ESG RESEARCH REPORT

The Impact of the COVID-19 Pandemic on Cybersecurity

A Cooperative Research Project by ESG and ISSA

By Jon Oltsik, Senior Principal Analyst and Fellow

July 2020

Contents

List of Figures

Executive Summary

Report Conclusions

As the global impact of COVID-19 manifested itself in the US in the middle of March, ESG and ISSA decided to conduct an in-depth survey in April 2020 of 364 cybersecurity and IT professionals from the global ISSA member list. The study was a point in time assessment of challenges posed by the pandemic. It is likely that challenges and solutions will continue to evolve over the next few years.

Based upon the data gathered as part of this project, the report highlights the following:

- Organizations were fairly prepared for the global pandemic. While COVID-19 has disrupted many aspects of day-to-day life, many organizations have been able to work through the unexpected new IT and cybersecurity requirements. In fact, 39% of respondents claim that they were very prepared to secure WFH devices and applications while 34% were prepared for these new requirements. It is worth noting, however, that 27% were underprepared. These organizations may have had smaller remote worker populations before the pandemic or limited cybersecurity staffs who were immediately overwhelmed by the urgent new security requirements of the pandemic.

- COVID-19/WFH have had an impact on cybersecurity professionals. Aside from overall cybersecurity actions, the global pandemic has had an impact on individuals on the security staff. The research indicates that COVID-19 has forced cybersecurity professionals to change their priorities/activities, increased their workloads, increased the number of meetings they have had to attend, and increased the stress levels associated with their jobs. CISOs should take note of these changes and closely monitor cybersecurity team members for signs of burnout.

- WFH presents many cybersecurity challenges. When asked to define the top challenges related to the new WFH environment, ISSA members pointed to securing remote devices, providing secure network access for remote employees, monitoring network traffic, and coordinating moves, adds, and changes with IT operations.

- COVID-19 has led to an increase in cyber-attacks. The cybersecurity professionals surveyed for this project see a spike in cyber-attacks related to the pandemic—20% have seen a significant increase in attempted cyber-attacks while 43% claim a slight increase in attempted cyber-attacks. In response to the increasing volume of cyber-attacks, organizations are ramping up threat intelligence analysis and fine-tuning security controls. Thirty-eight percent of organizations say they are very active in monitoring and developing countermeasures for new types of cyber threats associated with COVID-19 while another 35% are active in these areas.

- COVID-19/WFH are driving improved collaboration. The research indicates that slightly more than one-third of organizations have experienced significant improvement in coordination between business, IT, and security executives as a result of COVID-19 issues, 38% have seen marginal relationship improvements, and 21% aren't convinced but hold out hope for coordination improvement.

- Many organizations don't believe the pandemic will impact 2020 cybersecurity spending. In terms of how cybersecurity budgets would be impacted by the pandemic, the plurality of organizations don't expect any changes to original 2020 forecasts. Of the others, 20% believe that COVID-19 security requirements will lead to an increase in security spending in 2020 while 25% think their organizations will be forced to decrease security spending this year.

- COVID-19 may impact cybersecurity priorities. ESG/ISSA believes that while it is noteworthy that 30% of the cybersecurity professionals participating in this project say that cybersecurity will be a higher priority, 70% report that

they don't know or don't believe that this crisis will lead to cybersecurity becoming a higher priority. Organizations prioritizing cybersecurity as a result of the pandemic will likely emerge as leaders in the next wave of cybersecurity process innovation and best practices.

Introduction

Research Objectives

COVID-19 clearly disrupted the "life and times of cybersecurity professionals" to an extent that could not be overlooked. Therefore, ESG and ISSA decided to conduct a survey focused on the impact of COVID-19 on cybersecurity professionals. This was a quantitative web-based survey comprised of 364 cybersecurity professionals and ISSA members conducted between April 29 and May 14, 2020. Survey participants represented small (i.e., less than 100 employees), midmarket (i.e., 100 to 999 employees), and enterprise-class (i.e., 1,000 employees or more) organizations in North America, Europe, Central/South America, Africa, and Asia (including Australia).

The survey was designed to answer the following questions about the impact of the COVID-19 pandemic on cybersecurity:

- As a result of the COVID-19 situation, approximately what percentage of respondents' knowledge workers are currently working from home? Are respondents personally working from home?
- How are efforts to support more employees working from home going, based on respondents' perception or feedback from employees?
- How prepared do respondents believe their organization was to secure the devices and applications employees are using at home?
- What are the most significant challenges associated with increasing the population of employees working from home?
- Have respondents seen an increase in the number of attempted cyber-attacks (e.g., phishing, social engineering attacks, ransomware, etc.) since the initial COVID-19 quarantine and related work-from-home period started?
- How active are respondents' organizations in monitoring and developing countermeasures for new types of cyber threats associated with COVID-19?
- How would respondents characterize the level of coordination between business, IT, and security executives in dealing with the ramifications of COVID-19 when they first arose? Has coordination between business, IT, and security executives (regarding COVID-19 issues) improved since the work-from-home situation began?
- How do respondents believe their organization's cybersecurity spending will be impacted for the remainder of 2020 as a result of COVID-19? In which specific areas of cybersecurity do respondents expect to see increased spending as a result of COVID-19 related business conditions?
- Do respondents think that their organization will be more flexible with work-at-home policies once the current COVID-19 pandemic subsides? How will organizations' cybersecurity strategies change as a result of COVID-19?
- How has COVID-19 and the associated work-from-home situation impacted respondents' jobs? Specifically, how do respondents feel about their jobs (shorter term) and careers (longer term) as a result of the ramifications of COVID-19?

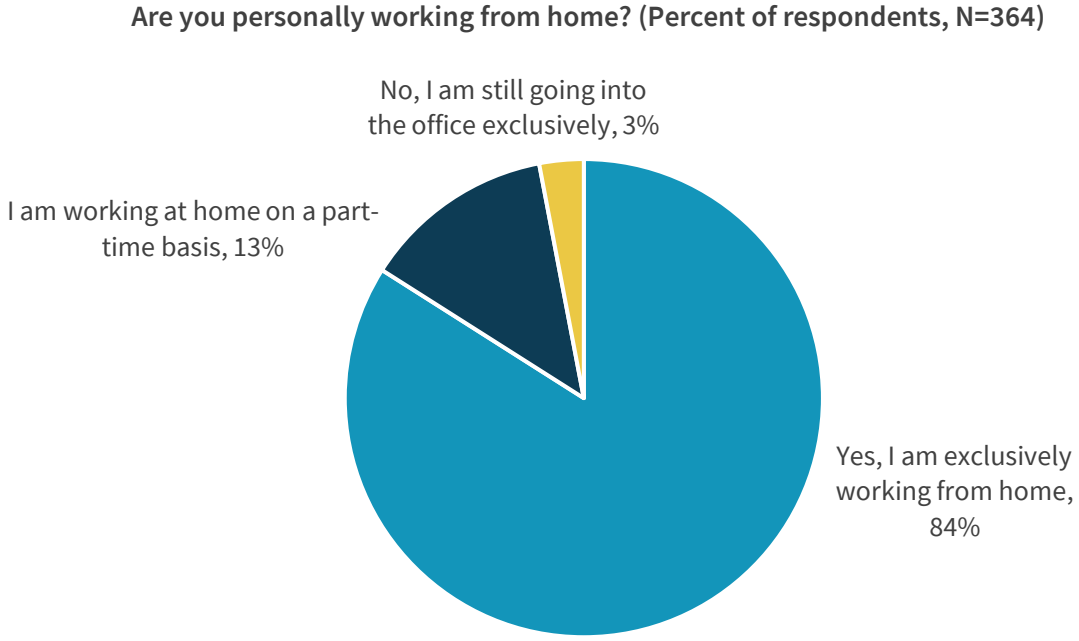
Survey participants represented a wide range of industries including information technology, financial services, government, business services and manufacturing. For more details, please see the *Research Methodology* and *Respondent Demographics* sections of this report.

Research Findings

ESG/ISSA Research Addendum: COVID-19

Like knowledge workers, most cybersecurity professionals are working from home. The highest percentage (84%) work exclusively from home while 13% do so on a part-time basis (see Figure 1).

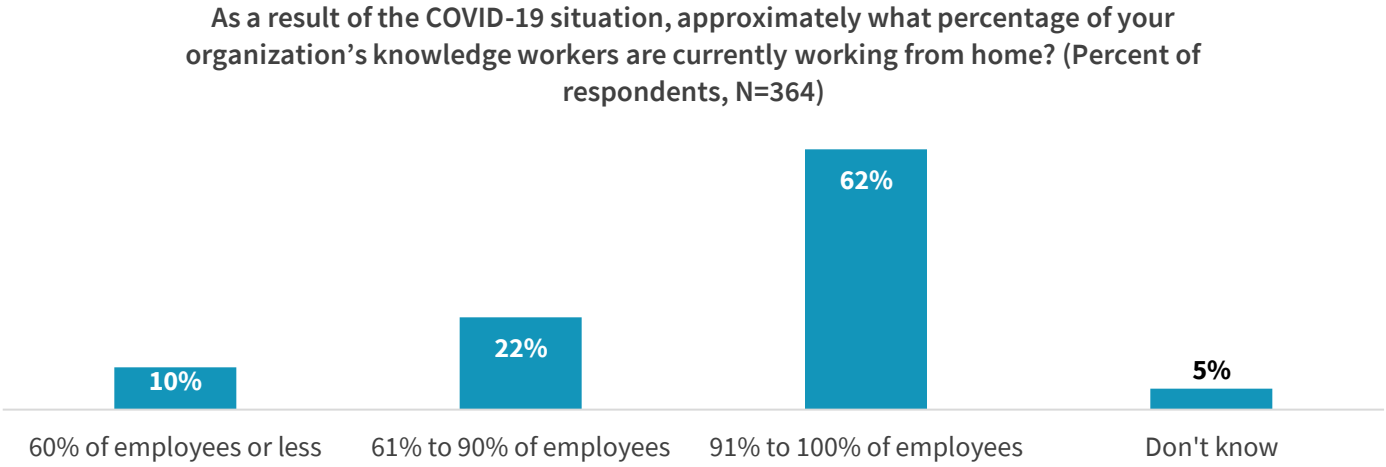
Figure 1. Cybersecurity Professionals Are Working from Home



Source: Enterprise Strategy Group

Of course, cybersecurity professionals aren't the only ones working from home—three-quarters of the cybersecurity professionals surveyed report that more than 80% of knowledge workers (defined as those with the ability to perform most or all of their job tasks from anywhere) at their organization are working remotely due to the pandemic (see Figure 2).

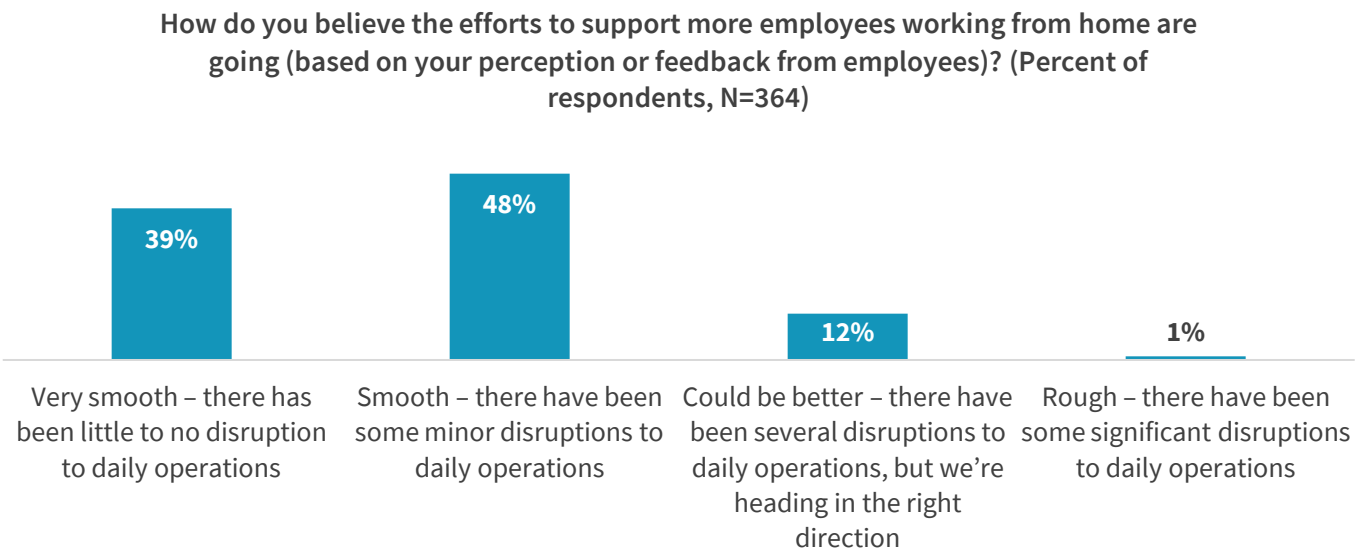
Figure 2. Percentage of WFH Workers as a Result of the Pandemic



Source: Enterprise Strategy Group

While COVID-19 has disrupted many aspects of day-to-day life, many organizations have been able to work through the unexpected new IT and cybersecurity requirements. In fact, 39% of respondents say that the effort to support a growing population of WFH employees have been very smooth with little disruption to daily operations, while another 48% claim that the transition has been smooth with only minor disruptions to daily operations (see Figure 3).

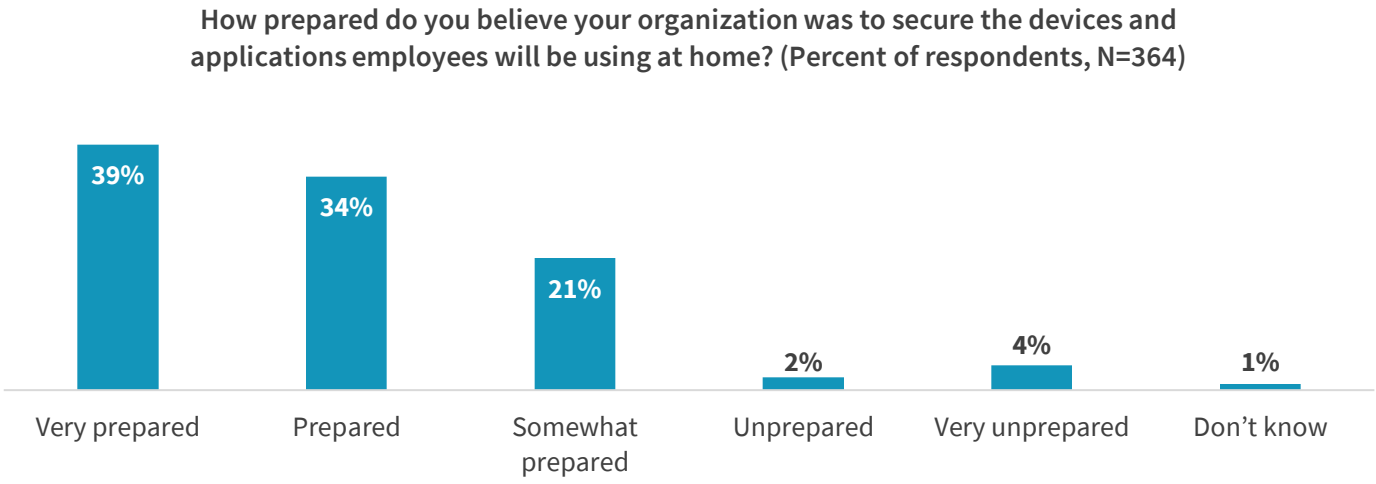
Figure 3. Rating the Efforts for WFH Support



Source: Enterprise Strategy Group

From a security perspective, cybersecurity teams have been called upon to secure devices and applications as workers migrated from corporate to home offices. Once again, cybersecurity professionals appear to be up for the task—39% of respondents claim that they were very prepared to secure WFH devices and applications while 34% were prepared for these new requirements (see Figure 4). It is worth noting, however, that 27% were underprepared (i.e., somewhat prepared, unprepared, or very unprepared). These organizations may have had smaller remote worker populations before the pandemic or had small cybersecurity staffs who were immediately overwhelmed by the urgent new security requirements of the pandemic.

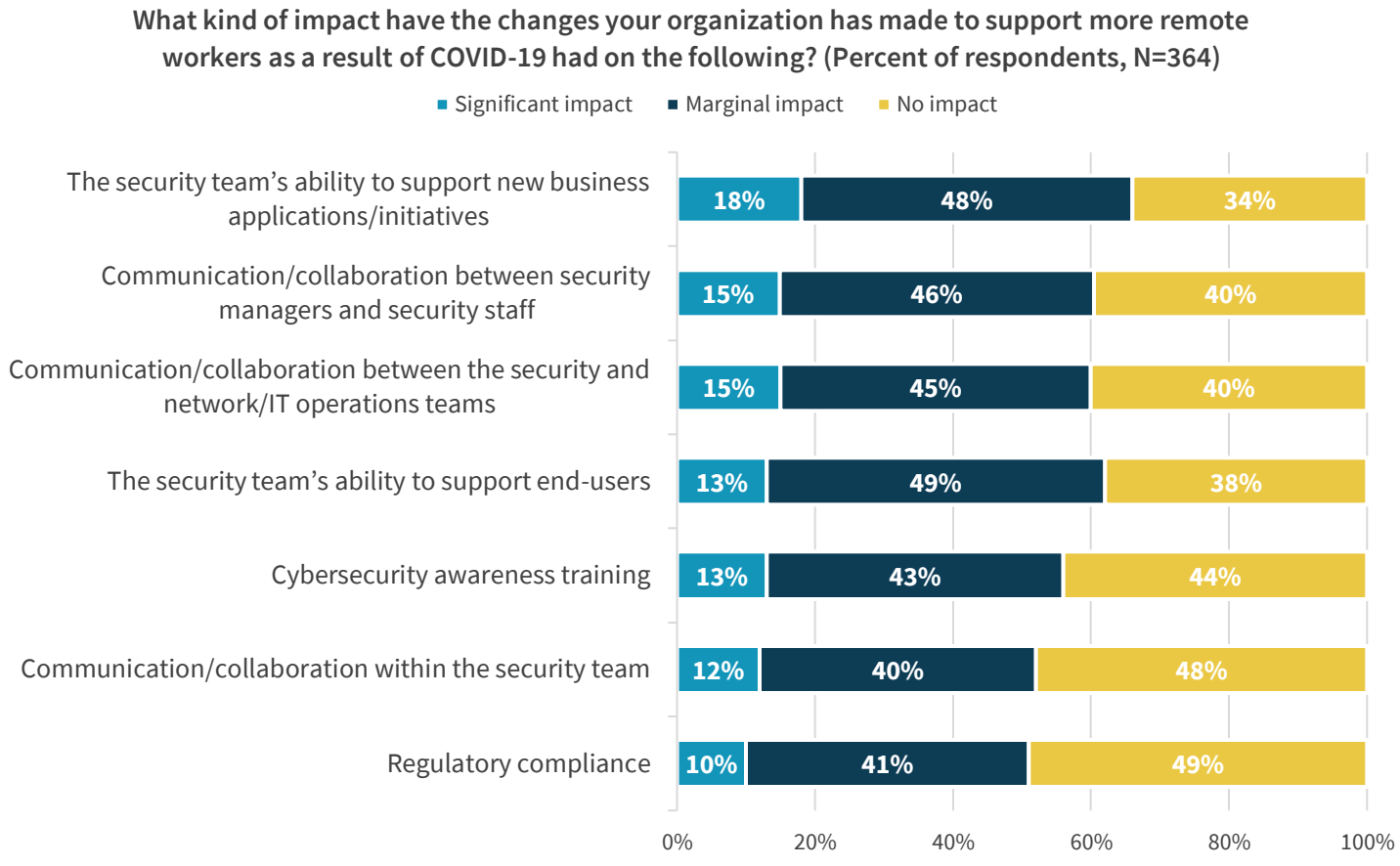
Figure 4. Rating the Efforts for WFH Support



Source: Enterprise Strategy Group

Which areas of cybersecurity have been most impacted by the pandemic? The research points to things like supporting new business applications/initiatives, communications within the security team, and communications between security and IT operations teams (see Figure 5). The large percentage of respondents selecting "no impact" is also worth noting here. While COVID-19 has disrupted just about everything in society, many organizations had cybersecurity plans in place, allowing them to adapt well.

Figure 5. Impact of COVID-19 on Cybersecurity Activities



Source: Enterprise Strategy Group

Overall, the ESG/ISSA data suggests that cybersecurity and IT teams have been able to build on their previous experience with remote worker support to scale technologies and operations. Nevertheless, rapid demands driven by COVID-19 have resulted in numerous cybersecurity challenges. According to Figure 6, topping this list are:

- Securing WFH system configurations. Twenty-seven percent say that making sure that all remote employee computing devices have been securely configured was a top challenge. This is likely because some users are sharing systems with other family members who may be playing games or running unapproved software. There also may be limited visibility into home systems.

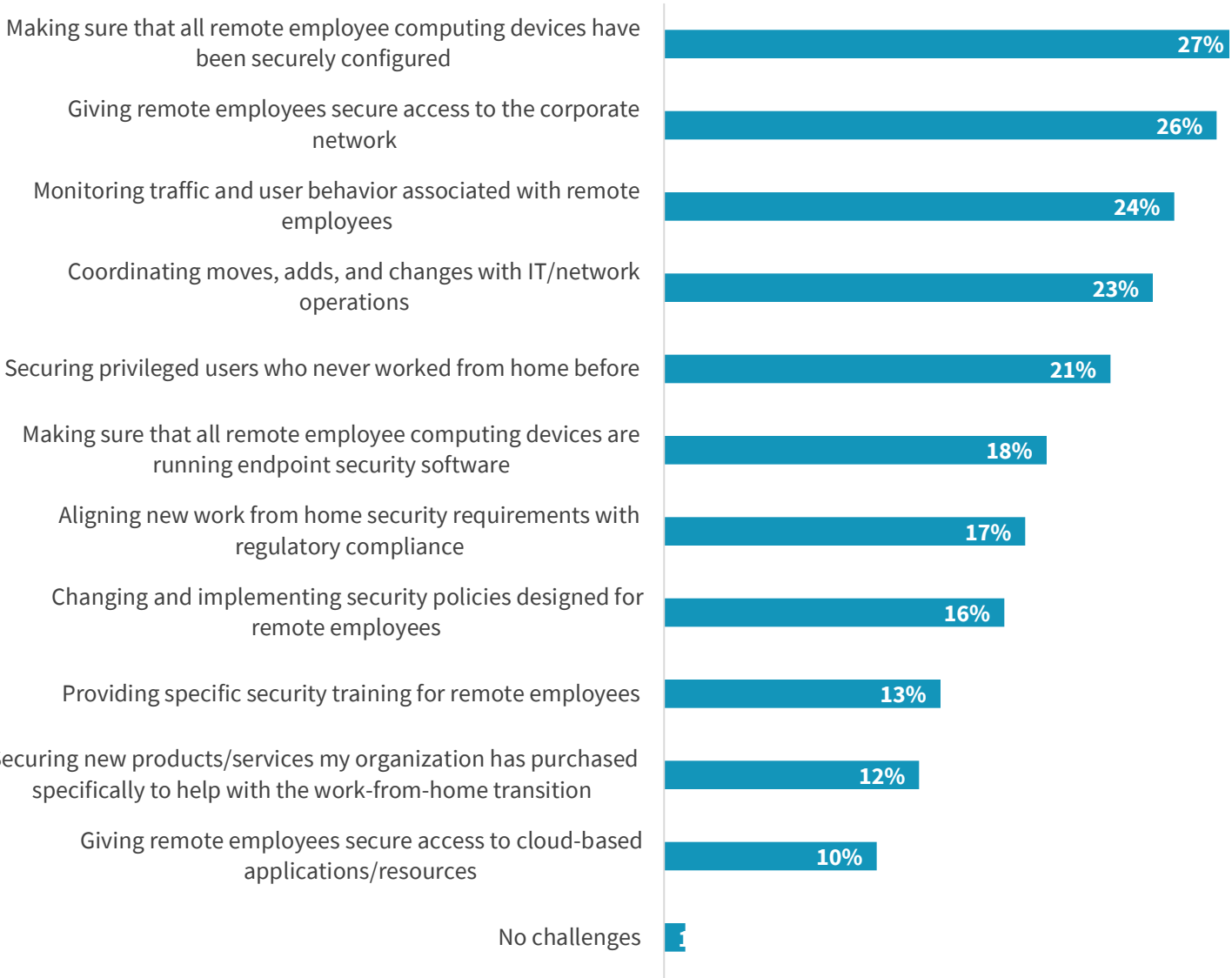
- Providing secure network access. Close behind, 26% of respondents say that giving remote employees secure access to the corporate network is a top challenge. This may be an infrastructure issue related to VPNs or related to access policies to sensitive applications and data from untrusted networks.

- Monitoring traffic. Nearly one-quarter (24%) of respondents say that monitoring traffic and user behavior associated with remote employees presents a challenge. In this case, security operations teams may lack visibility into users' direct-to-Internet behavior, or they may be struggling to scale network monitoring tools to accommodate massive growth in network ingress/egress traffic.

The list of challenges is closely clustered. This indicates that many organizations have multiple security challenges to address.

Figure 6. WFH Security Challenges

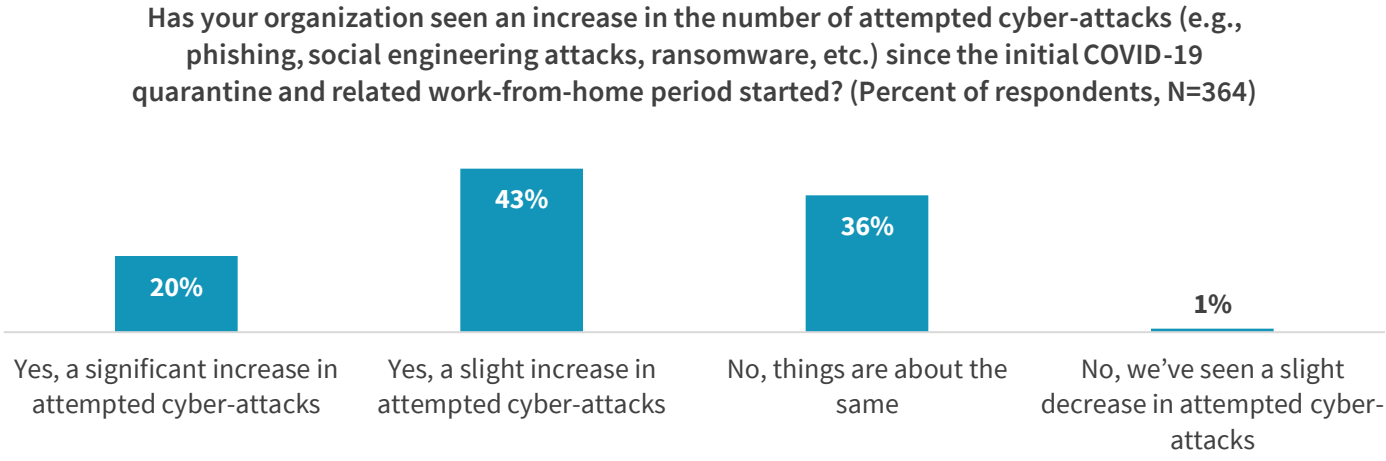
Which of the following are the most significant challenges associated with increasing the population of employees working from home at your organization? (Percent of respondents, N=364, three responses accepted)



Source: Enterprise Strategy Group

Cyber-criminals love disasters—floods, earthquakes, and wildfires represent business opportunities as concerned citizens surf the web for information or ways they can help. While most disasters are localized, COVID-19 has a global impact, making it a once-in-a-lifetime opportunity for hackers and online scammers. According to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3), cyber-attacks roughly quadrupled since the COVID-19 pandemic began. The cybersecurity professionals surveyed for this project see a similar spike in cyber-attacks related to the pandemic—20% have seen a significant increase in attempted cyber-attacks while 43% claim a slight increase in attempted cyber-attacks (see Figure 7).

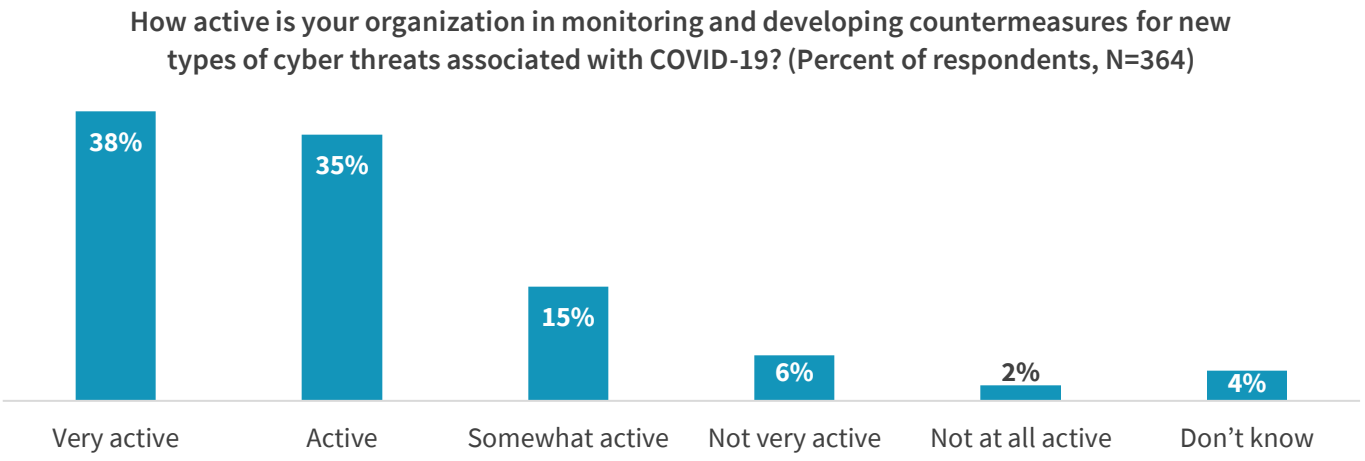
Figure 7. Attempted Cyber-attacks Related to COVID-19



Source: Enterprise Strategy Group

In response to the increasing volume of cyber-attacks, organizations are ramping up threat intelligence analysis and fine-tuning security controls. Thirty-eight percent of organizations say they are very active in monitoring and developing countermeasures for new types of cyber threats associated with COVID-19 while another 35% are active in these areas (see Figure 8).

Figure 8. Activity Around COVID-19 Cyber Threats

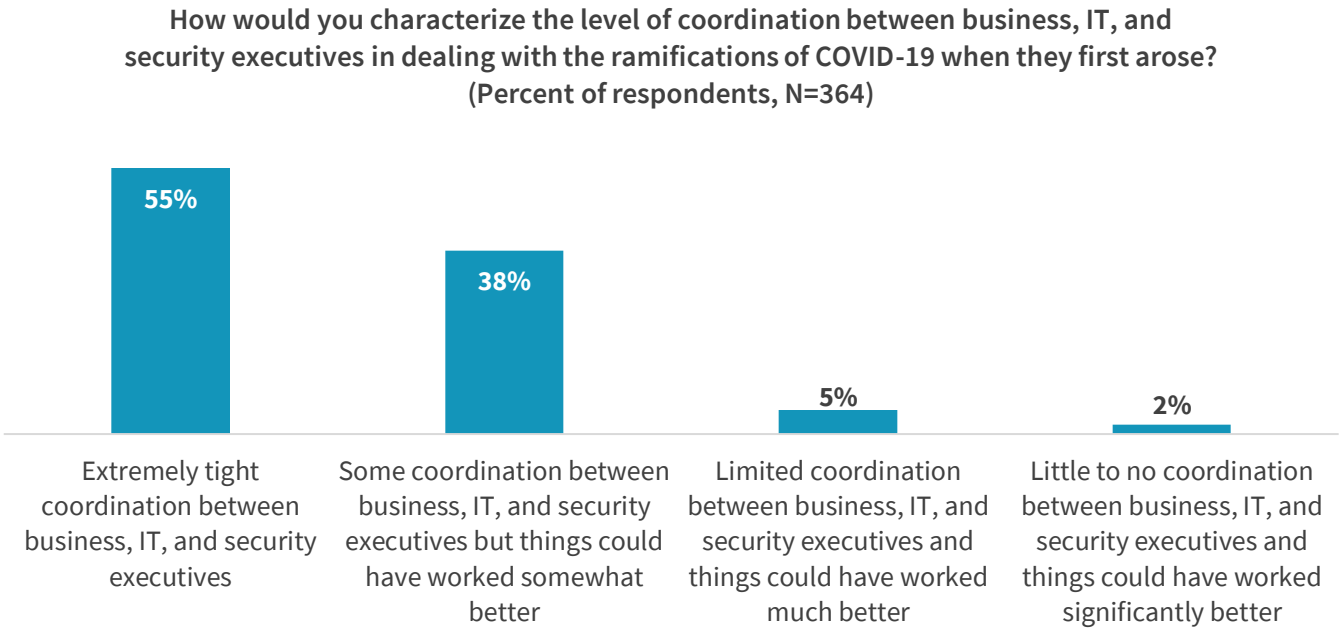


Source: Enterprise Strategy Group

COVID-19, Cybersecurity, and the Business

Responding to something as disruptive as a global pandemic requires unprecedented collaboration between business, IT, and cybersecurity teams. The good news is that many organizations have responded positively. Indeed, 55% of respondents say that the level of coordination between business, IT, and security executives in dealing with the ramifications of COVID-19 were extremely tight when they first arose (see Figure 9). While this is impressive, the level of coordination could have been better at 45% of organizations. This is not surprising, since many executives and corporate directors still don't understand the business value of cybersecurity. This value is certainly on display regarding new requirements resulting from COVID-19.

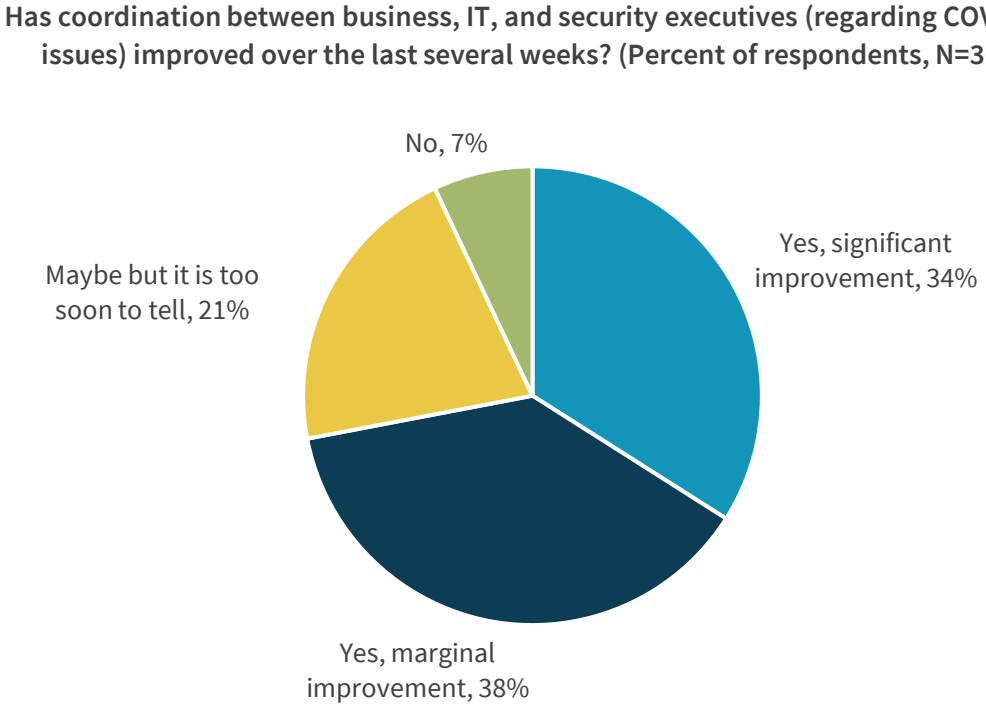
Figure 9. Level of Coordination as a Result of COVID-19



Source: Enterprise Strategy Group

While more than half of organizations had a good working relationship between business, IT, and security groups, there is always room for lessons learned and process improvement. The research indicates that just over one-third (34%) of organizations have experienced significant improvement in coordination between business, IT, and security executives as a result of COVID-19 issues, 38% have seen marginal relationship improvements, and 21% aren't convinced but hold out hope for coordination improvement (see Figure 10).

Figure 10. Coordination Improvement Due to COVID-19



Source: Enterprise Strategy Group

Given the economic realities caused by the pandemic, ESG and ISSA wondered how cybersecurity budgets would be impacted. Many organizations (41%) don't expect any changes to 2020 cybersecurity spending. Of the others, 20% believe that COVID-19 security requirements will lead to an increase in security spending in 2020 while 25% think their organizations will be forced to decrease security spending this year (see Figure 11).

As hard as it is to process, the pandemic may be in its early stages. Some public health professionals predict waves of outbreaks that may lead to further business disruption. This may be why 13% of respondents said that they don't know or it's too early to tell whether security spending would be impacted.

Figure 11. Impact of COVID-19 on Cybersecurity Spending

Source: Enterprise Strategy Group

When organizations shut down offices and asked employees to work from home, IT and cybersecurity infrastructure and priorities changed. A large WFH population also exposed or exacerbated existing underlying cybersecurity issues. After months of assessing new realities, cybersecurity professionals were asked if they expect to see any security spending increases in spending as a result of COVID-19 related business conditions (see Figure 12). At least half of the ISSA members surveyed pointed to several areas in which they expect their spending to increase, including identity and access management, endpoint security, web and email security, and data security.

The ESG/ISSA data seems to point to ongoing changes with security perimeters migrating closer to users and valuable assets wherever they are located.

Figure 12. Potential Cybersecurity Technology Spending Increases Due to COVID-19

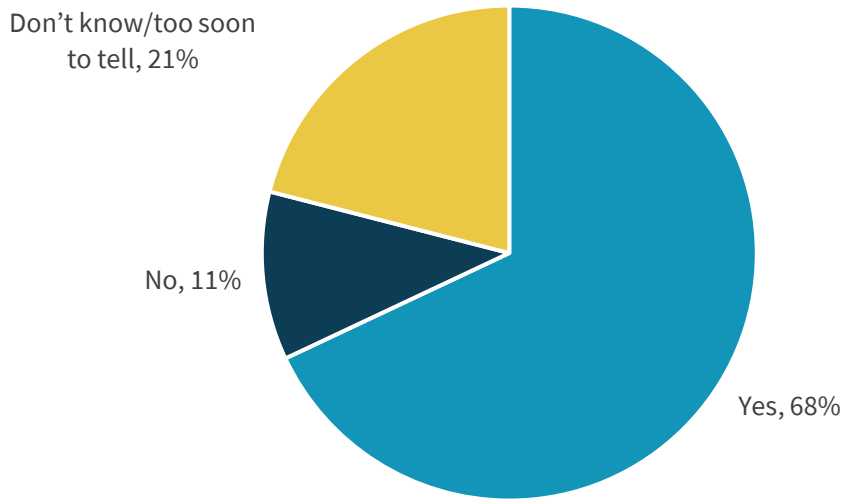
Source: Enterprise Strategy Group

The ESG/ISSA data seems to indicate that organizations are realizing that employees can maintain or even increase their productivity while working from home. This may be why 68% of respondents believe that their organizations will be more flexible with work-at-home policies once the current COVID-19 pandemic subsides (see Figure 13).

While the global pandemic will eventually wane, its impact on cybersecurity may be profound, as organizations increase WFH programs, further embrace cloud computing, and ramp up threat intelligence programs. While 68% don't anticipate a change in their organization's prioritization of cybersecurity, ESG/ISSA believe it is noteworthy that 30% of the cybersecurity professionals participating in this project say that cybersecurity will be a higher priority (see Figure 14). These organizations will likely lead the next wave of cybersecurity process innovation and best practices.

Figure 13. The Future of WFH Policies Post COVID-19

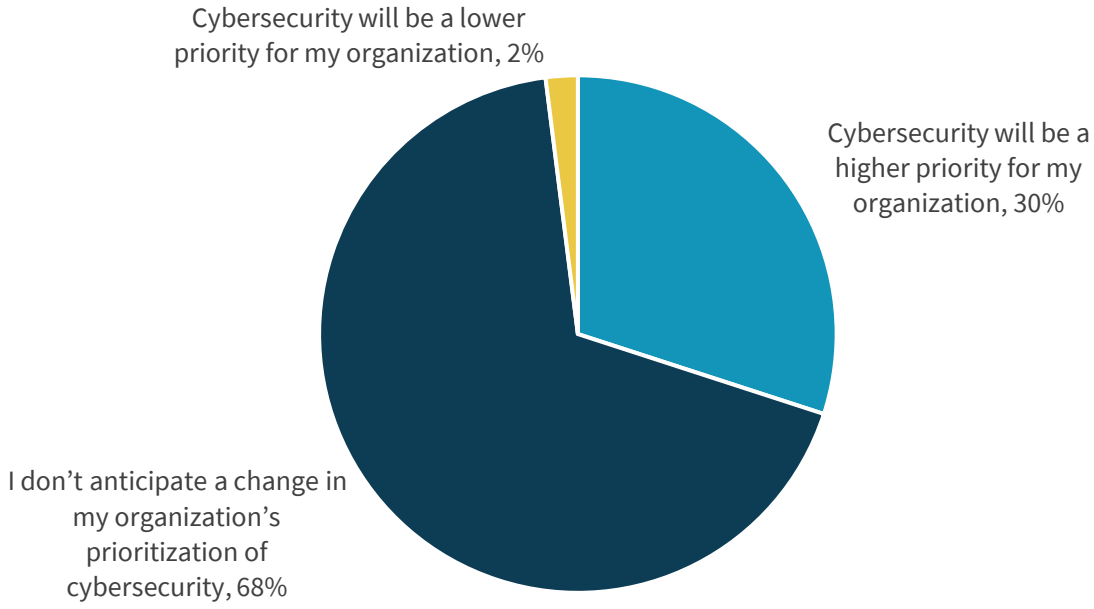
Do you think that your organization will be more flexible with work-at-home policies once the current COVID-19 pandemic subsides? (Percent of respondents, N=364)



Source: Enterprise Strategy Group

Figure 14. COVID-19 and Cybersecurity Strategy Changes

In your opinion, how will your organization's cybersecurity strategy change as a result of COVID-19? (Percent of respondents, N=364)

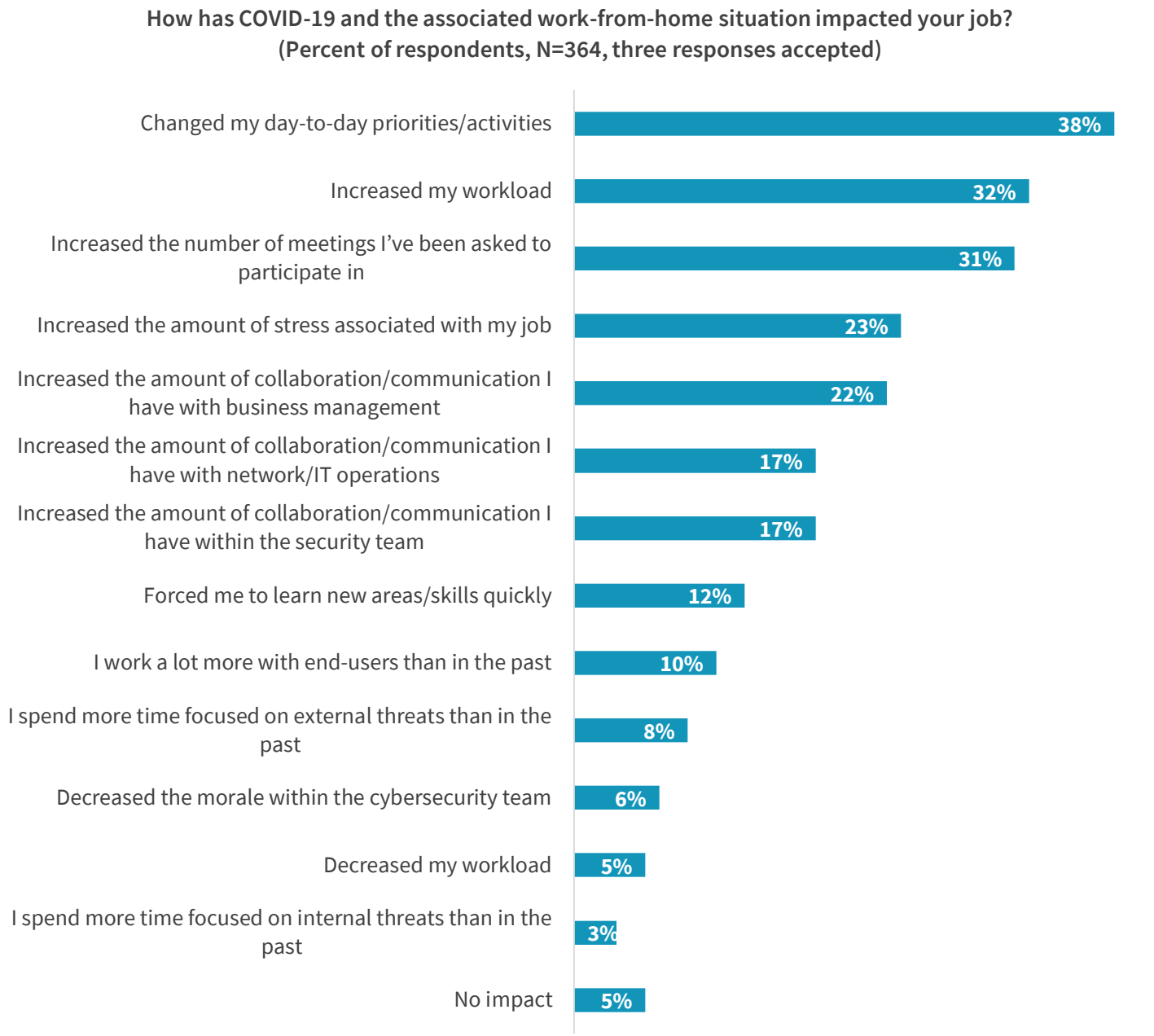


Source: Enterprise Strategy Group

COVID-19 Impact on Cybersecurity Professionals

How has COVID-19 impacted cybersecurity jobs themselves? More than one-third (38%) say it has changed day-to-day priorities/activities, 32% believe it has increased their workload, and 31% claim that it has increased the number of meetings they participate in (see Figure 15). CISOs should monitor employees for job-related tension, as 23% of respondents report that COVID-19/WFH have increased the amount of stress associated with their jobs.

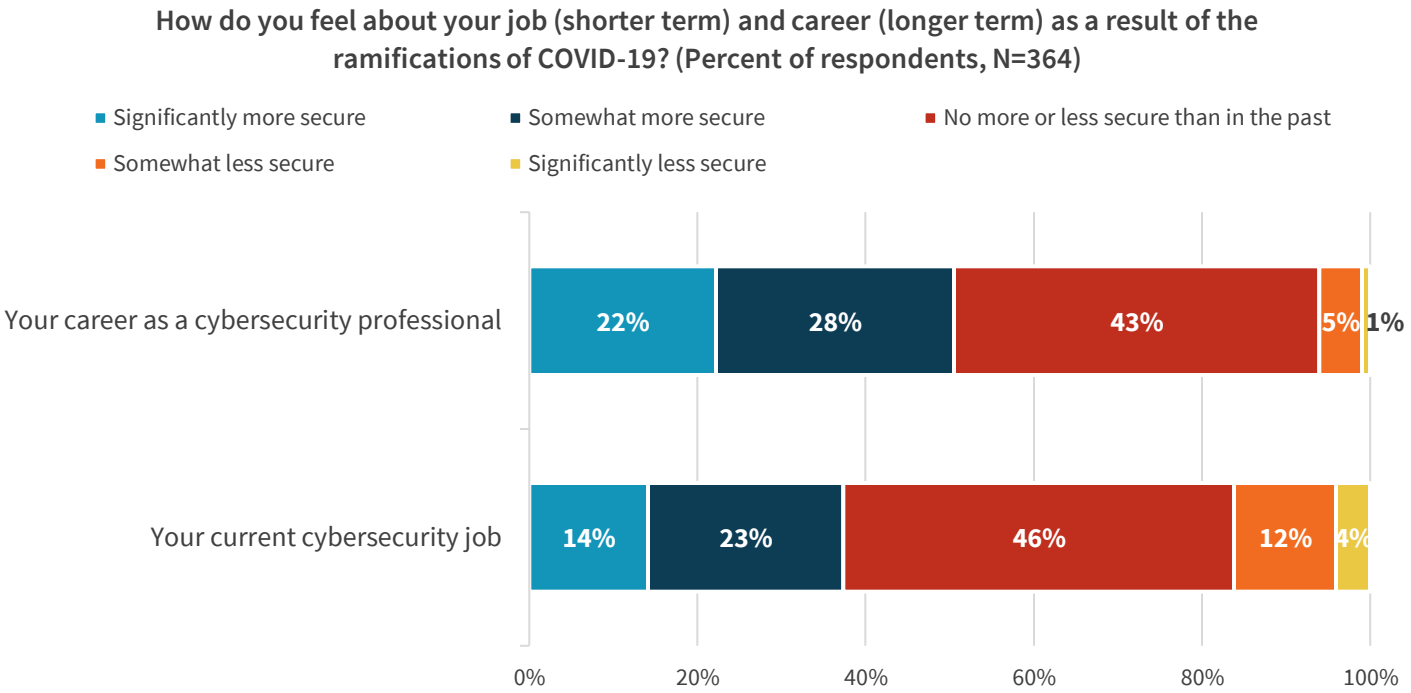
Figure 15. COVID-19 Impact on Cybersecurity Jobs



Source: Enterprise Strategy Group

Is COVID-19 causing cybersecurity professionals to be concerned about their jobs or career choice? Overall, the answer seems to be "no" to both questions (see Figure 16). It is noteworthy, however, that the data seems to indicate that there is more uncertainty about current cybersecurity jobs—16% feel somewhat less or significantly less secure about their current job while 6% feel somewhat or significantly less secure about a cybersecurity career. This illustrates short-term uncertainty—no one knows how long or devastating COVID-19 will be.

Figure 16. Cybersecurity Job and Career Security in Relation to COVID-19



Source: Enterprise Strategy Group

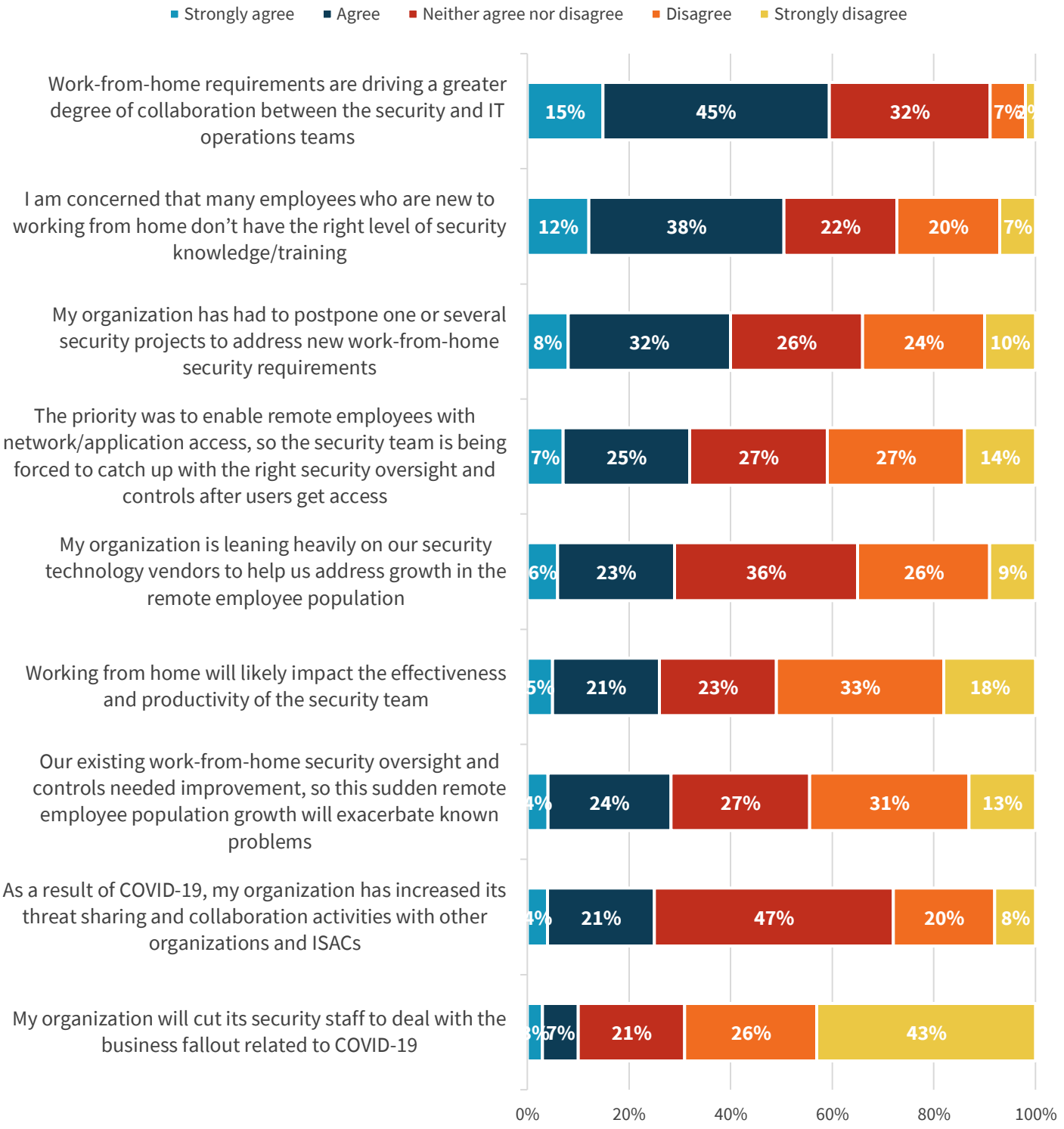
Survey respondents were presented with a series of statements and asked whether they agreed or disagreed with each (see Figure 17). The data indicates that at least half of cybersecurity professionals agree that:

- WFH is driving security and IT operations collaboration. Remote employees need connectivity, device security, and policy management oversight. These requirements are driving greater communications and coordination between security and IT teams.
- Some employees don't have the right level of security knowledge/training for WFH. With spikes in cyber-attacks like online scams and phishing emails, security awareness training becomes even more important. CISOs should reassess how employees are trained and whether current methodologies are appropriate for a remote workforce.

It is also noteworthy that 40% of ISSA members say that their organization has had to postpone security projects to address WFH requirements. These are likely multi-phased projects that require a lot of face-to-face meetings and coordination.

Figure 17. Cybersecurity Professionals' Opinions on COVID-19

Please rate your personal level of agreement with each of the following statements pertaining to some of the cybersecurity implications of the current work-from-home situation. (Percent of respondents, N=364)



Source: Enterprise Strategy Group

Conclusion

Although no one was planning for a global pandemic, many organizations had the work-from-home infrastructure in place to support the necessary changes. The main issue they faced centered around scaling technology infrastructure as quickly as possible. From a security perspective, organizations are experiencing a spike in cyber threats, driven by COVID-19 scams and a related increase in cybercrime. To address this increase, organizations must bolster their capabilities to analyze and operationalize cyber threat intelligence (CTI).

Cybersecurity processes and personnel are being pressure-tested as well. WFH initiatives demand tighter coordination between security and IT operations teams, and since it's unclear how long the pandemic will last, organizations should closely monitor and manage this relationship accordingly. At an individual level, an already overwhelmed cybersecurity staff is being asked to do even more. COVID-19 and WFH have changed security professionals' priorities, increased workload, and changed their internal communication habits, and these valiant efforts must be monitored to maintain team morale and, ultimately, a strong and consistent approach to security.

Cybersecurity spending may be in play, and while many organizations don't expect changes to their security budgets, they will likely change priorities. The research points to growing investments in areas like identity and access management, endpoint security, and web/email security. WFH appears to be the new normal, with most cybersecurity professionals expecting that their organizations will be more flexible about WFH after the pandemic. Given this, cybersecurity professionals should be ready to distribute security controls, modify policies, and ramp up security data collection, processing, and analytics.

Takeaways for Cybersecurity Professionals

The pandemic caused rapid changes that aren't going away anytime soon and may define the new normal. Accordingly, cybersecurity professionals should:

1. Adjust processes and communications spanning across security and IT departments.
2. Monitor their workloads and seek help when needed.
3. Fine-tune access and usage policies.
4. Prepare for new volumes and types of cyber threats.
5. Get ready for the new normal by moving security controls closer to assets like users, devices, and cloud-based workloads. This must be accompanied with an integrated architecture and central management.

Takeaways for CISOs and Organizations

While many organizations are weathering the storm, there's still work ahead. CISOs should:

1. Evaluate how well the security team responded to WFH demands. Find and fix any bottlenecks. Update the business continuity plan (BCP) and disaster recovery plan (DRP) to include new protocols and lessons learned.
2. Build policies for WFH, business enablement, and strong security.
3. Work with CIOs to unify security and IT operations teams. This may include organizational changes, compensation adjustments, and new metrics.

4. Monitor the workload and mental health of the cybersecurity team.

5. Assign a security engineering team to design a flexible but strong security architecture that supports a distributed remote workforce and the associated business processes.

Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of security and IT professionals from the ISSA member list (and beyond) in North America, Europe, Central/South America, Africa, and Asia (including Australia) between April 29, 2020 and May 14, 2020. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, we were left with a final total sample of 364 security and IT professionals.

Please see the *Respondent Demographics* section of this report for more information on these respondents.

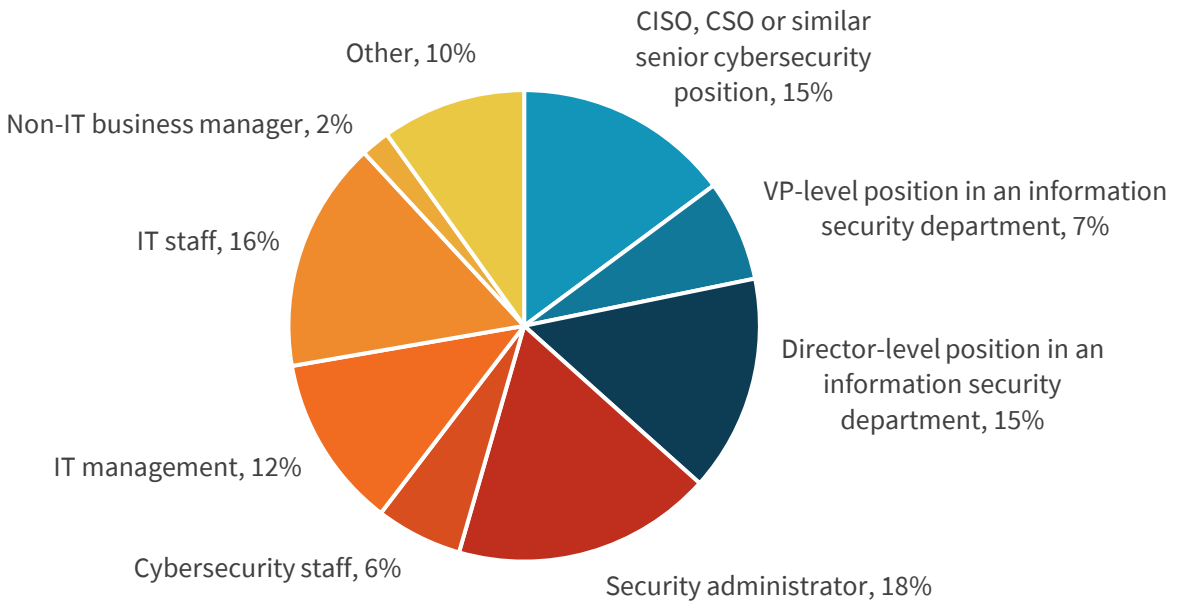
Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Respondent Demographics

The data presented in this report is based on a survey of 364 qualified respondents. Figure 18 through Figure 23 detail the demographics of the respondent base at an individual and organizational level.

Figure 18. Respondents by Current Position

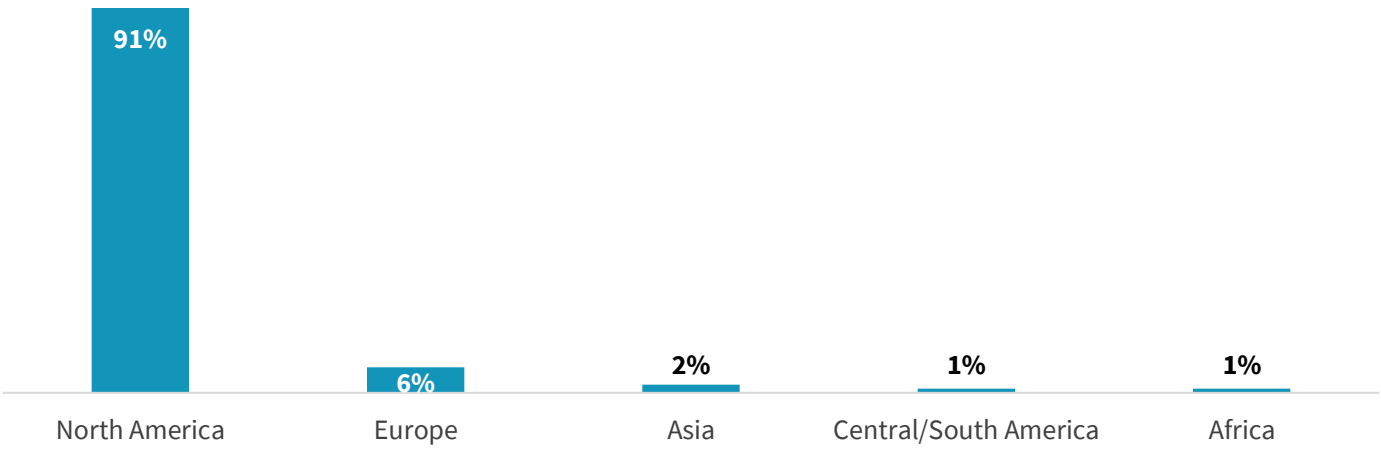
Which of the following best describes your current position within your organization? (Percent of respondents, N=364)



Source: Enterprise Strategy Group

Figure 19. Respondents by Region

Please indicate where you are based (i.e., where you live and work). (Percent of respondents, N=364)

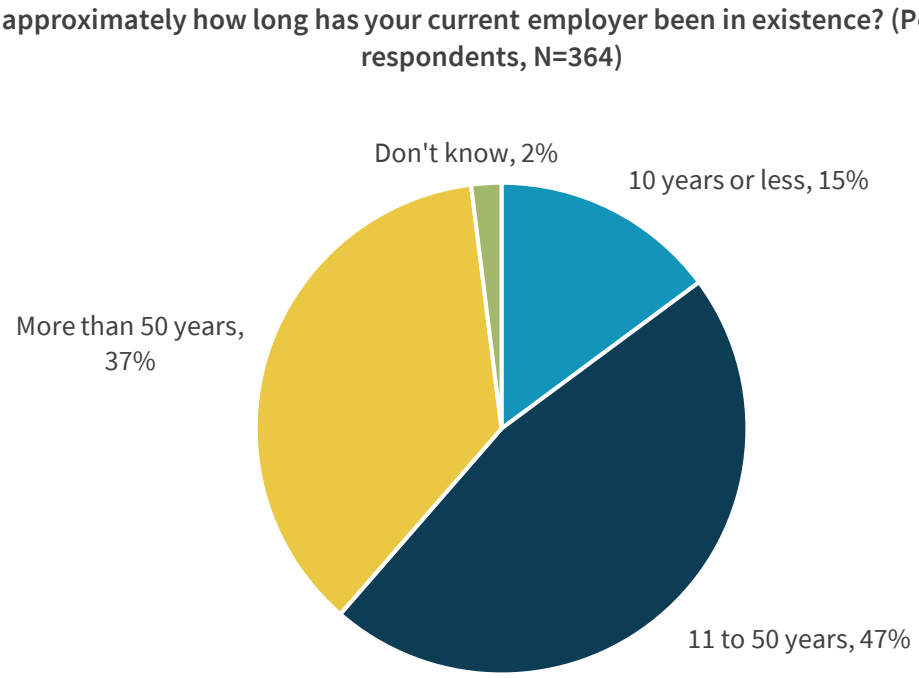


Source: Enterprise Strategy Group

Figure 20. Respondents by Number of Employees

Source: Enterprise Strategy Group

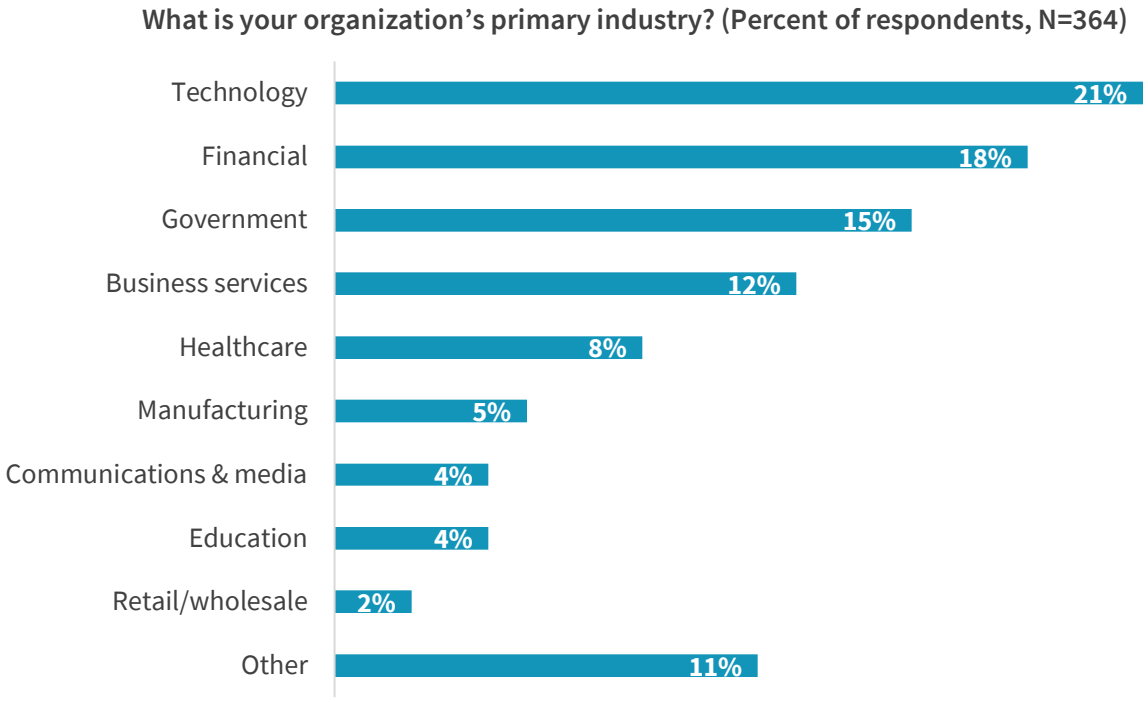
Figure 21. Respondents by Age of Organization



Source: Enterprise Strategy Group

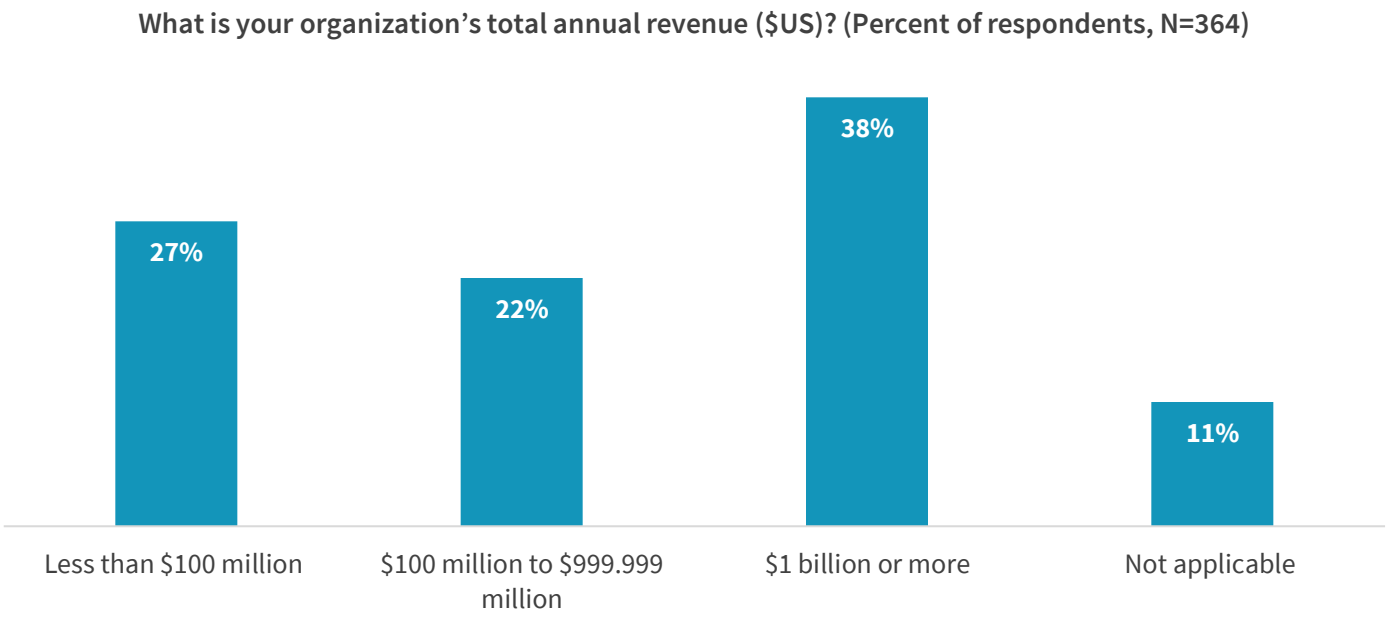
Respondents were asked to identify their organization's primary industry. In total, ESG received completed, qualified responses from individuals in 19 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Error! Reference source not found.

Figure 22. Respondents by Industry



Source: Enterprise Strategy Group

Figure 23. Respondents by Annual Revenue



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