black hat® USA 2022

www.blackhat.com

July 2022

The 2022 Black Hat USA Attendee Survey

Supply Chain and Cloud Security Risks Are Top of Mind

Black Hat attendees are not sleeping well. Between concerns about attacks against cloud services, ransomware, and the growing risks to the global supply chain, these security pros have a lot to be worried about.

169100_DR22

TABLE OF CONTENTS

Table of Contents

Figures

EXECUTIVE SUMMARY

Looking back, it's clear that 2021 was the year of supply chain. Average consumers probably never even stopped to think about where the different parts for their automobiles and electronics came from until supply chain issues suddenly made delivery times obscenely long and prices soared. Droughts in one part of the world resulted in shortages in certain foodstuffs in other parts of the globe. Supply chain was suddenly something everyone could understand and have firsthand experience with.

The cybersecurity industry had its own share of supply chain woes in 2021 as security professionals scrambled to understand the scope of the SolarWinds attack and saw widely used applications and platforms be compromised. Remediation of the Log4j vulnerability spilled over into 2022, and as pandemic restrictions ease, security professionals are now faced with the challenge of securing a sprawling IT landscape with cloud services and third-party services mixed in with their own assets.

We polled past attendees of the annual Black Hat USA conference — among the most sophisticated and technical IT security researchers and professionals in the industry — to gain some insights into what may be in store for the remainder of 2022 and the coming year. In a survey of 180 top security professionals from a wide variety of industries, we found that cybersecurity experts have serious concerns about the safety of commercial applications and that ransomware attacks continue to be disruptive. They worry about new attacks as they shift even more of their application workloads to the cloud.

The survey, which has been conducted annually since 2015, interviewed current and former attendees of the Black Hat USA conference, one of the cybersecurity industry's most prestigious and technically deep conferences. Among the survey respondents were top executives, CISOs, CIOs, CTOs, security specialists, and researchers from organizations in more than 20 sectors, ranging from financial services to healthcare to

government. More than half (59%) hold the CISSP security certification; many respondents also hold other certifications, including CompTIA Security (36%), CEH (30%), and MCSE (23%).

The 2022 Black Hat Attendee Survey asked security professionals to offer their insights on the current state of cybersecurity following recent attacks targeting critical infrastructure and software supply chain. We asked about the potential implications of disinformation campaigns, which affected the vaccine rollout for COVID-19 and the Russian invasion of Ukraine. We asked questions about the long-term effects of the changes caused by the COVID-19 pandemic, including the rapid pace of digital transformation and the rise of remote and hybrid work. Finally, security professionals offered insights into what it's like to work in the industry.

The survey results suggest that the world's top cybersecurity professionals are widely concerned that the rapid shift to digital business models and remote work poses significant risk to corporate data. They believe that disinformation campaigns will leave the political realm and target enterprises. And on top of it all, the overworked and overstressed security workforce is fast nearing burnout.

Among the key findings of the 2022 Black Hat USA Attendee Survey:

- A majority (59%) of respondents say they believe the threat of ransomware to their organizations has increased in the last two years; 81% say they would not pay the ransom.
- 44% of Black Hat attendees believe that government and private industry are adequately prepared to respond to critical infrastructure attacks, double what was said in the 2021 survey.
- 34% of respondents are concerned about vulnerabilities in off-the-shelf software or systems purchased from third parties. Just 26% say the same about vulnerabilities in commercial software or cloud services introduced by the use of open source components.
- 61% are less confident about the security of commercial applications, but 69% have processes in place to audit and test the security of open source components used in their environment.

- The changes to business models made during the COVID-19 pandemic has made organizations more reliant on cloud services and other external service providers (46%) and increased threats from cyberattackers seeking to exploit remote workers and systems (43%).
- 72% of cybersecurity professionals believe they will have to respond to a major cybersecurity incident in their own organization in the next 12 months. In 2021, this figure was 73%, up from 70% in 2020, and 65% in 2019.
- A little over half (53%) of Black Hat attendees say it is likely that disinformation attacks will leave the political arena and start targeting enterprises.
- Despite concerns about ransomware and attacks targeting cloud services and supply chain, phishing remains the No. 1 threat for organizations.
- Cybersecurity professionals are mentally exhausted, with a little less than half expressing some form of mental burnout.
- The majority of security professionals consider multifactor authentication tools (87%) and encryption (80%) to be highly effective. Passwords and mobile security tools, not so much.

ABOUT US

For more than 20 years Black Hat has provided attendees with the very latest in information security research, development, and trends. These high-profile global events and training are driven by the needs of the security community, striving to bring together the best minds in the industry. More information is available at: http://www.blackhat.com.

SYNOPSIS

RESEARCH

Survey Name 2022 Black Hat USA Attendee Survey

Survey Date May 2022

Primary Region North America

Number of Respondents 180 IT and security professionals. The greatest possible margin of error for the total respondent base (N=180) is +/-7.3 percentage points. Informa, the parent company of Black Hat, was responsible for all aspects of survey administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

Purpose To gauge the attitudes and concerns of one of the IT security industry's most experienced and highly trained audiences: attendees of the Black Hat USA conference.

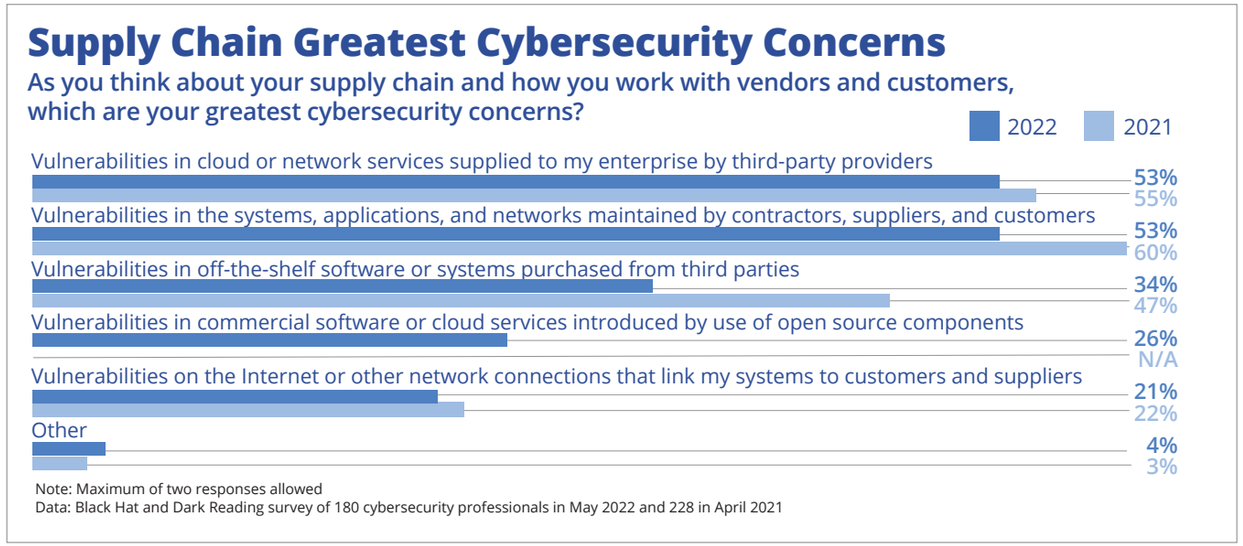
Methodology In April and May 2022, Black Hat and Informa researchers conducted a survey of IT and security professionals who attended the Black Hat USA conference in 2021 and/or were planning to do so in 2022. The online survey yielded data from 180 management and staff security professionals, predominantly at large companies, with 55% working at companies with 1,000 or more employees. They are also well-credentialed, as 59% of the respondents hold the CISSP security professional credential, 36% hold a CompTIA security certification, and 30% are certified ethical hackers (CEH).

Threats Are Evolving as IT Environments Change

After years of warnings and alerts highlighting the risks, 2021 was the year organizations learned the various ways that the global supply chain could be abused to compromise a large number of victims. The compromised supply chain became reality in a very big way in late 2020, when researchers discovered that a Russia-backed group had successfully tampered with the network management software distributed by SolarWinds and compromised more than 18,000 enterprises and government agencies in an extremely sophisticated espionage operation. That was just the beginning, as 2021 turned into the Year of Supply Chain Attacks.

Attackers combined multiple vulnerabilities and a new Web shell targeting the file transfer application from Accellion (now known as Kiteworks) and successfully stole data belonging to 100 organizations. Attackers found a series of zero-day vulnerabilities that could be used to break into and steal all files from any Internet-accessible Exchange server. And then there was Log4j in December, with the discovery of a vulnerability in an open source software component present in practically every Java enterprise application, which could be used to take control of the application. The cleanup process to fix affected applications spilled over well in to 2022 and highlighted the difficulty of addressing flaws in a widely used application.

Figure 1



When asked to think about the supply chain and relationships with vendors and customers, 53% of respondents in the 2022 Black Hat Attendee Survey name vulnerabilities in cloud or network services supplied to their enterprise by third-party providers as their greatest cybersecurity concerns (**Figure 1)**. An equal number of respondents name vulnerabilities in the systems, applications, and networks that are maintained by contractors, suppliers, and customers. For 34% of respondents,

vulnerabilities in off-the-shelf software of systems purchased from third parties are in their top two concerns, and 26% are concerned the most about vulnerabilities in commercial software or cloud services introduced by open source components.

It's worth noting that in the 2021 Black Hat Attendee Survey, 60% were concerned about vulnerabilities in third-party systems and applications, 55% were worried about vulnerabilities in cloud or network services, and 47% were concerned about vulnerabilities in off-the-shelf software. The 2021 survey did not ask about open source components, which is why it appears that respondents were concerned in 2021 at higher numbers. What is clear is that for a sizable number of security professionals (61%), the vulnerabilities in Microsoft Exchange and other off-the-shelf applications shook their confidence in the security of off-the-shelf applications (**Figure 2**).

FAST FACT

53%

report vulnerabilities in cloud services by third-party providers is the top cybersecurity concern.

Figure 2

Vulnerabilities in the Supply Chain

Please tell us how strongly you agree or disagree with the following statements about vulnerabilities in the supply chain.

	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree
My organization has processes in place to audit/test the security of open source components used in our IT environment	25%	44%	20%	11%
With recent vulnerabilities in Microsoft Exchange and other off-the-shelf applications, my security team is now less confident about the security/integrity of commercial applications	17%	44%	31%	8%
My organization had a difficult time addressing the vulnerability in Apache Log4j library	10%	26%	38%	26%

Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals, May 2022

About half of the respondents (52%) in the survey have instituted changes in how the organization audits and tests the security of off-the-shelf and commercial applications, which is much lower than the 63% who said the same in 2021, right after the SolarWinds hack **(Figure 3**). It's notable that 16% in the 2022 survey believe their existing processes are sufficient — suggesting that the gap may be because some organizations put in the work to make those process improvements last year.

In the months since Log4j, it is reassuring that 69% of security professionals in the survey say their organization has processes in place to audit and test the security of open source components used in their environment.

Another area where security left the realm of possibility and became real? Critical infrastructure. For 94% of the respondents, attacks against Colonial Pipeline and JBS are proof that there already have been

cyberattacks against critical infrastructure in the United States (**Figure 4**). In the survey, 98% say critical infrastructure attacks are not the sole domain of nation-state actors and that a single attacker could also cause a major disaster in the United States. The pessimism is high, as 96% see industrial control systems and networks as outdated and vulnerable, and just 44% believe there is adequate coordination between government and private industry regarding critical infrastructure security.

The Pandemic's Impact Lives On

Computing and business models changed drastically during the COVID-19 pandemic as businesses rushed out new digital services and adapted corporate processes to accommodate a remote and hybrid workforce. These changes have an impact on enterprise security, as 43% of security professionals in the 2022 Black Hat Attendee Survey believe their organizations are more vulnerable to cyberattacks than before the pandemic (**Figure 5**). Nearly

Figure 3

New Processes for Auditing Off-the-Shelf Applications

Has your organization instituted new processes for auditing and/or testing the security of off-the-shelf applications in your organization's IT environment?

Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals in May 2022 and 228 in April 2021

Figure 4

Critical Infrastructure Beliefs

Please tell us how strongly you agree or disagree with the following statements about critical infrastructure security.

	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree
Critical infrastructure attacks aren't limited to just nation-states; a single attacker, or a politically motivated group, could also cause a major disaster in the US critical infrastructure	78%	20%	2%	0%
I believe many of our current industrial control systems are outdated and vulnerable to attack	69%	27%	4%	0%
I believe that attacks against Colonial Pipeline and JBS show that we've already had a successful cyberattack on the critical infrastructure of the United States	67%	27%	4%	2%
Enterprises should separate operational technology (OT) systems from IT systems	59%	28%	10%	3%
I believe that there is adequate coordination between government and private industry regarding security of US critical infrastructure	8%	36%	40%	16%

Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals, May 2022

three-quarters (72%) of the Black Hat attendees believe they will have to respond to a major cybersecurity incident in the next 12 months. And their overall worldview is especially grim: 87% say no matter how careful people are with their personal information and devices, it's likely that the data and credentials are already available to criminals.

Seventy-nine percent of security professionals believe the majority of work-from-home users will never go back to the office full-time, suggesting that these hybrid business environments will not go away anytime soon.

With pandemic restrictions easing, security teams are thinking about how to ensure the security infrastructure evolves to accommodate the new IT environment. When asked about the pandemic's most significant impacts on cybersecurity, the top three answers are new security requirements for remote workers (65%), greater reliance on cloud services and other external service providers (46%), and increased threats from attackers exploiting remote workers and remote system vulnerabilities (43%) (**Figure 6**). Another significant impact is the shift in focus away from perimeter-based defenses to broader tools such as attack surface management and cloud permissions (32%).

When asked which security challenges will be the most difficult in the next year, 60% say detecting attacks and threats in a decentralized and cloud-oriented IT environment, and 52% say finding security vulnerabilities in a decentralized and cloud-oriented IT environment (**Figure 7**). There are also concerns about training end

Figure 5

Cybersecurity Beliefs

Please tell us how strongly you agree or disagree with the following statements.

	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree
No matter how careful you are with your personal information and devices, it's likely that your data and/or credentials are available to criminals online right now	42%	45%	10%	3%
I believe that the majority of my work-from-home users will never go back to the office full time	41%	38%	16%	5%
I have no doubt that we will have to respond to a major cybersecurity incident in the next 12 months	28%	44%	28%	0%
The shortage of women and minorities in the information security profession is a concern to me	27%	35%	21%	17%
I believe it will be possible for individuals to protect their online identity and privacy at some point in the future	16%	40%	34%	10%
As a result of the global pandemic, my organization is more vulnerable to cyberattacks than ever before	14%	29%	42%	15%

Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals, May 2022

users on security awareness and policy when working remotely (21%) and redesigning the enterprise security architecture to accommodate the new models (21%).

A Focus on Supply Chain and Cloud

When asked about the threats and challenges of greatest concern today, 39% of Black Hat attendees in the survey cite phishing and other forms of social engineering; 35% say targeted sophisticated attacks; 28% say attacks on suppliers, contractors, or other partners connected to the organization's network; and 26% say potential compromise of cloud services providers (**Figure 8**).

When asked what threats and challenges would be of greatest concern two years from now, 28% say attacks on suppliers, contractors, or other partners; 27% say potential compromise of cloud services providers; 26%, phishing; and 24%, sophisticated attacks (**Figure 9**).

The shift to a decentralized network environment is shining a spotlight on supply chain

Figure 6

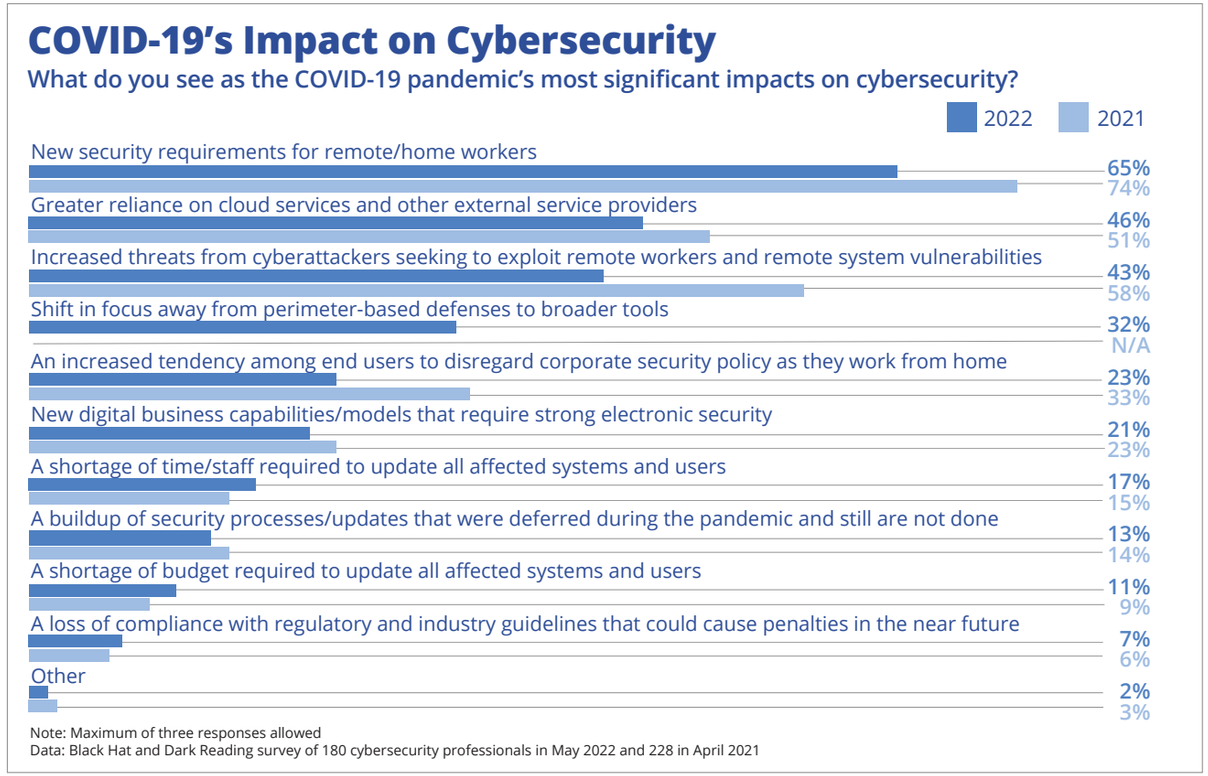
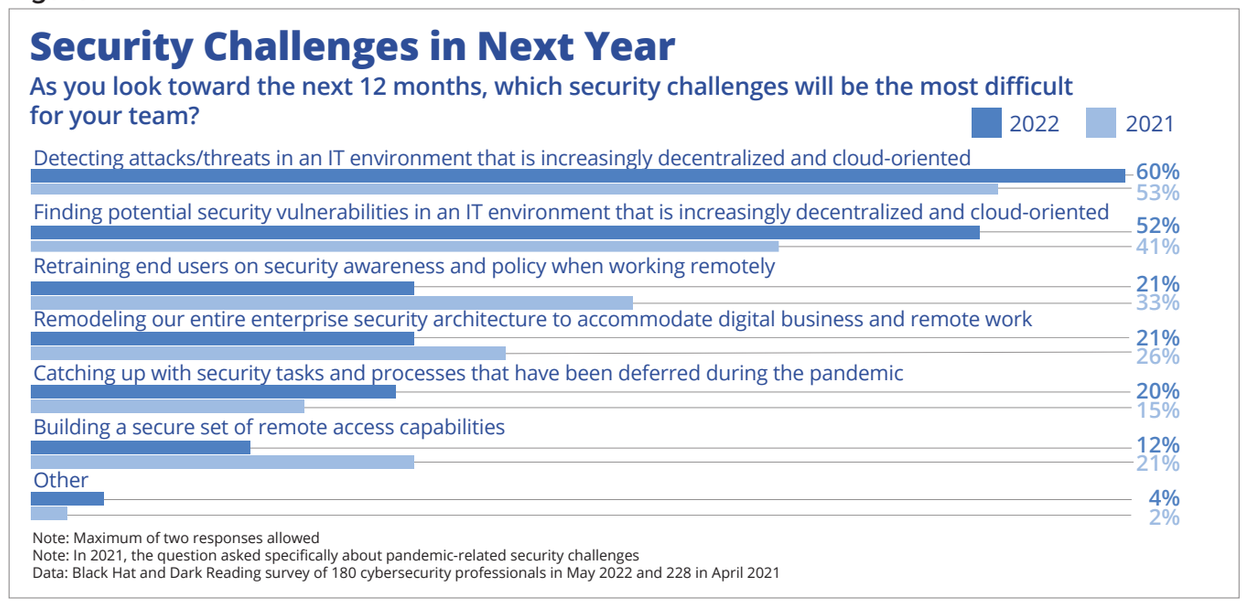


Figure 7



black hat USA 2022

risk and cloud security issues, and will likely be an issue for the next few years. This focus on supply chain and cloud services may be the reason why attacks on remote access tools and networks used by remote workers dropped in priority. In the 2021 survey, 27% cited attacks on remote access tools and networks used by remote workers, but only 15% in 2022 see that as a top concern.

Ransomware Demands Attention

Ransomware has been a scourge for enterprise security teams for years, but they have evolved from just encrypting data in exchange for ransom to sophisticated campaigns capable of destroying systems or wiping out data. The 2022 Verizon "Data Breach Investigations Report" (DBIR) found ransomware events are on the rise, with 25% of the breaches analyzed in the report containing a ransomware component. That concurs with the 2022 Black Hat Attendee Survey, in which 59% of respondents say they believe the ransomware threat to their organizations increased, not decreased, over the past two years (**Figure 10**). In fact, just 8% say ransomware attacks have decreased over the past two years.

FAST FACT

96%

say their team has been able to successfully block or minimize the impact of ransomware attacks in the past year.

Figure 8

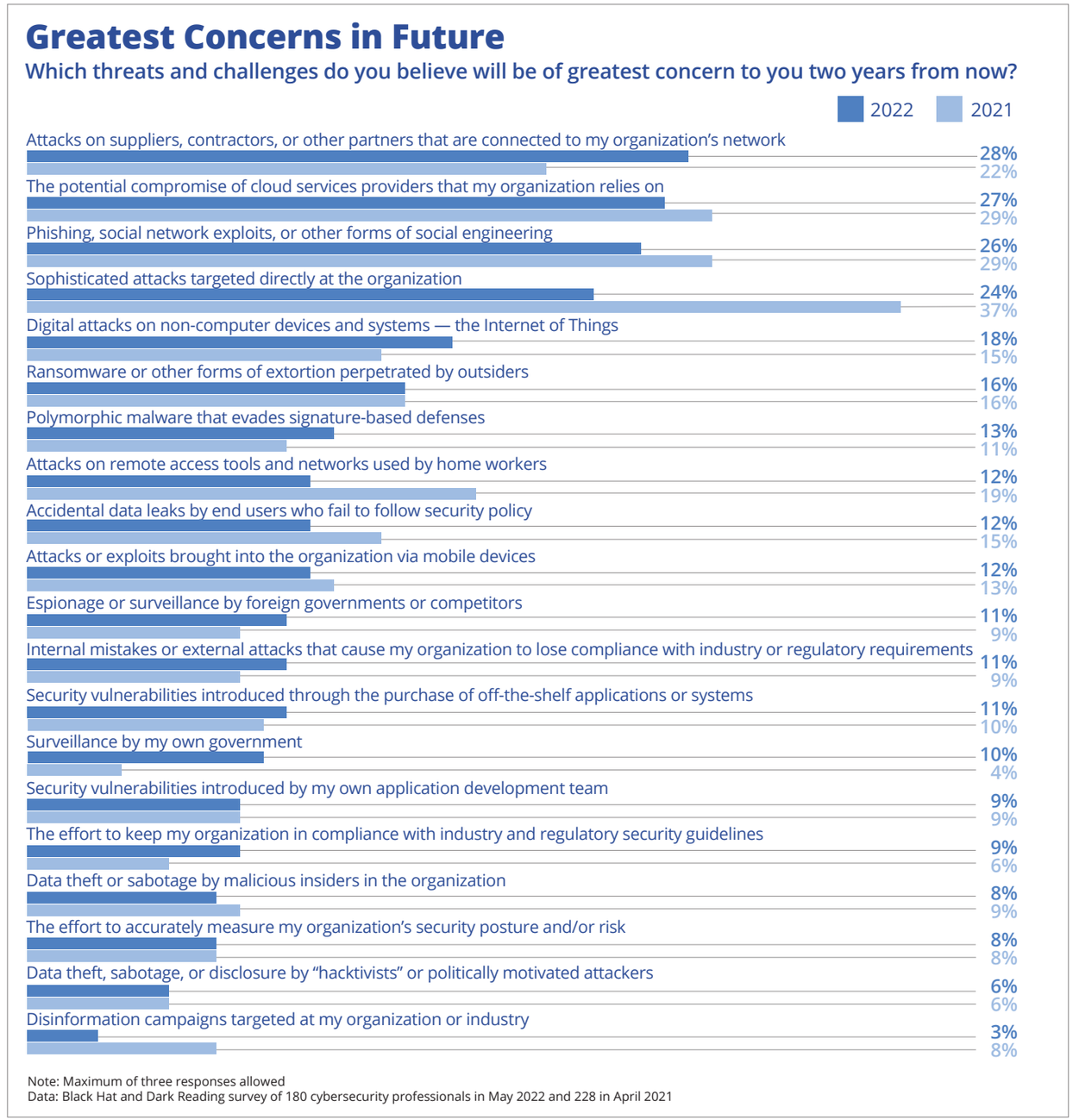
black hat USA 2022

Even with a higher number of attacks, these security professionals seem to be able to deal with ransomware, as 96% say they have been able to successfully block, or minimize the impact of, ransomware attacks against their organizations over the past year (**Figure 11**). When asked if their organization has sufficient processes in place to recover from a ransomware attack, 90% say they do.

If there is one lesson to learn from data breaches in recent years, it's that no organization is an island. Their security depends on the actions of their suppliers and partners. Attackers can jump to the organization's larger network from the supplier network, so it is reassuring that 70% of respondents say their organization has had conversations with suppliers and partners about their plans for dealing with ransomware attacks.

When asked whether they would pay the ransom, only 6% say their organizations would likely pay the ransom, while 81% would ignore the attacker and restore the data from

Figure 9



Note: Maximum of three responses allowed
Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals in May 2022 and 228 in April 2021

backup, which seems to suggest that paying the ransom is unusual among this group (**Figure 12**). However, the fact that 13% of the respondents say things such as "depends on the situation" or "depends on the impact and exactly which data had been exfiltrated" suggests that the figure for those who might pay the ransom is much higher than originally thought. Cyber insurance also likely plays a role in the pay-or-don't-pay calculus, as 68% of Black Hat attendees in this survey say their cyber-insurance policy covers costs associated with ransomware incidents.

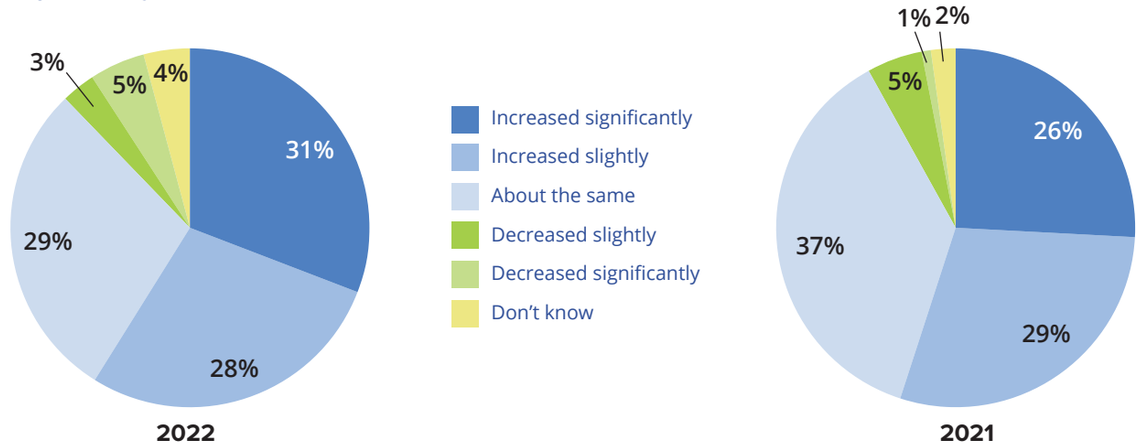
Disinformation Targets Commercial Brands

Security professionals have experienced or observed disinformation in political and social spheres over the past few years, as disinformation attacks sowed confusion over election results, encouraged a violent insurrection in the United States, undermined the efficacy of COVID-19 vaccines, and attempted to obscure the reality of the Russian invasion of Ukraine. This past spring, the Department of Homeland Security announced the Disinformation Governance Board to combat

Figure 10

Increased Threat of Ransomware

Do you believe the threat of ransomware to your organization has increased or decreased over the past two years?



Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals in May 2022 and 228 in April 2021

Figure 11

Dealing With Ransomware

Please tell us how strongly you agree or disagree with the following statements about ransomware.

	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree
My team has been able to successfully block/minimize the impact of ransomware attacks against my organization over the past year	50%	46%	2%	2%
My organization has sufficient processes in place to recover from a ransomware attack	34%	56%	9%	1%
My organization has had conversations with suppliers and partners about their plans for dealing with ransomware attacks	30%	40%	19%	11%
Our cyber-insurance policy covers costs associated with ransomware incidents	24%	44%	17%	15%

Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals, May 2022

disinformation. DHS was forced to pause the board and review future plans after it came under relentless disinformation attacks to discredit the board and its leader, Nina Jankowicz.

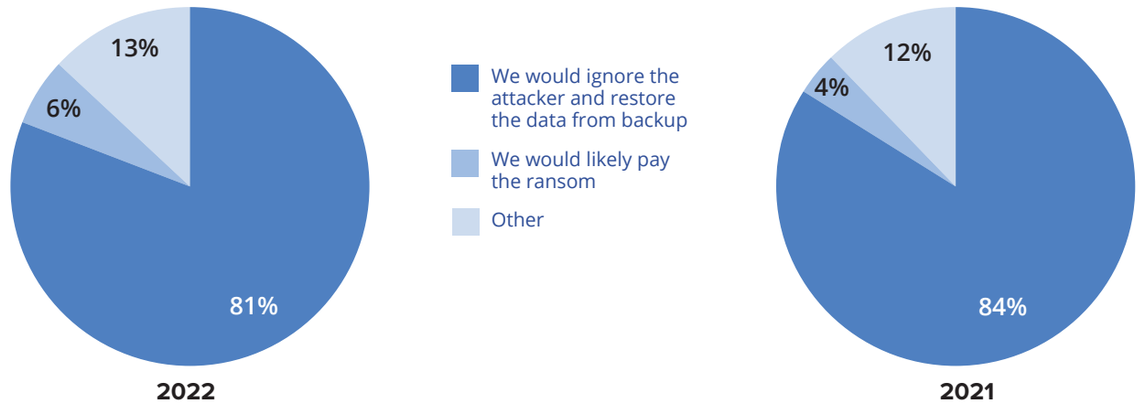
With the success of disinformation attacks in the political realm, many security professionals are concerned that criminals and sophisticated actors are going to shift to the enterprise. In our survey, 72% say disinformation is a serious threat to the industry and almost impossible to prevent (**Figure 13**).

Criminals and sophisticated actors are alreadyexperimenting with disinformation campaigns against the enterprise. For example, a forged US Department of Defense memo claiming there were national security concerns over a semiconductor giant's plans to acquire another technology company drove down the stock prices of both companies. Or when an anonymous QAnon follower falsely claimed that furniture and home décor company Wayfair operated a vast child-trafficking operation last year.

Figure 12

Response to Ransomware

If your organization were infected by ransomware, how would you likely respond?



Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals in May 2022 and 228 in April 2021

Figure 13

Threat of Disinformation

Please tell us how strongly you agree or disagree with the following statements about the threat of disinformation to your organization.

	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree
I believe that disinformation is a serious threat to my industry and almost impossible to prevent	30%	42%	22%	6%
My team would be able to mitigate a disinformation campaign against my organization	21%	51%	20%	8%
I believe we have the tools necessary to detect and mitigate disinformation campaigns	13%	36%	34%	17%

Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals, May 2022

The company took a reputational hit and there were claims that Wayfair CEO Niraj Shah had resigned as a result of his involvement with the operation. Followers of Q also attempted to short the stock.

Even with the prospect of disinformation attacks looming on the horizon, they don't appear to be of immediate concern. Just 53% believe it's likely that attackers will wage disinformation campaigns against their organizations in the coming year.

Security professionals in the survey also are optimistic about their abilities to deal with disinformation attacks, as 72% are confident in their organizations' abilities to mitigate a disinformation attack, and 49% say they have the necessary tools to detect and mitigate these attack campaigns. Fighting disinformation requires coordination between customer relations, brand protection, and data security/privacy.

FAST FACT

67%

report that their organization does not have enough security staff to defend against current threats.

No Sleep for Security Pros

Around a quarter of respondents to the survey, when asked what keeps them awake at night, mention people. They are worried about hiring enough security staff. That even with security awareness training, users will still make mistakes and fall for phishing and social engineering scams. There are concerns that employees will ignore or work around corporate policies. There are also concerns about malicious insiders, or the fact that executive leadership doesn't seem to understand the security risks. Ransomware and other types of attacks, such as an account compromise or a Web application attack, form the second most common topic. Several respondents are overwhelmed, saying "everything" keeps them up at night. One respondent takes a more pragmatic approach: "Nothing keeps me awake at night. There will always be work to do."

Concerns about staffing and budget remain perennial. When asked whether they have enough security staff to defend their organizations against current threats, only 33% say yes, a drop from 40% in 2021 (**Figure 14**). Half of the respondents could "use a little help." And only 43% have enough budget to build a proper defense, a slight drop from 2021 (44%) (**Figure 15**). The figures are similar for being "a little under budget" between 2022 (42%) and 2021 (41%).

Despite all the challenges facing security professionals, uncertainty about technology doesn't seem to be an issue. Black Hat attendees in our 2022 survey seem more confident in the technology they are using than they were in 2021. They were more confident in 2021 than in 2020, so the increase in confidence is a very pleasant trend. When asked about the effectiveness of specific technologies, respondents give high marks to multifactor authentication (87%), encryption (80%), endpoint security tools (79%), and endpoint detection and response tools (78%) (**Figure 16**). Firewalls rounded out the top five (73%).

Perceptions About Technology

Overall, security professionals seem to have a more positive outlook on the effectiveness of security technologies in 2022 compared with 2021. In last year's survey, respondents tended to be mostly neutral

in their responses if they didn't think the technology was effective. Passwords were the exception, 32% rating them as effective, 35% rating them as ineffective, and 33% staying neutral. There were some technologies that security professionals are not enthusiastic about, such as 26% of respondents who give low marks for effectiveness to antivirus tech, compared with just 21% in 2021. Data leak prevention tools are another item that seems to no longer be as well-regarded, with 19% of the respondents giving DLP a low effectiveness score, compared with 16% in 2021. It's possible that the greater number of breaches and ransomware attacks may have soured security professionals' opinion of these tools.

However, there seems to be a bit of a knowledge gap for some security technologies. One-fifth to one-third of respondents say they have never heard of — or are just learning about — technologies such as cloud workload protection platform (36%), secure access service

Figure 14

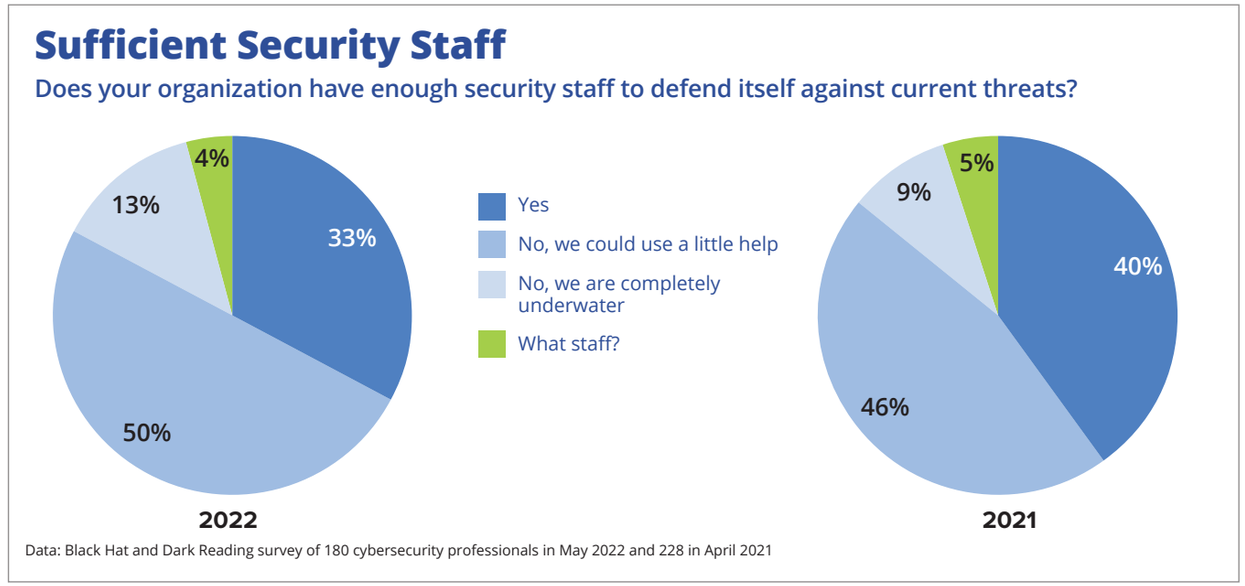
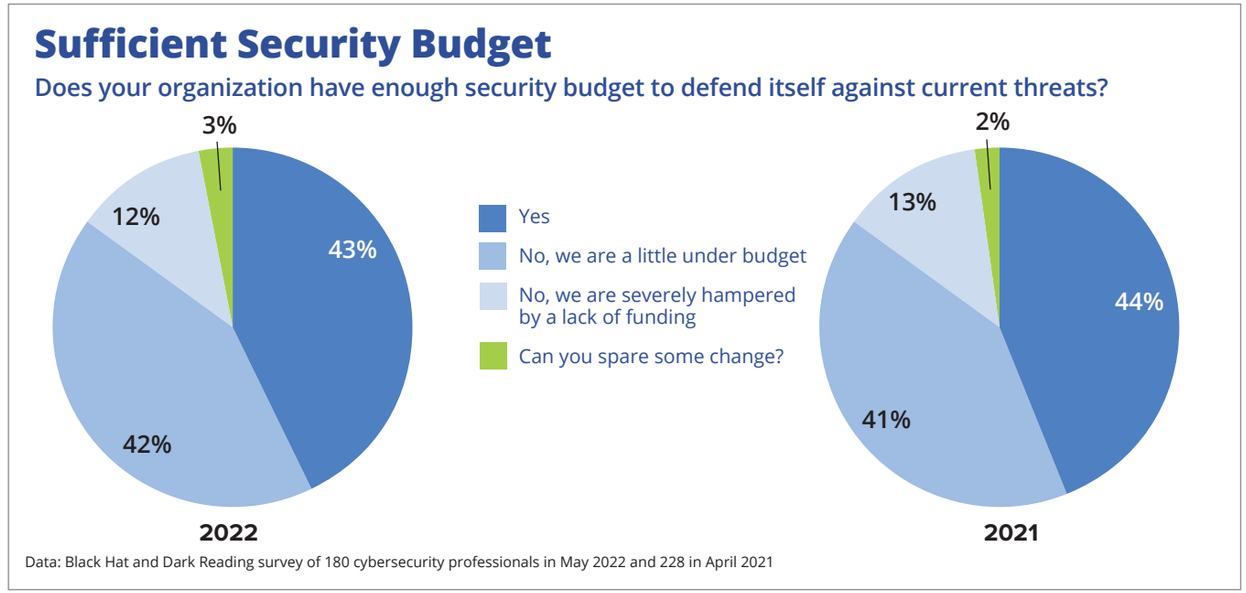


Figure 15



edge (27%), cloud-native application protection platform (27%), and extended detection and response (20%) (**Figure 17**). Considering the concerns respondents expressed about cloud in the survey, we would expect respondents to be seeking out cloud security technologies. That doesn't appear to be the case. While 69% of respondents have implemented or plan to implement cloud permissions management, 22% have no such plans. And while 63% are implementing or have implemented cloud security posture management, 22% don't plan to. Just 36% of respondents have implemented or are implementing cloud workload protection platforms, and 28% have no implementation plans. Finally, only 44% have implementation plans for cloud-native application protection platforms, compared with 29% who have no plans to do so.

It may be less rejection of the technology (understand the technology but no plans to implement it) and more about the fact that security professionals are not interested in stand-alone tools. This puts an interesting spin on IBM's recent announcement about

Figure 16

Effectiveness of Technologies for Protecting Enterprise Data

Please rate the effectiveness of the following technologies in protecting enterprise data on a scale of 1 to 10.

	Effective (score of 7 to 10)	Neutral (score of 5 or 6)	Not effective (score of 1 to 4)
Multifactor authentication tools	87%	9%	4%
Encryption	80%	15%	5%
Endpoint security tools	79%	17%	4%
Endpoint detection and response (EDR) tools	78%	16%	6%
Firewalls	73%	21%	6%
Security information and event management (SIEM)	70%	19%	11%
Third-party penetration testing	70%	18%	12%
Cloud security tools	69%	23%	8%
Extended detection and response (XDR)	68%	24%	8%
Threat intelligence	67%	19%	14%
DNS security tools	67%	21%	12%
Security awareness training tools	66%	22%	12%
Application security tools	66%	25%	9%
Security data analysis tools	58%	29%	13%
Managed security service providers	56%	28%	16%
Data leak protection	56%	25%	19%
Cloud services providers	55%	32%	13%
Artificial intelligence/machine learning	51%	27%	22%
Antivirus	51%	23%	26%
Orchestration tools	50%	30%	20%
Mobile security tools	43%	38%	19%
Deception/honeypots	37%	41%	22%
Passwords	32%	33%	35%

Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals, May 2022

acquiring attack surface management company Randori. Just 48% of respondents have implementation plans for attack surface management, compared with 35% who don't. One way to boost adoption is by offering the technology as a feature in a broader security platform rather than as a stand-alone product.

Security Is Personal

Mental health is increasingly becoming a bigger part of the conversation among security professionals. Factors such as the unrelenting pace of the job, the constant firefighting, and worries over what would happen to the organization if the practitioner missed something all can take a toll. That stress level is evident among our respondents. When asked whether they feel "burned out" in their jobs, half of the respondents say they do not — a rating of 6 or lower on a 10-point scale, compared with 56% in 2021 (**Figure 18**). However, 50% of respondents say they are almost burned out (scoring 7, 8, or 9 on a 10-point scale) in the 2022 survey, up from 44% in 2021.

Figure 17

Familiarity With Technologies

How familiar are you with the following technologies for protecting the enterprise?

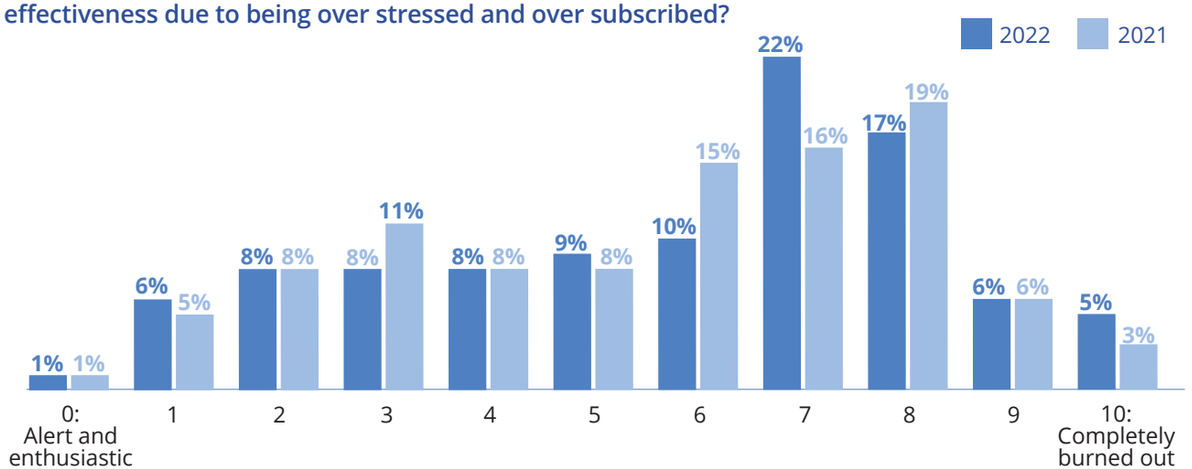
	Familiar with it and have Implemented it	Familiar with it and planning deployment	Understand it but no implementation plans	Just learning about it	Never heard of it
Account credentials management	55%	26%	14%	5%	0%
Cloud permissions management	35%	34%	22%	9%	0%
Cloud security posture management	31%	32%	22%	11%	4%
Extended detection and response (XDR)	29%	26%	25%	14%	6%
Attack surface management	26%	22%	35%	11%	6%
Cloud-native application protection platform	20%	24%	29%	13%	14%
Secure access service edge (SASE)	16%	25%	32%	18%	9%
Cloud workload protection platform	16%	20%	28%	16%	20%

Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals, May 2022

Figure 18

Security Industry Burnout

How would you rate yourself in terms of job burnout, loss of productivity, or loss of effectiveness due to being over stressed and over subscribed?



Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals in May 2022 and 228 in April 2021

Clearly, the constant drumbeat of attacks and breaches is taking its toll.

Something has to be done to move the needle further to the left for mental health so that security professionals don't hit 10 — "completely burned out."

The good news is that organizations seem to be taking employee mental health into consideration. While the largest group of respondents (37%) say their organization offers mental health resources for all employees, a reassuring 31% of respondents say their organization has either been actively rolling out mental health resources to security teams or made security teams aware of the resources available (**Figure 19**). Another 5% say their managers have sought out resources for the team. While this is good news, the fact that 24% say there are no resources or programs available shows there is a lot of work left to be done.

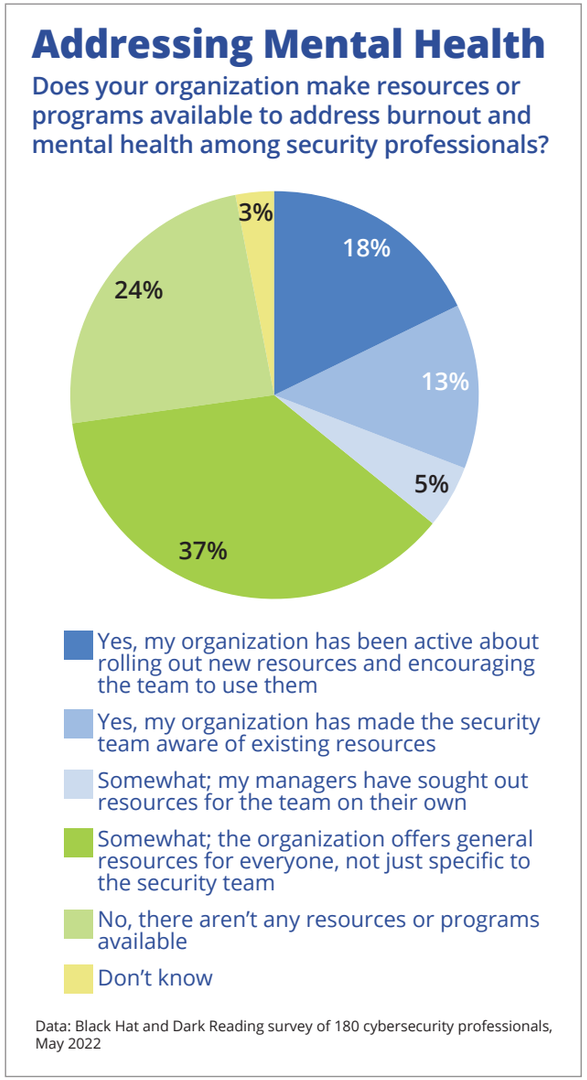
Cybersecurity has always been a fluid industry, with unemployment low and professionals moving to new roles and opportunities. The survey highlights that fluidity. A little over a quarter of professionals (26%) say they are actively looking for an IT security position, and just 27% say they are not likely to move at this time (**Figure 20**). The middle 47% is interesting — 23% are keeping their eyes open for new opportunities but not actively looking, while 24% are not looking but if someone called, they would listen.

FAST FACT

50%

of cybersecurity professionals say they are suffering from job burnout, such as the loss of productivity or loss of effectiveness due to being over stressed and over subscribed.

Figure 19



Conclusion

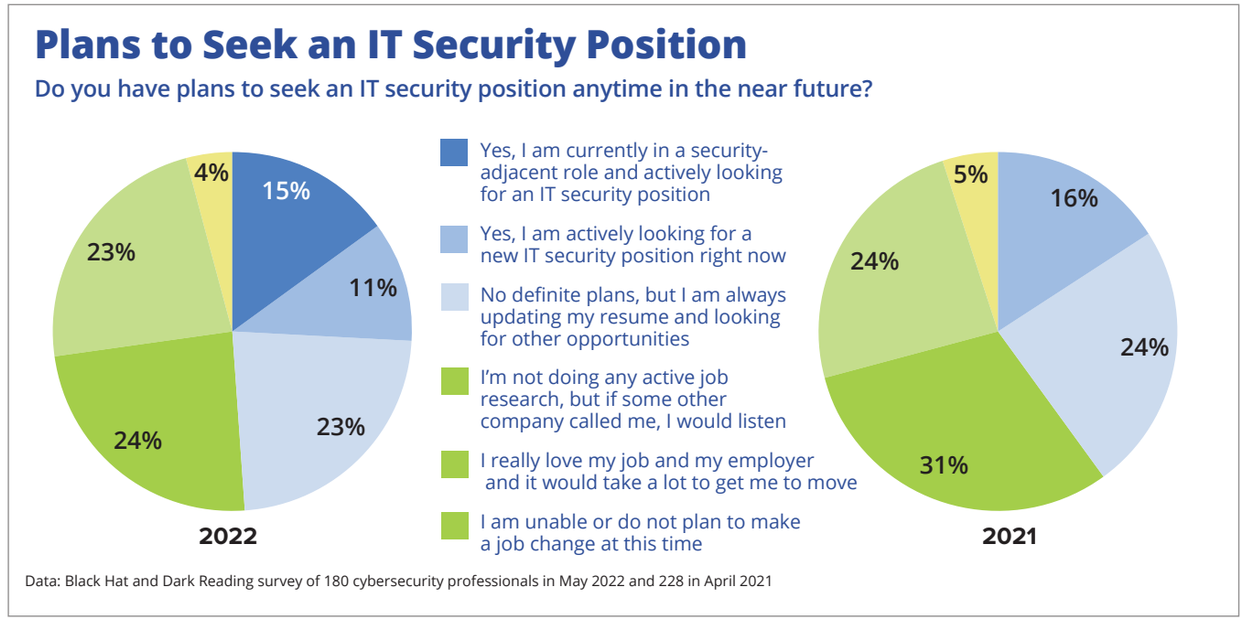
Over the past year, an unrelenting wave of supply chain attacks and ransomware attacks has highlighted just how reliant the world is on software applications and cloud service platforms. As restrictions from the COVID-19 pandemic ease, organizations are learning how to keep the changes they have made to their IT environments and add new controls to mitigate the risks to these remote systems. Security professionals are juggling even more challenges than before. Enterprise security is no longer just about securing endpoints and protecting the network. Defense includes protecting critical infrastructure, understanding the attack

surface because there are enterprise assets that are no longer within the network perimeter, and new threats such as disinformation attacks already are looming.

Cybersecurity professionals are warning the industry that sophisticated attacks aimed directly at the organization pose serious challenges and that attacks against critical infrastructure have moved out of the realm of possibility into reality. Enterprises need to separate operational technology systems from IT systems, and government and commercial organizations need to improve how they work together to protect critical infrastructure. Phishing remains one of the biggest problems facing organizations today.

These professionals expect to be grappling with major cyberattacks in their organizations in the next 12 months, and they will be doing so knowing that they don't have quite enough staff or security budget to do so effectively. That will just contribute to the poor state of their mental health. The rise of new threats is painting a grim picture of the industry unless some changes are made. •

Figure 20

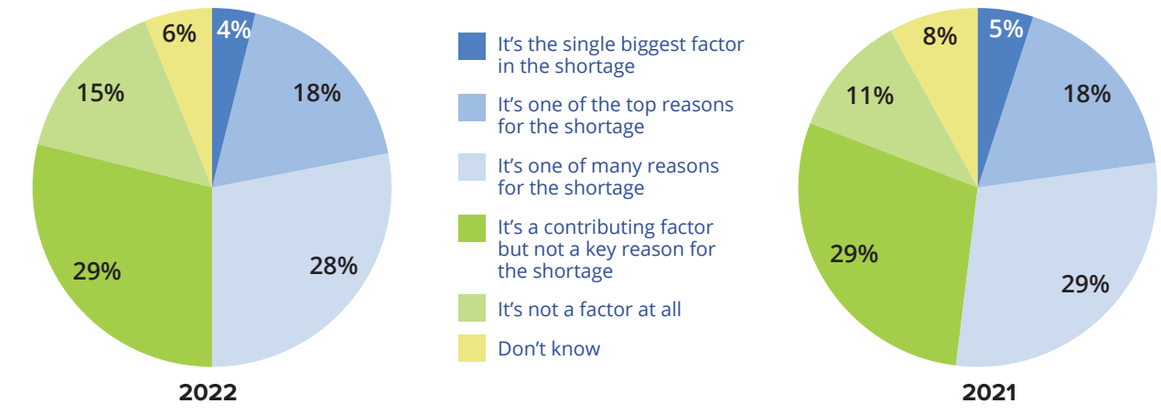


APPENDIX

Figure 21

Impact of Lack of Women and Minorities in Cybersecurity

Research indicates that women and minorities are significantly underrepresented in the security industry. What impact does this have on the overall shortage of skilled security workers in the US market?

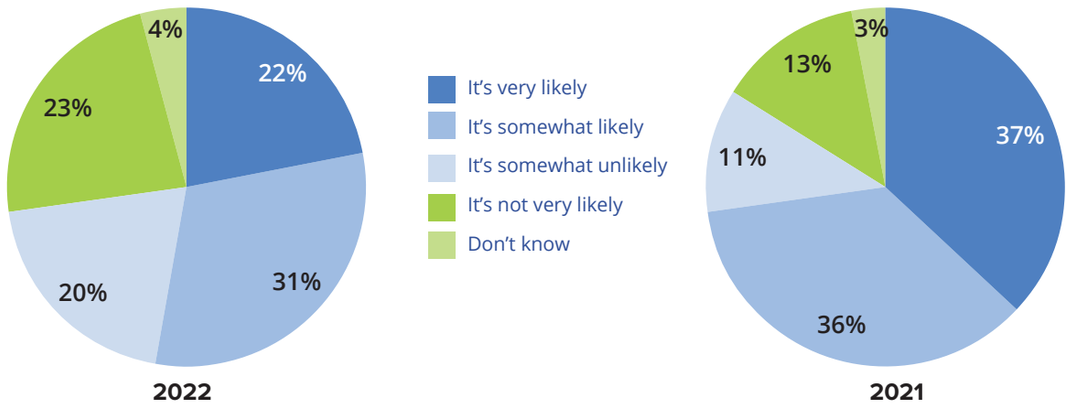


Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals in May 2022 and 228 in April 2021

Figure 22

Disinformation Campaigns

Having seen the success of disinformation campaigns around COVID-19 and the invasion of Ukraine, do you believe that attackers will launch similar disinformation campaigns against your organization or industry in the coming year?

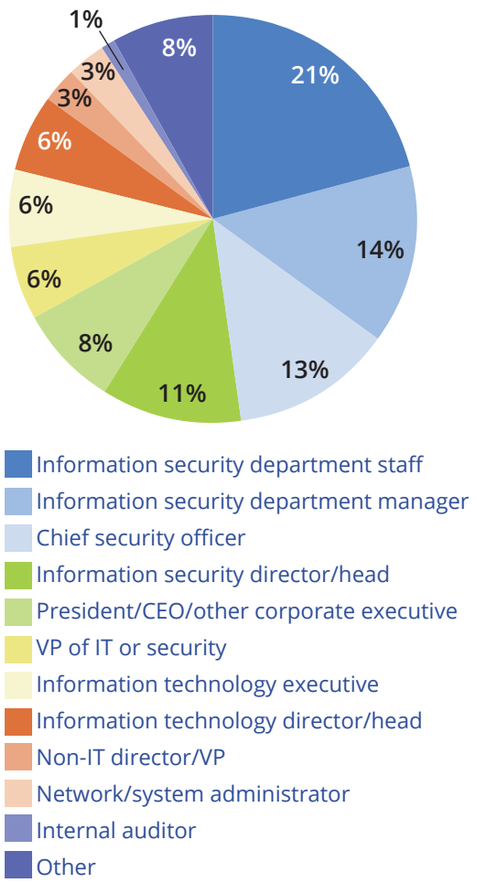


Note: In 2021 the question asked about the success of disinformation campaigns waged against political candidates in recent elections
Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals in May 2022 and 228 in April 2021

Figure 23

Respondent Job Title

Which of the following best describes your job title?

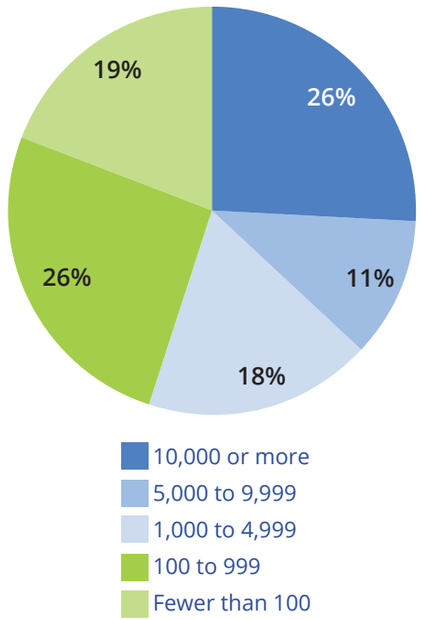


Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals, May 2022

Figure 24

Respondent Company Size

How many employees are in your company in total?



Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals, May 2022

Figure 25

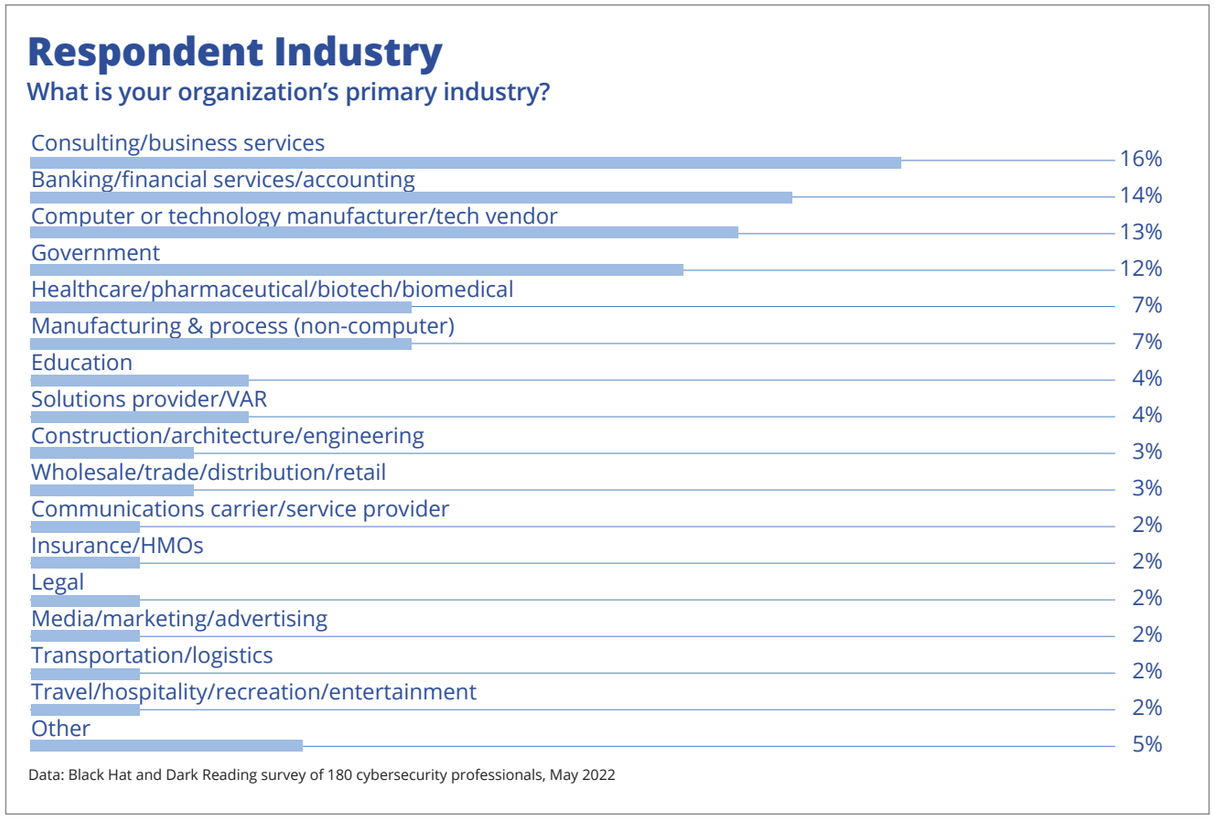

Respondent Industry
What is your organization's primary industry?
Consulting/business services 16%
Banking/financial services/accounting 14%
Computer or technology manufacturer/tech vendor 13%
Government 12%
Healthcare/pharmaceutical/biotech/biomedical 7%
Manufacturing & process (non-computer) 7%
Education 4%
Solutions provider/VAR 4%
Construction/architecture/engineering 3%
Wholesale/trade/distribution/retail 3%
Communications carrier/service provider 2%
Insurance/HMOs 2%
Legal 2%
Media/marketing/advertising 2%
Transportation/logistics 2%
Travel/hospitality/recreation/entertainment 2%
Other 5%
Data: Black Hat and Dark Reading survey of 180 cybersecurity professionals, May 2022

Figure 26

Figure 27