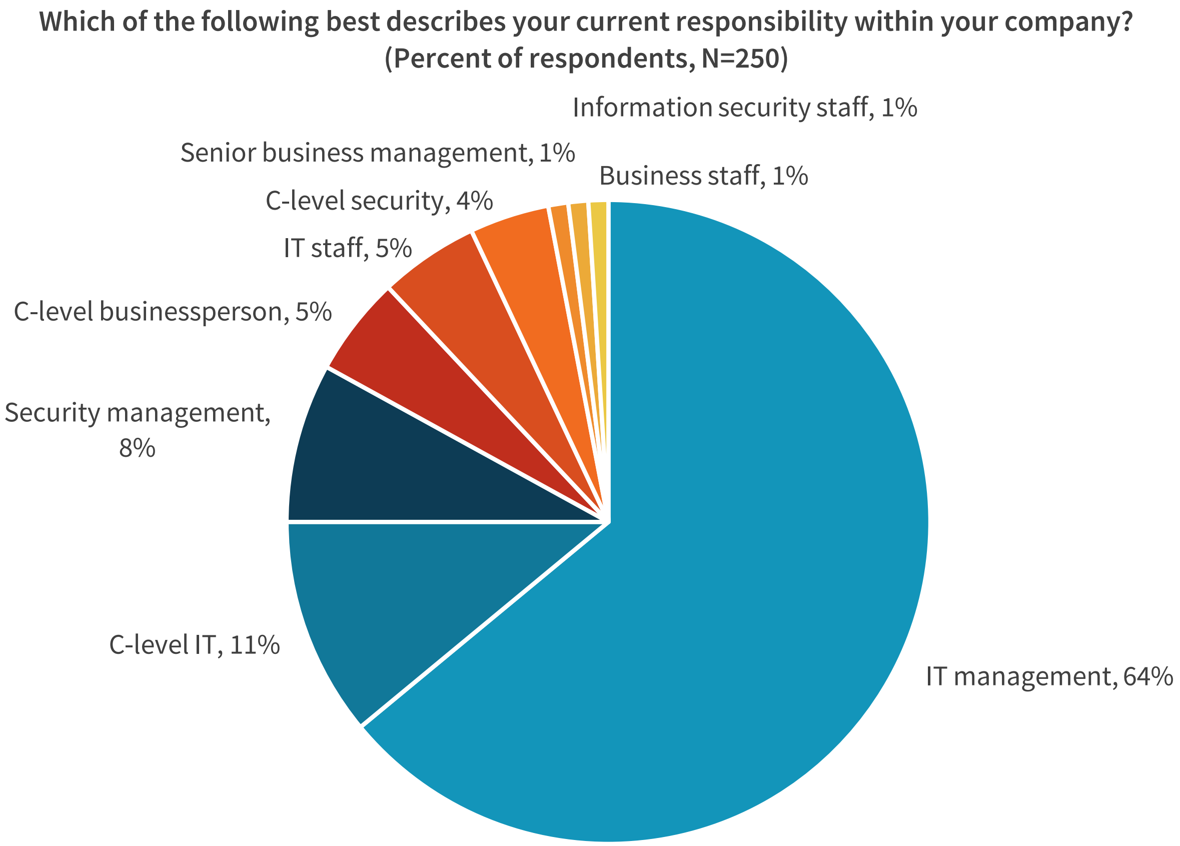
To gather data for this report, ESG conducted a comprehensive online survey of IT information security decision makers from private- and public-sector organizations in North America (US and Canada). The survey was fielded between January 6, 2020 and February 3, 2020.

To qualify for this survey, respondents were required to be senior IT/information security decision makers with good knowledge of their organizations' networking and security controls. All respondents must have been employed at organizations with 20 to 500 more employees, representing multiple verticals, including technology, manufacturing, education, and business services, among others.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

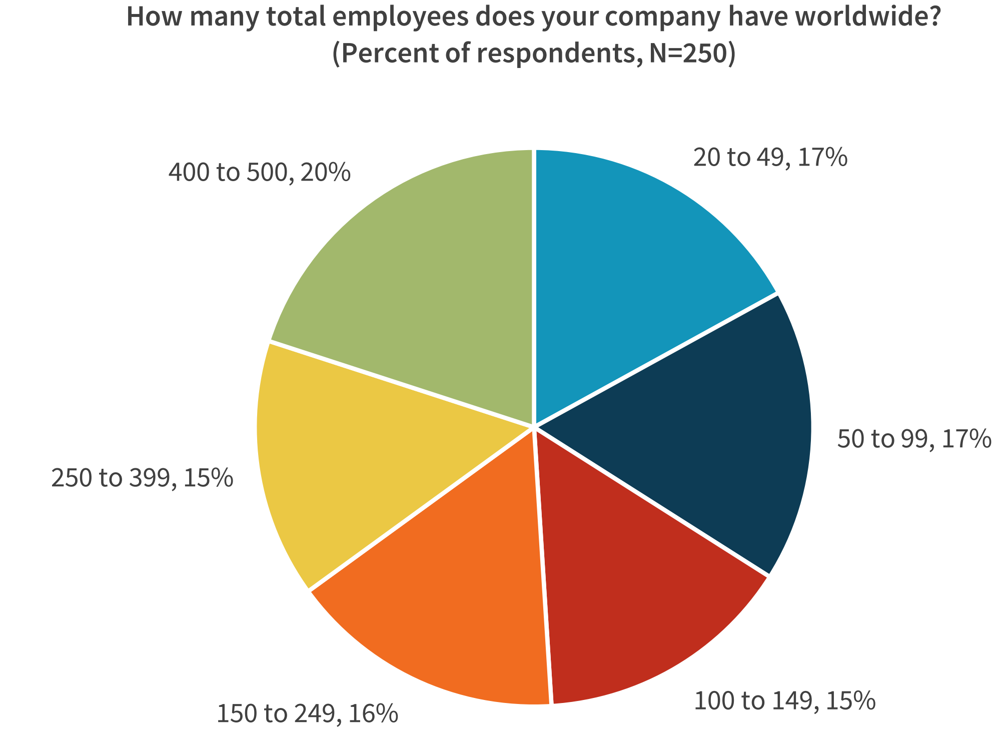
Figures 13 - 16 detail the demographics of the respondent base: individual respondents' current job responsibilities, as well as respondent organizations' total number of employees, primary industry, and annual revenue.

Figure 13. Survey Respondents, by Job Responsibility



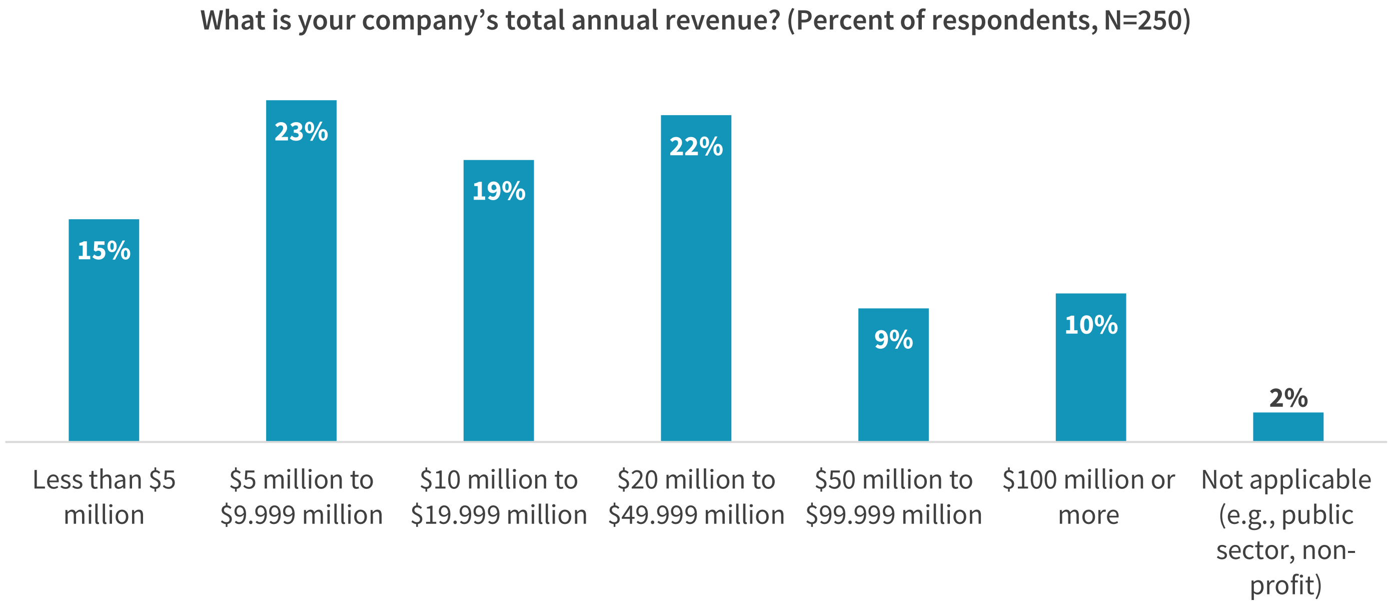
Source: Enterprise Strategy Group

Figure 14. Survey Respondents, by Company Size (Number of Employees)



Source: Enterprise Strategy Group

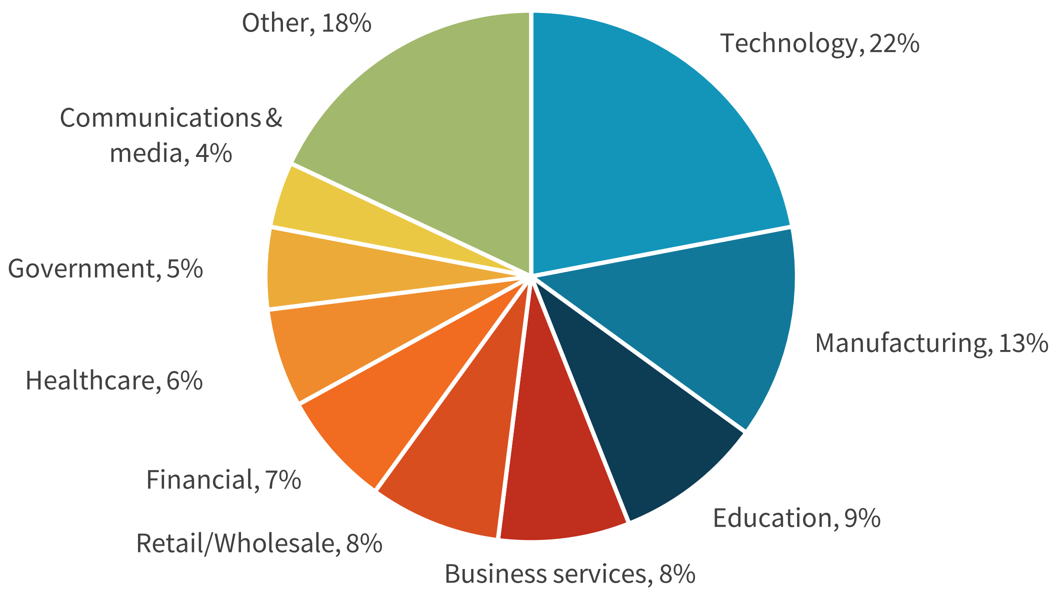
Figure 15. Survey Respondents, by Company Size (Revenue)



Source: Enterprise Strategy Group

Figure 16. Survey Respondents, by Industry

What is your company's primary industry? (Percent of respondents, N=250)



Source: Enterprise Strategy Group

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188