Enterprise Strategy Group | **Getting to the bigger truth.™**

Research Insights Report

The Rise of Direct Internet Access (DIA)

Securing Remote Users and Branch Offices

By Jon Oltsik, ESG Senior Principal Analyst and ESG Fellow

May 2019

This ESG White Paper was commissioned by Cisco Systems
and is distributed under license from ESG.

Contents

Executive Summary

In 2018, the Enterprise Strategy Group (ESG) completed a research survey of 450 cybersecurity, IT, and networking security professionals with knowledge of or responsibility for the policies, processes, and controls used for remote office/branch office (ROBO) security.

Based upon the research collected for this project, ESG concludes:

- **Cloud computing is driving changes to ROBO networks.** Survey respondents worked at organizations with an average of 368 ROBO locations. The research also indicates that most organizations use a lot of SaaS applications and have high percentages of roaming users. The prolific movement toward cloud and mobility is changing ROBO networking as organizations move from backhauling all traffic to direct-to-Internet connections at remote and branch offices. Many firms are also moving from traditional WAN services to more flexible SD-WAN technologies. All these changes are impacting and changing ROBO security.

- **Today's ROBO security is fraught with challenges.** Security management is growing more difficult, as ROBO and roaming users connect to a mix of cloud-based and internal applications and many organizations report that they lack the right level of visibility to keep up with ROBO security complexity. ROBO and roaming user security also depends upon strong collaborative processes between infosec and network operations teams. Unfortunately, the two groups don't always work well together. These challenges reduce the effectiveness of ROBO and roaming security processes and controls, making remote users more susceptible to cyber-attacks and system compromises.

- **ROBO security changes are taking shape.** The research indicates that organizations are making substantial changes to safeguard ROBOs and roaming users from cyber threats. Many are replacing today's disconnected point tools with multi-function security platforms that consolidate and integrate security controls. Many are using network proxies for inspecting and filtering all traffic to and from remote users. Finally, many organizations are deploying or plan to deploy cloud-based network security controls, like secure Internet gateways (SIGs). Cloud-based SIGs are increasingly attractive as they can offer threat protection, central management, and strong network performance for user productivity. In this way, they can improve security efficacy, streamline security operations, and enable ROBO business processes.

It is worth noting that these trends tend to be most dramatic among highly distributed enterprises and, to a lesser extent, those in North America. Differences between regions and organizational size are noted throughout this ESG Research Insights Report.

Overview

Nearly nine out of ten (88%) respondents that began ESG's survey worked for organizations with at least five ROBO locations while 42% of qualified respondents worked for organizations with more than 250 ROBO locations. Across the entire survey population, the average number of ROBO locations was 368, with the North American average (403) higher than western Europe (302).

The data also reveals:

- **High-volume and growing use of software-as-a-service (SaaS).** Nearly one-third (32%) of respondents report that SaaS applications account for 50% or more of their organizations' business applications today. Usage will continue to grow in the future, as 60% of respondents claim that SaaS applications will account for 50% or more of their organizations' business applications in two years.

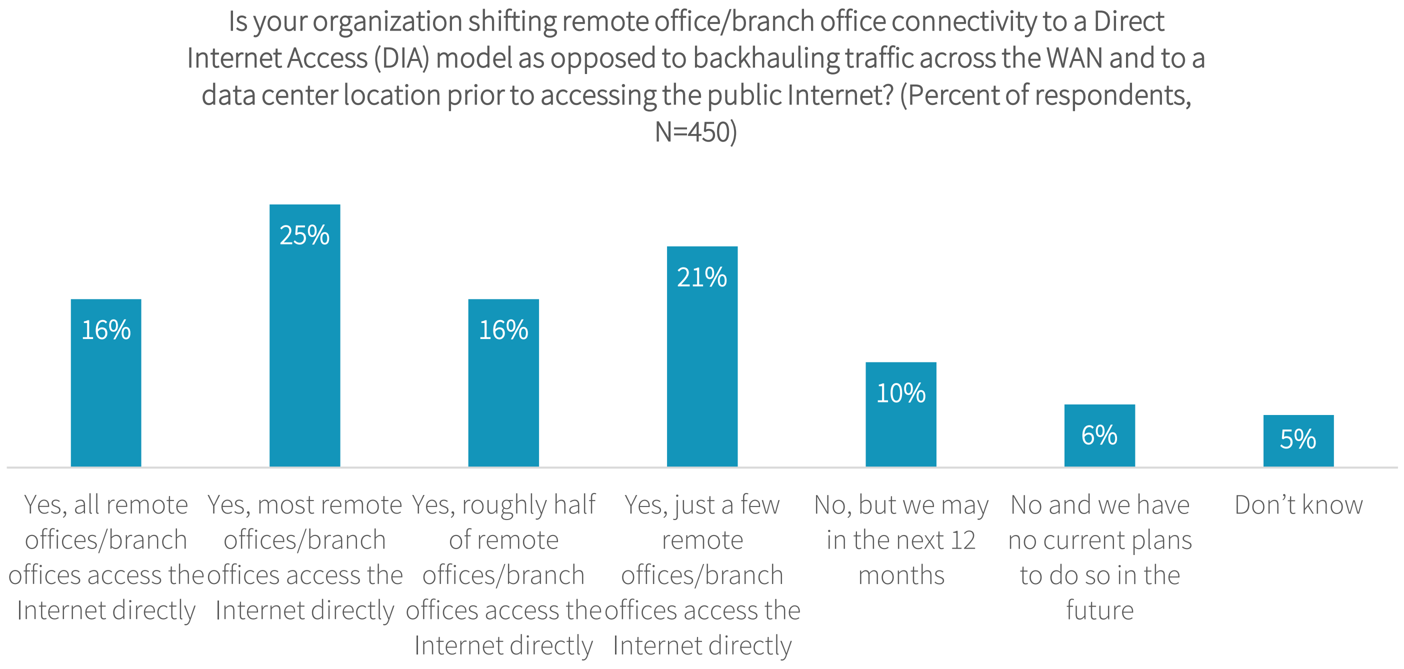
- **Large populations of roaming users.** Survey respondents were asked to estimate the percentage of employees who could be considered "roaming users" at their organization. The term "roaming user" was defined as follows: Those who work from a home office, on the road, or any other non-corporate location at least 20% of the time (note: respondents were asked to exclude time spent at a ROBO from roaming time). Based upon this definition, roaming users make up a mean value of 40% of all employees today, growing to 50% in the next two years. It is worth noting that the percentage of roaming users varied by region. Forty-three percent of North American employees are considered roaming users compared to 36% of European workers. This gap will narrow in the future, however. The data forecasts that 51% of North American employees and 48% of European workers will be considered roaming users in two years.

- **Difficulties with cybersecurity staffing.** This came as no surprise due to the global cybersecurity skills shortage. Seventeen percent of respondents claim that it is very difficult for their organization to find and recruit qualified security professionals. Staffing issues varied by region—21% of North American organizations say it is very difficult to find and recruit qualified security professionals compared to 9% of European organizations.

ROBO Networking Technology Trends

ROBOs are also moving from backhauling all traffic through corporate networks to a Direct Internet Access (DIA) networking model. More than half of respondents (57%) claim that at least half of their ROBOs access the Internet directly today (see Figure 1). In total, 79% of organizations are shifting to a Direct Internet Access model for some of their ROBOs.

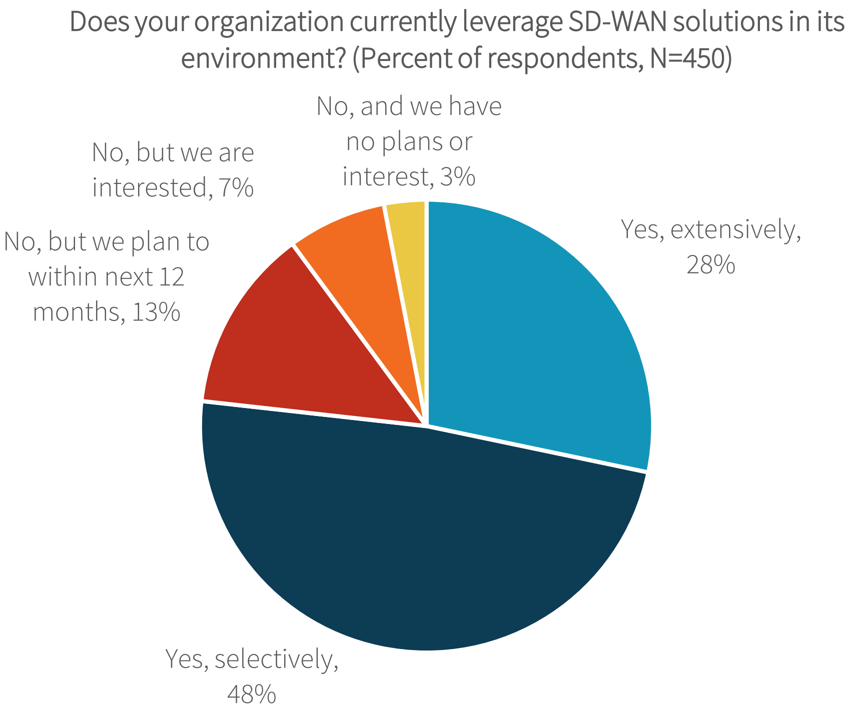
Figure 1. Organizations Are Moving to a Direct-to-Internet Networking Model



Source: Enterprise Strategy Group

Along with DIA, the ESG research points to another strong networking trend—organizations are eschewing traditional WAN services like MPLS and dedicated circuits in favor of software-defined WAN (SD-WAN) technology. Twenty-eight percent of organizations already use SD-WAN solutions extensively, while 48% use SD-WAN technology selectively (see Figure 2).

Figure 2. Increasing Use of SD-WAN Technology

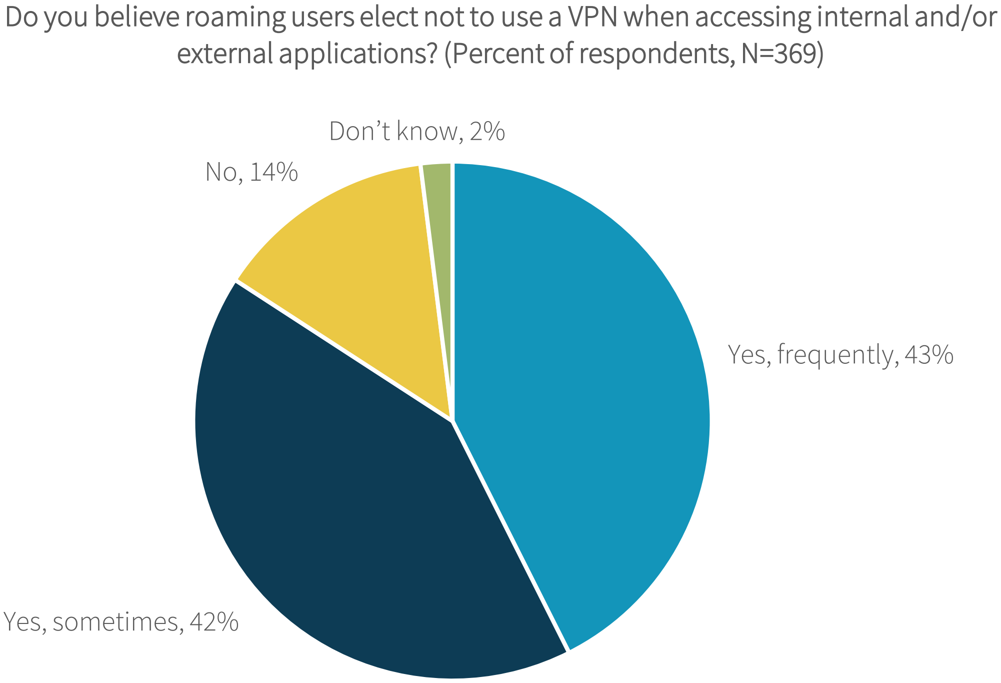


Source: Enterprise Strategy Group

The use of technologies like DIA and SD-WAN for ROBO connectivity introduces some challenges with network access controls. Historically, remote, branch office, and roaming users connected to internal and external applications via VPNs, and this meant that remote user traffic was "hair pinned" through corporate networks to and from websites, SaaS applications, or cloud-resident workloads. This traditional VPN model may also be strained. The research indicates that 82% of organizations continue to mandate the use of VPNs. Of those organizations with a VPN mandate, 43% believe that roaming users frequently circumvent VPN use while 42% avoid VPN use sometimes (see Figure 3).

This data seems to predict a changing future for network access controls, as VPN technology transforms into software-defined perimeters (SDPs) built upon a zero-trust networking model. SDPs will be needed to provide the right levels of access controls with end-to-end security for a DIA-connected world.

Figure 3. Roaming Users Work Around Corporate VPNs



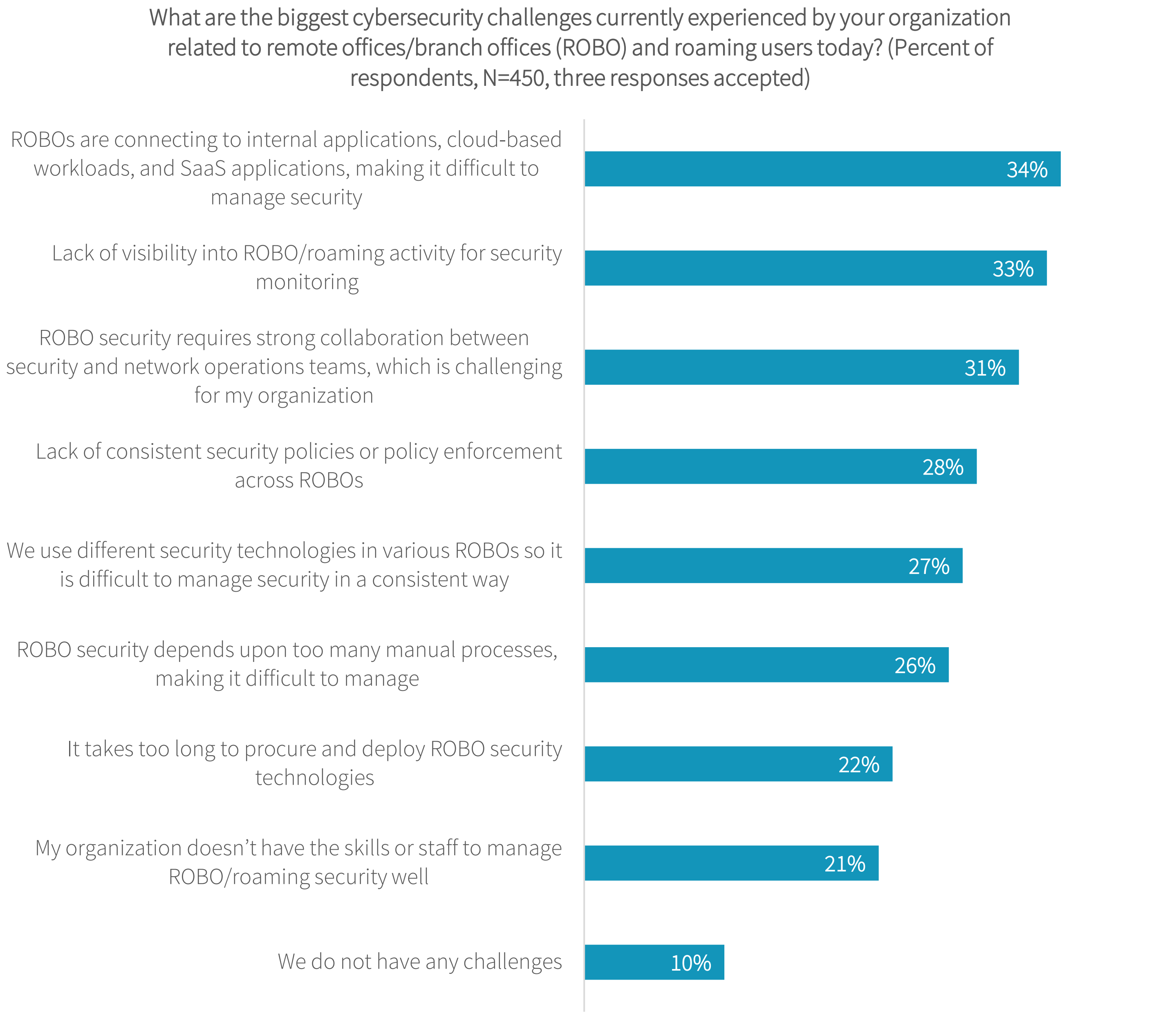
Source: Enterprise Strategy Group

ROBO Security

Remote and branch offices are notoriously difficult to secure for several reasons. Organizations tend to have dozens or hundreds of ROBOs, making it difficult to scale security policies, processes, and controls effectively. These problems are evident in areas like security device procurement, provisioning, configuration, and ongoing operations. ROBO offices may also lack dedicated security or even IT professionals who can provide for the care and feeding of security devices. Finally, employees working in ROBOs tend to receive less security awareness training than those in more populated corporate offices.

These and other issues create many security challenges. The research points to problems such as managing ROBO security in an environment of cloud-based workloads and SaaS, a lack of visibility into ROBO and roaming user activities, and collaboration issues between security and network operations teams (see Figure 4).

Figure 4. ROBO Security Challenges



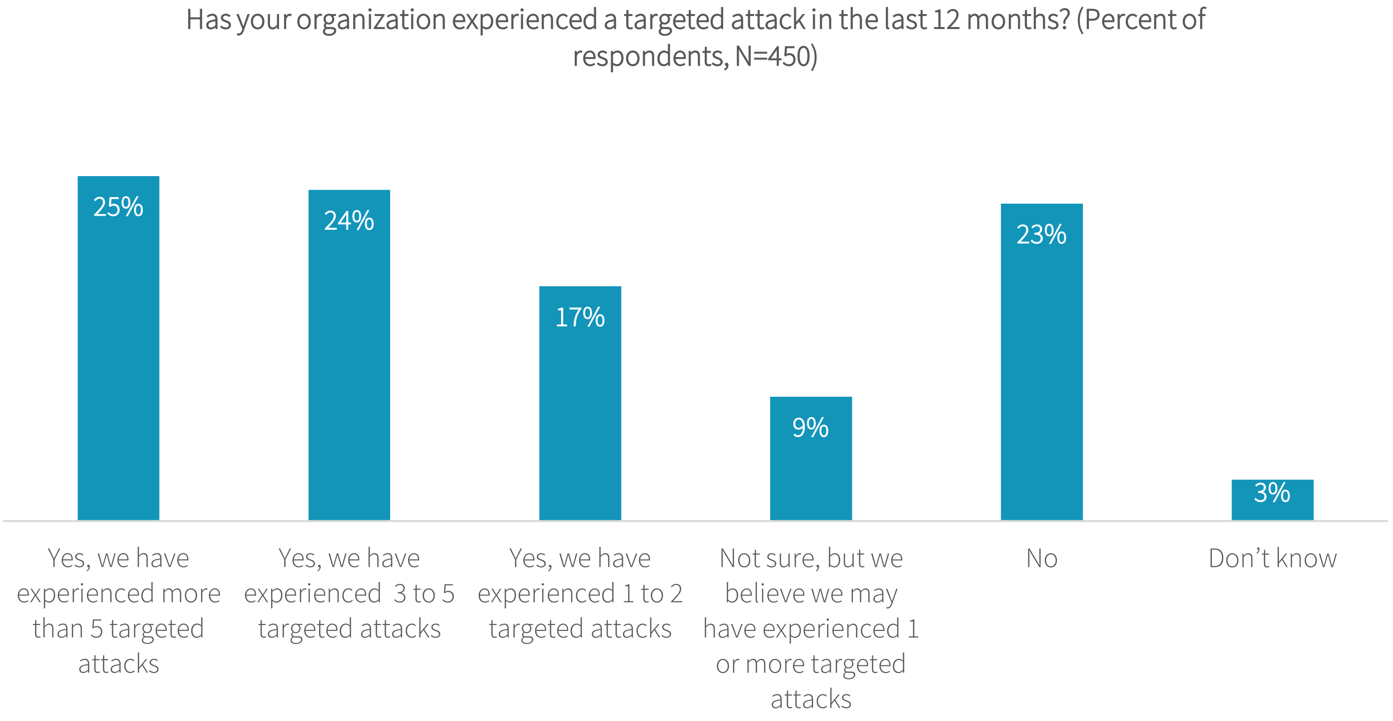
Source: Enterprise Strategy Group

One possible reason for these challenges can be traced to the use of point tools for cybersecurity. The research reveals that 31% of organizations use between 25 and 49 different point tools for cybersecurity, 35% use between 50 and 74 different point tools for cybersecurity, and 11% use between 75 and 99 different point tools for cybersecurity. Each point tool must be procured, tested, configured, deployed, and operated daily. Furthermore, security analysts are forced to evaluate their security posture on a tool-by-tool basis. Point tools are not scalable, as they are dependent upon time-consuming and error-prone manual processes.

Aside from operational issues, ROBO security challenges also create unacceptably high levels of cyber risk for organizations. This is a real concern because many organizations face a constant stream of attacks from cyber-adversaries. ESG research data indicates that two-thirds (66%) of survey respondents say that their organization has experienced at least one targeted attack over the past 12 months (see Figure 5).

Targeted attacks vary by region and number of ROBOs. Nearly one-third (32%) of North American organizations have experienced at least five targeted attacks, compared to only 12% of western European organizations. Additionally, 41% of organizations with more than 100 ROBOs experienced at least five targeted attacks, compared to 8% of those with fewer than 100 ROBOs.

Figure 5. Targeted Attacks Experienced

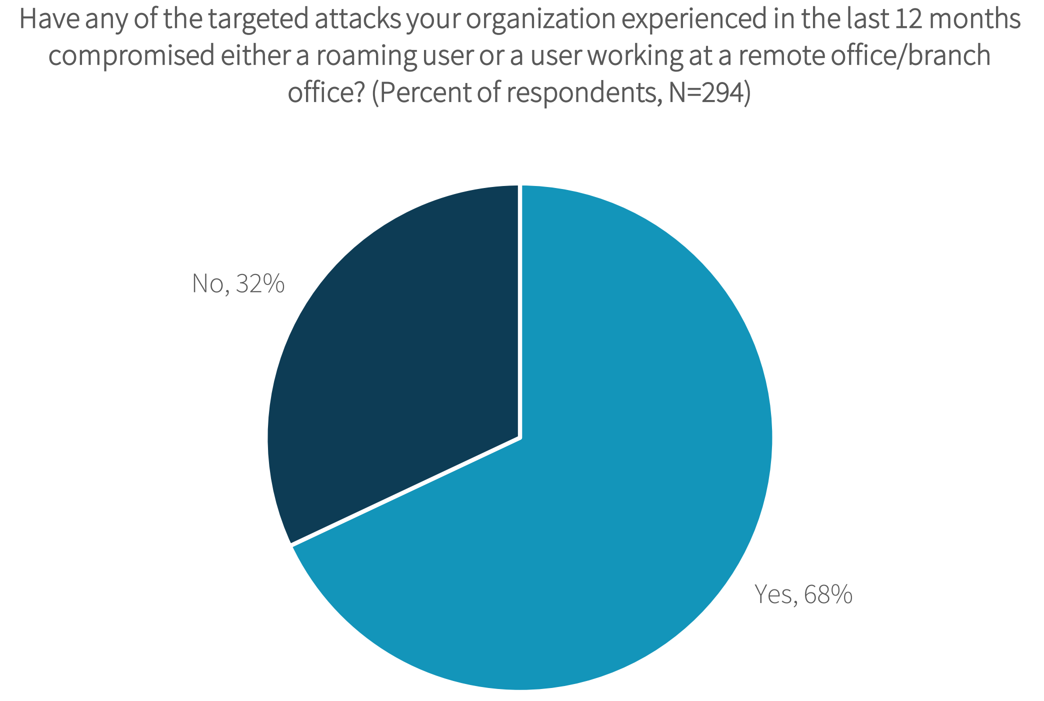


Source: Enterprise Strategy Group

It should be noted that 43% of respondents believe that roaming users are the most vulnerable cohort to a targeted attack while 35% believe that ROBO users are the most vulnerable, and just 20% report that employees at corporate offices are the most vulnerable. This belief seems to be accurate, as 68% of survey respondents report that ROBOs and roaming users were the source of compromise of recent attacks (see Figure 6).

Based on this ESG research, it appears that the lack of security oversight and user training for ROBO and roaming users comes at a cost—frequent security incidents and increased cyber risk. ROBO and roaming users often act as a port of entry for cyber-adversaries as they compromise systems, move laterally across networks, and ultimately exfiltrate data.

Figure 6. ROBO and Roaming Users Are Often the Victims of Cyber-attacks



Source: Enterprise Strategy Group

Emerging Strategies for ROBO and Roaming User Security

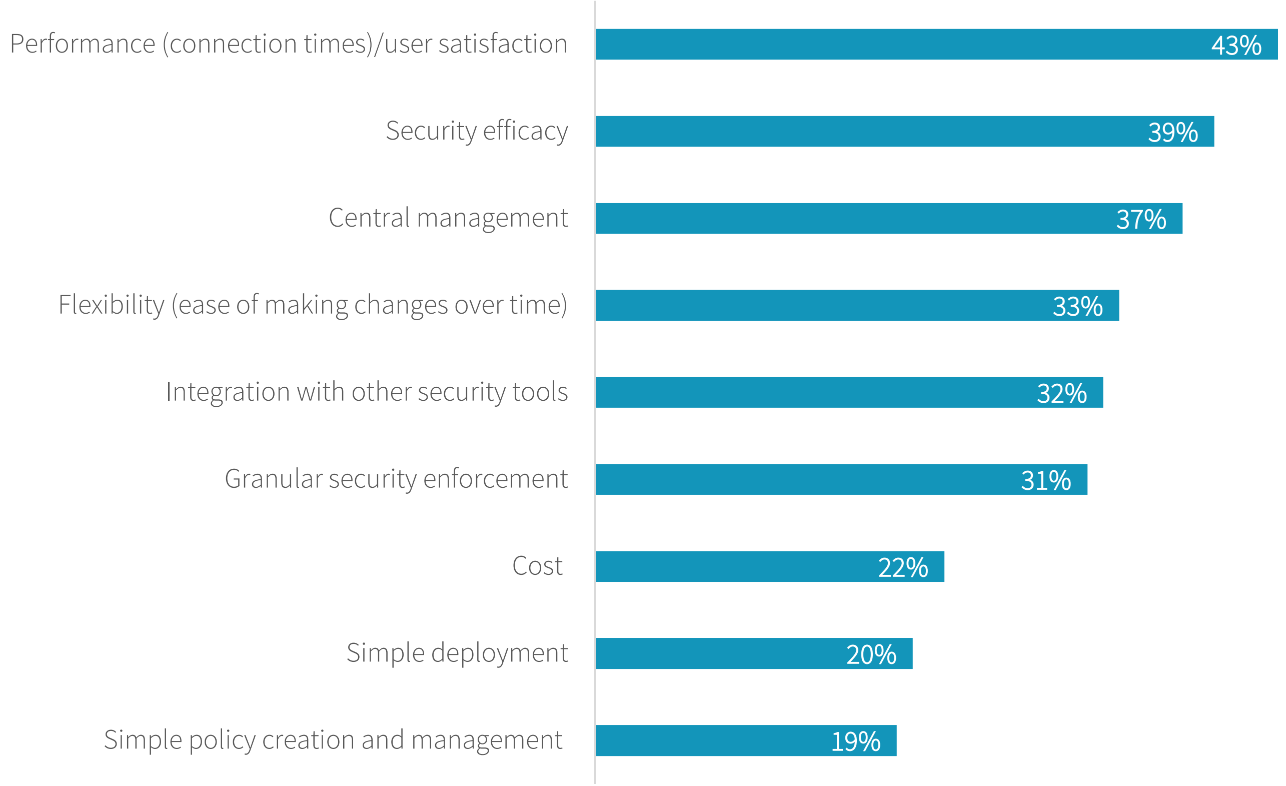
As more ROBO users utilize more SaaS applications for their daily tasks, performance issues are driving the adoption of DIA and SD-WAN. CISOs should consider new strategies that can leverage these shifts as an opportunity to efficiently improve security while supporting the underlying business needs. As part of this project, ESG wanted to understand the most important considerations for this transition. When securing DIA ROBO connections, survey respondents claim that organizations seek to emphasize (see Figure 7):

- **Performance.** Security must be transparent rather than act as an impediment for ROBO user productivity.
- **Security efficacy.** While running in the background, security controls must be as effective as possible, blocking or detecting cyber-attacks with accuracy and timeliness.
- **Central management.** Organizations want central command-and-control for distributed security controls deployed at ROBO locations. In this way, they can streamline operations for activities like configuration management, policy management, and change management.

Security efficacy and central management are valuable attributes that can also help organizations address issues related to the global cybersecurity skills shortage. This is especially important since 46% of survey respondents report that it is very difficult or difficult to find and recruit qualified security professionals with advanced skills.

Figure 7. Most Important Characteristics of Security Controls for DIA Traffic

When securing your organization's remote office/branch office direct-to-Internet traffic, which characteristics of security controls used are most important to you? (Percent of respondents, N=352, three responses accepted)



Source: Enterprise Strategy Group

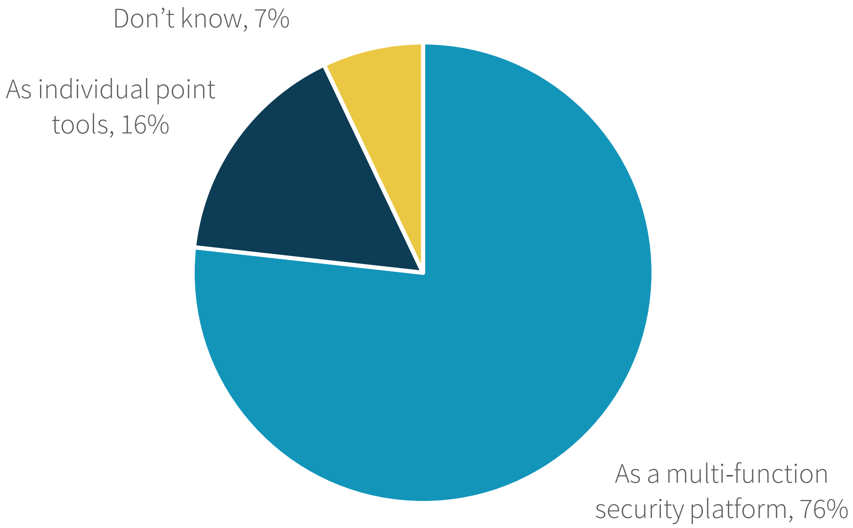
As far as the most important security controls for DIA, 52% of respondents say firewalls are most important, 45% say DNS-layer security, 42% say malware sandboxes, and 42% say CASB (note: multiple responses were accepted for this question).

ROBO Security Changes in Play

CISOs have a lot of work ahead to align security controls with the transition to DIA and SD-WAN while simultaneously increasing security efficacy and consolidating point tools for operational efficiency. The research points to some of the ways organizations are addressing these requirements. For example, 76% of those surveyed want to consume security controls as a multi-function security platform, while only 16% want to use individual point tools (see Figure 8). The security controls deemed most important for DIA (i.e., network firewalls, DNS-layer security, malware sandboxes, and CASB) could be combined into a multi-function security platform supported by central management.

Figure 8. Organizations Prefer Multi-function Security Platforms for DIA

Considering remote offices/branch offices specifically, how would your organization prefer to consume security controls (i.e., to remote offices/branch offices that have Direct Internet Access)? (Percent of respondents, N=450)



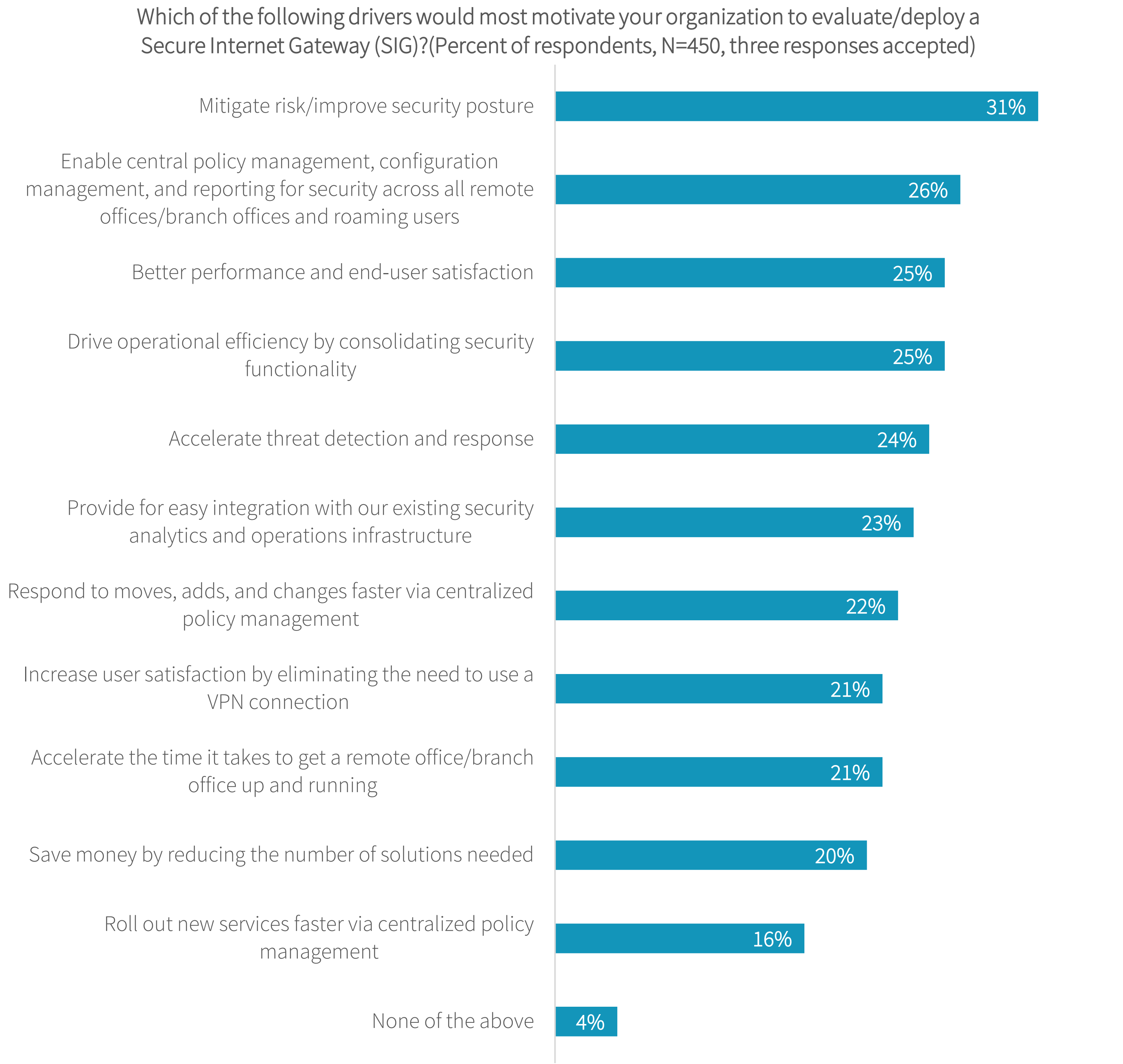
Source: Enterprise Strategy Group

Network proxies represent one way to aggregate multiple point tools into a single offering. As traffic passes through a proxy, it can be inspected, filtered, forwarded, and monitored according to access policies, and protected from emerging types of threats. Network proxies seem to make sense for DIA and SD-WANs—64% of organizations utilizing network proxies claim that all or most network traffic from ROBOs passes through a network proxy, while 62% of all or most traffic from roaming users passes through a network proxy. As far as form factor goes, 67% of respondents believe that their organization will replace all proxy servers/services residing on their corporate networks with cloud-based alternatives in the future. Similarly, 85% of organizations are deploying or planning to deploy cloud-based firewall-as-a-service offerings for their ROBOs or even across all locations (i.e., ROBOs and corporate offices that currently use on-premises firewalls).

One way to gain the benefits of network proxies, firewalls, DNS-layer security, and CASBs in a cloud-based form factor is through the use of secure Internet gateway (SIG) services. In this model, traffic to and from the Internet is sent through a SIG to enforce access control policies, protect users from malicious traffic, and secure usage of SaaS apps. Based upon the data presented above, it comes as no surprise that 87% of survey respondents agree that a SIG could be an effective way to protect ROBOs and roaming users.

Finally, ESG asked respondents what would entice their organization to evaluate or deploy a SIG. Responses align well with Figure 7 as organizations would be motivated to move if a SIG could mitigate risk and/or improve their security posture, enable central management (i.e., of multiple ROBO/roaming user security controls), and offer better performance and end-user satisfaction (see Figure 9).

Figure 9. Drivers that Would Motivate a SIG Evaluation or Purchase



Source: Enterprise Strategy Group

The Bigger Truth

Based upon the research presented in this report, it is clear that there are many simultaneous changes taking place. Organizations are moving workloads to the public cloud and embracing SaaS applications. As more of their application portfolio migrates to the cloud, organizations are experiencing an impact to their network infrastructure—especially as it relates to connecting ROBOs and roaming users, where organizations are moving toward DIA and SD-WAN technologies.

Organizations must realize that these evolving ROBO/roaming security tactics are a mismatch for this transition, as they are difficult to manage, don't provide the right level of visibility, and can't support security and network operations teams effectively.

Rather than continuing to address ROBO and roaming user security with an assortment of disconnected point tools, CISOs must:

- **Develop an appropriate model for network access to enable remote users.** The research seems to indicate that VPNs may hamper remote users as business applications migrate from corporate networks to the cloud. Since CISOs know that security cannot impede productivity, this issue should be a top priority. Organizations should address this by exploring software-defined perimeter (SDP) and zero-trust technologies that provide the right level of network and application access based upon attributes like user identity, device type, location, and changes in cyber-risk. In this way, security teams can maintain the control and security of VPNs while they support and improve cloud access control.

- **Consolidate tools for security efficacy and operational efficiency.** This and other ESG research clearly indicates that organizations' reliance on security point tools is a mismatch for today's sophisticated threats and growing attack surface. This is certainly a factor in why 76% of organizations prefer to consume ROBO security tools as a multi-function platform. Consolidating tools and moving toward central management can lead to better data sharing, automated responses, faster decision making, and simplified security operations. CISOs need these kinds of benefits to improve ROBO security—especially in support of the DIA trend.

- **Consider cloud-based form factors for security controls.** As a result of the cybersecurity skills shortage, many organizations employ cybersecurity teams with too much to do and not enough people to keep up with the workload. One way to address this cycle is through the use of cloud-based security controls that eliminate the need to procure, test, configure, deploy, and operate on-premises infrastructure. This is especially useful for security support across dozens or hundreds of ROBOs, as many locations have few if any security (or IT) personnel to manage security devices on a day-to-day basis. The best cloud-based security controls can help CISOs improve security efficacy, streamline operations, and promote a productive work environment for ROBO and roaming users.

Appendix: Research Methodology and Respondent Demographics

To gather data for this report, ESG conducted a comprehensive online survey of cybersecurity, IT, and networking security professionals with knowledge of or responsibility for the policies, processes, and controls used for remote office/branch office (ROBO) security. Two-thirds of survey respondents were in North America while 34% resided and worked in western Europe. Twenty percent of respondents worked at organizations with fewer than 1,000 employees, 26% worked at organizations with 1,000 to 4,999 employees, 23% worked at organizations with 5,000 to 9,999 employees, 12% worked at organizations with 10,000 to 19,999 employees, and 19% worked at organizations with more than 20,000 employees. Respondents represented numerous industry and government segments, with the largest participation coming from information technology (20%), manufacturing (17%), financial services (17%), business services (8%), and communication and media (8%).

The survey was fielded between November 6, 2018 and November 29,2018.

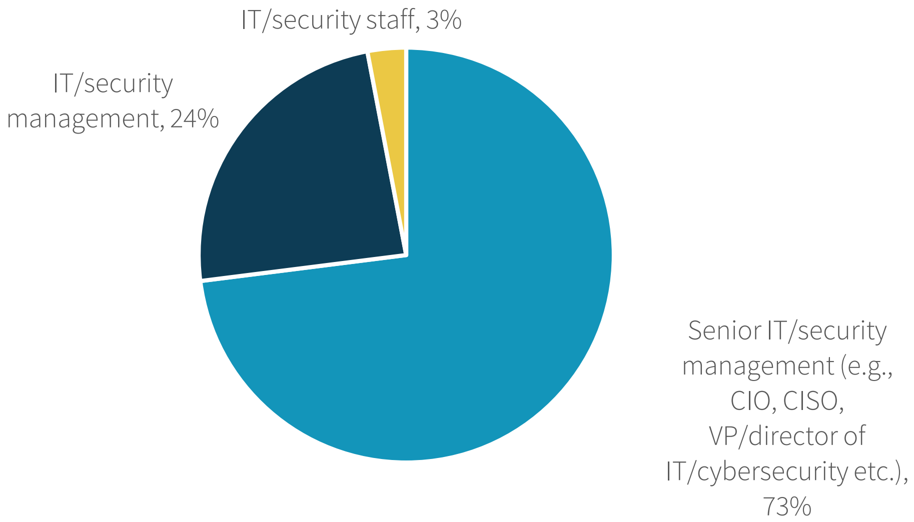
After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 450 respondents remained.

All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

The figures below detail the full 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 10. Survey Respondents, by Job Responsibility

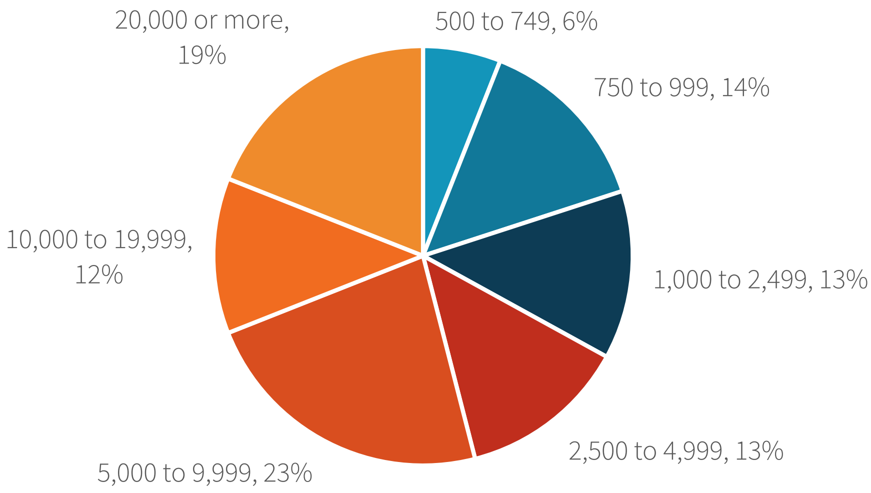
Which of the following best describes your current responsibility within your organization? (Percent of respondents, N=450)



Source: Enterprise Strategy Group

Figure 11. Survey Respondents, by Company Size (Number of Employees)

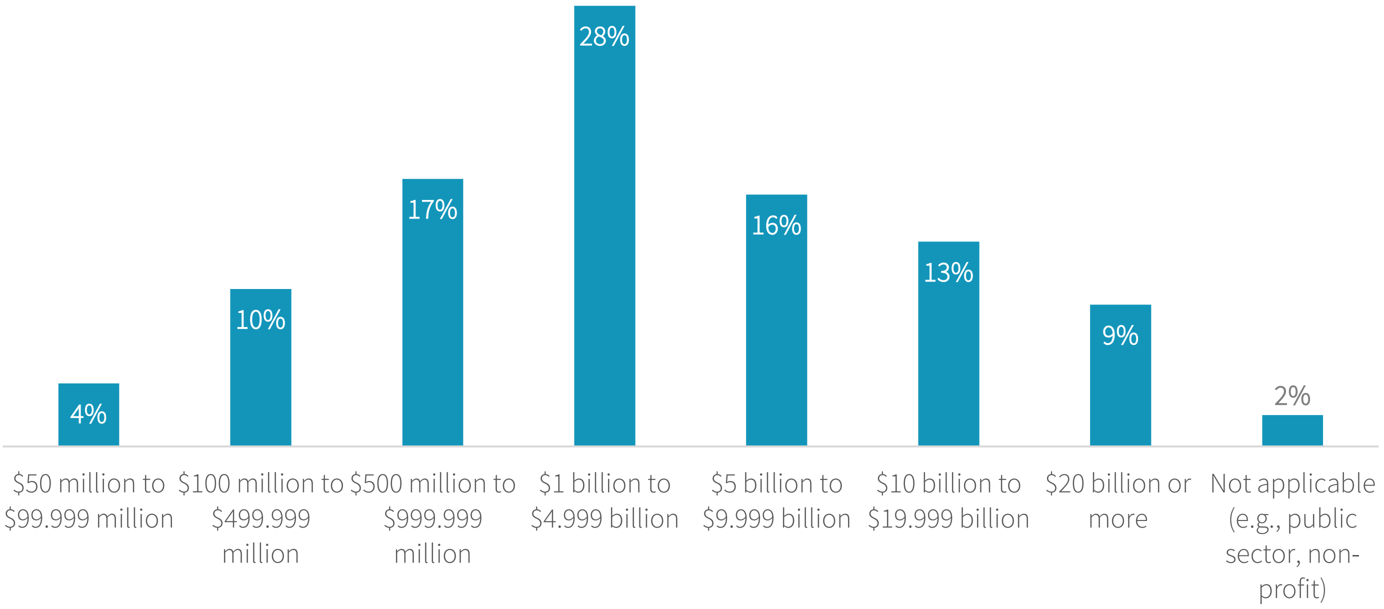
How many total employees does your organization have worldwide? (Percent of respondents, N=450)



Source: Enterprise Strategy Group

Figure 12. Survey Respondents, by Company Size (Revenue)

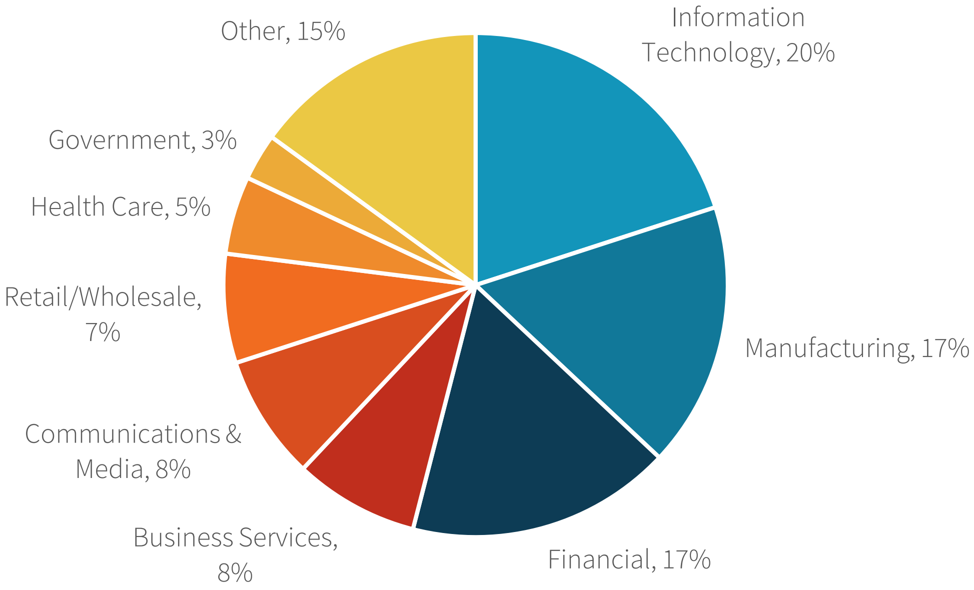
What is your organization's total annual revenue ($US)? (Percent of respondents, N=450)



Source: Enterprise Strategy Group

Figure 13. Survey Respondents, by Industry

What is your organization's primary industry? (Percent of respondents, N=450)



Source: Enterprise Strategy Group

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