Ponemon INSTITUTE

The Impact of the New Normal on Workplace Privacy: A Study of Business & IT and IT Security Managers

Sponsored by 3M

Independently conducted by Ponemon Institute LLC

Publication Date: June 2021

The statements, information, views, and opinions expressed in this report are those of the persons being interviewed by the Ponemon Institute and do not necessarily reflect 3M's factual understanding or its views or opinions. While this report was sponsored by 3M, 3M did not participate in the interviews, the preparation for the interviews or the gathering of responses of those being interviewed. The report is intended for occupational use by persons with the knowledge and technical skills to use such information. It is supplemental only and is not intended to replace any detailed information about 3M products that can be found in written 3M Product Literature.

Ponemon INSTITUTE

The Impact of the New Normal on Workplace Privacy: A Study of Business and IT and IT Security Managers

Presented by Ponemon Institute, June 2021

Part 1. Introduction

The significant increase in remote working due to COVID-19 has forever changed the workplace and has been called by many the "new normal". The purpose of this research is to understand the privacy trends and challenges from the perspective of the following individuals due to a significant number of their organization's employees working outside the office:

- IT and IT security managers
- Business managers

Sponsored by 3M, Ponemon Institute surveyed 564 IT and IT security managers and 617 business managers in the United States. All participants in this research work in organizations that required employees to work from home due to COVID-19.

All IT and IT security managers are involved in the evaluation, selection and/or implementation of IT hardware and software products or services in their organization. The majority of these respondents belong to ISACA (55 percent), (ISC)2 (51 percent) and ISSA (51 percent).

In the context of this research, working remotely is the ability for an organization's employees and other users to perform work from locations other than its facilities. Remote workers use various devices such as desktop and laptop computers, smartphones and tablets to read and send email access websites, share documents and perform many other tasks. These devices may be controlled by the organization, third parties or by the users themselves (BYOD). Most of these workers use remote access, which is the ability for an organization's users to access its non-public computing resources from external locations other than the organization's facilities.

Following are the key takeaways from the IT and IT security manager survey.

- Coffee shops and shared workspaces are the new "offices" for many remote workers, which is putting sensitive and confidential information at risk. The average percentage of employees working remotely has more than doubled since COVID-19 from an average of 24 percent to 65 percent.

- To accommodate remote workers, organizations are supplying them with smartphones and tablets. Because of the increase in online conferences, remote workers are mostly requesting headsets and webcams.

- Remote working is a "pain in the neck". Sixty-four percent of respondents say the time employees spend on their devices has significantly increased (34 percent) or increased (30 percent). The biggest complaints from employees are chronic neck and back pain and headaches.

- In a remote working environment, organizations are losing control over the security of sensitive and confidential information. Sixty-five percent of respondents say it is easier to protect data when employees are working in the office.

- Remote workers' exposure of sensitive information on their screens is a significant concern. Sixty-four percent of IT and IT security managers say they are very concerned that prying eyes will see the sensitive information on remote workers' screens. These respondents say

their organizations conduct training and awareness programs that cover the remote worker risk (51 percent) and institute new mobile device policies (41 percent). Only 40 percent of respondents say their organizations require employees' home workspace to be private and not allow others to be near the device.

- The importance of password hygiene is most often communicated to remote workers. Sixty-seven percent of respondents say their organizations have a policy on IT device privacy and security requirements for remote workers. Of these respondents, 59 percent of respondents say their organizations' policy focuses on the importance of password hygiene and 58 percent of respondents say it explains what constitutes suspicious emails and how to handle them.

- The biggest privacy and security concerns are the inability to secure communications on external networks outside their organization's control (67 percent of respondents) and the difficulty in securing external access to internal-only resources (50 percent of respondents).

- To address privacy and security concerns, organizations protect company-owned devices with up-to-date antivirus, device encryption and firewalls (51 percent of respondents) and encrypt sensitive data stored on devices (50 percent of respondents).

- Monitoring the network 24/7 and encryption of sensitive data stored on devices are the primary steps taken to create a secure remote working environment, according to 56 percent and 51 percent of respondents, respectively.

- The top five technologies used to improve the organization's privacy and security posture are incident response platforms (62 percent of respondents), anti-virus/anti-malware (59 percent of respondents), big data analytics for cybersecurity (56 percent of respondents), identity management & authentication (53 percent of respondents) and intrusion detection & prevention systems (51 percent of respondents).

- Technology investment decisions go virtual. Sixty-three percent of IT and IT security managers say it has become more difficult to make decisions about investments in technology solutions since COVID-19. Sixty-five percent of respondents say they are more dependent on virtual events.

- To make investment decisions, respondents are mainly dependent upon peers or co-workers (54 percent of respondents) or industry websites (51 percent of respondents). In the next year, respondents predict they will purchase software (67 percent of respondents), laptop/tablets (65 percent of respondents) and cell phones (61 percent of respondents).

- Post COVID-19, the physical workspace will be transformed. More precautions will be taken to protect the health and safety of employees (66 percent of respondents) and there will be more distance between employees (58 percent of respondents). Respondents predict that an average of 45 percent of their employees will return to the office and an average of 47 percent will work both remotely and in the office.

Following are the key takeaways from the survey of business managers

- Most business managers say they do not work exclusively in their home. As discussed previously, IT and IT security managers say that an average of 40 percent of their organizations' remote workforce spends time in coffee shops and shared workspaces where it is not easy to keep information safe from prying eyes. Seventy-seven percent of remote workers say they spend at least a portion of their time working outside their homes. Only 23 percent of business managers say they work remotely from home exclusively.

- Not only are business managers working in shared workspaces, but they also cannot keep others from seeing their work. Only 34 percent of respondents say where they work at home makes it possible for them to prevent others, including family members or roommates from seeing their work.

- Only 43 percent of respondents say they are concerned when displaying sensitive or confidential information on their screen when working remotely, either in the home or somewhere else. Only 40 percent of respondents say their organization has increased its privacy policies since more employees are working remotely.

- Working from home is not secure. Only 34 percent of respondents say where they work at home **makes it possible for them to protect others from seeing their work.** Fifty-six percent of respondents say they have a home office. However, many are working in the kitchen (53 percent of respondents) and such common areas as the family room, living room or TV room (43 percent of respondents).

- Another privacy and security threat is not being proactive in protecting information. Fifty-five percent of business managers do not take steps to prevent others from viewing their screens. If they do, 67 percent of these respondents turn the screen and 54 percent of respondents say they leave the room with their devices.

- A remote workforce is experiencing health issues. Respondents report that on average they are spending 44 percent more time in front of their device screen. As a result, many are experiencing chronic neck and back pain (62 percent of respondents) and headaches (54 percent of respondents. Of the 75 percent of respondents who say their health has been affected, 42 percent say they are taking regular walks and 36 percent say they started setting an alarm to end screen time.

- Laptops or notebook computers are most often used for remote working. Most respondents use company-provided devices (45 percent) or combinations of personal and company-provided devices (22 percent). However, one-third of respondents say they are using their own personal devices when working remotely.

- Remote workers would like to return to the office. While 49 percent of respondents say their employers will expect them to stay working remotely, 47 percent would like to return to the office.

- Most respondents will be comfortable traveling on business post-COVID-19. Before COVID-19, 51 percent of respondents say they very often traveled on business. Fifty-seven percent of respondents say they will be very comfortable traveling once again. Of the 43 percent of respondents who say they are not comfortable, it is because of the unpleasantness of wearing a mask, the possible of a mandate requiring vaccinations and the concern about becoming ill.

Part 2. Key findings from the IT and IT security manager survey

In this section, we provide an analysis of the IT and IT security manager findings. Part 3 of the report features the findings from the business manager survey. The complete audited findings are presented in the Appendix of this report.

Following are the IT and IT security manager topics:

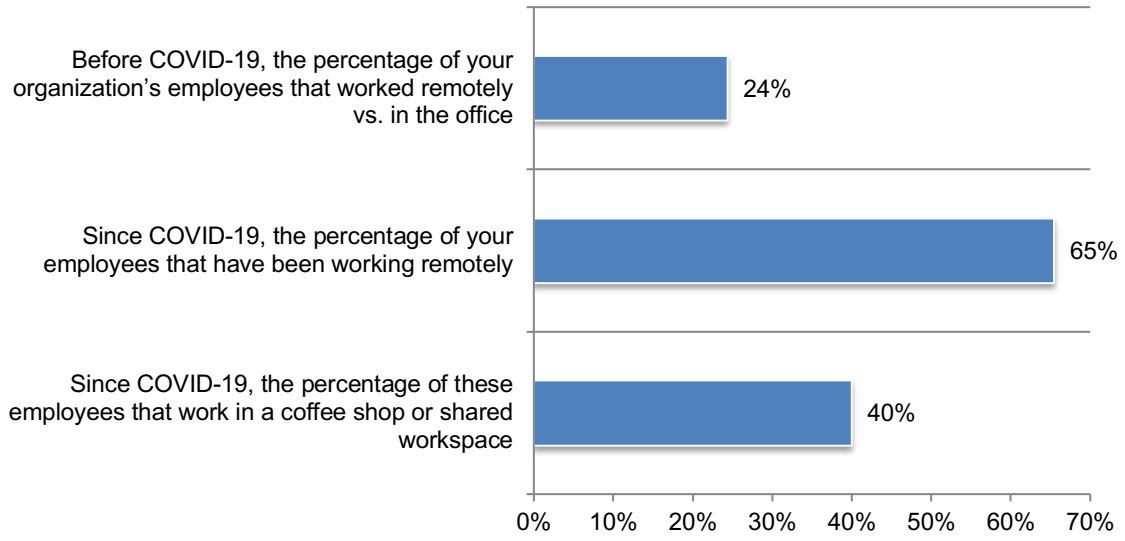
- Shifting to a "new normal"
- Privacy and security risks in the "new normal"
- Purchasing technology for a remote workforce
- Predicting a post-COVID-19

Shifting to a "new normal"

Privacy risks have increased significantly because many remote workers are now working in a coffee shop or shared workspace. Sixty-five percent of respondents say it is easier to protect their organizations' sensitive and confidential information when employees are working in the office.

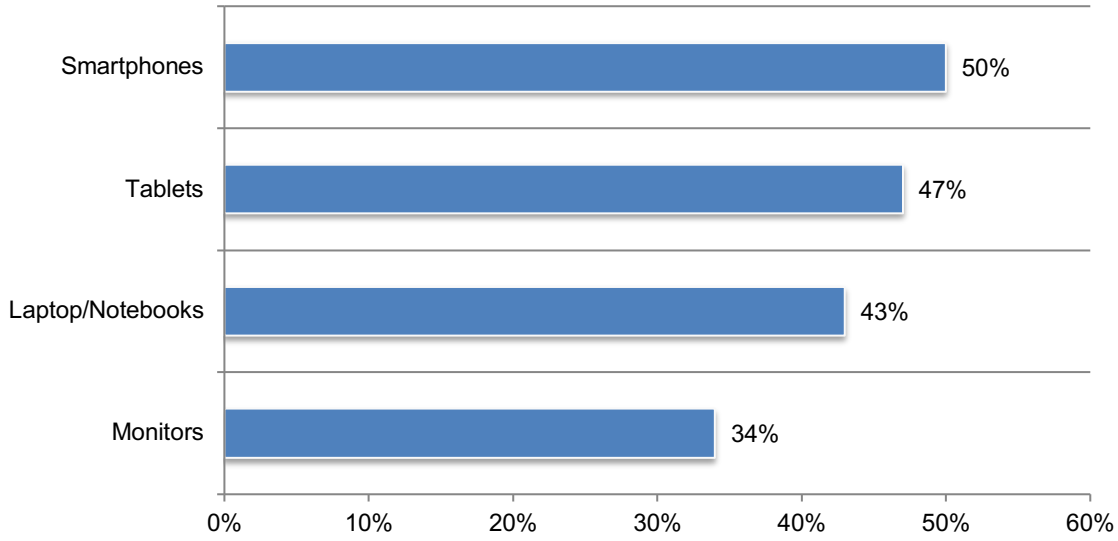
However, as shown in Figure 1. the average percentage of employees working remotely has more than doubled due to COVID-19. On average, 40 percent of the remote workforce are putting their organizations at risk by doing their work in a coffee shop or shared workspace.

Figure 1. Changes in the workplace due to COVID-19
Extrapolated values presented



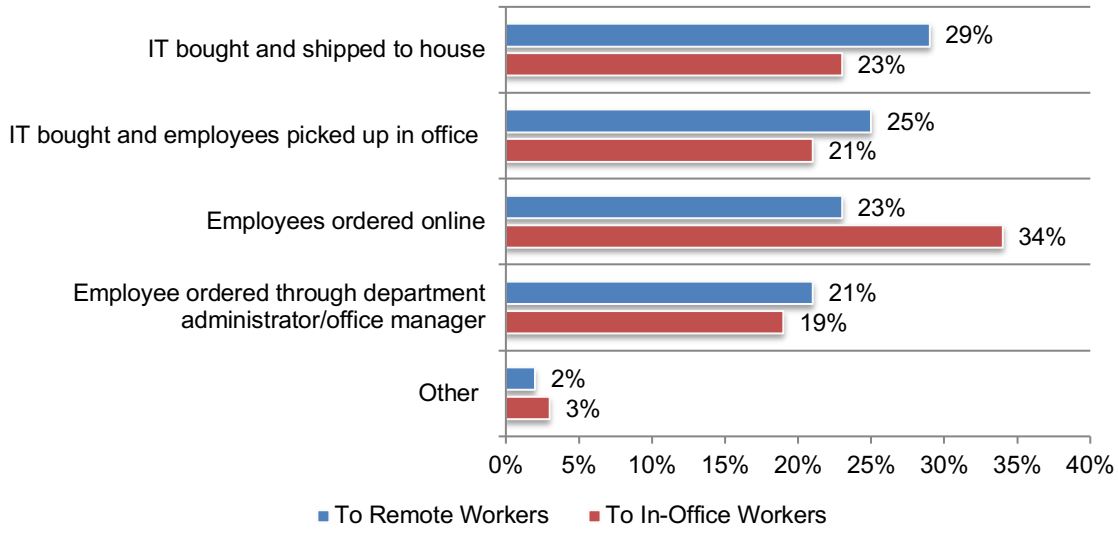
Organizations have increased the deployment of smartphones and tablets to remote workers during COVID-19. According to Figure 2, 50 percent of IT and IT security managers say their organization has increased the deployment of smartphones and 47 percent of these respondents say their organizations has increased the deployment of tablets.

Figure 2. What devices are more often provided to accommodate employees working remotely due to COVID-19?
Deployed more frequently responses presented



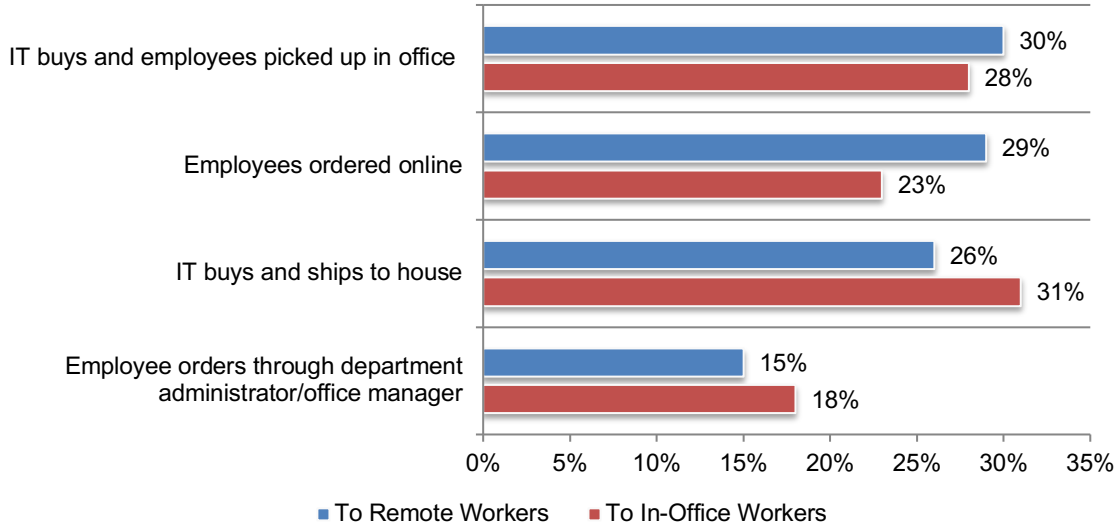
Prior to COVID-19 how were IT accessories distributed to a remote workforce? As shown in Figure 3, prior to COVID-19 most remote workers had their IT accessories shipped to their home after the organization purchased them (29 percent of respondents) and in-house workers ordered what they needed online (34 percent of respondents).

Figure 3. How were IT accessories distributed to the workforce prior to COVID-19?



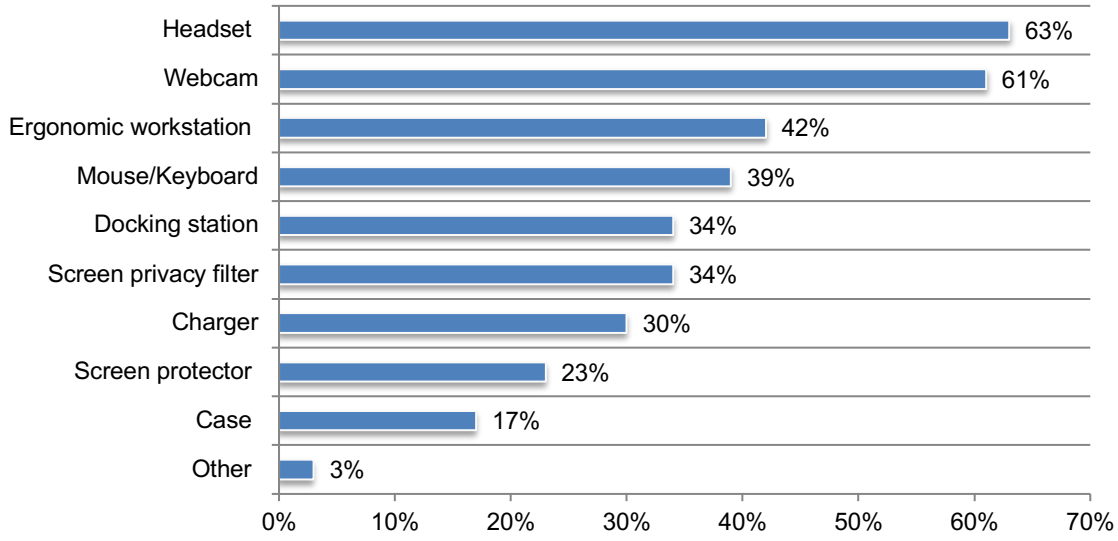
Since COVID-19, IT accessories are picked up at the office by remote workers (30 percent of respondents) or ordered online (29 percent of respondents). In-office workers are buying and having the accessories shipped to the house (31 percent of respondents) or they pick up the accessories at the office (28 percent of respondents), as shown in Figure 4.

Figure 4. Since COVID-19 how are IT accessories distributed?



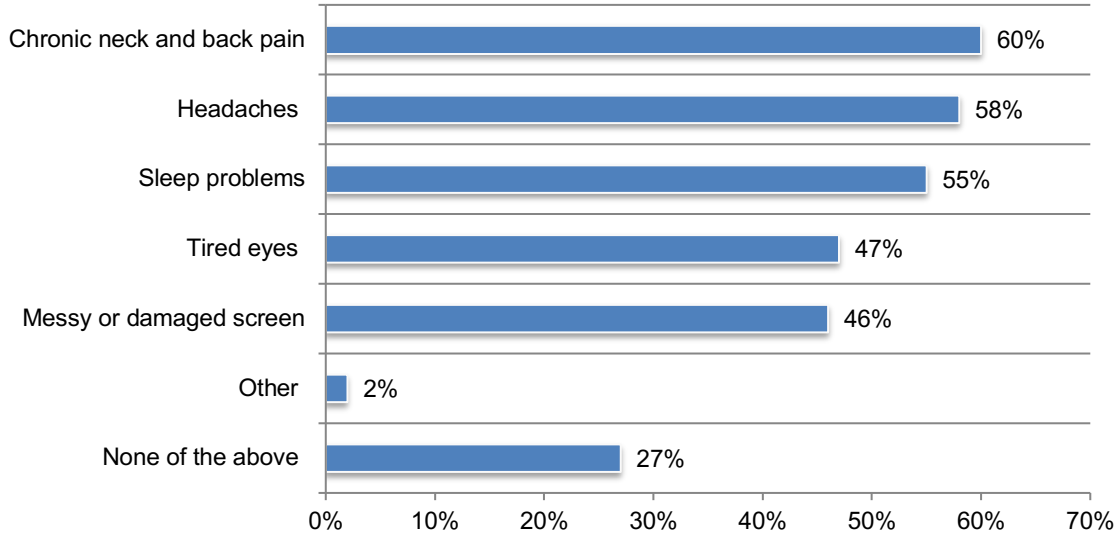
The increase in online meetings makes webcams and headsets the most popular IT accessories. As shown in Figure 5, the most popular accessories are headsets (63 percent of respondents) and webcams (61 percent of respondents).

Figure 5. Since COVID-19 what accessories have been most requested?
More than one response permitted



Remote workers are spending more time on their devices and, as a consequence, have a variety of health issues. Sixty-four percent of respondents say the time employees spend on their devices has significantly increased (34 percent) or increased (30 percent). As shown in Figure 6, the biggest complaints from employees are chronic neck and back pain (60 percent of respondents), headaches (58 percent of respondents) and sleep problems (55 percent of respondents).

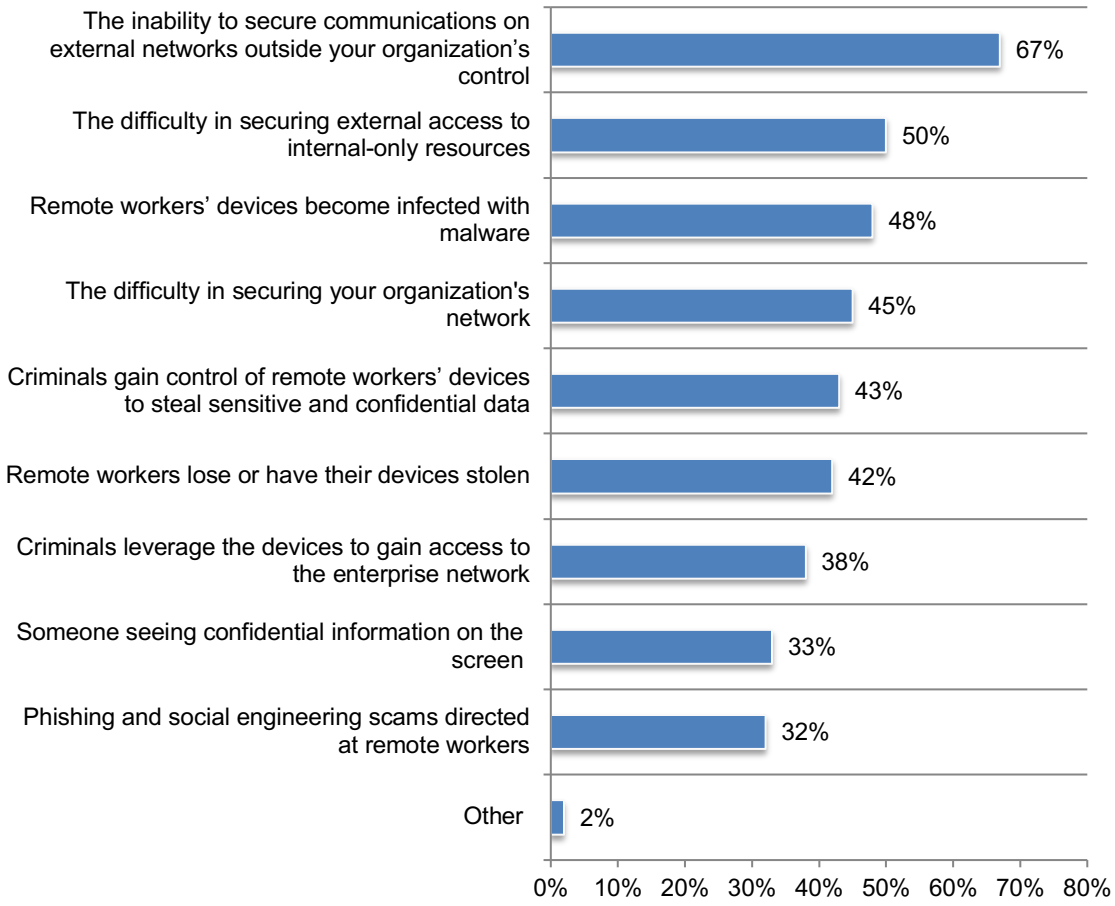
Figure 6. Remote working and the health consequences
More than one response permitted



Privacy and security risks in the "new normal"

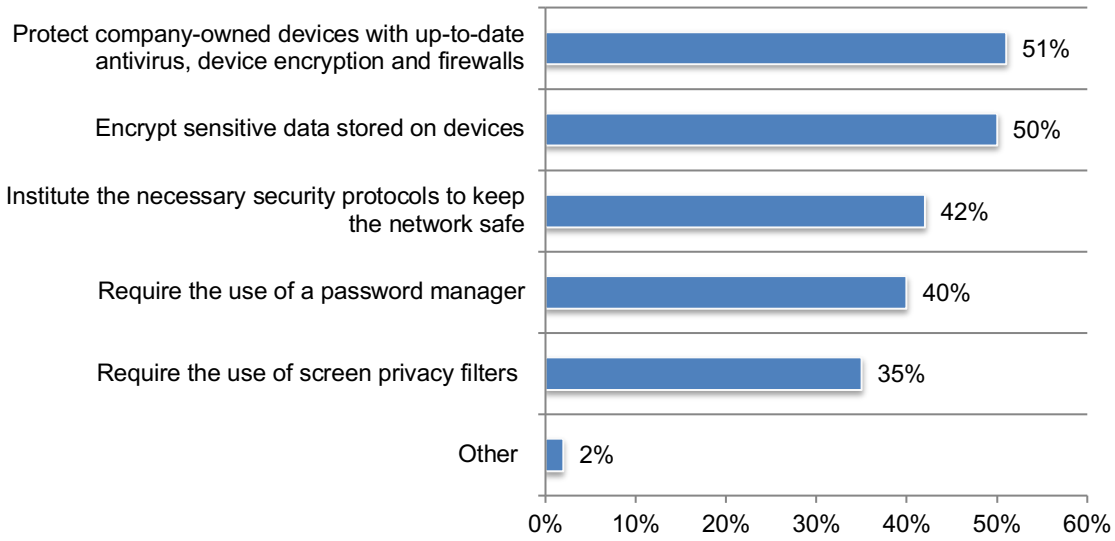
Remote working presents new security and privacy risks for organizations. The biggest concern in a remote workforce environment is the inability to secure communications on external networks outside their organization's controls, according to 67 percent of respondents as shown in Figure 7. This is followed by 50 percent of respondents who say it is the difficulty in securing external access to internal-only resources.

Figure 7. What are the privacy and security risks caused by remote workers your organization is most concerned about?
More than one response permitted



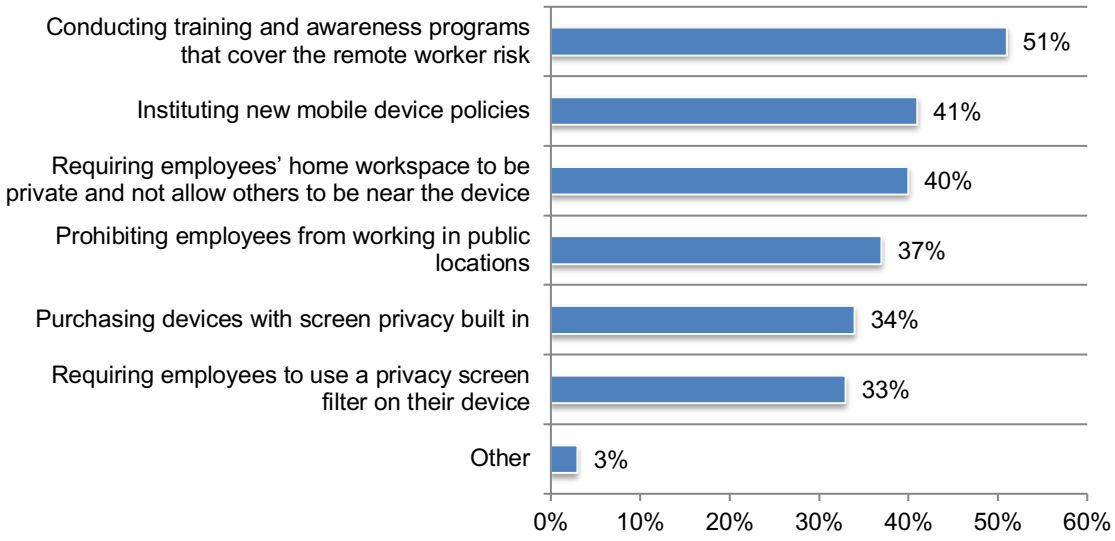
More than half (51 percent) of respondents say their organizations protect company-owned devices with up-to-date antivirus, device encryption and firewalls, as shown in Figure 8. This is followed by 50 percent of respondents who say their organizations encrypt sensitive data stored on devices.

Figure 8. How does your organization address these concerns?
More than one response permitted



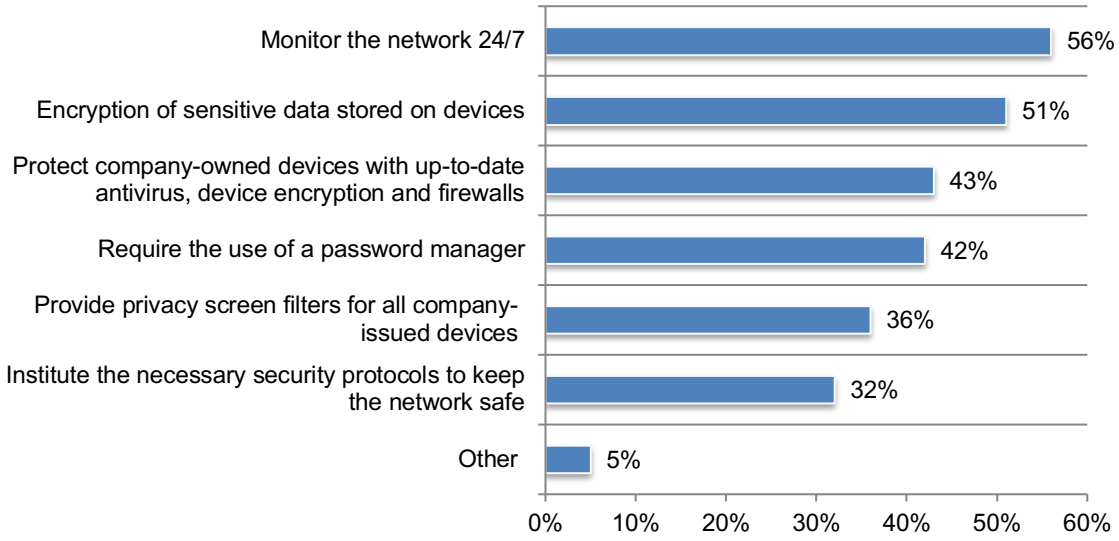
Remote workers exposure of sensitive information on their screens is a significant concern. Sixty-four percent of IT and IT security managers say they are very concerned that prying eyes will see the sensitive information on remote workers screens. As shown in Figure 9, organizations that are concerned are conducting training and awareness programs that cover the remote worker risk (51 percent of respondents), instituting new mobile device policies (41 percent of respondents) and requiring employees' home workspace to be private and not allow others to be near the device (40 percent of respondents).

Figure 9. How is your organization preventing the exposure of sensitive data on their screens while working remotely?
More than one response permitted



Monitoring and encryption are the primary steps taken to create a secure remote working environment. According to Figure 10, 56 percent of respondents say their organizations monitor the network 24/7 and 51 percent of respondents say their organizations encrypt sensitive data stored on devices.

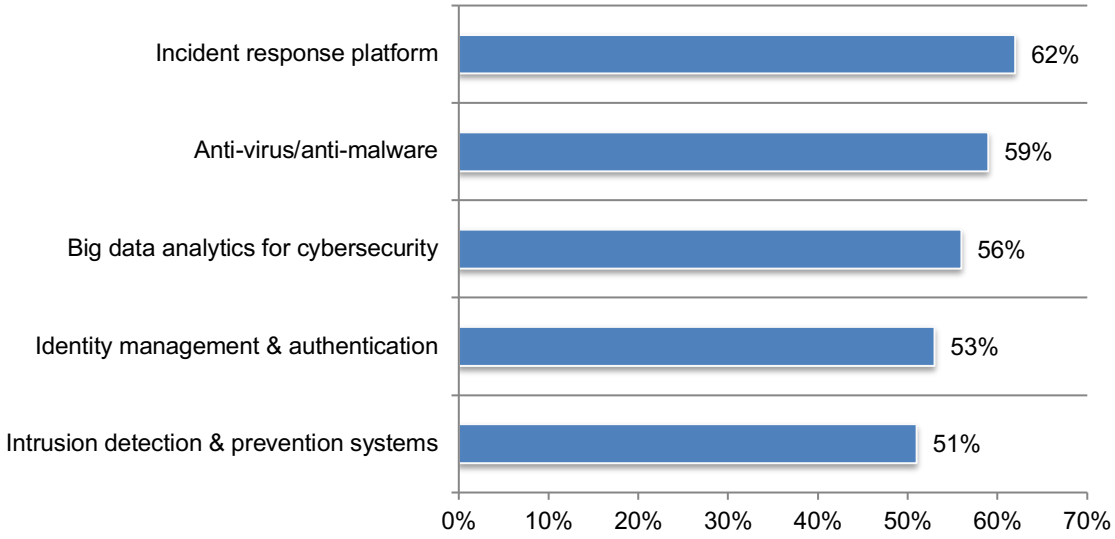
Figure 10. What steps does your organization take to create a secure environment for working remotely?
More than one response permitted



Incident response platforms are considered most effective in helping organizations improve their privacy and security posture. Figure 11 presents the top five technologies IT and IT security managers believe are most effective in improving privacy and security in a remote working environment.

Sixty-two percent of respondents say incident response platforms are most effective followed by anti-virus/anti-malware (59 percent of respondents), big data analytics for cybersecurity (56 percent of respondents), identity management & authentication (53 percent of respondents) and intrusion detection & prevention systems (51 percent of respondents).

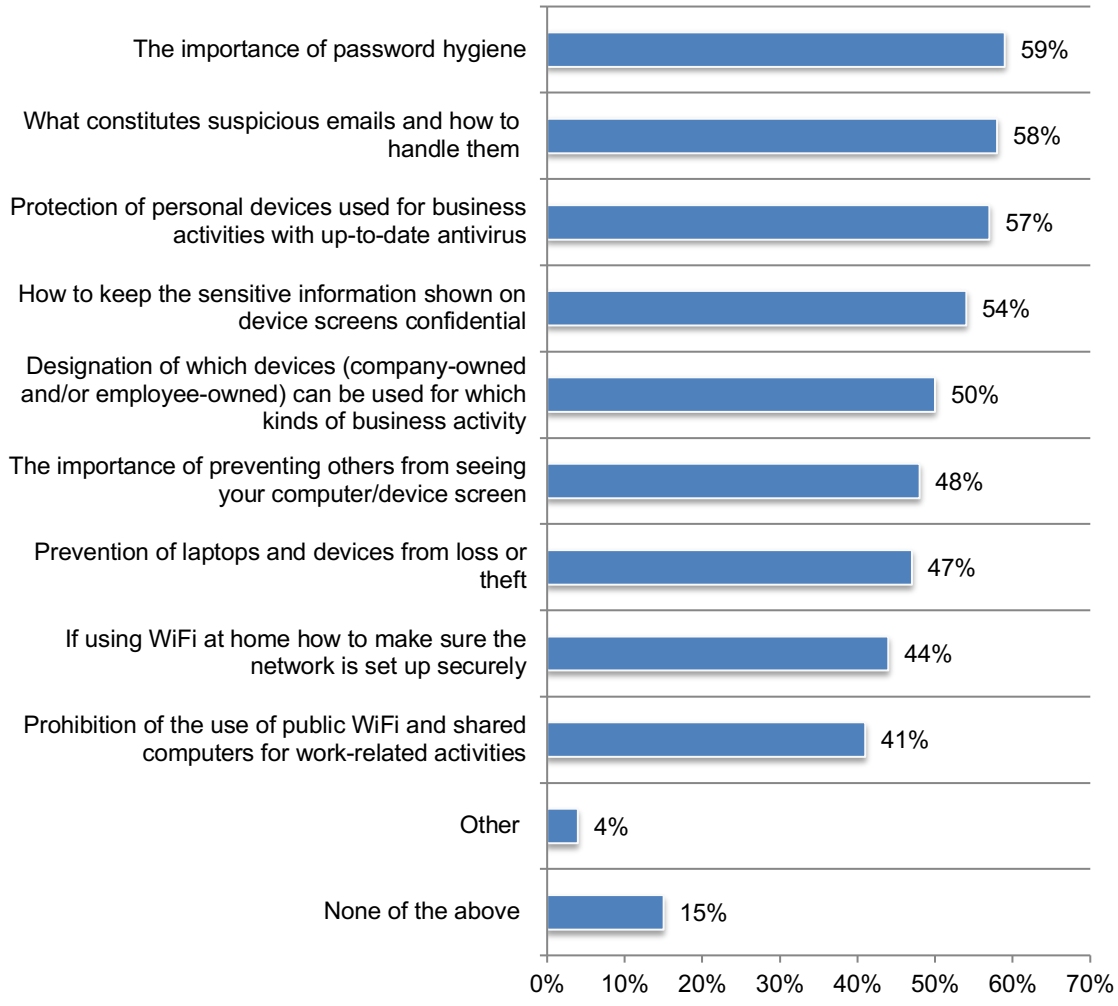
Figure 11. The top five technologies most effective in improving the organization's privacy and security posture
More than one response permitted



The importance of password hygiene is most often communicated to remote workers. It is important to note that most organizations have a policy on IT device privacy and security requirements for remote workers (67 percent of respondents).

As shown in Figure 12, 59 percent of respondents say the policy includes the importance of password hygiene followed by what constitutes suspicious emails and how to handle them (58 percent of respondents), protection of personal devices used for business activities with up-to-date antivirus (57 percent of respondents), how to keep the sensitive information shown on device screens confidential (54 percent of respondents), designation of which devices (company-owned and/or employee-owned) can be used for which kinds of business activity (50 percent of respondents) and the importance of preventing others from seeing your computer/device screen (48 percent of respondents).

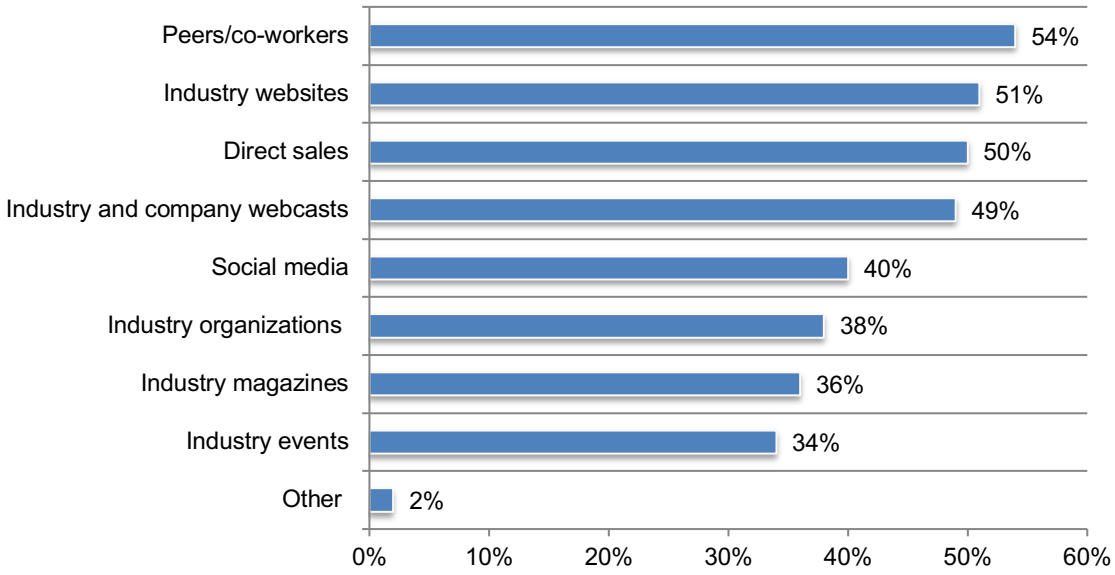
Figure 12. What does your policy on IT device privacy and security requirements for remote workers?
More than one response permitted



Purchasing technology for a remote workforce

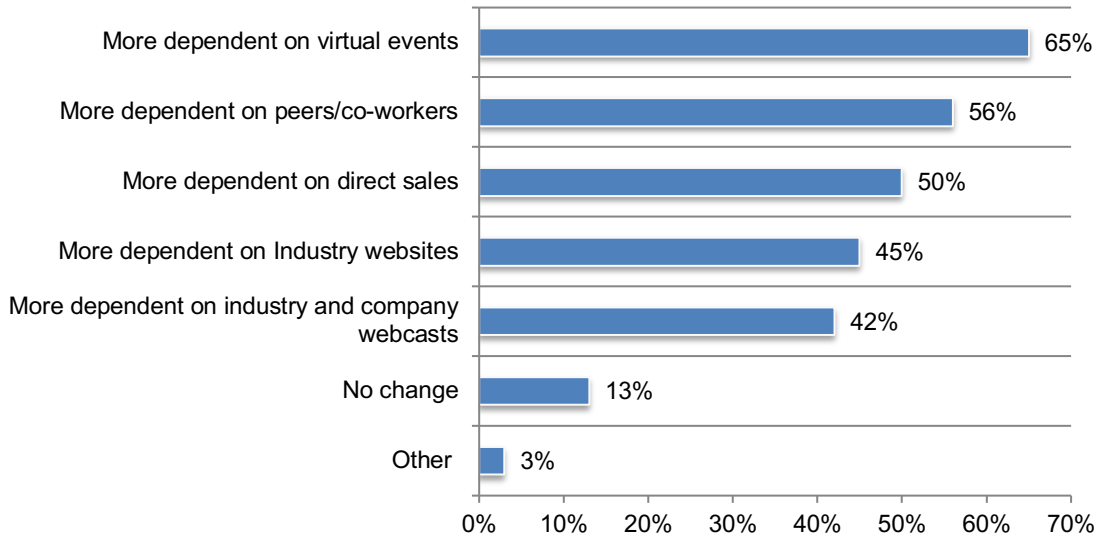
A remote workforce makes it more of a challenge to purchase technology. Sixty-three percent of respondents say it has become more difficult to make decisions about investments in technology solutions solution since COVID-19. As shown in Figure 13, respondents are mainly dependent upon peers/co-workers (54 percent of respondents) or industry websites (51 percent of respondents). In the next year, respondents predict they will purchase software (67 percent of respondents), laptop/tablets (65 percent of respondents) and cell phones (61 percent of respondents).

Figure 13. How do you learn about new IT hardware, software and accessories?
More than one response permitted



Investment decisions in technology go virtual. As shown in Figure 14, 65 percent of respondents say they are more dependent upon virtual events followed by more dependency on peers/co-workers (56 percent of respondents) and more dependent on direct sales (50 percent of respondents).

Figure 14. Since COVID-19 how has your information-gathering process changed?
More than one response permitted

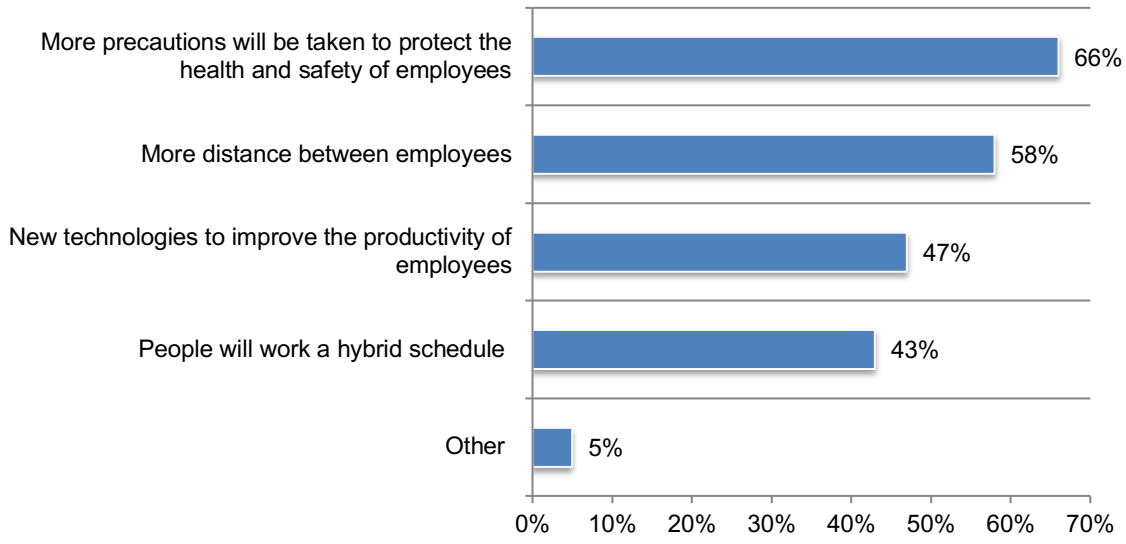


IT and IT security managers predict the future in a post COVID-19 workplace

In the future, the physical workspace will be transformed. As discussed, the workplace will never be the same. According to respondents, an average of 45 percent of employees will return to the office and an average of 47 percent will work both remotely and in the office.

Sixty-two percent of respondents say COVID-19 has caused their organizations to rethink how its physical office space will be set up and utilized once employees return to the office. As shown in Figure 15, 66 percent of respondents say more precautions will be taken to protect the health and safety of employees and 58 percent of respondents say there will be more distance between employees.

Figure 15. What changes do you think the "office of the future" will have in a post-COVID-19 world?
More than one response permitted



Part 3. Key findings from the survey of business managers

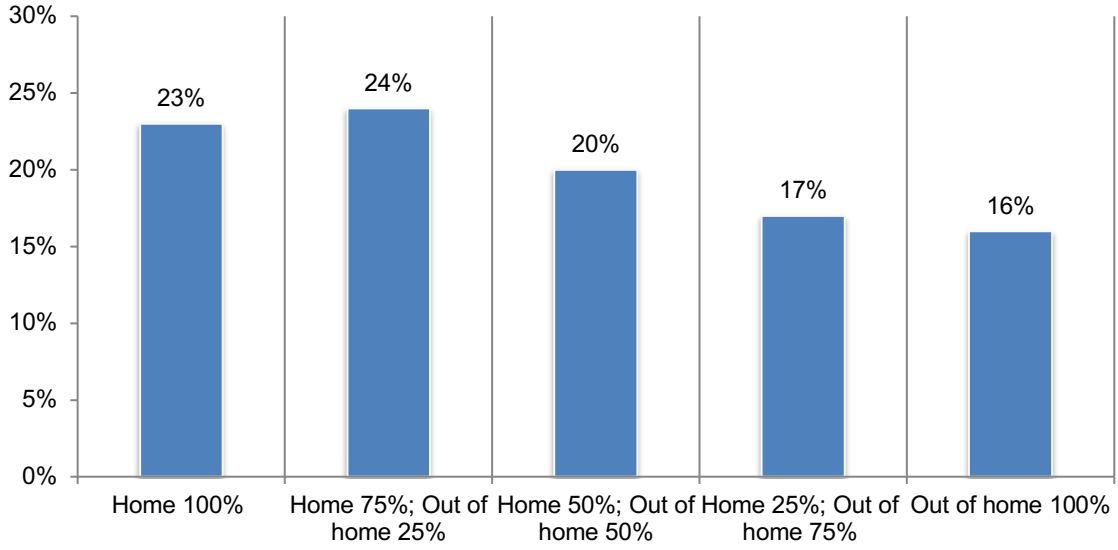
In this section, we provide an analysis of the findings from the survey of 617 business professionals. Following are the topics covered in this section.

- Can remote workers protect the privacy of their organizations' sensitive and confidential information?
- The employee experience when working remotely
- Looking to the future

Most business managers say they do not work exclusively in their home. As discussed in Part 2, IT and IT security managers say that an average of 40 percent of their organizations' remote workforce spends time in coffee shops and shared workspaces where it is not easy to keep information safe from prying eyes.

This is consistent with the findings shown in Figure 16. Specifically, only 23 percent of respondents say they work 100 percent of the time in their home.

Figure 16. What percentage of your time is spent working in your home vs. going to a coffee shop, shared workspace or other place outside your home?

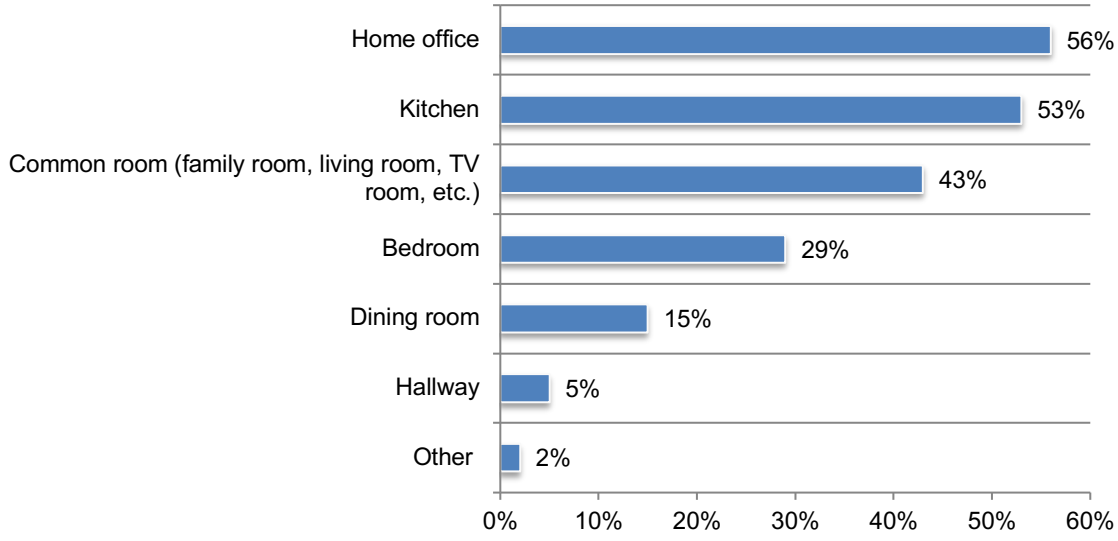


Most respondents say they cannot keep prying eyes from seeing their work. Only 34 percent of respondents say where they work at home makes it possible for them to prevent others, including family members or roommates, from seeing their work.

Also contributing to the remote worker risk is that only 43 percent of respondents say they are concerned when displaying sensitive or confidential data on their screen when working remotely—either in the home or somewhere else and only 40 percent of respondents say their company has increased its enforcement of its privacy policies since more employees are working remotely.

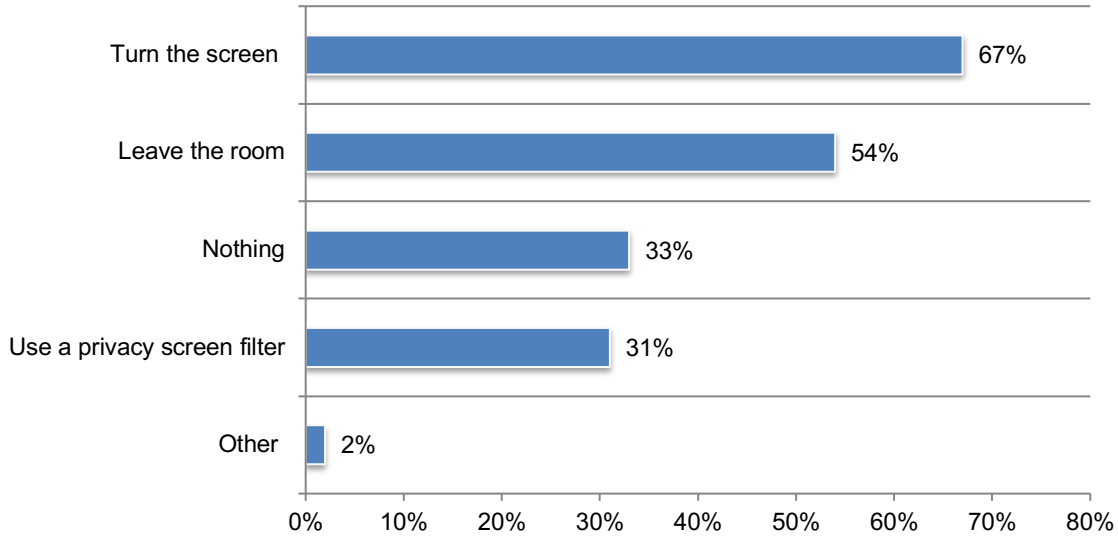
According to Figure 17, 56 percent of respondents say they work in their home office where there is a better chance of avoiding prying eyes. However, many are working in such open spaces as the kitchen (53 percent) followed by 43 percent of respondents who say they work in the family or living rooms and other common spaces.

Figure 17. Where in the home is your workspace set up?
More than one response permitted



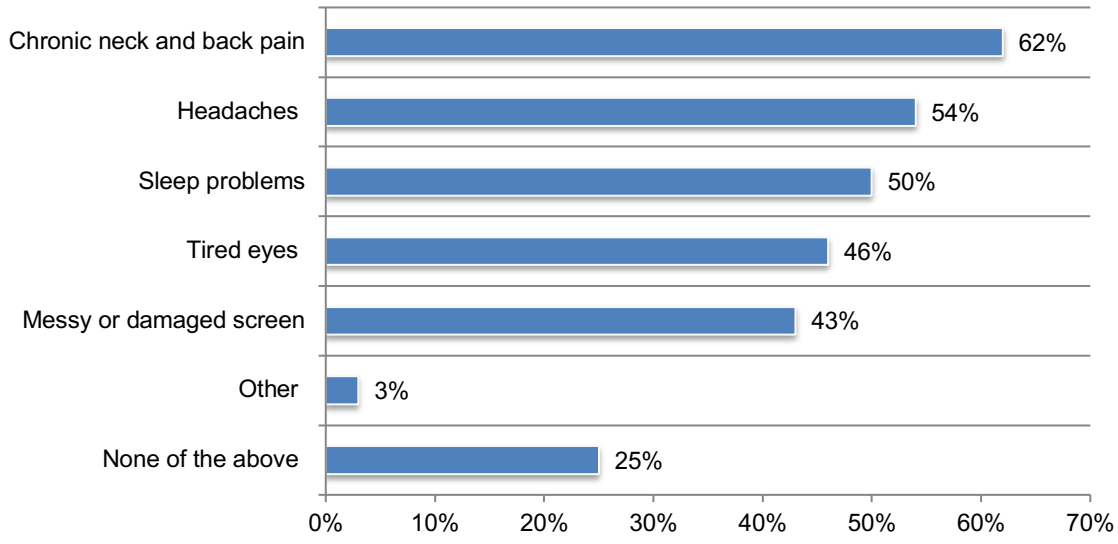
Turning the screen is the number one step taken to shield sensitive information. Despite the prevalence of employees working in open spaces, 55 percent of business managers do not take steps to prevent others from viewing their screens. If they do, 67 percent of these respondents turn the screen and 54 percent of respondents say they leave the room with their devices.

Figure 18. What steps do you take to shield your device from prying eyes?
More than one response permitted



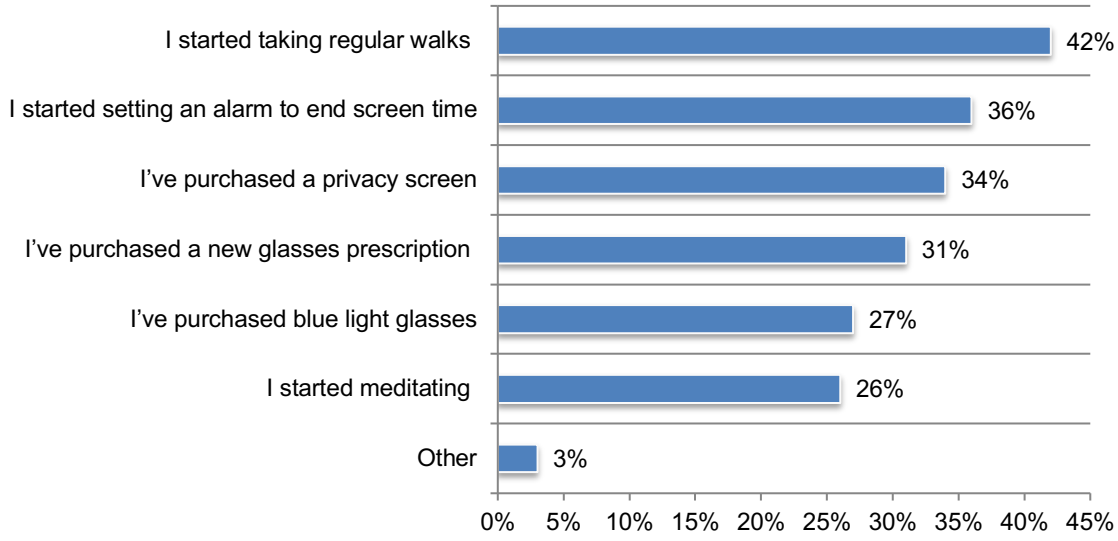
A remote workforce is experiencing health issues. Respondents report that on average they are spending 44 percent more time in front of their device screen. As a result, many are experiencing chronic neck and back pain (62 percent of respondents) and headaches (54 percent of respondents), as shown in Figure 19.

Figure 19. If more time is spent in front of your device screen, are you experiencing any of the following symptoms?
More than one response permitted



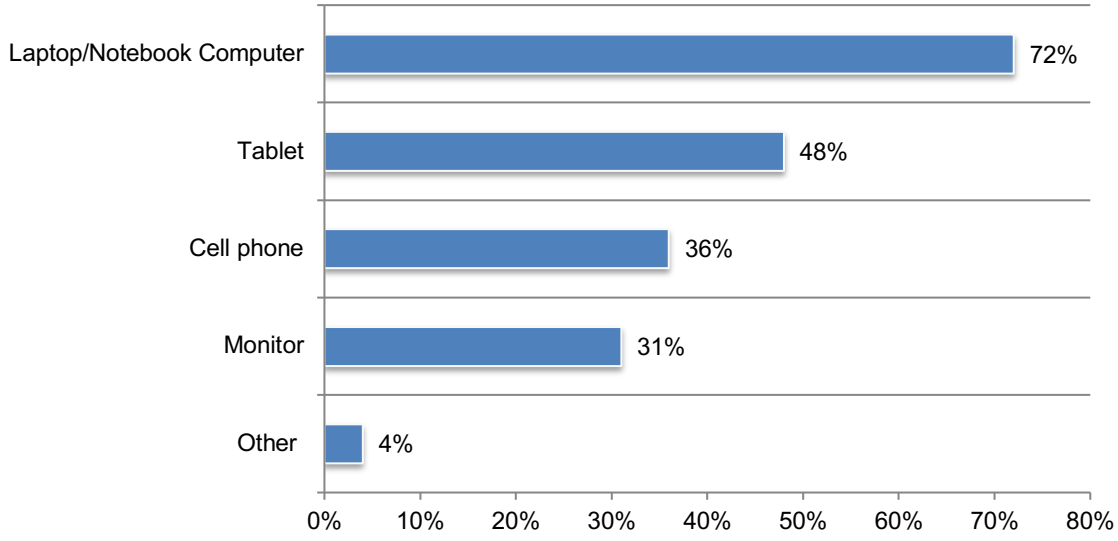
Of the 75 percent of respondents who say their health has been affected, 42 percent of respondents say they are taking regular walks and 36 percent say they have started setting an alarm to end screen time (36 percent of respondents), as shown in Figure 20.

Figure 20. What actions are you taking to deal with these health issues?
More than one response permitted



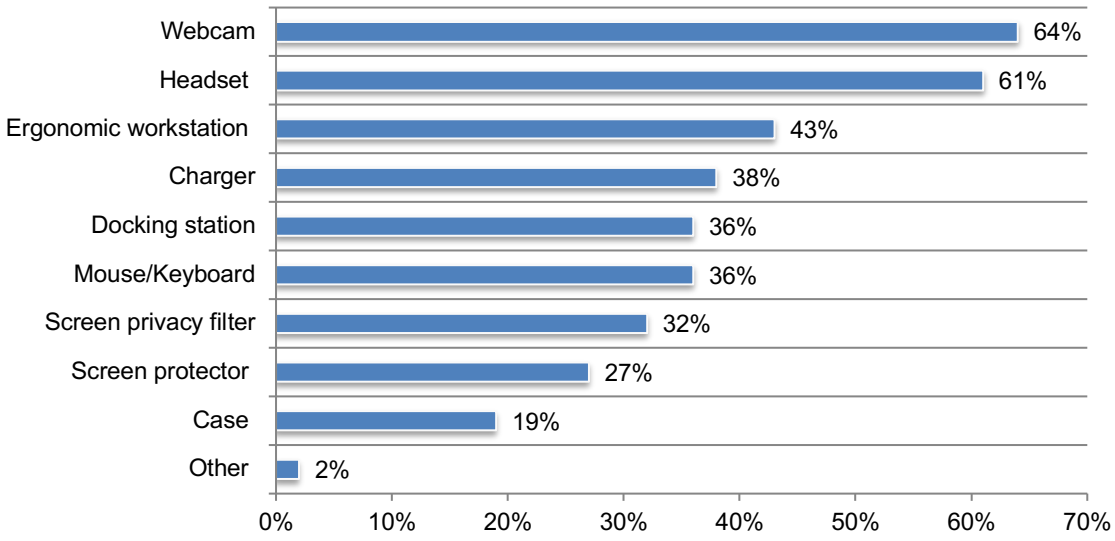
Laptops or notebook computers are most often used for remote working. Most respondents use company-provided devices (45 percent) or combinations of personal and company-provided devices (22 percent). However, one-third of respondents say they are using their own personal devices when working remotely. As shown in Figure 21, laptops and tablets are most often used by remote workers

Figure 21. What devices do you primarily use while working remotely due to COVID-19?
More than one response permitted



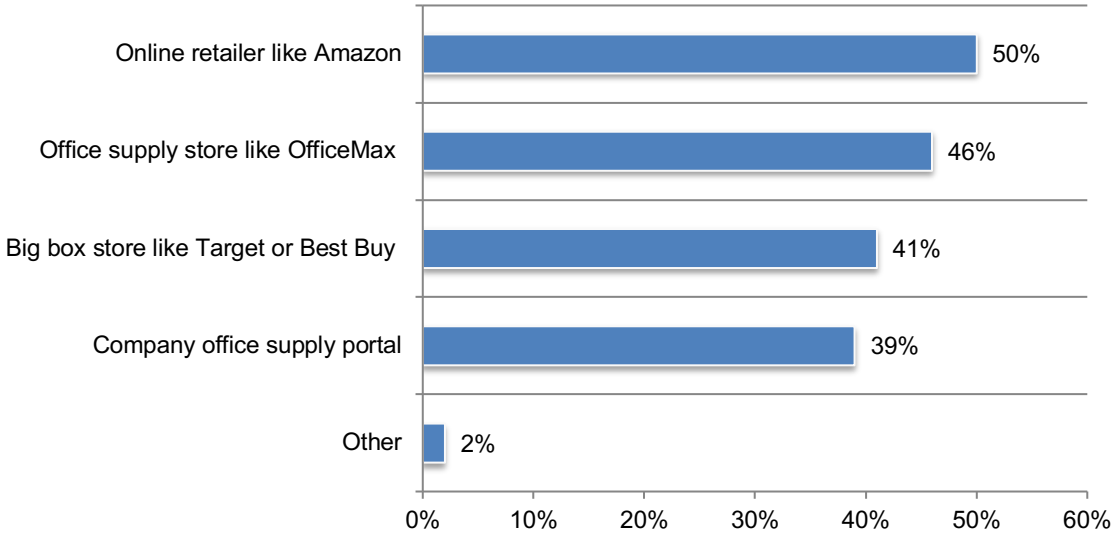
More online conferences increase the need for webcams and headsets. As shown in Figure 22, 64 percent of respondents and 61 percent of respondents say they have requested webcams and headsets, respectively.

Figure 22. What kind of accessories do you need for your primary device since starting to work remotely?
More than one response permitted



Amazon and OfficeMax are the primary sources for remote workers' purchases. If respondents purchase these accessories on their own, 60 percent of respondents say they purchase through a company approved website. According to Figure 23, 50 percent of respondents say they purchase accessories for their devices from Amazon followed by an office supply store like OfficeMax.

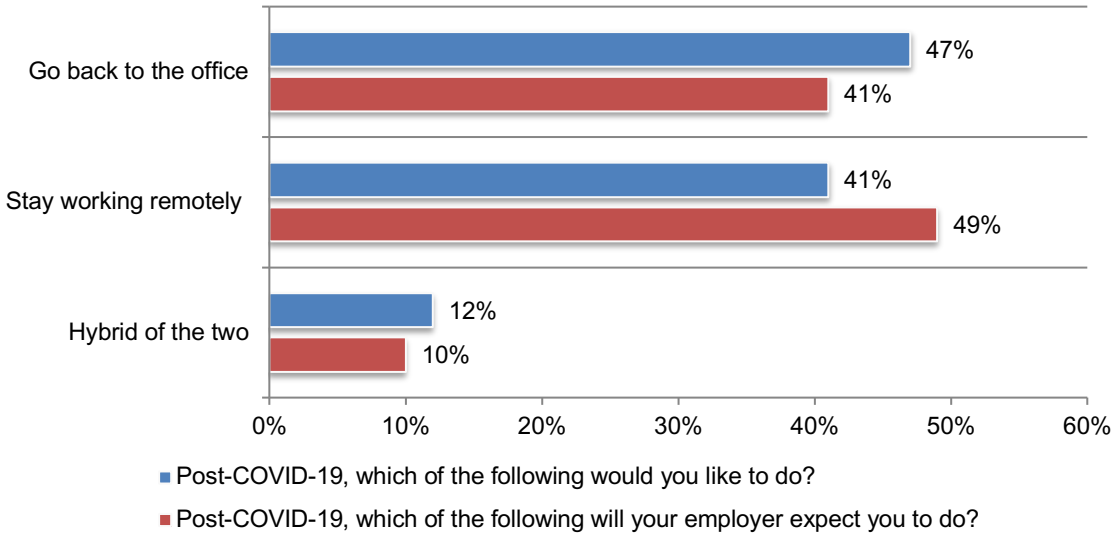
Figure 23. If you bought accessories yourself, where did you get them?
More than one response permitted



Looking to the future

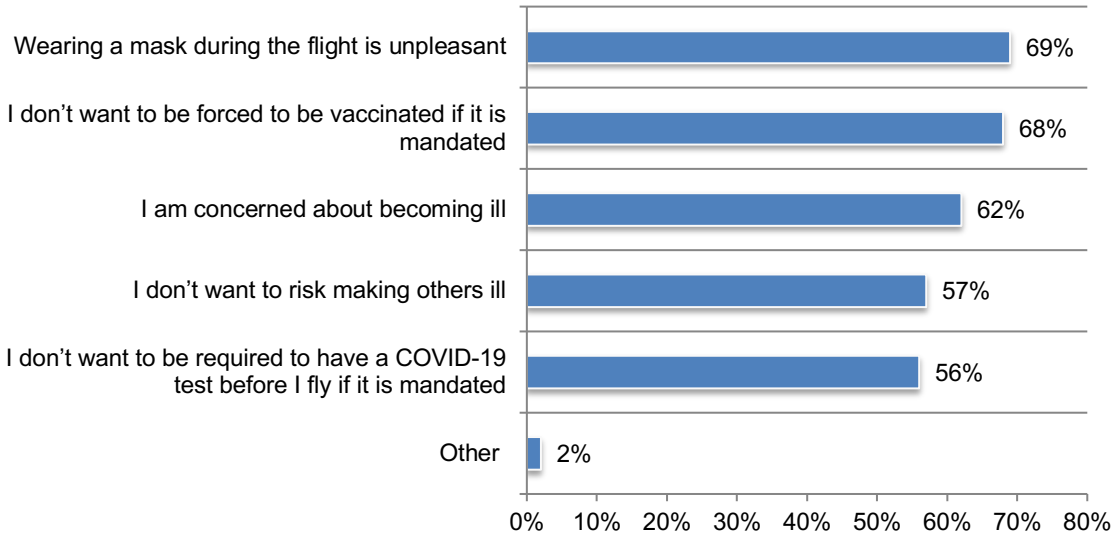
Post-COVID-19 business managers would like to return to the office. According to Figure 24, 49 percent of respondents say their employers will expect them to continue to work remotely. However, 47 percent of business managers would like to return to the office.

Figure 24. Post-COVID-19 what do remote workers and employers want to do?



Most respondents will be comfortable traveling on business Post-COVID-19. Before COVID-19, 51 percent of respondents say they very often traveled on business. Fifty-seven percent of respondent say they will be very comfortable traveling once again. As shown in Figure 25, of the 43 percent of respondents who say they are not comfortable, it is because of the unpleasantness of wearing a mask (69 percent of respondents), the mandate of being vaccinated (68 percent of respondents) and I am concerned about becoming ill (62 percent of respondents).

Figure 25. Why are you not comfortable traveling?



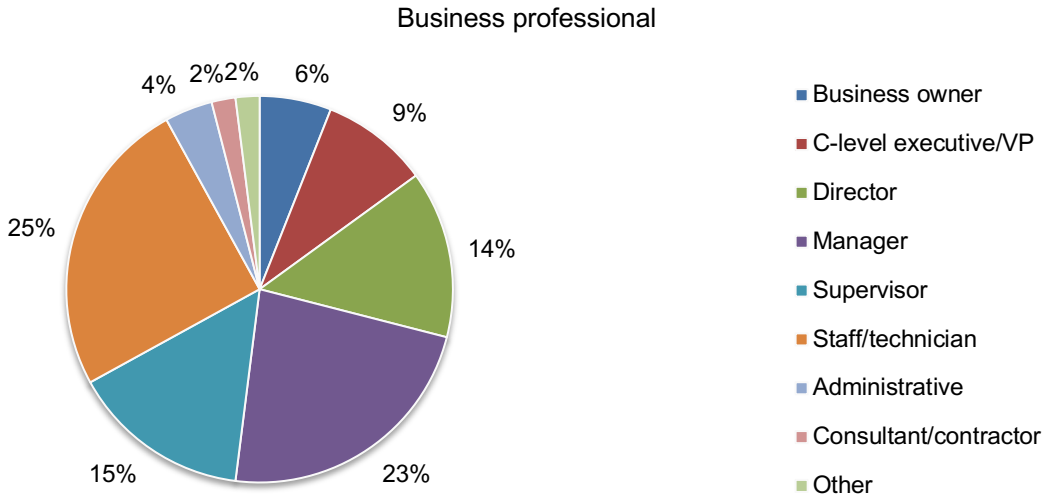
Part 4. Methodology

A random sampling frame of 16,526 business professionals and 15,033 IT and IT security practitioners located in the United States were selected as participants to this survey. As shown in Table 1, 674 business professionals and 620IT managers completed the survey. Screening removed 57 business professional surveys and 56 IT manager surveys. The final sample was 617 business professional surveys (a 3.7 percent response rate) and 565 IT managers surveys (a 4.0 percent response rate).

Table 1. Sample response	Business professionals	IT and IT security managers
Total sampling frame	16,525	15,033
Total returns	674	620
Rejected surveys	57	56
Screened surveys	16,525	15,033
Final sample	617	564
Response rate	3.7%	4.0%

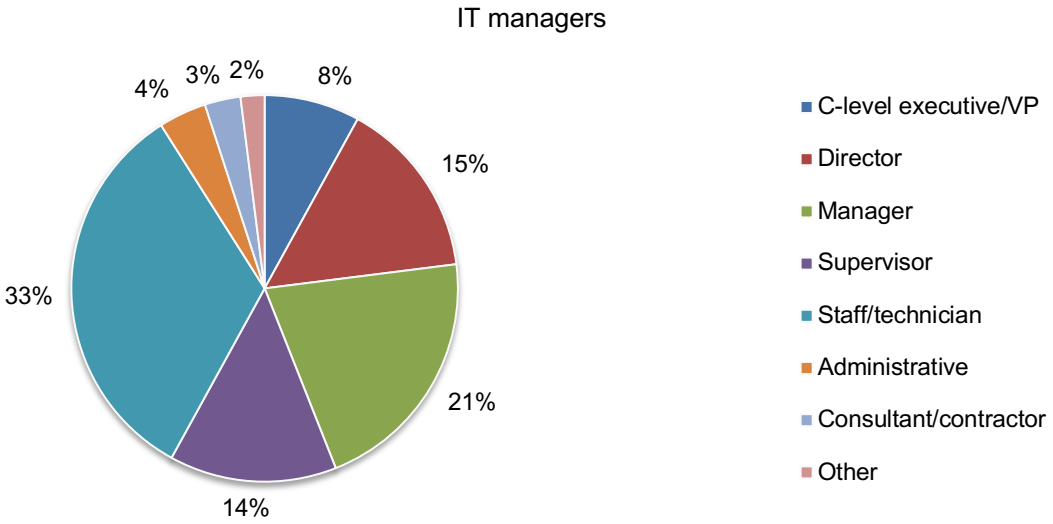
Pie Chart 1 reports the business professional respondent's organizational level within participating organizations. More than half (67 percent) of respondents are at or above the supervisory levels. The largest segment is staff/technician.

Pie Chart 2. What organizational level best describes your current position?



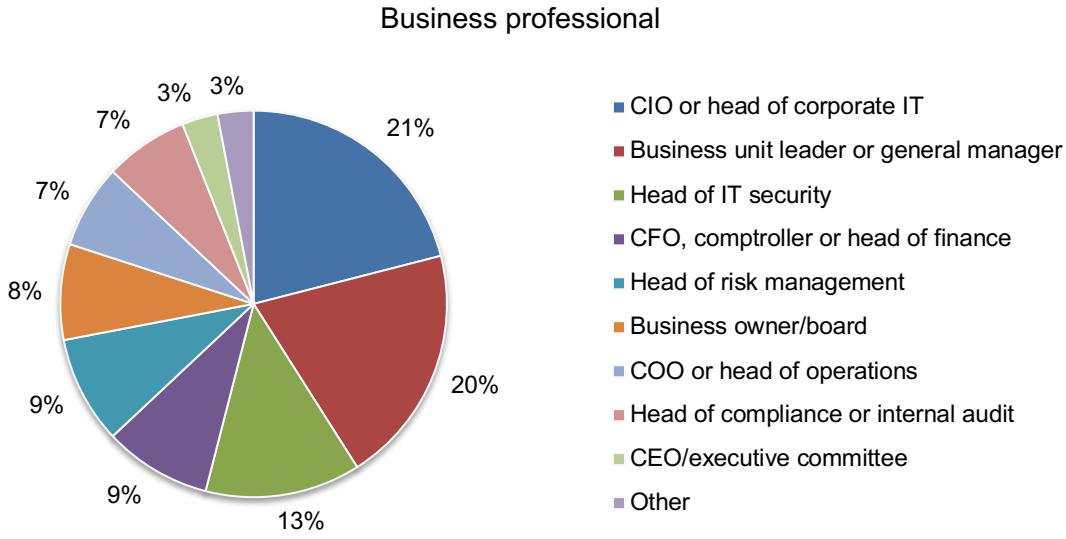
Pie Chart 2 reports the IT manager respondent's organizational level within participating organizations. More than half (58 percent) of respondents are at or above the supervisory levels. The largest segment at 33 percent is staff/technician.

Pie Chart 2. What organizational level best describes your current position?



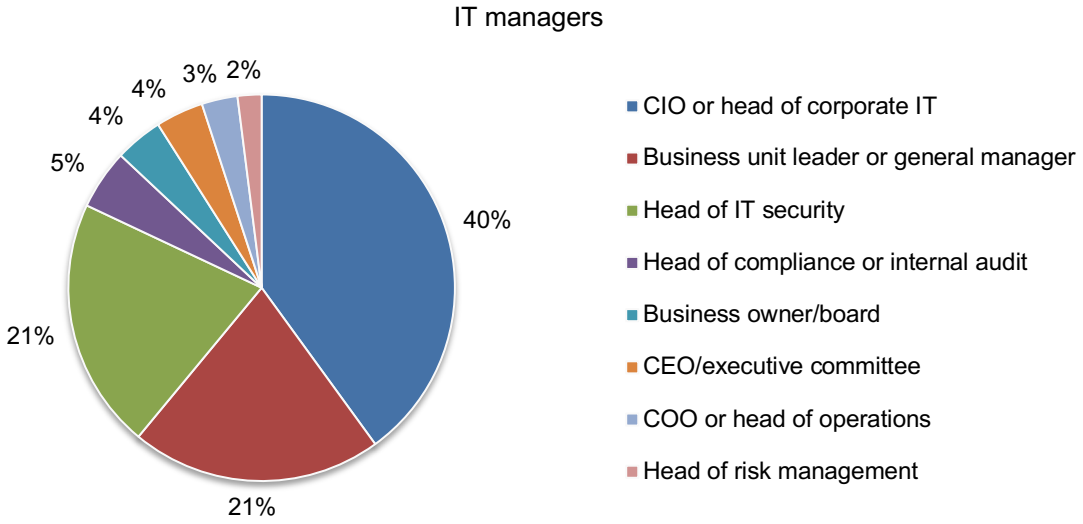
According to Pie Chart 3, 21 percent of business professionals report directly to the CIO or head of corporate IT and 20 percent report to the business unit leader or general manager.

Pie Chart 3. The primary person you or the IT security leader reports to within the organization



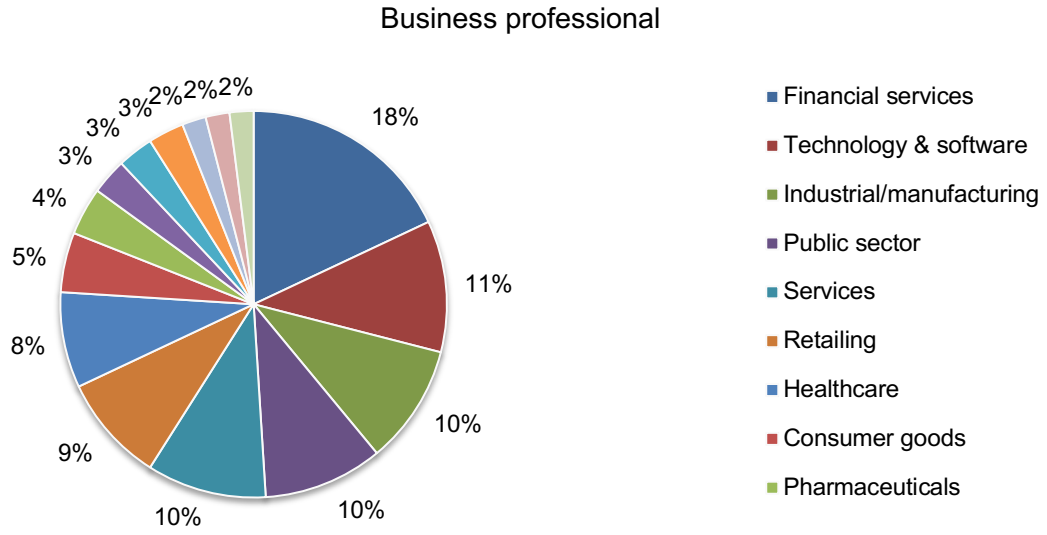
According to Pie Chart 4, 40 percent of IT managers report directly to the CIO or head of corporate IT and 21 percent report to the business unit leader or general manager.

Pie Chart 4. The primary person you or the IT security leader reports to within the organization



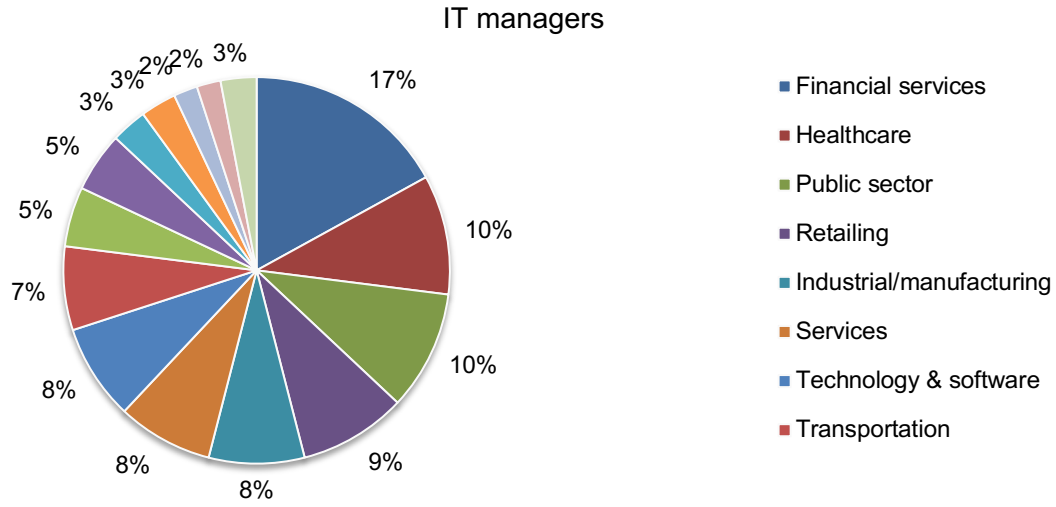
Pie Chart 5 reports the business professionals primary industry segments. Eighteen percent of respondents are in financial services and 11 percent are in technology and software. Another 10 percent are in industrial/manufacturing, public sector, and services.

Pie Chart 5. Distribution of respondents according to primary industry classification



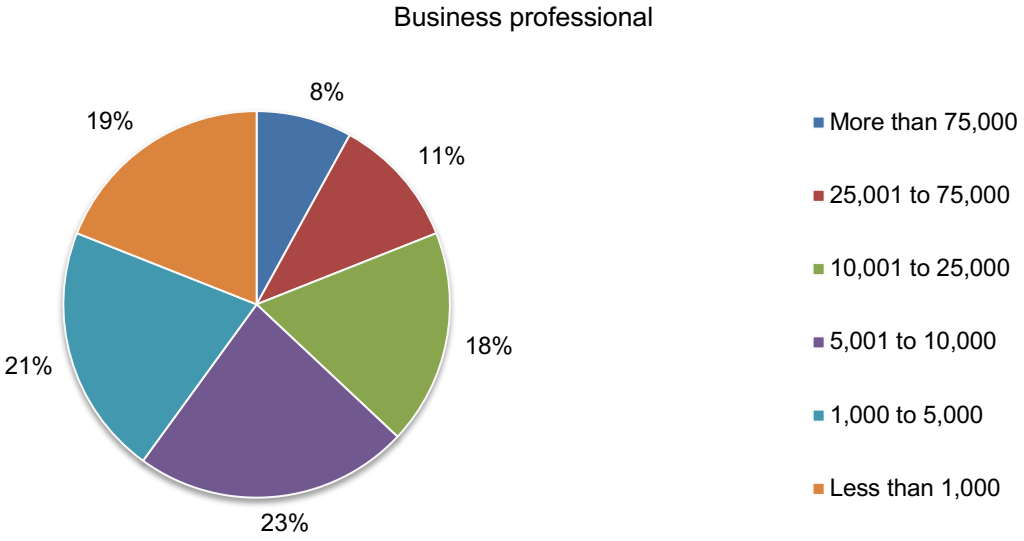
Pie Chart 6 reports the IT managers primary industry segments. Seventeen percent of respondents are in financial services, 10 percent are in healthcare, 10 percent are in public sector, and 9 percent are in retail.

Pie Chart 6. Distribution of respondents according to primary industry classification



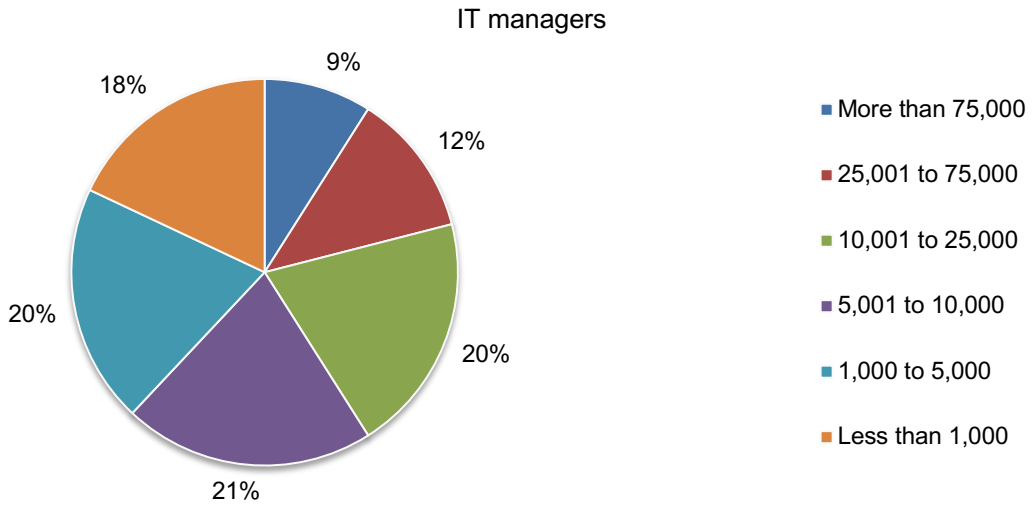
Sixty percent of respondents are from organizations with a global headcount of more than 5,000 employees, as shown in Pie Chart 7.

Pie Chart 7. Worldwide headcount of the organization



Sixty-two percent of respondents are from organizations with a global headcount of more than 5,000 employees, as shown in Pie Chart 8.

Pie Chart 8. Worldwide headcount of the organization



Part 5. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners and business professionals. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions. All survey responses were captured in March 2021.

IT and IT security managers	FY2021
Total sampling frame	15,033
Total returns	620
Rejected or screened surveys	56
Final sample	564
Response rate	4%

Part 1. Screening questions

S1. What best describes your role in your organization? Check all that apply.	FY2021
Setting IT priorities and strategy	36%
Managing IT budgets	42%
Evaluating and/or selecting IT hardware	56%
Evaluating and/or selecting IT software	53%
Evaluating and/or selecting IT vendors	61%
Distributing new IT hardware and software to employees	45%
Evaluating IT hardware and software performance	50%
None of the above (Stop)	0%
Total	343%

S2. How do you rate your level of involvement in the evaluation, selection, and/or implementation of IT hardware and software products or services in your organization?	FY2021
Very high level of involvement	34%
High level of involvement	37%
Moderate level of involvement	17%
Low level of involvement	12%
Not involved (Stop)	0%
Total	100%

S3. In the last year, has your organization required its employees to work from home due to COVID-19?	FY2021
Yes	78%
No	22%
Total	100%

Part 2. IT and IT security managers' perspective on a remote workforce

Q1. **Before** COVID-19, what percentage of your organization's employees worked remotely vs. in the office?	FY2021
0%	35%
10% to 25%	28%
26% to 50%	20%
51% to 75%	12%
76% to 100%	5%
Total	100%
Extrapolated value	24%

Q2. **Since** COVID-19, what percentage of your employees have been working remotely?	FY2021
0%	5%
10% to 25%	5%
26% to 50%	13%
51% to 75%	31%
76% to 100%	46%
Total	100%
Extrapolated value	65%

Q3. **Since** COVID-19, What percentage of these employees work in a coffee shop or shared workspace?	FY2021
0%	17%
10% to 25%	25%
26% to 50%	19%
51% to 75%	23%
76% to 100%	16%
Total	100%
Extrapolated value	40%

Q4. What privacy and security risks caused by remote workers are you most concerned about? Please select the **top four** concerns.	FY2021
The difficulty in securing your organization's network	45%
The difficulty in securing external access to internal-only resources	50%
Someone seeing confidential information on the screen	33%
Criminals gain control of remote workers' devices to steal sensitive and confidential data	43%
Criminals leverage the devices to gain access to the enterprise network	38%
Remote workers lose or have their devices stolen	42%
The inability to secure communications on external networks outside your organization's control	67%
Remote workers' devices become infected with malware	48%
Phishing and social engineering scams directed at remote workers	32%
Other	2%
Total	400%

Q5. What steps does your organization take to address these concerns? Please select all that apply.	FY2021
Protect company-owned devices with up-to-date antivirus, device encryption and firewalls	51%
Require the use of a password manager	40%
Require the use of screen privacy filters	35%
Institute the necessary security protocols to keep the network safe	42%
Encrypt sensitive data stored on devices	50%
Other	2%
Total	220%

Q6a. How concerned are you that your organization's employees will expose sensitive data on their screens while working remotely? Please use the 10-point scale from 1 = not concerned to 10 = very concerned.	FY2021
1 to 2	7%
3 to 4	16%
5 to 6	13%
7 to 8	28%
9 to 10	36%
Total	100%
Extrapolated value	6.90

Q6b. If you are concerned or very concerned (6+ responses on the 10-point scale) what is your organization doing to prevent this? Select all that apply.	FY2021
Purchasing devices with screen privacy built in	34%
Instituting new mobile device policies	41%
Prohibiting employees from working in public locations	37%
Requiring employees to use a privacy screen filter on their device	33%
Requiring employees' home workspace to be private and not allow others to be near the device	40%
Conducting training and awareness programs that cover the remote worker risk	51%
Other	3%
Total	239%

Q7. Did you deploy more or less of the following devices to employees to accommodate working remotely due to COVID-19?	
Laptop / Notebooks	FY2021
More	43%
Less	25%
Same	32%
Total	100%

Monitors	FY2021
More	34%
Less	21%
Same	45%
Total	100%

Smartphones	FY2021
More	50%
Less	21%
Same	29%
Total	100%

Tablets	FY2021
More	47%
Less	28%
Same	25%
Total	100%

Q8. **Before COVID-19**, how did you typically distribute IT accessories to your workforce?	
8a. To Remote Workers:	FY2021
Employees ordered online	23%
IT bought and employees picked up in office	25%
IT bought and shipped to house	29%
Employee ordered through department administrator / office manager	21%
Other	2%
Total	100%

8b. To In-Office Workers:	FY2021
Employees ordered online	34%
IT bought and employees picked up in office	21%
IT bought and shipped to house	23%
Employee ordered through department administrator / office manager	19%
Other	3%
Total	100%

Q9. **During COVID-19**, how do you typically distribute IT accessories to your workforce?	
9a. To Remote Workers:	FY2021
Employees ordered online	29%
IT buys and employees picked up in office	30%
IT buys and ships to house	26%
Employee orders through department administrator / office manager	15%
Other	0%
Total	100%

9b. To In-Office Workers:	FY2021
Employees ordered online	23%
IT buys and employees pick up in office	28%
IT buys and ships to house	31%
Employee orders through department administrator / office manager	18%
Other	0%
Total	100%

Q10a. **Since** COVID-19. how has the time employees spend on their devices changed each week while working remotely?	FY2021
Significantly increased	34%
Increased	30%
Increased somewhat	11%
Decreased (please skip to Q11)	13%
Decreased significantly (please skip to Q11)	12%
Total	100%

Q10b. If increased, have they complained about any of the following symptoms? Please check all that apply.	FY2021
Headaches	58%
Tired eyes	47%
Messy or damaged screen	46%
Chronic neck and back pain	60%
Sleep problems	55%
Other	2%
None of the above	27%
Total	295%

Q11. Since COVID-19, what kind of accessories have your employees requested for their primary device? Please check all that apply.	FY2021
Webcam	61%
Headset	63%
Screen privacy filter	34%
Screen protector	23%
Mouse/Keyboard	39%
Ergonomic workstation	42%
Docking station	34%
Charger	30%
Case	17%
Other	3%
Total	346%

Q12. Since COVID-19, has it become more difficult to make decisions about investments in technology solutions or accessories?	FY2021
Yes	63%
No	37%
Total	100%

Q13. What types of technology solutions or accessories do you plan to purchase for your company within the next year? Check all that apply.	FY2021
Laptop/Tablet	65%
Cell phone	61%
Webcam	47%
Headset	31%
Software	67%
Screen privacy filter	23%
Screen protector	18%
Mouse/Keyboard	25%
Ergonomic workstation	30%
Other	2%
None of the above	19%
Total	388%

Q14a. How do you learn about new IT hardware, software and accessories? Check all that apply.	FY2021
Industry events	34%
Industry magazines	36%
Industry websites	51%
Industry and company webcasts	49%
Industry organizations	38%
Peers/co-workers	54%
Social media	40%
Direct sales	50%
Other	2%
Total	354%

Q14b. Since **COVID-19** how has your information-gathering process changed?	FY2021
More dependent on virtual events	65%
More dependent on Industry websites	45%
More dependent on industry and company webcasts	42%
More dependent on peers/co-workers	56%
More dependent on direct sales	50%
No change	13%
Other	3%
Total	274%

Q15. What industry organizations do you belong to? Please select all that apply.	FY2021
(ISC)2 (International Information Systems Security Certification Consortium)	51%
ISACA (Information Systems Audit and Control Association)	55%
AITP (Association of Information Technology Professionals)	37%
ITIL (Information Technology Infrastructure Library)	15%
Forum of Incident Response and Security Teams	18%
The SANS Institute	43%
ISSA (Information Systems Security Association)	51%
CIS (Center for Internet Security)	46%
Other	5%
Total	321%

Q16. Does your organization have a policy on IT device privacy and security requirements for remote workers?	FY2021
Yes	67%
No	33%
Total	100%

Q17. And what does the policy cover? Please select all that apply.	FY2021
The importance of password hygiene	59%
The importance of preventing others from seeing your computer/device screen	48%
How to keep the sensitive information shown on device screens confidential	54%
Prevention of laptops and devices from loss or theft	47%
Protection of personal devices used for business activities with up-to-date antivirus	57%
Designation of which devices (company-owned and/or employee-owned) can be used for which kinds of business activity	50%
What constitutes suspicious emails and how to handle them	58%
Prohibition of the use of public WiFi and shared computers for work-related activities	41%
If using WiFi at home how to make sure the network is set up securely	44%
Other	4%
None of the above	15%
Total	477%

Q18. What steps does your organization take to create a secure environment for working remotely? Please select all that apply.	FY2021
Protect company-owned devices with up-to-date antivirus, device encryption and firewalls	43%
Require the use of a password manager	42%
Monitor the network 24/7	56%
Provide privacy screen filters for all company-issued devices	36%
Institute the necessary security protocols to keep the network safe	32%
Encryption of sensitive data stored on devices	51%
Other	5%
Total	265%

Q19. Which of the following technologies have been the most effective in helping your organization improve its privacy and security posture? Please select your top 10 choices.	FY2021
Anti-virus/anti-malware	59%
Artificial intelligence	42%
Big data analytics for cybersecurity	56%
Code review and debugging systems	23%
Data loss prevention (DLP)	35%
Data tokenization technology	17%
DDoS solutions	43%
Data risk management	30%
Encryption for data at rest	43%
Encryption for data in motion	41%
Endpoint security solution	50%
Governance solutions (GRC)	47%
Identity management & authentication	53%
Incident response platform	62%
Intrusion detection & prevention systems	51%
Machine learning	35%
Network traffic surveillance	34%
Next generation firewalls	23%
Orchestration & automation	28%
Privacy screen filters	31%
Security information and event management (SIEM)	45%
User Behavioral Analytics (UBA)	38%
Virtual private networks (VPN)	42%
Web application firewalls (WAF)	47%
Wireless security solutions	23%
Other	2%
Total	1000%

Q20a. When things return to “normal”, what percentage of your employees will return to the office?	FY2021
0%	6%
10% to 25%	21%
26% to 50%	35%
51% to 75%	20%
76% to 100%	18%
Total	100%
Extrapolated value	45%

Q20b. When things return to “normal”, what percentage of your employees will work both remotely and in the office?	FY2021
0%	6%
10% to 25%	17%
26% to 50%	35%
51% to 75%	24%
76% to 100%	18%
Total	100%
Extrapolated value	47%

Q21. Is it easier to protect the privacy of your organization's sensitive and confidential information when employees are working in the office?	FY2021
Yes	65%
No	30%
Unsure	5%
Total	100%

Q22. Has COVID-19 caused your company to re-think how its physical office space will be set up and utilized once people return to the office?	FY2021
Yes	62%
No	38%
Total	100%

Q23. If yes, what changes do you think the "office of the future" will have in a **post-COVID-19** world?	FY2021
More precautions will be taken to protect the health and safety of employees	66%
More distance between employees	58%
New technologies to improve the productivity of employees	47%
People will work a hybrid schedule	43%
Other	5%
Total	219%

Role and organizational characteristics

D1. What best describes your position level within the organization?	FY2021
C-level executive/VP	8%
Director	15%
Manager	21%
Supervisor	14%
Staff/technician	33%
Administrative	4%
Consultant/contractor	3%
Other	2%
Total	100%

D2. Which of the following functions do you report to in your current role?	FY2021
Business owner/board	4%
CEO/executive committee	4%
COO or head of operations	3%
CFO, comptroller or head of finance	0%
CIO or head of corporate IT	40%
Business unit leader or general manager	21%
Head of compliance or internal audit	5%
Head of risk management	2%
Head of IT security	21%
Other	0%
Total	100%

D3. What best describes your organization's primary industry classification?	FY2021
Aerospace & defense	1%
Agriculture & food services	0%
Communications	2%
Construction and real estate	3%
Consumer goods	5%
Consumer products	2%
Education & research	3%
Entertainment, media and publishing	0%
Financial services	17%
Healthcare	10%
Industrial/manufacturing	8%
Logistics and distribution	0%
Pharmaceuticals	5%
Public sector	10%
Retailing	9%
Services	8%
Technology & software	8%
Transportation	7%
Other	2%
Total	100%

D4. What range best describes the full-time headcount of your global organization?	FY2021
Less than 1,000	18%
1,000 to 5,000	20%
5,001 to 10,000	21%
10,001 to 25,000	20%
25,001 to 75,000	12%
More than 75,000	9%
Total	100%

Survey response of business managers	FY2021
Total sampling frame	16,525
Total returns	674
Rejected or screened surveys	57
Final sample	617
Response rate	3.7%

Part 3. Survey of business managers: screening question

S1. In the last year, have you moved your workspace from a traditional office to your home due to COVID-19?	FY2021
Yes	60%
No	40%
Total	100%

Q1. Approximately what percentage of your time is spent working in your home vs. going to a coffee shop, shared workspace, or other place outside your home?	FY2021
Home 100%	23%
Home 75%; Out of home 25%	24%
Home 50%; Out of home 50%	20%
Home 25%; Out of home 75%	17%
Out of home 100% (Please skip to Q3)	16%
Total	100%

Q2. Where in your home is your primary workspace set up? Select all that apply.	FY2021
Kitchen	53%
Bedroom	29%
Dining room	15%
Common room (family room, living room, tv room, etc.)	43%
Home office	56%
Hallway	5%
Other	2%
Total	203%

Q3. Does your primary workspace organically allow you to prevent others, including family members or roommates, from seeing your work?	FY2021
Yes	34%
No	66%
Total	100%

Q4. Do you ever feel concerned when displaying sensitive/confidential data on your screen when you're working remotely? Please use the ten-point scale from 1 = not concerned to 10 = very concerned.	FY2021
1 to 2	5%
3 to 4	18%
5 to 6	34%
7 to 8	26%
9 to 10	17%
Total	100%
Extrapolated value	6.14

Q5a. Do you ever take steps or make adjustments to prevent others from viewing your screen when working remote?	FY2021
Yes	45%
No	55%
Total	100%

Q5b. If yes, what steps do you take to shield your device screen from prying eyes?	FY2021
Turn the screen	67%
Leave the room	54%
Use a privacy screen filter	31%
Nothing	33%
Other	2%
Total	187%

Q6. Did your company increase its enforcement of its privacy policies since more employees have been working remotely?	FY2021
Yes	40%
No	52%
Unsure	8%
Total	100%

Q7a. Since working remotely, how much more time do you think you're spending in front of your device screen?	FY2021
0-10%	5%
10-20%	7%
20-30%	18%
30-40%	21%
40-50%	17%
50-60%	9%
60-70%	7%
70-80%	5%
80-90%	6%
90-100%	5%
Total	100%
Extrapolated value	44%

7b. If time has increased by more than 30%-40%, are you experiencing any of the following symptoms? Please select all that apply.	FY2021
Headaches	54%
Tired eyes	46%
Messy or damaged screen	43%
Chronic neck and back pain	62%
Sleep problems	50%
Other	3%
None of the above	25%
Total	283%

Q7c. What actions have you taken? Please select all that apply.	FY2021
I've purchased blue light glasses	27%
I've purchased a privacy screen	34%
I've purchased a new glasses prescription	31%
I started taking regular walks	42%
I started meditating	26%
I started setting an alarm to end screen time	36%
Other	3%
Total	199%

Q8. What device do you primarily use while working remotely due to COVID-19? Select all that apply.	FY2021
Laptop / Notebook Computer	72%
Tablet	48%
Cell phone	36%
Monitor	31%
Other	4%
Total	191%

Q9. Is this device a company-provided device or personal device?	FY2021
Company-provided	45%
Personal	33%
Using combination of personal and company-provided	22%
Total	100%

Q10. What kind of accessories have you needed for your primary device since starting to work remotely? Select all that apply.	FY2021
Webcam	64%
Headset	61%
Screen privacy filter	32%
Screen protector	27%
Mouse/Keyboard	36%
Ergonomic workstation	43%
Docking station	36%
Charger	38%
Case	19%
Other	2%
Total	358%

Q11a. Who is your primary contact at your company to obtain accessories for your devices?	FY2021
IT department employee (please skip to Q12)	46%
IT manager (please skip to Q12)	42%
My manager (please skip to Q12)	51%
A co-worker (please skip to Q12)	47%
Department administrator / office manager (please skip to Q12)	35%
I order online via company approved website	60%
I buy on my own and get reimbursed when approved	37%
I buy and pay for my own accessories	44%
Other	0%
Total	362%

Q11b. If you bought accessories yourself, where did you get them?	FY2021
Online retailer like Amazon	50%
Big box store like Target or Best Buy	41%
Office supply store like OfficeMax	46%
Company office supply portal	39%
Other	2%
Total	178%

Q12. Post-COVID-19, which of the following would you like to do? Please select one choice only.	FY2021
Go back to the office	47%
Stay working remotely	41%
Hybrid of the two	12%
Total	100%

Q13. Post-COVID-19, which of the following will your employer expect you to do? Please select one choice only.	FY2021
Go back to the office	41%
Stay working remotely	49%
Hybrid of the two	10%
Total	100%

Q14. Pre-COVID-19, how often did you travel for business? Please use the 1 to 10 scale from 1 = not often to 10 = very often.	FY2021
1 to 2	7%
3 to 4	16%
5 to 6	26%
7 to 8	28%
9 to 10	23%
Total	100%
Extrapolated value	6.38

Q15a. Post-COVID-19, how comfortable will you be when traveling for business? Please use the ten-point scale from 1 = not comfortable to 10 = very comfortable.	FY2021
1 to 2	6%
3 to 4	14%
5 to 6	23%
7 to 8	31%
9 to 10	26%
Total	100%
Extrapolated value	6.64

Q15b. If you are not comfortable (a response between 1 and 5) why? Please select all that apply.	FY2021
I am concerned about becoming ill	62%
Wearing a mask during the flight is unpleasant	69%
I don't want to risk making others ill	57%
I don't want to be forced to be vaccinated if it is mandated	68%
I don't want to be required to have a COVID-19 test before I fly if it is mandated	56%
Other	2%
Total	314%

Role and organizational characteristics of business managers

D1. What best describes your position level within the organization?	FY2021
Business owner	6%
C-level executive/VP	9%
Director	14%
Manager	23%
Supervisor	15%
Staff/technician	25%
Administrative	4%
Consultant/contractor	2%
Other	2%
Total	100%

D2. Which of the following functions do you report to in your current role?	FY2021
Business owner/board	8%
CEO/executive committee	3%
COO or head of operations	7%
CFO, comptroller or head of finance	9%
CIO or head of corporate IT	21%
Business unit leader or general manager	20%
Head of compliance or internal audit	7%
Head of risk management	9%
Head of IT security	13%
Other	3%
Total	100%

D3. What best describes your organization's primary industry classification?	FY2021
Aerospace & defense	1%
Agriculture & food services	1%
Communications	3%
Construction and real estate	2%
Consumer goods	5%
Education & research	2%
Entertainment, media and publishing	3%
Financial services	18%
Healthcare	8%
Industrial/manufacturing	10%
Pharmaceuticals	4%
Public sector	10%
Retailing	9%
Services	10%
Technology & software	11%
Transportation	3%
Other	0%
Total	100%

D4. What range best describes the full-time headcount of your global organization?	FY2021
Less than 1,000	19%
1,000 to 5,000	21%
5,001 to 10,000	23%
10,001 to 25,000	18%
25,001 to 75,000	11%
More than 75,000	8%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.