

# How Enterprises Are Assessing Cybersecurity Risk in Today's Environment

The adoption of cloud services spurred by the COVID-19 pandemic has resulted in pressure on cyber-risk professionals to focus on vulnerabilities and new exposures that stem from pandemic-driven changes.

- 4 About the Author
- 5 Executive Summary
- 7 Research Synopsis
- 8 Cloud and COVID-19 Elevate Enterprise Cyber-Risk
- 11 Endpoint Security and Other Risk Factors
- 15 Complexity and the Risk Assessment Challenge
- 20 Conclusion
- 21 Appendix

**Figures**

- Figure 1: Use of Cloud Services
- Figure 2: Biggest Cybersecurity Challenges
- Figure 3: Top Security Threats
- Figure 4: Likely Causes of Future Major Breach
- Figure 5: Cloud Services Security Concerns
- Figure 6: Aspects of COVID-19 Crisis Contributing to Increased Risk
- Figure 7: Organizations’ Cybersecurity Strategies and Processes
- Figure 8: Top Endpoint Security Concerns
- Figure 9: Security Breaches Over Past Year
- Figure 10: Effects of Supply Chain Attacks
- Figure 11: Threat of Russian Cyberattackers
- Figure 12: Effectiveness of Technologies
- Figure 13: Vulnerability to Security Breaches
- Figure 14: Reasons for Increased Vulnerability
- Figure 15: Respondent Job Title
- Figure 16: Respondent Industry
- Figure 17: Respondent Company Size
- Figure 18: Respondent Company Revenue

## INTRODUCING Vulcan Free

The industry's only free cyber risk prioritization tool!

TRY VULCAN FREE





## About the Author

**Jai Vijayan**

Dark Reading

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He specializes in writing on information security and data privacy topics. He was most recently a Senior Editor at Computerworld. He is a regular contributor to Dark Reading, CSO Online, and TechBeacon.

SUMMARY  
EXECUTIVE

Enterprises have ramped up adoption of cloud services over the past 12 months to support the shift to a more distributed work environment and online-first business models spurred by the COVID-19 pandemic. The accelerated transition has affected the cyber-risk profile at many organizations in a major way and increased pressure on decision-makers to heighten their focus on cloud vulnerabilities and new exposures from pandemic-driven changes.

Dark Reading asked 150 IT and security decision-makers about current threats, data breach risks, their organization's preparation for security incidents, and how they assess cybersecurity risks in the current environment. Survey respondents included individuals who identified themselves as CIO, CTO, CSO, CISO, and IT director from organizations across more than 18 industries, such as healthcare, manufacturing, financial services, manufacturing, government, and utilities.

The results revealed substantial concern over cloud-related risks. A high percentage are uncertain about the ability of their cloud providers to detect a data breach, the increasing number of exploits targeted at cloud providers, and the growing number of intrusions into cloud environments. Many are concerned that the increased use of cloud services has made their organization more vulnerable to a data breach compared with a year ago.

IT and security decision-makers are taking many other factors into account as they assess risk for the coming year. These include COVID-19-related issues such as remote-access risks, endpoint vulnerabilities, and pandemic-themed social engineering attacks. Many expect fundamental, long-term changes to their organization's computing and data security strategies because of trends related to the pandemic, such as the shift to more remote work and accelerated cloud adoption. A high percentage are struggling to minimize threats from ransomware actors, nation-state groups, vulnerabilities in the supply chain, and users with legitimate access to enterprise systems and data.

A substantial percentage of organizations are continuing to struggle with technology complexity, policy enforcement, risk assessments, and raising user awareness on cybersecurity matters. Even so, most IT and security decision-makers are confident that they have effective measures for assessing their security posture and about their organization's preparedness to respond to a data breach. Changes related to the COVID-19 crisis continued to be a major contributor to elevated enterprise cyber-risk but at a smaller percentage of organizations compared with a year ago.

Here are some key data points from the survey:

- 75% of IT and security decision-makers expect that the effects of the COVID-19 pandemic will fundamentally change the computing and data security strategies of their organization for the long term.
- 40% say pandemic-related phishing and social engineering attacks have heightened enterprise risk over the last 12 months.
- 46% are uncertain whether their cloud service providers can detect a breach affecting customer data in their environment.
- 16% of survey respondents perceive their organization as being more vulnerable to a data breach compared with a year ago.
- 35% of respondents see complexity as the biggest information or network security challenge facing the company. Policy enforcement (28%) and risk assessments (24%) are two major areas of concern.
- 76% of survey respondents say their organization has an effective method for measuring their current security posture.
- 58% of respondents describe cybercriminals as posing the biggest threat to enterprise data. Forty percent point to authorized users or employees as the threat they feared most.
- 23% of organizations are covered for cybersecurity breaches under a broader business insurance policy.



## ABOUT US

*Dark Reading Reports* offer original data and insights on the latest trends and practices in IT security. Compiled and written by experts, Dark Reading Reports illustrate the plans and directions of the cybersecurity community and provide advice on the steps enterprises can take to protect their most critical data.

### Dark Reading Reports

# SYNOPSIS

**Survey Name:** Dark Reading 2021 Strategic Security Survey

**Survey Date:** August 2021

**Number of Respondents:** 150 technology and cybersecurity professionals at companies of all sizes from a variety of industries. The margin of error for the total respondent base (N=150) is +/-7.9 percentage points.

**Methodology:** The survey queried decision-makers with job titles that involve IT or IT security (cybersecurity) at organizations across more than 18 industry sectors. One-third (33%) have director or head job titles on the IT or security side; 14% have CIO, CTO, CSO, or CPO titles. The survey was conducted online. Respondents were recruited via email invitations containing an embedded link to the survey. The email invitations were sent to a select group of Informa Tech’s qualified database; Informa is the parent company of Dark Reading. Informa Tech was responsible for all survey design, administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

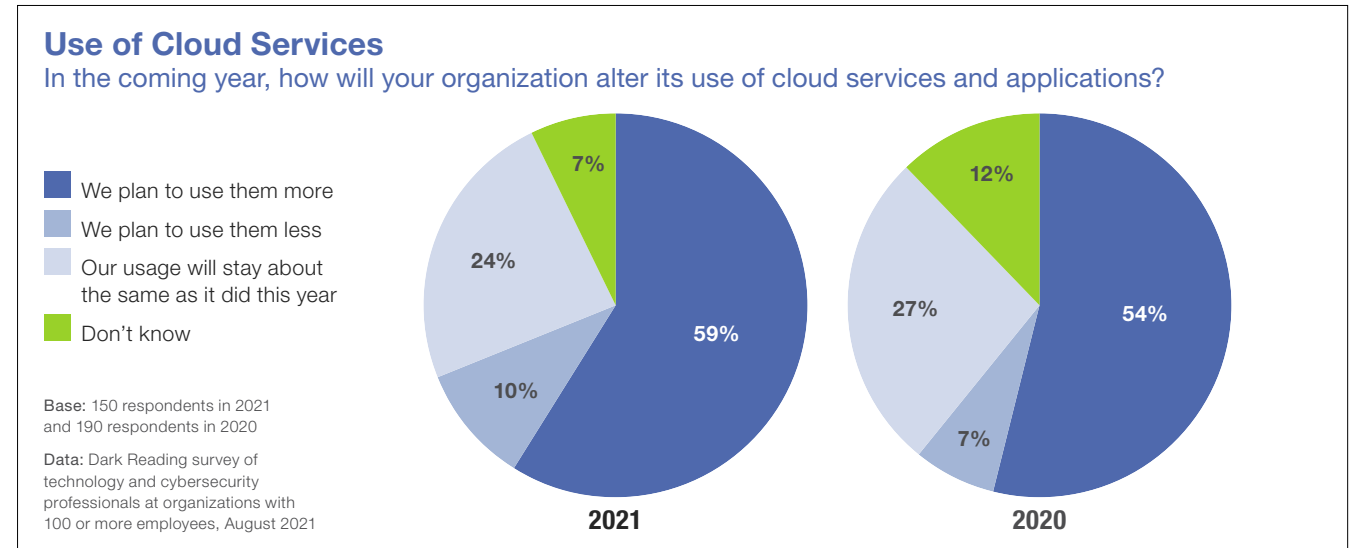
## Cloud and COVID-19 Elevate Enterprise Cyber-Risk

Cloud security concerns and vulnerabilities tied to pandemic-driven changes have become key considerations in enterprise cyber-risk management strategies. Over the past 12 months, many organizations have ramped up adoption of cloud services to support remote workforces and ensure resilient business operations. The cloud became a critical enabler of digital transformation initiatives as many organizations switched to an online-first operating model.

Dark Reading's 2021 Strategic Security Survey shows that 59% organizations plan to use more cloud applications and services in the coming year (**Figure 1**). Gartner expects [worldwide spending](#) on public cloud services by such companies will grow more than 23% in 2021, from \$270 billion last year to \$332 billion, with the pandemic serving as a "multiplier for CIOs' interest in the cloud."

The accelerating shift away from on-premises infrastructures has significantly raised the level of cyber-risk associated with cloud services for many technology leaders. Twenty-four percent now perceive cloud data

**Figure 1.**



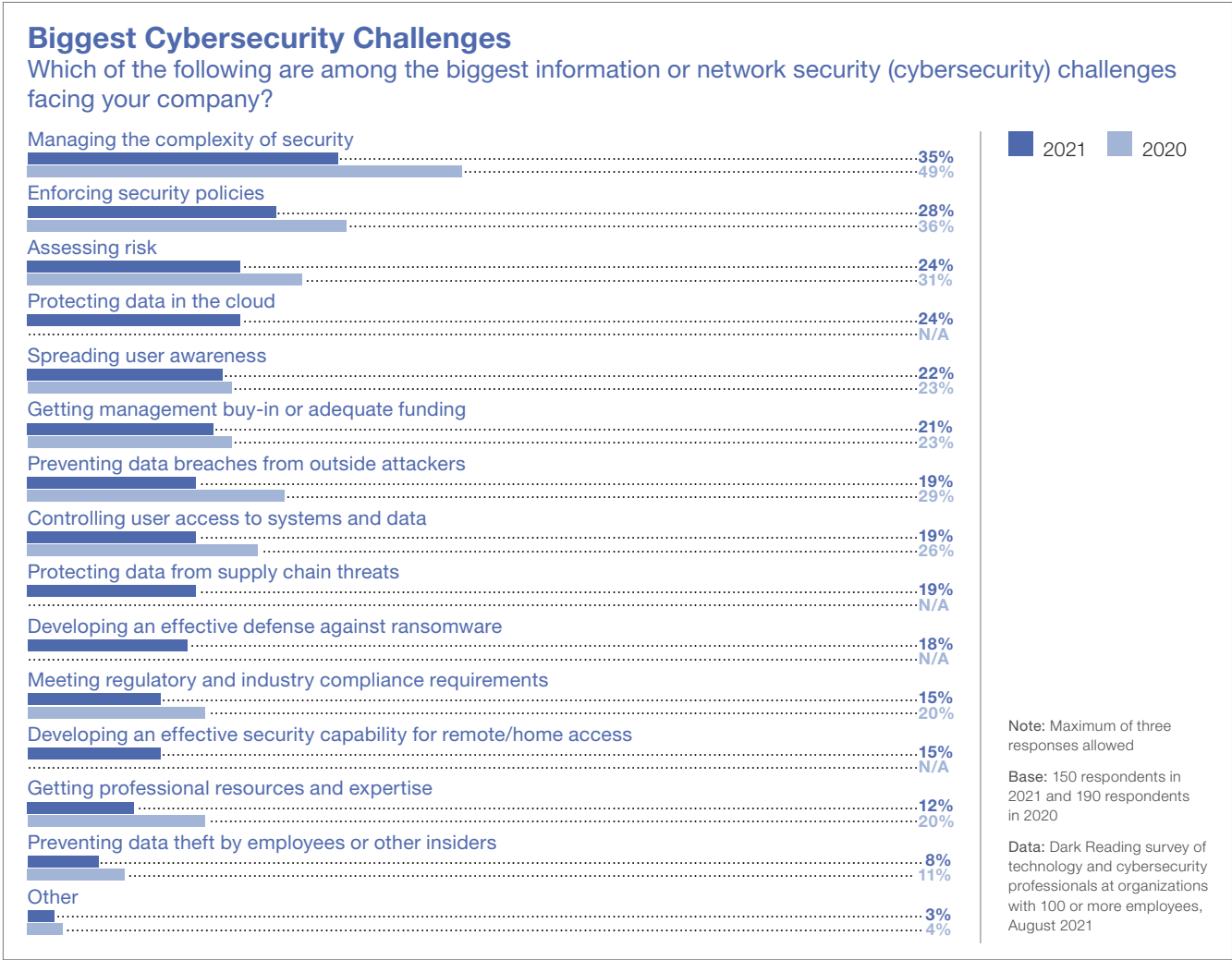
protection as one of their top information security challenges (**Figure 2**), and 18% perceive cloud providers as the biggest threat to enterprise data (**Figure 3**). Nearly a quarter (23%) of IT and security managers are convinced that if their organization experiences a data breach in the coming year, the primary reason for it will be a security failure at their cloud or Web services provider (**Figure 4**). As one Dark Reading survey taker notes, the pandemic caused many ad hoc changes that have not been holistically vetted. "Since many new services are cloud based, but by different providers, alignment of these

services will be extremely challenging."

Concerns are particularly high about the security preparedness of cloud service providers and the growing threats targeting the environment. Forty-six percent of respondents, for instance, are uncertain about the ability of their cloud provider to detect a data breach that affects enterprise data — up sharply from the 36% that expressed a similar concern in our 2020 survey (**Figure 5**). Forty-two percent — compared with just 30% last year — are spooked about the growing number of cloud security intrusions, and 37% are worried



Figure 2.



(24%). None of these issues are new. But they have assumed much greater significance with enterprises rapidly moving more of their workloads to the cloud in the past year.

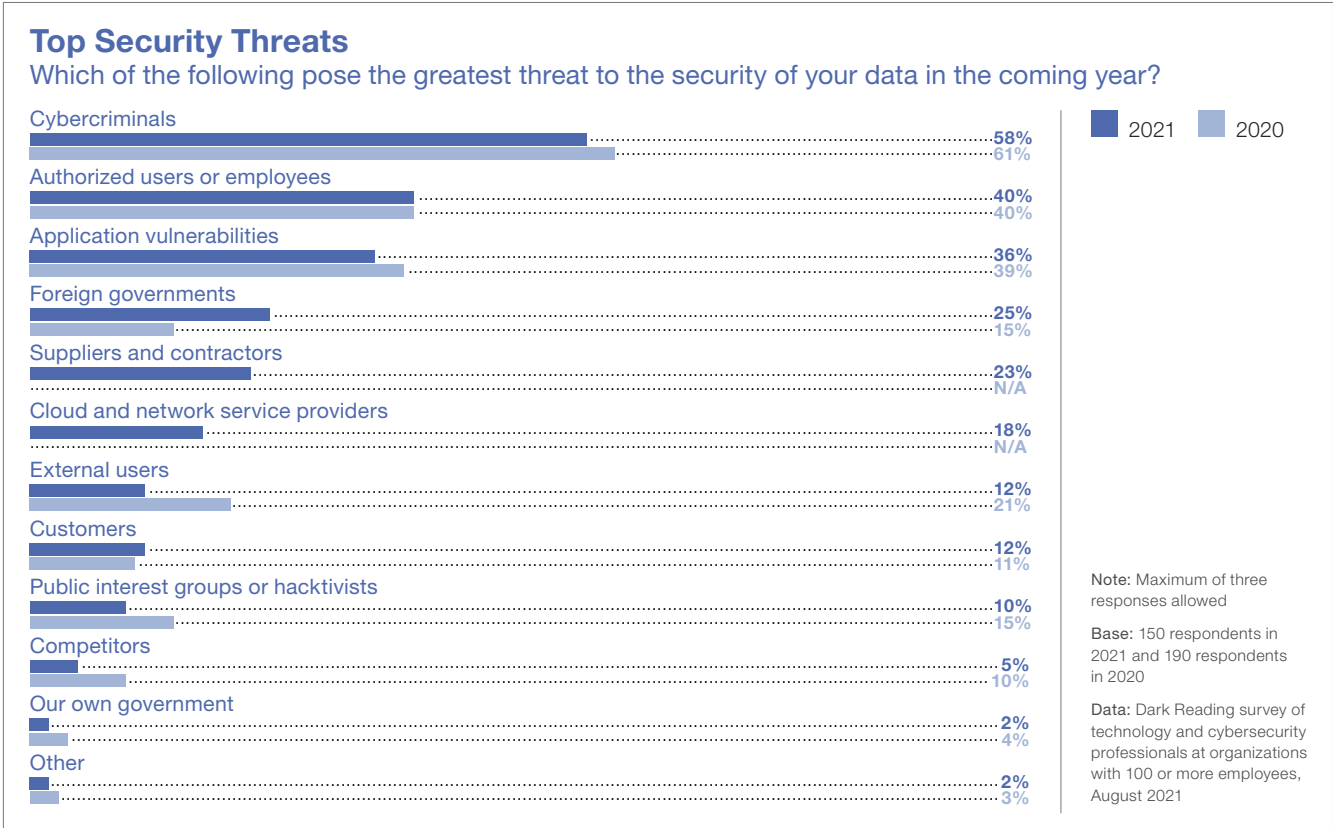
The uncertainty over cloud security that survey respondents express appears to be the direct result of the number of cloud security incidents over the past year. A survey of 200 IT managers that analyst firm [IDC](#) conducted for Ermetic found 98% of organizations had experienced a cloud-related breach in the past 12 months, up from 79% in 2020. More than two-thirds (67%) experienced three or more cloud breaches, and 63% had sensitive data compromised in these incidents. Other analyst firms have reported a similar increase in cloud security incidents.

The COVID-19 pandemic elevated enterprise cyber-risk in other ways as well in 2021. Nearly two years into the crisis, many organizations still have their hands full dealing with pandemic-themed social engineering scams and malware, vulnerabilities in remote access infrastructures and endpoints, and with new digital services or business models that create additional risk. There

about the increasing number of exploits targeting cloud service providers. Concerns are similarly high over a lack of visibility over enterprise data in the cloud (37%), the inability

to enforce enterprise security policies on data stored via cloud services (33%), and the willingness of cloud providers to work with enterprises in the event of a data breach

Figure 3.



were numerous reports throughout the year of cybercriminals and state-sponsored advanced persistent threat actors using pandemic-themed domains, emails, and text messages to distribute malware that would steal credentials and carry out other malicious activities. However, it is a smaller percentage of respondents that identified these factors as

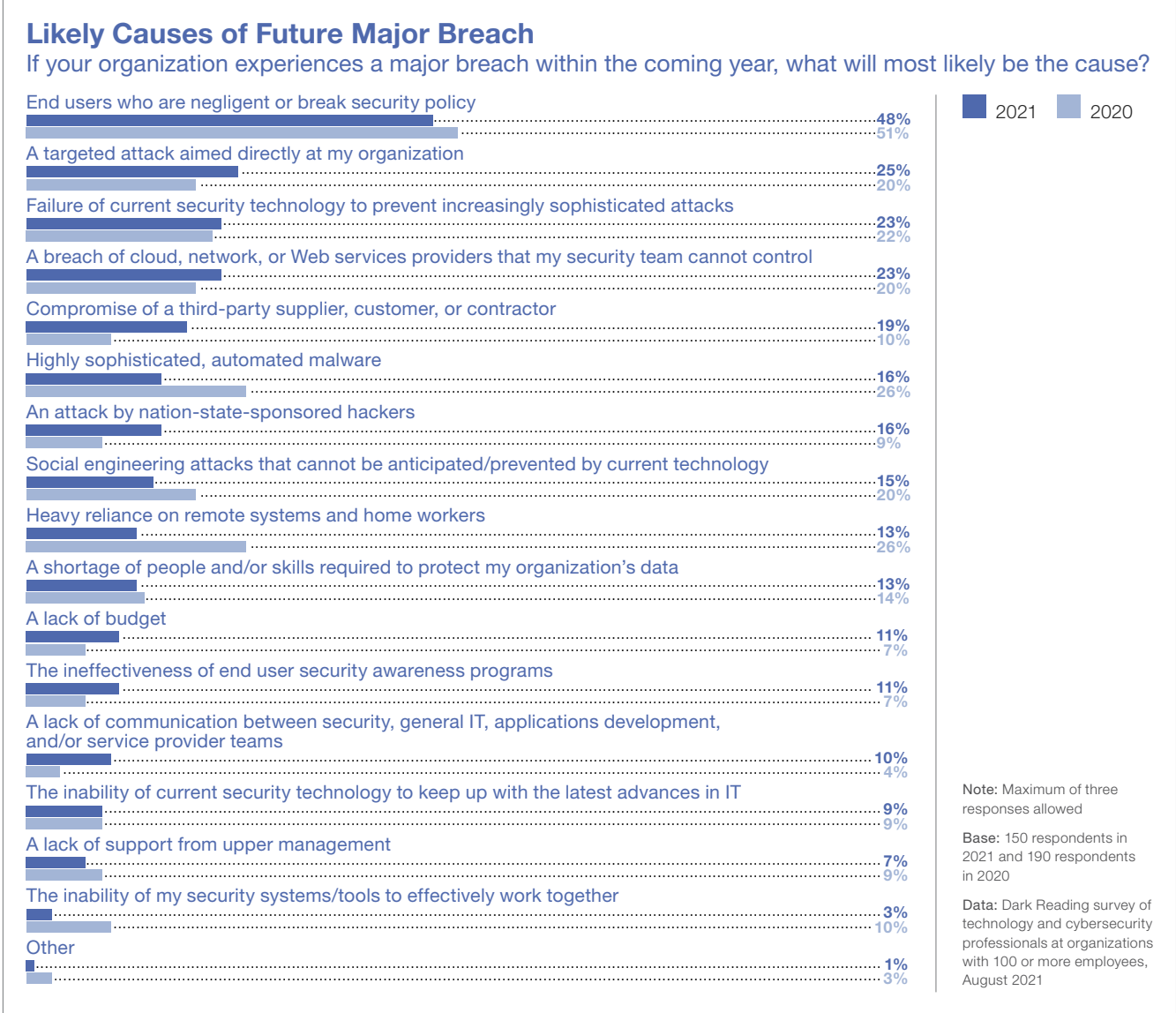
elevating cyber-risk when compared with a year ago.

For instance, just 40% of respondents describe pandemic-themed phishing campaigns as heightening cyber-risk in Dark Reading’s 2021 survey, down from 52% last year (Figure 6). Similarly, fewer respondents

this year, 34%, identify vulnerabilities in remote access systems as elevating cyber-risk, compared with 39% last year, and just 25% are worried about quarantined workers using insecure devices, down from the 38% concerned about the issue last year. Vulnerabilities in service provider connections used by quarantined home workers were a concern for 17% of respondents this year, down from 24% in 2020. The data suggests that an encouraging percentage of enterprise security teams made headway in addressing new risks stemming from the sudden change in work and business environments stemming from the pandemic.

At the same time, Dark Reading’s survey shows that most respondents — 75% — now also believe that the IT changes they implemented because of the pandemic will fundamentally change their organization’s cyber-risk profile and data security strategies over the long term (Figure 7). The sentiment likely stems from the growing realization among technology leaders that some pandemic-driven changes — such as the broad adoption of remote work models — are here to stay. A survey of 439 US employers

Figure 4.



that [XpertHr](#) conducted this year showed that 72% plan on offering a hybrid part-remote, part-office-based work option for employees once the pandemic has passed.

Endpoint Security and Other Risk Factors

Cloud- and pandemic-related issues had a big impact on enterprise cyber-risk profiles in the last 12 months. But these were certainly not the only risks that enterprise security groups had to manage.

Dark Reading’s survey shows that endpoint security remains a big concern for IT and risk leaders because of the continued attacker focus on users and the devices they use to access enterprise networks and data. Phishing attacks continued to be the most visible manifestation of this trend, with 58% of respondents citing it as their primary endpoint security risk (**Figure 8**) and 53% of organizations having experienced at least one phishing-related security incident over the past year (**Figure 9**). The data points are consistent with findings from other studies, such as Verizon’s “[2021 Data Breach Investigations Report](#),” which showed phishing was present in 36% of the breaches

Figure 5.



the company investigated in 2020 — an increase of 11% from the year before. Of the 3,841 phishing incidents that Verizon investigated, 1,767 involved confirmed data disclosure.

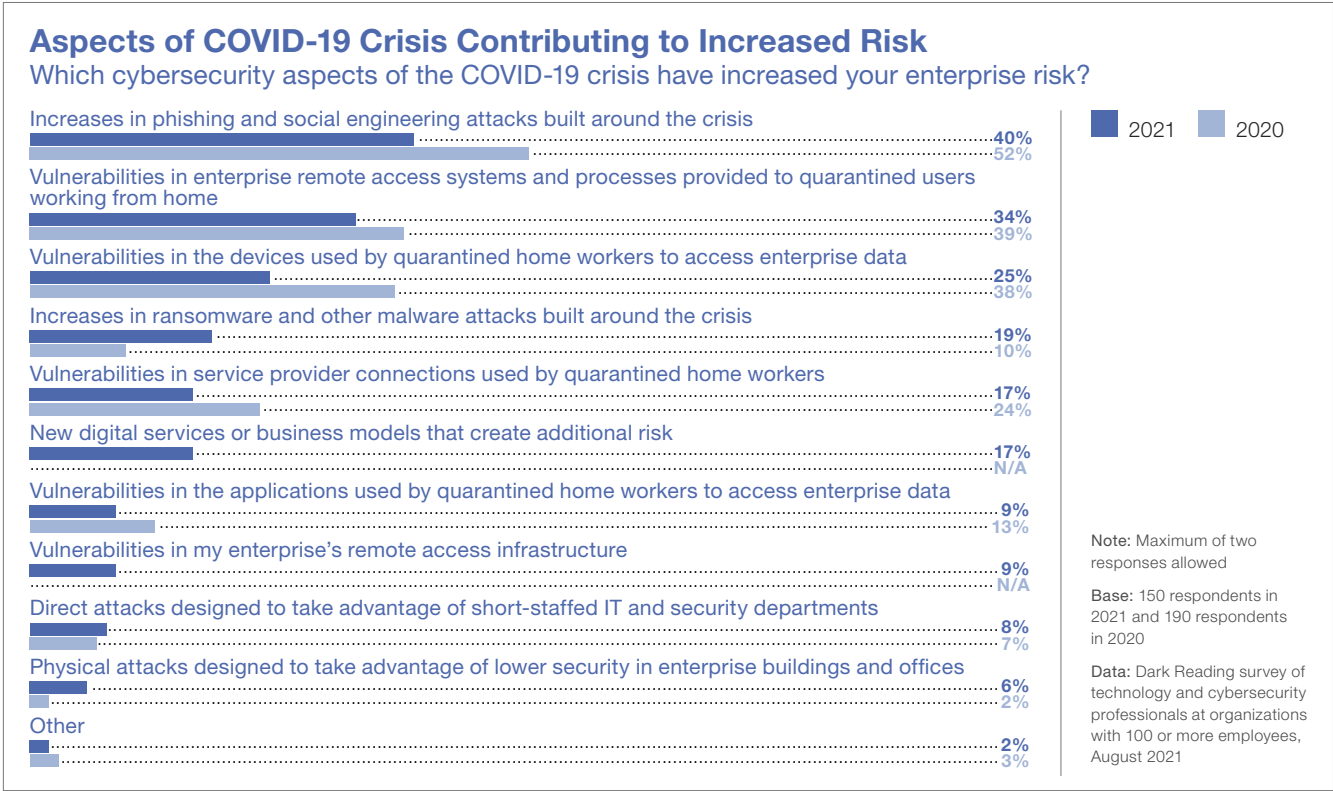
Forty-two percent of enterprise security pros express concern about attackers compromising devices used by remote and home workers to gain access to enterprise data. Twenty-five percent are worried about infected user devices connecting to the

corporate network and putting enterprise data at risk. Both issues have become major concerns for enterprise risk managers because of an explosion in the use of personal and unmanaged devices among workers since the pandemic forced a shift to remote work. A study that [CyberEdge](#) conducted last October found the percentage of companies that permitted employees to use personal devices to access company applications soaring from 42% before the pandemic to 66% in a matter of months.

As has been the case for some time, the human element continues to be a big contributor to enterprise cyber-risk in other ways as well. One example: users who unwittingly download malware on their systems because of negligence and/or poor cyber hygiene. More than a quarter (27%) of security and IT managers are concerned about the threat from this vector, and 41% of organizations experienced at least one malware breach in the last 12 months. Nineteen percent are keeping a wary eye for users who encounter identity theft or bank account fraud via a corporate-issued device.

Enterprise security managers are not just looking at attack and compromise vectors when assessing cyber-risk. They are also concerned about the actors behind the attacks and their motivations. Dark Reading's survey shows that most security and IT professionals (58%) consider financially motivated cybercriminals — such as ransomware operators — as posing the greatest threat to data security. One big reason appears to be high-profile incidents such as the ransomware attack on Colonial Pipeline in May that caused temporary

Figure 6.



gas shortages along the US East Coast and another on JBS Meats that spawned concerns about meat supply disruptions. Seventy percent of Dark Reading survey respondents describe the incidents as significantly elevating concerns about ransomware.

Some breaches that were disclosed over the

past 12 months, such as one that SolarWinds disclosed last December and another at Kaseya, stirred broad concerns about risks to enterprise security from vulnerabilities in the technology supply chain. In both attacks, threat actors used products belonging to the respective vendors to distribute malware on systems belonging to their downstream customers. Forty-eight percent

of respondents in Dark Reading’s survey are implementing changes in the way they audit and monitor their suppliers because of these attacks (**Figure 10**). Another 30% would like to make similar changes but don’t wield enough influence to change the behavior of their supply chain partners.

The fact that many of these attacks were carried out by nation-state-backed threat actors — particularly from Russia and China — also has put foreign governments on the radar of more enterprise risk managers than ever. Twenty-five percent of them now consider foreign governments as affecting their risk profile — up from 15% last year, and 59% believe that Russian actors pose a threat to their specific organization (**Figure 11**). Their concerns were likely fueled by warnings from the US government of threat actors from Russia carrying out supply chain attacks and cyber-espionage campaigns against US targets and of the Chinese government using criminal hackers to break into US organizations. One survey respondent describes both Russia and China as having “highly advanced teams of scientists, military, and other state-sponsored teams dedicated

Figure 7.

Organizations’ Cybersecurity Strategies and Processes

Please rate your agreement with the following statements.

	Strongly agree	Agree	Disagree	Strongly disagree	Don't know
My organization has an effective method for measuring the current state of its security posture	13%	63%	18%	2%	4%
I believe the effects of the COVID-19 pandemic will fundamentally change my organization's computing and data security strategies for the long term	18%	57%	17%	4%	4%
The attacks on Colonial Pipeline and JBS have significantly increased my organization’s concerns about ransomware	15%	55%	17%	8%	5%
I believe that my organization’s cybersecurity staff are stretched too thin, which may result in burnout and/or increased risk to critical data	28%	42%	22%	5%	3%
My organization has an effective method for measuring the effectiveness/performance of its security department	17%	47%	29%	4%	3%
I believe my organization has an effective long-term strategy for protecting data security handled by home users	19%	44%	25%	6%	6%
I believe my organization will have to respond to a major data breach or compromise in the coming year	18%	44%	16%	5%	17%
I believe my organization is well-prepared to respond to a major data breach in the coming year	16%	44%	27%	5%	8%
I am confident that my organization has an effective strategy for response to a ransomware attack.	14%	45%	26%	5%	10%
I believe my organization has an effective process for measuring the cybersecurity risk that my organization will face in the coming year	11%	48%	29%	5%	7%
Supply chain attacks such as SolarWinds and Kaseya have significantly decreased my confidence in my organization’s supply chain security	13%	37%	34%	10%	6%
Since the SolarWinds attack, my organization has initiated significant changes in its approach to supply chain security	3%	43%	32%	9%	13%

Data: Dark Reading survey of 150 technology and cybersecurity professionals at organizations with 100 or more employees, August 2021



Figure 8.



to disrupting American and other democracies by any means possible.”

Significantly, security leaders continue to perceive users with trusted access to enterprise systems as posing the next biggest risk to enterprise data after cybercriminals. Forty percent — the same percentage as last year — identified end users as posing the greatest threat to enterprise data security in the 2021 survey,

and 48% believe that if their organization experiences a data breach in the next year, an end user will be responsible for it.

The opinion is almost certainly colored by the numerous breaches that have resulted in recent years from a lack of end-user awareness, negligence, and errors. Just one example: phishing attacks that end with the user downloading malware on their systems. Growing incidents of attackers using stolen

or leaked employee credentials to access enterprise networks are likely another factor contributing to the high level of concern around end users. One study earlier this year found a doubling in the number of annual incidents involving credential compromise between 2016 and 2020.

Organizations should embed “security into the user’s daily functions without making it so cumbersome that people view it as an inconvenience to be worked around rather than an essential tool in running day to day business,” one survey taker says.

“I sincerely believe that the zero-trust initiatives will have to be enforced” to minimize risk from end users and their devices, another respondent notes.

**Complexity and the Risk Assessment Challenge**

Organizations have deployed a wide range of technologies to manage enterprise cyber-risk. The controls include those for protecting against breaches, such as next-generation firewalls, anti-malware tools, and email filtering products, and those for detecting and mitigating the impact of a

Figure 9.

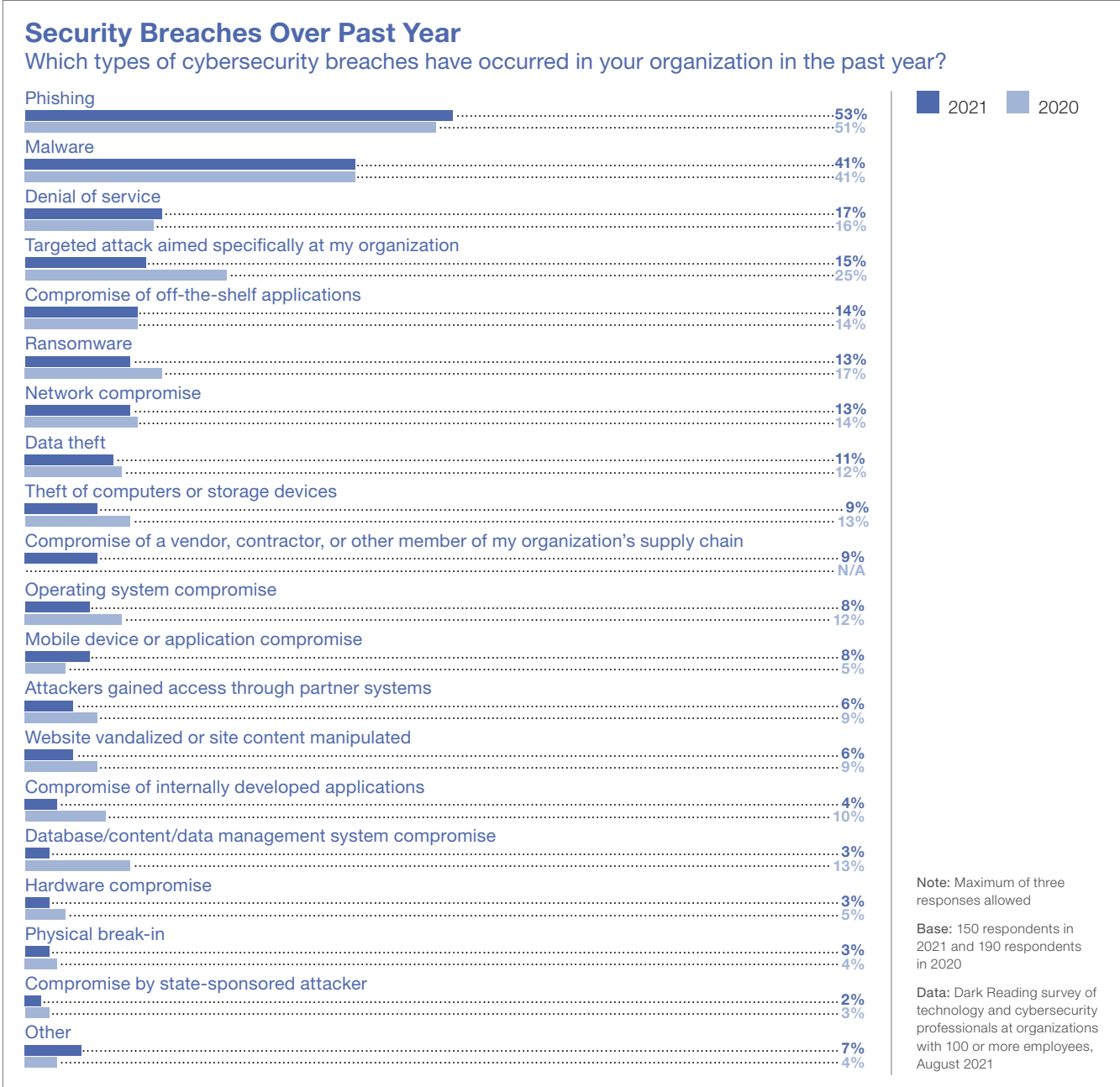


Figure 10.

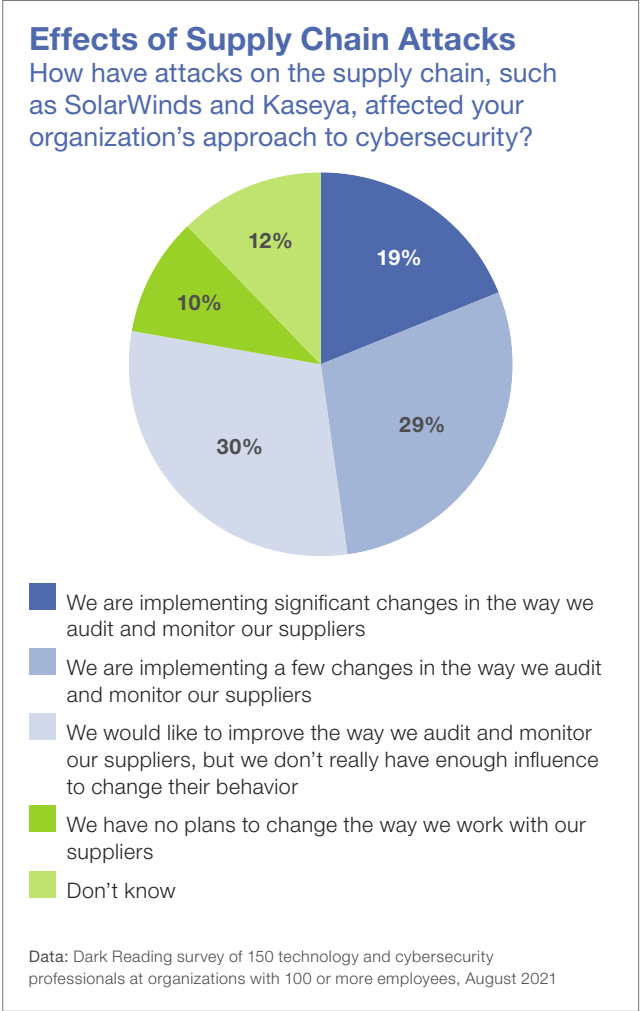
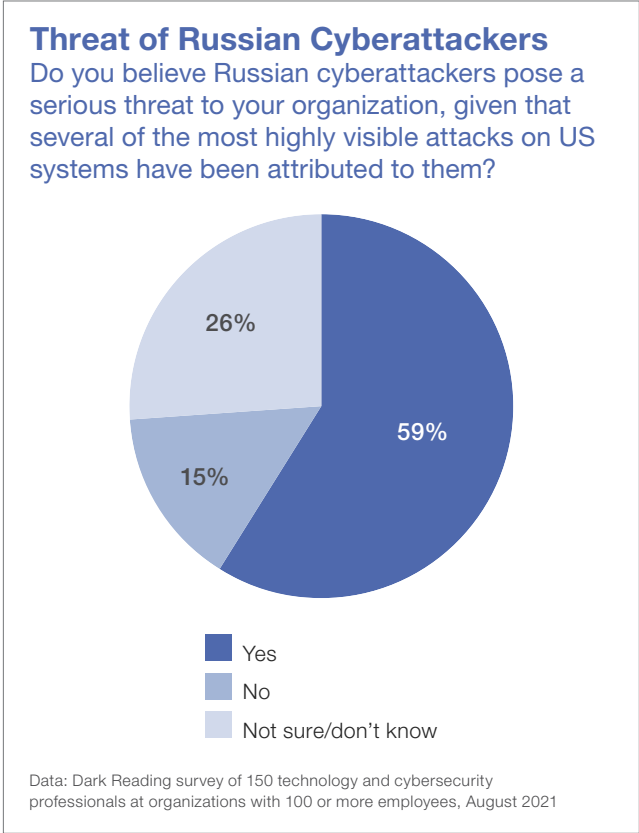


Figure 11.



data breach. Controls in this latter category include intrusion detection systems, endpoint detection and response products, and data encryption tools.

Many organizations have also implemented a range of security best practices to mitigate risk, including multifactor authentication, malware analysis, strong passwords, and

end-user awareness and training. Sixty-nine percent rate controls for vulnerability assessment and penetration testing as effective or highly effective, and 53% say the same about their usage of external threat intelligence service (Figure 12).

Collectively, the security controls and best practices have engendered a sense of confidence in IT and security managers about their organization’s cyber-risk management capabilities. More than three-quarters (76%) believe they can measure their current security posture in an effective manner, and 64% say their organization has an effective method for measuring the effectiveness of the cybersecurity group. Most (63%) also believe their organization has an effective long-term strategy for protecting data handled by home users and for responding to a major data breach.

Despite the apparent confidence in security controls and processes, enterprise risk managers also appear pragmatic about the realities of the current threat landscape. Sixty-two percent, for instance, expect they will have to respond to a major data breach in the next 12 months. Half of respondents have

lost confidence in their company’s ability to mitigate supply chain risks, and 16% believe their organization is more vulnerable to a data breach than a year ago (Figure 13). The most common reasons for the increased were growing attack volumes (67%), increasing threat sophistication (56%), rapid growth of ransomware (56%), and shortage of skilled workers (56%) (Figure 14). Each of these factors has had a major impact on enterprise cyber-risk for the past several years.

Complexity, policy enforcement and risk assessment continue to pose big challenges for IT and security risk managers as well. When asked to identify their organization’s biggest security challenges, 35% point to the complexity of security technology, 28% cite problems enforcing security policies, and 24% have problems assessing cyber-risk. The angst likely stems from changes related to the COVID-19 pandemic. For instance, security analysts have noted how the shift to remote and hybrid cloud environments has added layers of complexity to the enterprise technology environments and made policy enforcement far more challenging for enterprise security managers. Thirty-three

Figure 12.

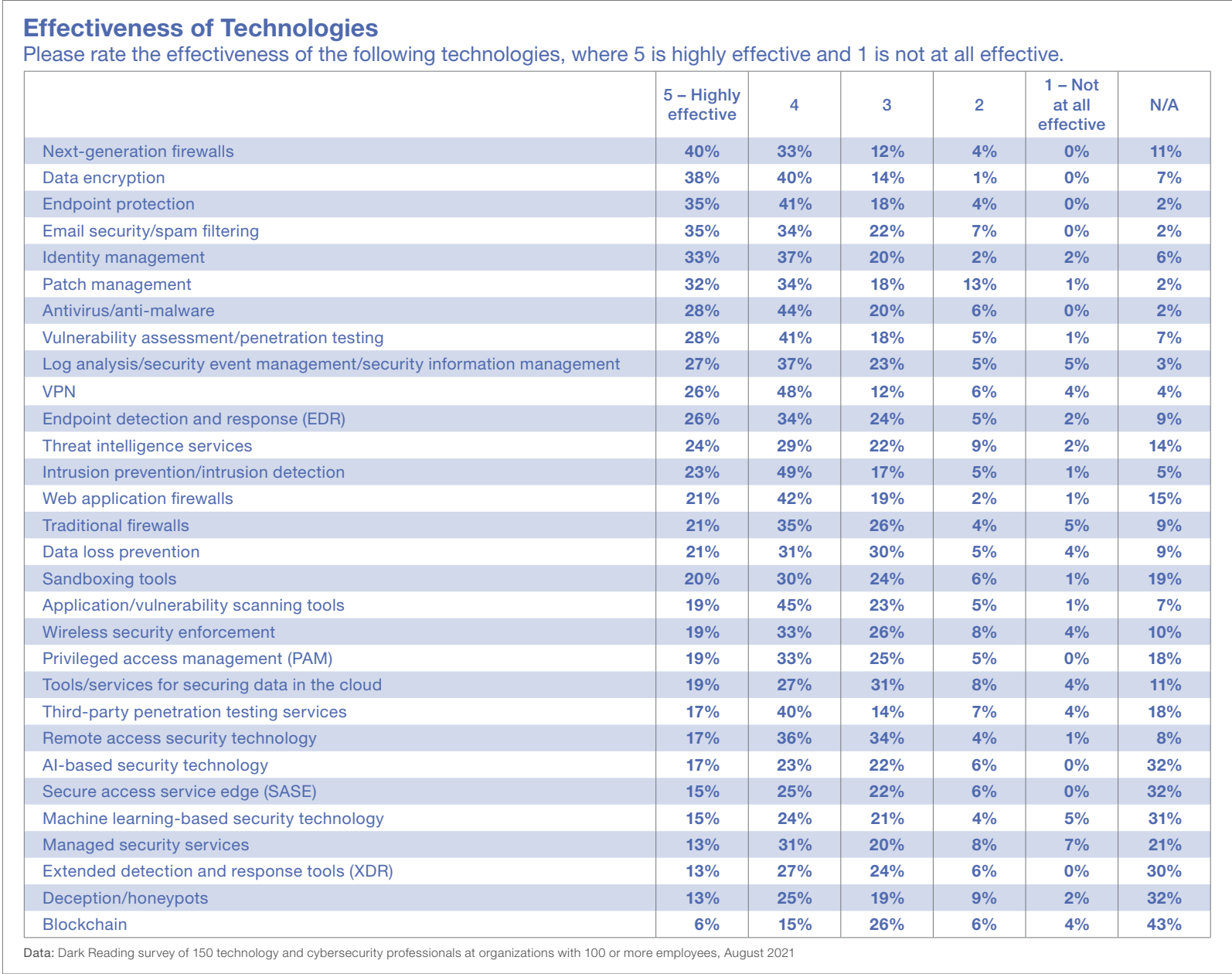


Figure 13.

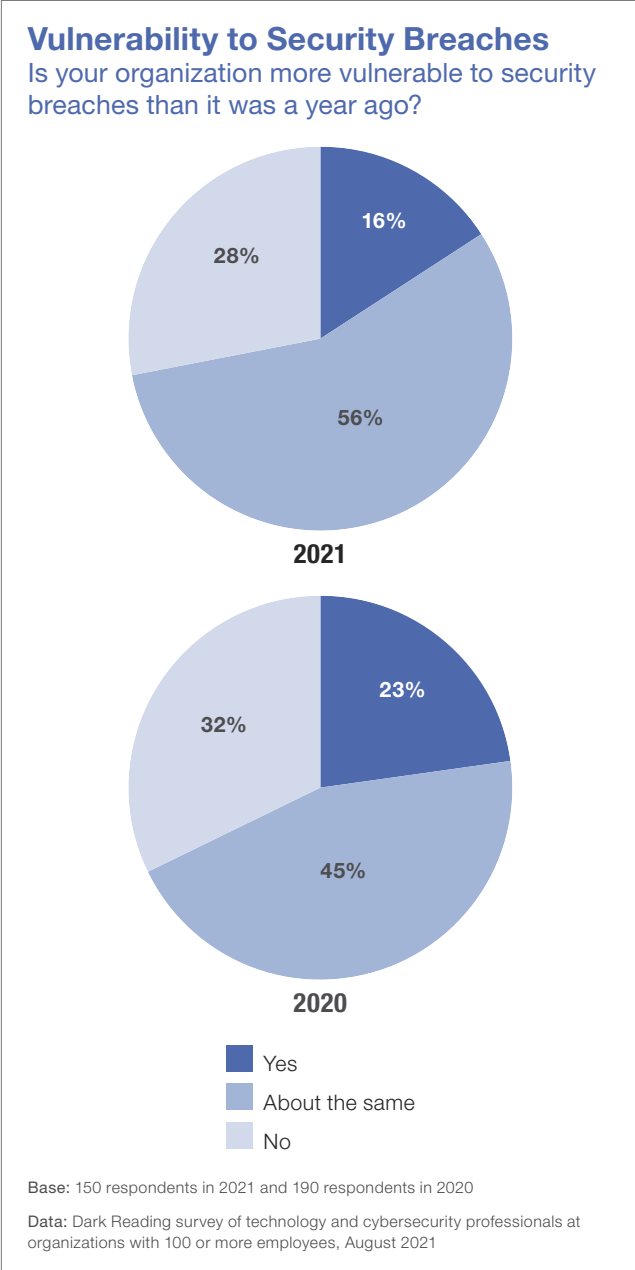
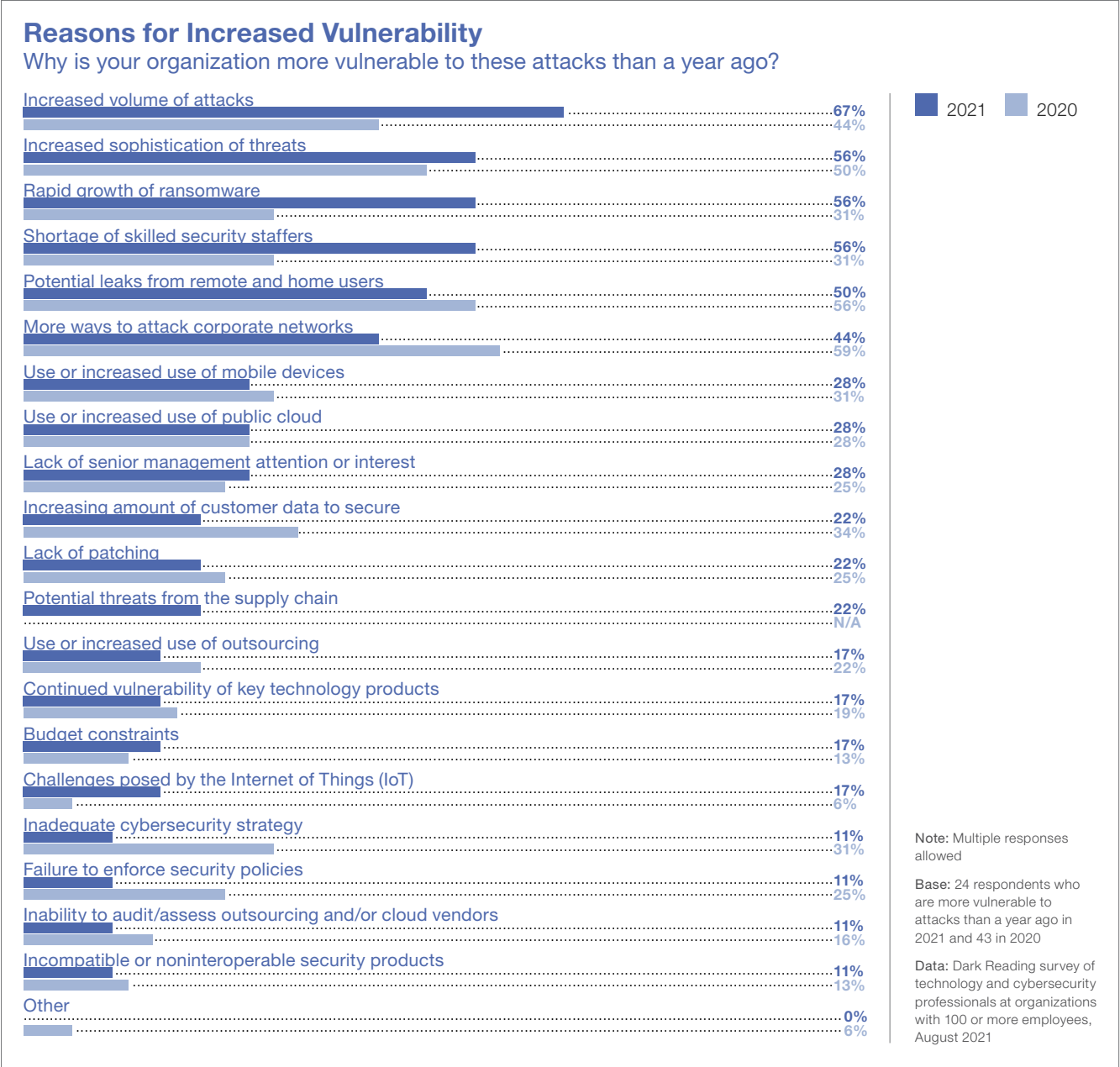


Figure 14.



percent are concerned about their inability to enforce my organizational security policies on data stored via cloud services.

Similarly, the growing adoption of cloud services and a distributed work model have made risk assessment harder. In addition to evaluating risks to on-premises systems, IT and security managers must now assess risk from remote users, home networks, and devices and to data scattered across a variety of on-premises and public cloud systems. As previously noted, 37% of security pros are concerned about a lack of visibility — and therefore control — over enterprise data stored in the cloud or transmitted via cloud services.

**Conclusion**

The rapid adoption of cloud services to support new workplace and business requirements because of the COVID-19 pandemic has had a significant effect on enterprise cyber-risk postures. The trend has exacerbated existing concerns over cloud security risks and lent greater significance to strategic issues such as policy enforcement, asset visibility, shared responsibility, and the willingness of major cloud providers to work with customers on security matters.

In responding to the new risks, security leaders must also contend with risks from a broad range of other — more familiar — factors such as phishing, ransomware, malware, and end users with privileged access to networks and data. Concerns are high about risks to enterprise data from cybercriminals, end users, ransomware operators, and foreign governments.

Enterprises have deployed a broad range of controls and policies for breach protection, detection, and response. A high percentage of security pros are confident in their ability to respond to a major security incident and believe they have a good handle on their organization’s risk posture. Even so, many expect a major breach in the next year because of increased attack volumes and growing threat sophistication.



Figure 15.

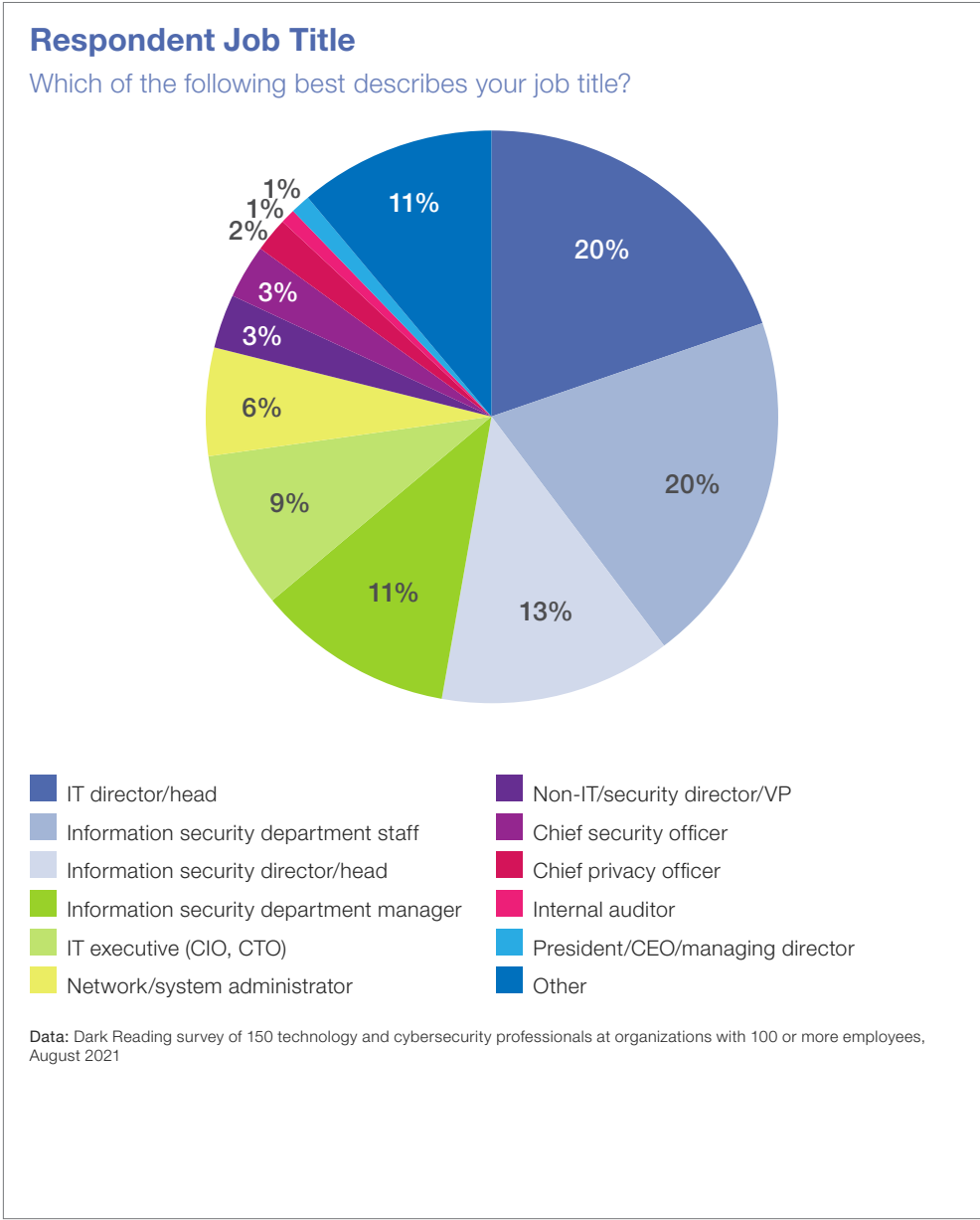
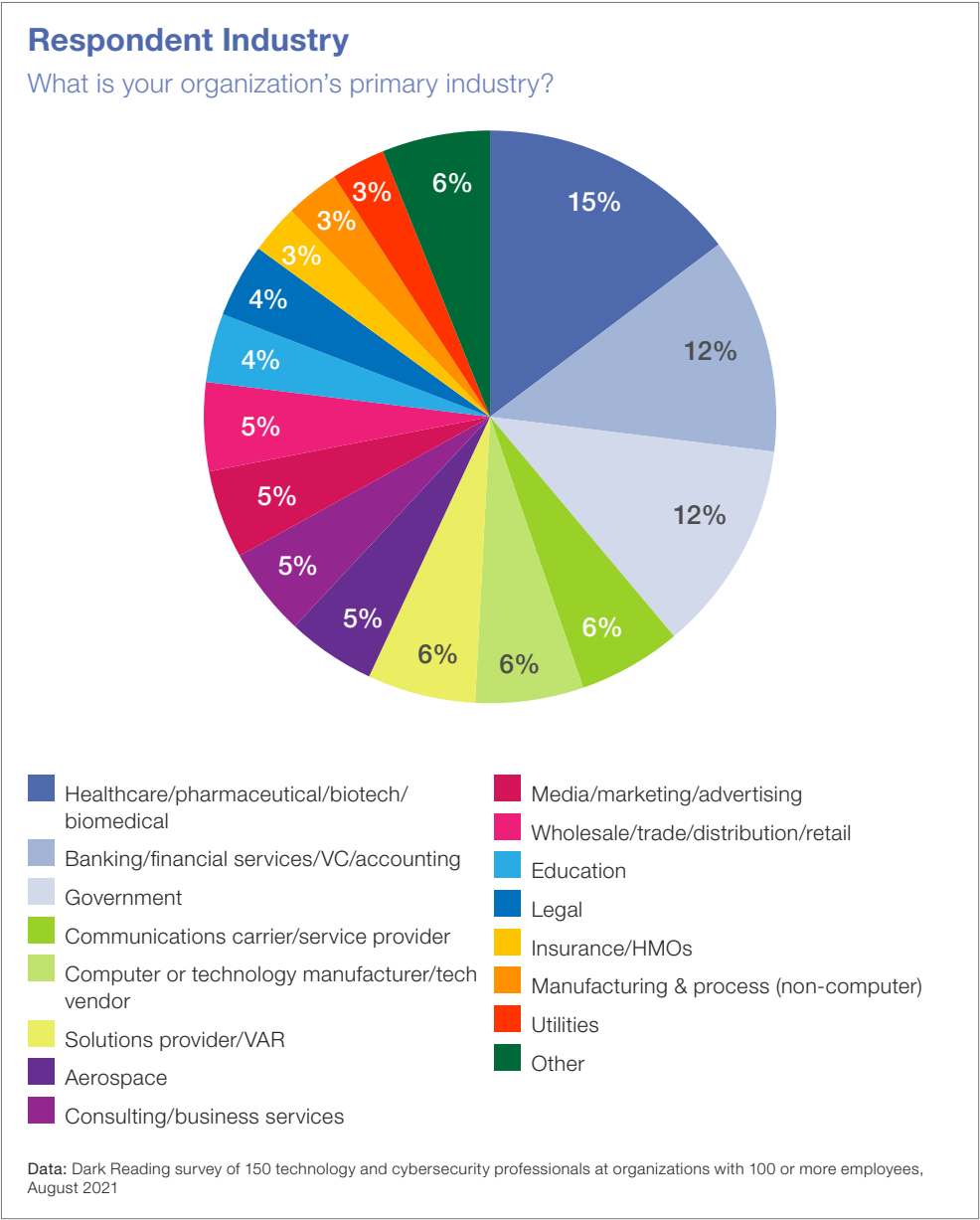




Figure 16.



Like this report?  
**Share it!**

 [Tweet](#)

 [Follow](#)


 [Share](#)

Figure 17.

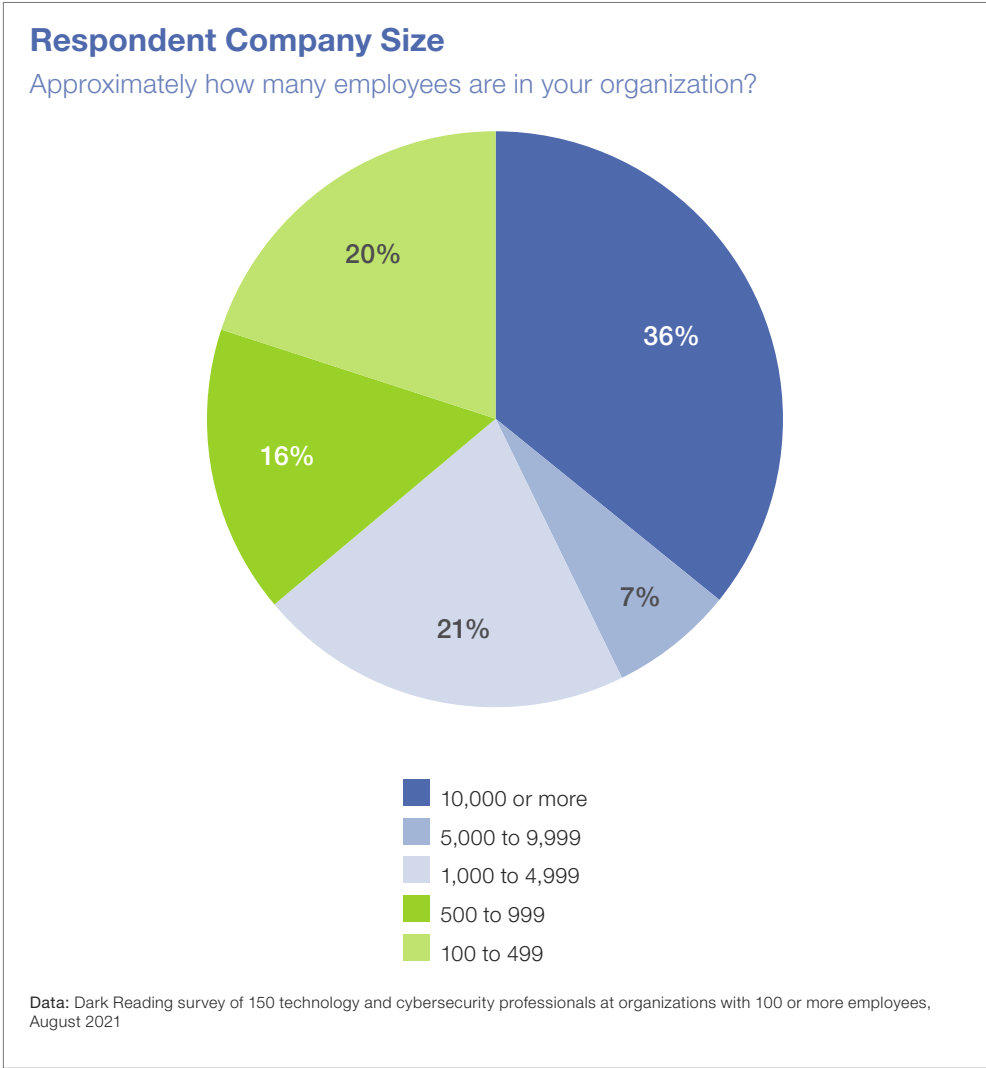


Figure 18.

