
black hat
USA 2020
www.blackhat.com
June 2020
Next
The 2020 Black Hat USA Attendee Survey
Cyber Threats in Turbulent Times
While a global pandemic turns enterprise networks upside down, America prepares for a critical election — and a growing threat of cyberattack. In this far-reaching survey, top security pros offer insight into what they're preparing for — and the threats they may not be able to stop.
informa
tech

TABLE OF CONTENTS

3 Executive Summary
7 Research Synopsis
8 Cybersecurity Strife in the Post-COVID Era
9 The Threat to US Elections, Government, and Critical Infrastructure
13 Enterprise Data at Risk
16 Technology Shortcomings
21 The State of the Cybersecurity Community
22 Conclusion
24 Appendix

Figures

Figure 1: Increase in Cyber Threat Due to COVID-19
Figure 2: Most Concerning Aspects of COVID-19
Figure 3: Cybersecurity Aspects of COVID-19 Contributing to Increased Risk
Figure 4: Long-term Impact of COVID-19
Figure 5: Impact of Cyberattacks on US Presidential Election
Figure 6: Significant Threats to Election Results
Figure 7: Today's Security Issues
Figure 8: Support of EARN IT Congressional Act
Figure 9: Greatest Threat to US Critical Infrastructure
Figure 10: Likelihood of a Major Security Breach in Next Year
Figure 11: Security Professionals' Greatest Concerns
Figure 12: Greatest Concerns in the Future
Figure 13: Sufficient Security Staff
Figure 14: Sufficient Security Budget
Figure 15: Effective Technologies for Protecting Enterprise Data
Figure 16: Attitudes Toward AI and Machine Learning
Figure 17: Attitudes Toward Blockchain Technology
Figure 18: Storing Consumer Data
Figure 19: Attitudes Toward Startup Vendors
Figure 20: Criteria for Evaluating Potential Startup Security Vendor
Figure 21: Impact of the Lack of Women and Minorities in Security
Figure 22: Security Industry Burnout
Figure 23: Plans to Seek an IT Security Position
Figure 24: Respondent Job Title
Figure 25: Respondent Company Size
Figure 26: Respondent Industry
Figure 27: Respondent Certifications
Figure 28: Respondent Annual Salary
Figure 29: Respondent Country of Residence

EXECUTIVE SUMMARY

For the cybersecurity industry, as for the rest of the world, the year 2020 has brought new meaning to the word “unprecedented.” A global pandemic, COVID-19, restricted billions of people to their homes and literally changed the nature of business overnight. From healthcare to retail to logistics, cybersecurity teams in every industry were forced to rethink their strategies for securing enterprise data as nearly all employees became telecommuters. Whole industries suddenly went from brick-and-mortar to e-business models. And the bad guys, already opportunistic and creative, began to attack enterprise networks in whole new ways.

But the sea changes didn’t stop there. After serious questions were raised by US elections in 2016, cybersecurity researchers and other experts posed a whole new range of concerns about the impact of cyber campaigns to influence the upcoming US presidential elections in 2020. And amid all of these global and national developments, IT security teams were also wrestling with the “normal” threats that have been steadily increasing every year: the Dutch government (6.9 million records), the Marriott hotel chain (5.2 million records), the US Defense Information Systems Agency, and the United Nations were among dozens of organizations that reported major breaches in the first quarter alone.

As some of the world’s top IT security professionals prepare to connect again at the annual Black Hat USA conference, these unprecedented developments have created a level of concern — and even personal stress — that has never been seen in the cybersecurity industry.

In a survey of 273 top security professionals from a wide variety of industries, Black Hat found that cybersecurity experts have serious concerns about the huge changes affecting IT infrastructure and data security around the world, including US critical infrastructure and their own enterprise networks. They also raise serious concerns about the integrity of this fall's US presidential election. And most of the respondents to the 2020 Black Hat USA Attendee Survey are worried about the state of the cybersecurity community as a whole — and about their own states of health and mind.

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 in-depth 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. Most of the respondents (69%) hold the CISSP security certification; many respondents also hold other certifications, including CEH (33%), CompTIA Security (31%), and MCSE (25%).

The 2020 Black Hat USA Attendee Survey asked security professionals to offer their insights into the current state of cybersecurity following the implementation of global quarantines to prevent the spread of COVID-19. We also asked respondents to weigh in on potential cybersecurity threats that might affect US elections and critical infrastructure. Finally, security professionals offered insights into the security of the data held by their own organizations, as well as their concerns about the state of the cybersecurity community and their personal well-being.

The survey results suggest that the world's top cybersecurity professionals are more concerned than ever about cybersecurity risk at the global, national, enterprise, and consumer levels. While cyber threats have been growing in volume and sophistication in recent years, most security professionals believe that the radical shift toward remote access is creating unprecedented risk for sensitive data.

Similarly, security experts widely believe that elections, critical infrastructure, and enterprise data are at a record-high risk of cyberattack, and that the overworked cybersecurity community has a critical need for greater support and communication.

Among the key findings of the 2020 Black Hat USA Attendee Survey are the following:

- 94% of security pros believe that the COVID-19 crisis increases the cyber threat to enterprise systems and data; 24% view the increased threat as critical and imminent.
- Of cyber threats posed by COVID-19, vulnerabilities in enterprise remote access systems supporting home workers are the chief concern (57%). Increased phishing and social engineering threats also rank highly (51%).
- Only 15% of security experts believe that cyber operations and threat flow will return to normal after the COVID-19 crisis passes; 84% believe that significant, lasting changes will occur, at least in some industries.
- Almost a third (31%) of security experts predict that the impact of cyberattacks and disinformation campaigns on 2020 government elections will be so great that the results will always be in doubt.
- Disinformation (71%) will have a much greater impact than hacking of voting machines and vote tabulation systems, cybersecurity professionals think. But more than two-thirds (69%) believe that any form of electronic voting is inherently risky and that paper ballots are significantly more secure.
- More than two-thirds of cybersecurity experts (69%) believe that Russian cyber initiatives will have a significant impact on the outcome of the US presidential election in 2020.

• Nearly 90% of respondents (87%) predict that a successful cyberattack on US critical infrastructure will occur in the next two years, up from 77% in 2019 and 69% in 2018; only 16% think that government and private industry are prepared to respond to such an attack, down from 21% in 2019.

• Seventy percent of cybersecurity pros believe they will have to respond to a major security breach in their own organization in the coming year, up from 59% in 2018; most do not think they have the staffing or budget to defend adequately against current and emerging threats.

• Security professionals view many of the technologies that they use in enterprises as ineffective. A majority of respondents view only nine technologies as effective.

• Almost two-thirds of enterprises (63%) are willing to consider startups as they seek ways to improve their technology, but they struggle with the large number of security startups and the shortage of time they have to evaluate them.

• Enterprises are also frustrated by the hype associated with some technologies that have been purported to be cybersecurity game changers. Eighty-three percent of security pros believe the defensive impact of blockchain technology will be limited; 73% think the same thing about artificial intelligence and machine learning.

• Nearly four in 10 security professionals (38%) consider themselves “burned out” by their work, up from 30% in 2019. Clearly, the job of the cybersecurity professional is not getting easier.

SYNOPSIS

RESEARCH

Survey Name: 2020 Black Hat USA Attendee Survey

Survey Date: April 2020

Region: United States

Number of Respondents: 273 IT and security professionals. The greatest possible margin of error for the total respondent base (N=273) is +/-5.9 percentage points. Informa, the parent company of Black Hat and Dark Reading, 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 2020, Black Hat and Dark Reading researchers conducted an online survey of IT and cybersecurity professionals who attended the Black Hat USA conference in 2019 and/or were planning to do so in 2020. The survey yielded data from 273 management and staff security professionals, predominantly at large companies, with 58% working at companies with 1,000 or more employees. Sixty-nine percent of the respondents hold the CISSP security professional credential; 33% were certified ethical hackers (CEH).

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 trainings 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.

Cybersecurity Strife in the Post-COVID Era

For every organization across the globe, the first half of 2020 brought a wholesale shift in human communication. The COVID-19 crisis forced employees, partners, and customers into their homes and made the world completely reliant on electronic communications for the first time ever. Virtually every industry has been driven to rethink its business, and cybersecurity professionals are no exception.

"Greater dependence on cloud computing and employee-controlled/owned devices and networks will lessen the visibility and control IT and security functions rely upon to manage risk," said one respondent to the 2020 Black Hat USA Attendee Survey. "This is a fundamental paradigm shift that will necessitate a change in the way we manage risk, allocate already scarce resources, and deploy controls. It should drive innovation in our field and provide new opportunities and challenges."

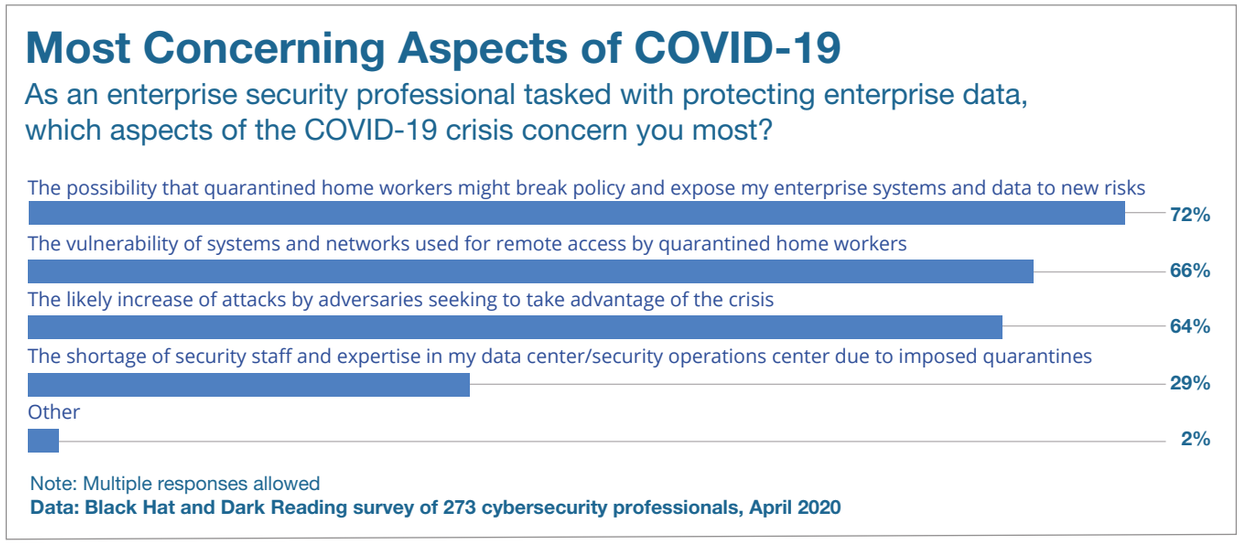
The vast majority of survey respondents agree. In fact, 94% said they believe they believe COVID-19 increases the cyber threat to enterprise systems and data; 24% said the increased threat is critical and imminent (**Figure 1**).

Figure 1

IT security pros' chief concern (72%) is that quarantined workers, many unfamiliar with work-from-home security practices, might break policy and expose enterprise systems and data to new risks (**Figure 2**). Many also believe that most current remote access systems were never built to carry such a level of secure data; 66% of respondents expressed concerns about the vulnerability of systems and networks used by quarantined workers.

But vulnerabilities in human practices and security technology are only part of the problem. Security experts also predict that cyberattackers, seeking to take advantage of a rapidly restructured line of communications, will continue to launch many new exploits that leverage the crisis. Fifty-one

Figure 2



percent of Black Hat USA Attendee Survey respondents said increases in phishing and social engineering attacks that exploit the crisis are among the most dangerous cyber threats posed by COVID-19 (**Figure 3**). Sixty-four percent said they are most concerned by a likely increase of attacks by adversaries seeking to take advantage of the crisis.

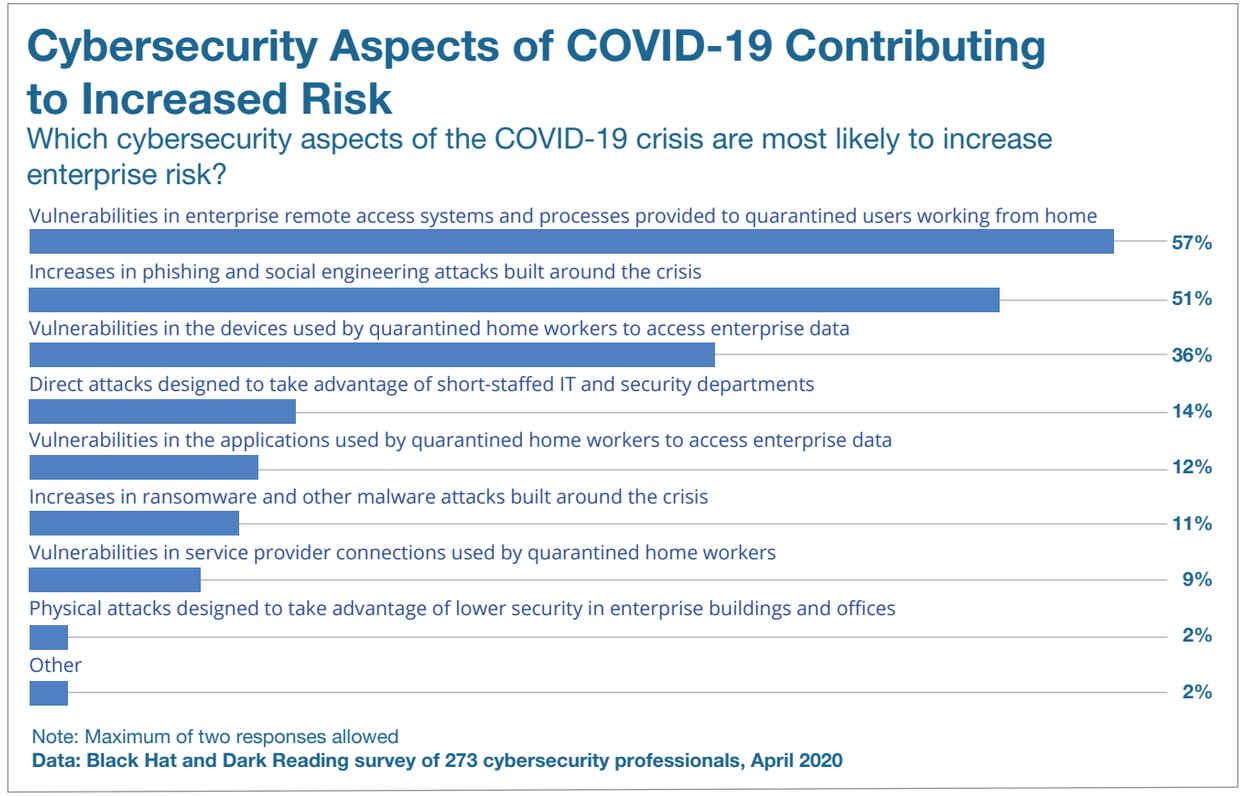
And while many of the Black Hat USA Attendee Survey respondents posted their answers in March and April — when many in the US believed the crisis would be short-lived — most respondents already recognized the long-term implications of the wholesale shift in online communications. In fact, some 84% of security professionals expressed the belief that the crisis would spur significant changes in methods of operation in at least some industries (**Figure 4**). Twelve percent said they believed that COVID-19 will be the beginning of an entirely new way of working and doing business that relies much more heavily on online communications and less on face-to-face interaction.

"I think that this pandemic will change the way we work, socialize, and communicate because we will feel more comfortable communicating online instead of in-person," said one respondent. "Even when we get back to 'normal,' we will feel more comfortable using technology for most things than we did before. As for cybersecurity, we will be at greater risk."

The Threat to US Elections, Government, and Critical Infrastructure

While they are wrestling to solve the pandemic-driven cybersecurity issues in their own enterprises, IT security professionals also have grave concerns about potential threats at the national level. As the presidential election of 2020 approaches, respondents to the Black Hat USA Attendee Survey voiced particular concerns about the integrity of voter information and voting systems, both of which are likely to be tested by politically motivated attackers

Figure 3



and foreign interests.

Nearly all IT security experts (85%) believe that cyber threat actors will have at least some impact on US elections in 2020 (**Figure 5**). Almost one-third (31%) believe that the impact will be critical and that the results of the coming election will always be in doubt as a result.

The greatest threat, according to security experts, is not the hacking of voting machines but systematic disinformation campaigns designed to smear the reputation of one candidate and/or falsely prop up the reputation of another. Seventy-one percent of Black Hat USA Attendee Survey respondents fear that these disinformation exploits will have the greatest impact on the elections (**Figure 6**). Most security pros expect these exploits to emanate primarily from Russia; more than two-thirds (69%) believe that Russian cyber initiatives will have a significant impact on the 2020 US presidential election (**Figure 7**).

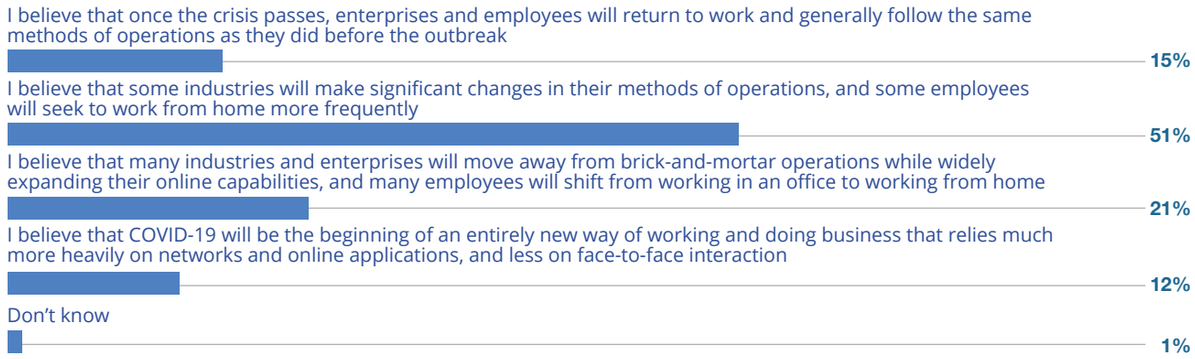
While disinformation is the primary concern, cybersecurity experts also continue to be concerned about the integrity of voting machines and the networks and systems used to tabulate voting data. This is not surprising, given that ethical hackers have demonstrated the ability to crack voting machines and systems at multiple Black Hat conferences over the years. More than two-thirds (69%) of survey respondents believe that voting electronically in any form is inherently risky, and that paper ballots are significantly more secure.

Cybersecurity professionals have doubts about virtually all aspects of the electronic

Figure 4

Long-term Impact of COVID-19

Which statement best describes your view on the long-term impact of the COVID-19 outbreak on computing and communications?

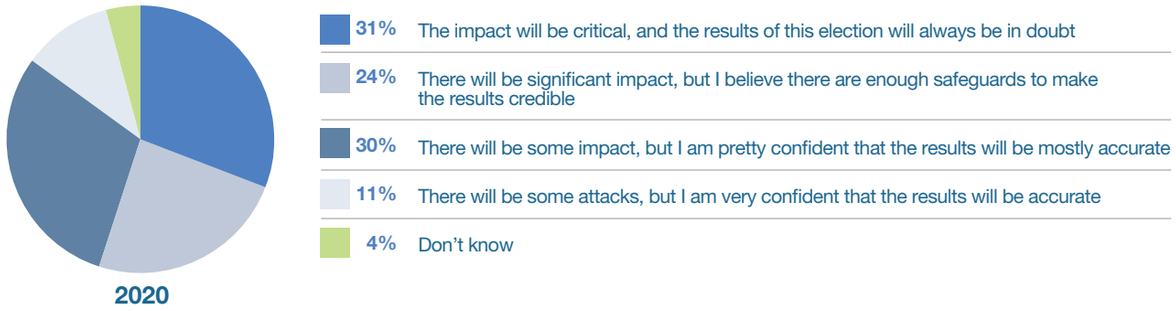


Data: Black Hat and Dark Reading survey of 273 cybersecurity professionals, April 2020

Figure 5

Impact of Cyberattacks on US Presidential Election

As the United States prepares for a presidential election in November, what do you think will be the impact of cyberattacks and disinformation campaigns on election results?

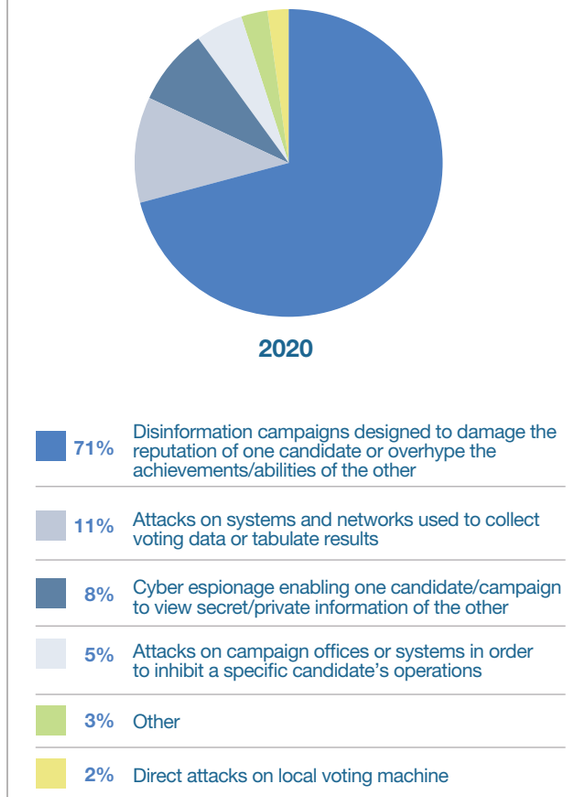


Data: Black Hat and Dark Reading survey of 273 cybersecurity professionals, April 2020

Figure 6

Significant Threats to Election Results

Of the various threats posed to the upcoming election, which do you believe will have the most significant impact on the results?



Data: Black Hat and Dark Reading survey of 273 cybersecurity professionals, April 2020

Figure 7

Today's Security Issues

Please rate your level of agreement with the following statements.

	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree
I believe that a shortage of well-trained and qualified security professionals is significantly affecting the safety and security of data, both personal and commercial	55%	37%	6%	2%
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	44%	43%	12%	1%
Using a mobile app for voting, in primaries or general elections, is an inherently risky practice that cannot be secured	40%	33%	22%	5%
I believe that a successful cyberattack on the critical infrastructure of the United States will occur in the next two years	39%	48%	12%	1%
Voting electronically in any form is inherently risky; paper ballots are significantly more secure	31%	38%	22%	9%
The shortage of women and minorities in the information security profession is a concern to me	30%	32%	22%	16%
I believe that Russian cyber initiatives will have a significant impact on the outcome of the 2020 US presidential election	27%	42%	21%	10%
I believe that in the future, it will be possible for individuals to protect their online identity and privacy	6%	32%	39%	23%
I believe that a comprehensive cyber insurance policy significantly owers the risk associated with cyber breaches in my organization	5%	29%	31%	35%
I believe that government and private industry are adequately prepared to respond to a major breach of US critical infrastructure	2%	14%	49%	35%

Data: Black Hat and Dark Reading survey of 273 cybersecurity professionals, April 2020

voting process. Almost three-quarters (73%) of respondents said that using a mobile application for voting, as was attempted in the Iowa Democratic primaries this year, is an inherently risky practice that cannot be secured. While only a few respondents (2%) said that direct attacks on local voting machines was their primary concern, others named attacks on campaign offices (5%), cyber espionage between political parties (8%), and attacks on systems used to tabulate voting results (11%) as their chief concern.

Inside the political arena, two-thirds (66%) of cybersecurity professionals are opposed to the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act of 2020, a bill proposed in the US Senate (**Figure 8**). The bill, which is aimed at helping law enforcement teams catch purveyors of child pornography, would require online communication services (including Facebook and Google) to provide a backdoor that would enable investigators to decipher encrypted messages. But two-thirds of Black Hat USA Attendee Survey respondents expressed concern that the proposed law would effectively outlaw end-to-end encryption over commercial services and put the privacy of individuals' private messages in jeopardy.

Outside the political arena, security pros voiced increasing concern that government and private industry are unprepared for

Figure 8

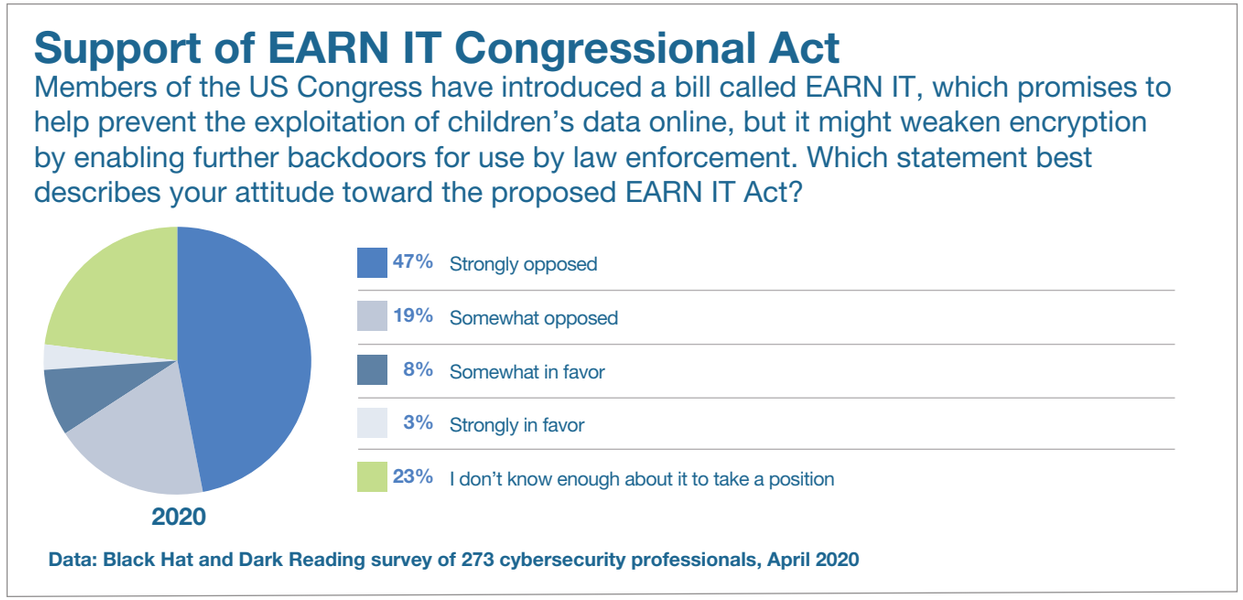
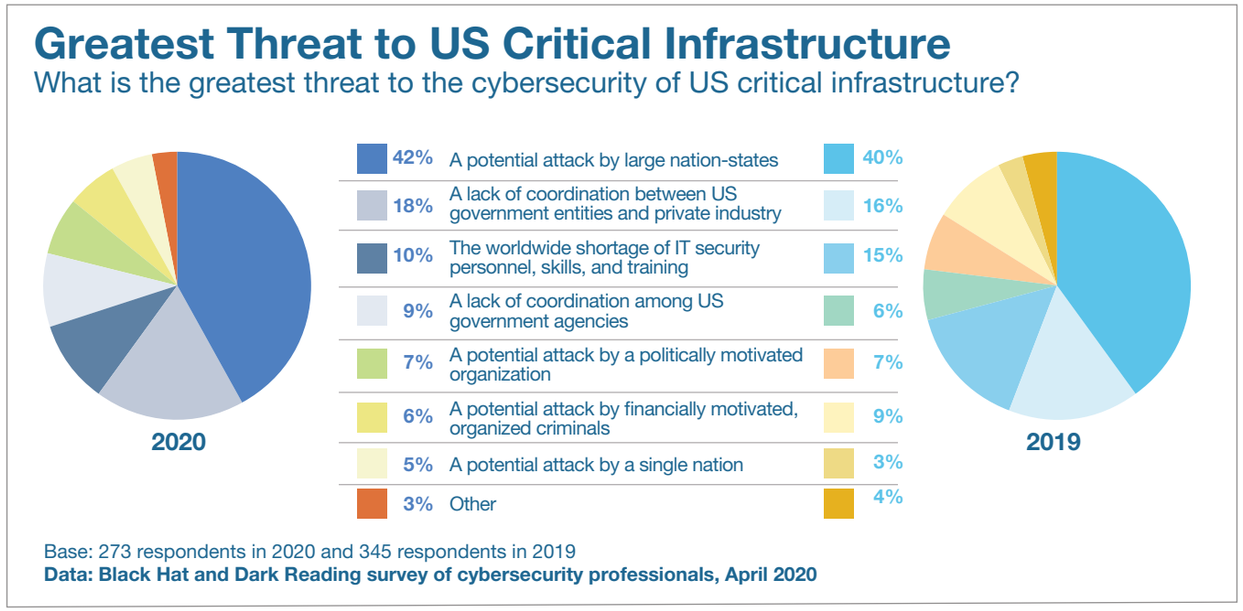


Figure 9



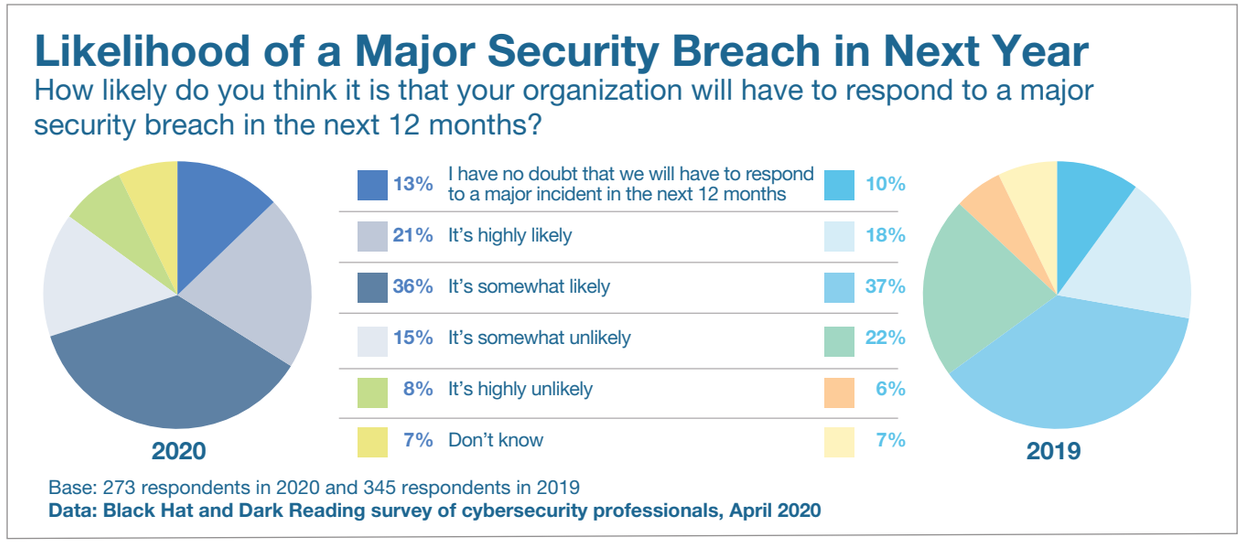
a forthcoming attack on US critical infrastructure. A landslide 87% of cybersecurity professionals believe that there will be a successful cyberattack on US critical infrastructure in the next two years — a 10% increase over the 2019 numbers. Only 16% of respondents think that government and private industry are adequately prepared to respond to such a breach — an all-time low in the Black Hat USA Attendee Survey.

What are the chief threats to US critical infrastructure? A cyberattack by a large nation-state, such as Russia or China, is the greatest concern, according to survey respondents (42%) (**Figure 9**). Eighteen percent said the most critical danger is a lack of coordination between US government entities and private industry. A shortage of IT security personnel was cited as the chief concern among 10% of security pros, while a lack of coordination among US government agencies (9%) was close behind.

Enterprise Data at Risk

While issues of national importance such as elections and critical infrastructure are on their minds, most cybersecurity profes-

Figure 10



sionals are also worried about problems even closer to home — their own enterprises. Seventy percent of Black Hat USA Attendee Survey respondents said it is likely that their organizations will have to respond to a major security breach in the next 12 months (**Figure 10**). Thirteen percent said such a breach is a certainty.

Such concerns are consistently reinforced by news reports. In 2019, data breaches were up 33% over 2018, leading to the exposure of some 7.9 billion records, according to statistics compiled by Risk Based Security. In the first quarter alone, the Dutch government (6.9 million records), Marriott (5.2 million records), the U.S. Defense Information Systems Agency, and the United Nations were among dozens of organizations that reported major breaches.

What keeps cybersecurity professionals awake at night? One of the newest sleep deprivers is an increasing concern over the integrity and security of cloud services that many enterprises now rely on to carry mission-critical information. After perennial concerns about sophisticated attacks aimed directly at their organizations (39%) and social engineering attacks that cannot be easily blocked by traditional defenses (39%), the potential compromise of cloud services (27%) has become the greatest concern of Black Hat USA Attendee Survey respondents (**Figure11**).

And concern about cloud security threats is increasing. When asked which threats they think will be of greatest concern two years from now, cybersecurity pros ranked cloud security vulnerabilities as their second-greatest concern (27%), after sophisticated, targeted attacks (31%) (**Figure 12**).

As noted earlier, the COVID-19-related IT shifts have also created significant concerns about remote access issues that in past years were much lower on the priority list. Attacks on remote access systems used by home workers are currently the No. 4 concern among security pros (22%), but most respondents did not expect that concern to last; remote access dropped to No. 8 in the expected list of concerns two years from now (15%).

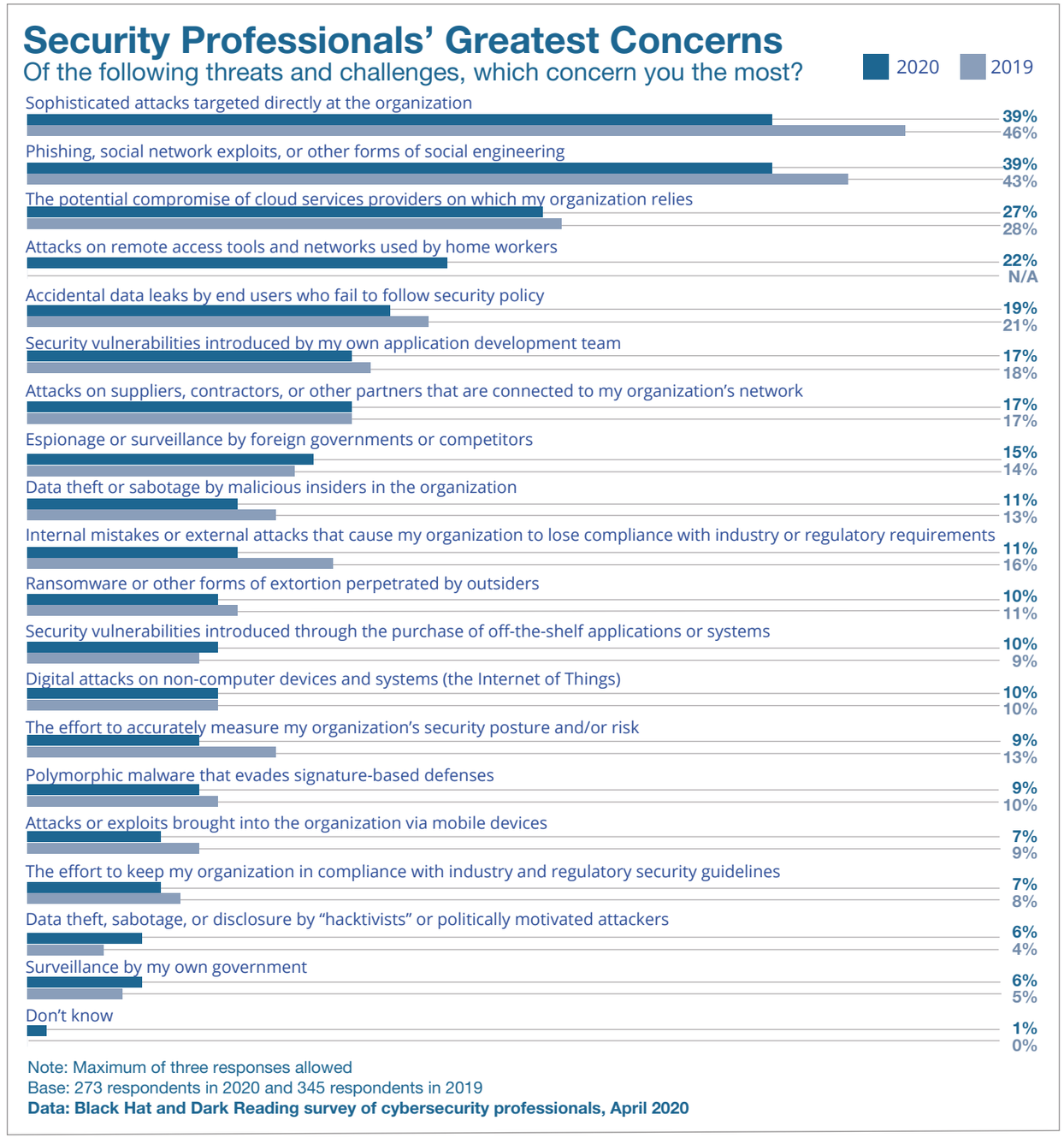
black hat USA 2020

Many IT security experts are most concerned about the human factor in cybersecurity, noting that end users are often careless and that online attackers frequently seek to exploit this carelessness. Phishing and social engineering attacks ranked second among the challenges that keep survey respondents awake at night; accidental data leaks by end users who fail to follow security policy ranked fifth.

"My biggest concern is a general lack of understanding among employees of how important security is," said one respondent. "Their willingness to click on any link to cat pictures truly concerns me. How is phishing still effective? Because some people refuse to believe that they are important enough to be a security risk."

As in past years, a chief reason for cybersecurity professionals' concerns is the continuing shortage of resources available to fight the growing threat. When asked whether they have sufficient security staff to defend their enterprises against current cyber threats, 59% said no (**Figure 13**).

Figure 11



black hat USA 2020

When asked if they had enough budget to defend their data against current threats, a majority (56%) said no (**Figure 14**).

And with the emerging economic crisis driven by the COVID-19 pandemic, some security pros are not expecting help anytime soon. "My biggest concern is the economic impact of COVID-19 and the board's financial commitment to cybersecurity," said one Black Hat USA Attendee Survey respondent.

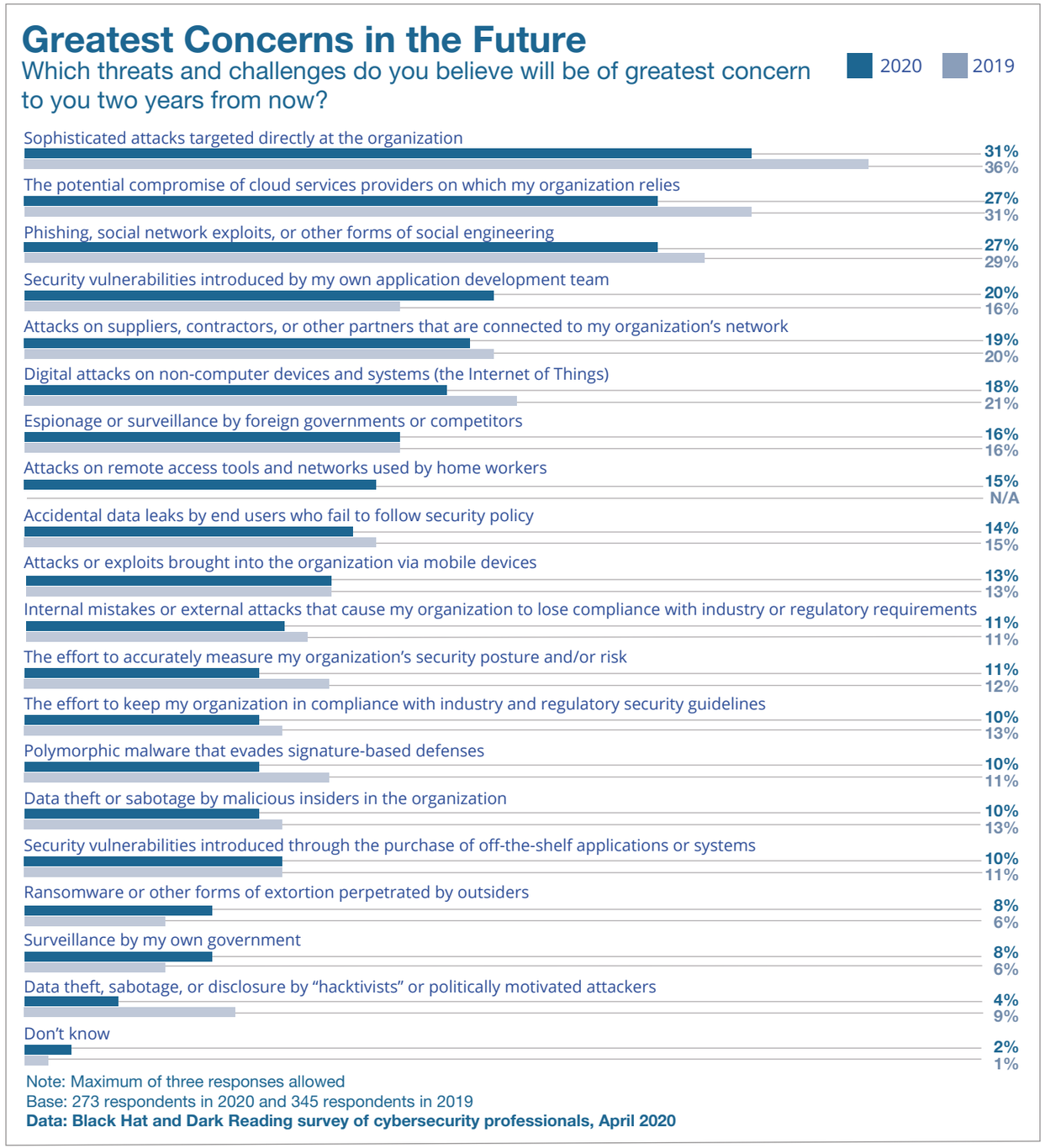
The shortage of qualified IT security staff remains a crucial issue across the cybersecurity issue. In the survey, 92% of respondents said that the security skills shortage is significantly affecting the safety and security of data, both personal and commercial.

"My biggest concern is the immaturity of our overall security team," said one respondent. "Has someone infiltrated our network, and we aren't skilled enough to realize it?

Technology Shortcomings

While resources are a major concern for those tasked with securing enterprise networks,

Figure 12



many also raised concerns about current security technologies and the challenge of procuring them. In our survey, we listed 21 different technologies that most enterprises are currently using to help protect their IT environments and asked respondents to rank the effectiveness of each. In the end, fewer than half of those technologies — only nine — were rated as "effective" by security professionals.

Multifactor authentication (84%), encryption (74%), and endpoint security tools (63%) received the highest "effectiveness" rating among Black Hat USA Attendee Survey respondents (**Figure 15**). Third-party-penetration testing (59%) and firewalls (58%) also rated toward the top. The security technologies rated least effective were passwords (25%), deception/honeypots (27%), and antivirus tools (31%). Cloud services providers (41%) and cloud security tools (46%) were rated ineffective by the majority of respondents.

Security professionals also expressed frustration about some technologies that have been repeatedly promoted as "game changers" in security technology. When

Figure 13

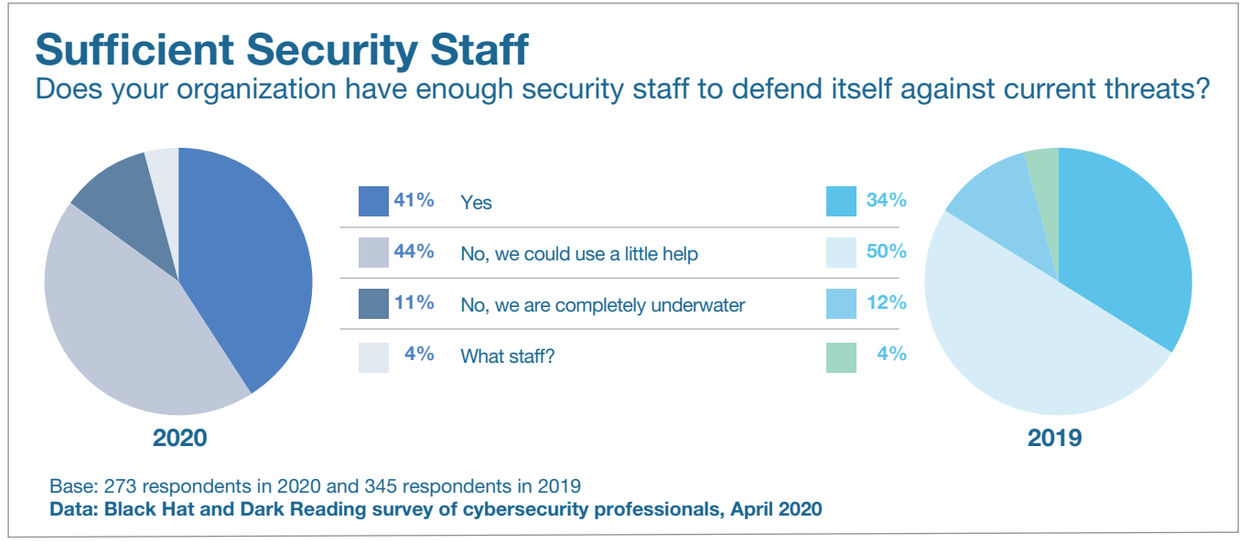


Figure 14

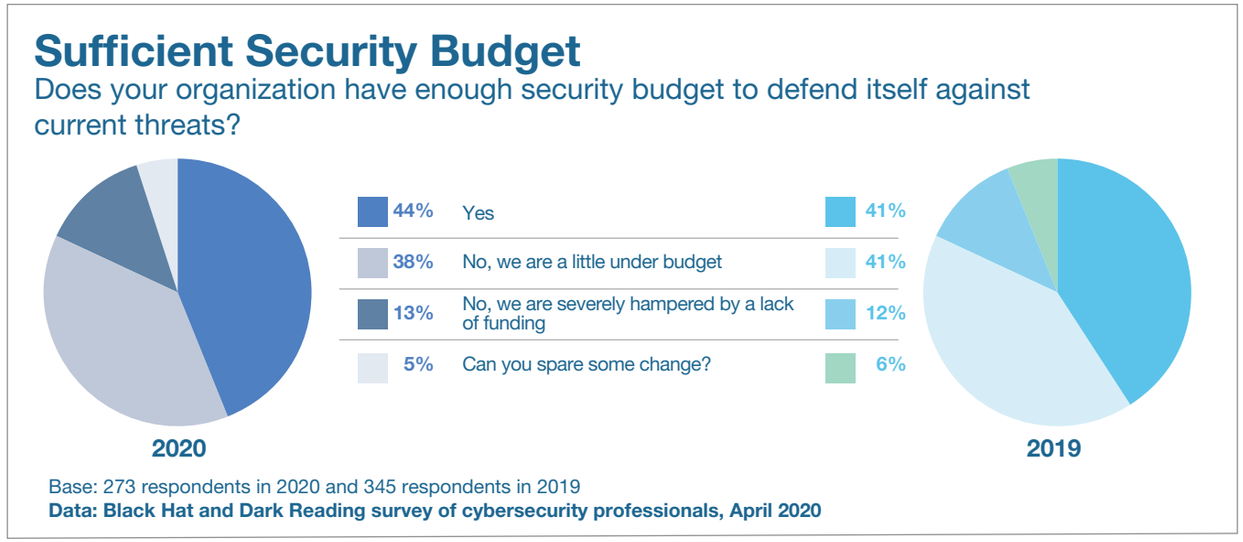


Figure 15

Effective Technologies for Protecting Enterprise Data

Please rate the effectiveness of the following technologies in protecting enterprise data on a scale of 0 to 10.

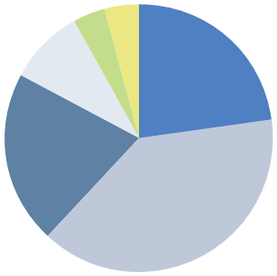
	Effective (rating of 7 to 10)	Neutral (rating of 4 to 6)	Not Effective (rating of 0 to 3)
Multifactor authentication tools	84%	13%	3%
Encryption	74%	25%	1%
Endpoint security tools	63%	32%	5%
Third-party penetration testing	59%	33%	8%
Firewalls	58%	36%	6%
Threat intelligence	56%	39%	5%
Security awareness training tools	56%	36%	8%
Security information and event management (SIEM)	55%	36%	9%
Endpoint detection and response (EDR) tools	51%	43%	6%
Application security tools	50%	47%	3%
Security data analysis tools	48%	48%	4%
Cloud security tools	46%	46%	8%
Managed security service providers	46%	40%	14%
Orchestration tools	44%	48%	8%
Cloud services providers	41%	45%	14%
Data leak protection	39%	51%	10%
Artificial intelligence/machine learning	33%	45%	22%
Mobile security tools	33%	54%	13%
Antivirus	31%	42%	27%
Deception/honeypots	27%	56%	17%
Passwords	25%	48%	27%

Data: Black Hat and Dark Reading survey of 273 cybersecurity professionals, April 2020

Figure 16

Attitudes Toward AI and Machine Learning

Which statement best describes your attitude toward artificial intelligence and machine learning?



2020

- 23% I believe these technologies are “game changers” that will make a major impact on the way security teams detect and defend against online attacks in the future
- 39% I believe these technologies will be useful in speeding/automating some security processes, but their impact on security overall will be limited
- 21% I believe these technologies will enable new security capabilities in a few cases, but the industry spends too much time talking about them
- 9% I believe these technologies are overhyped and are unlikely to be of much use to me in my security initiatives
- 4% I believe these technologies will be more useful to attackers than to defenders
- 4% Don’t know

Data: Black Hat and Dark Reading survey of 273 cybersecurity professionals, April 2020

Figure 17

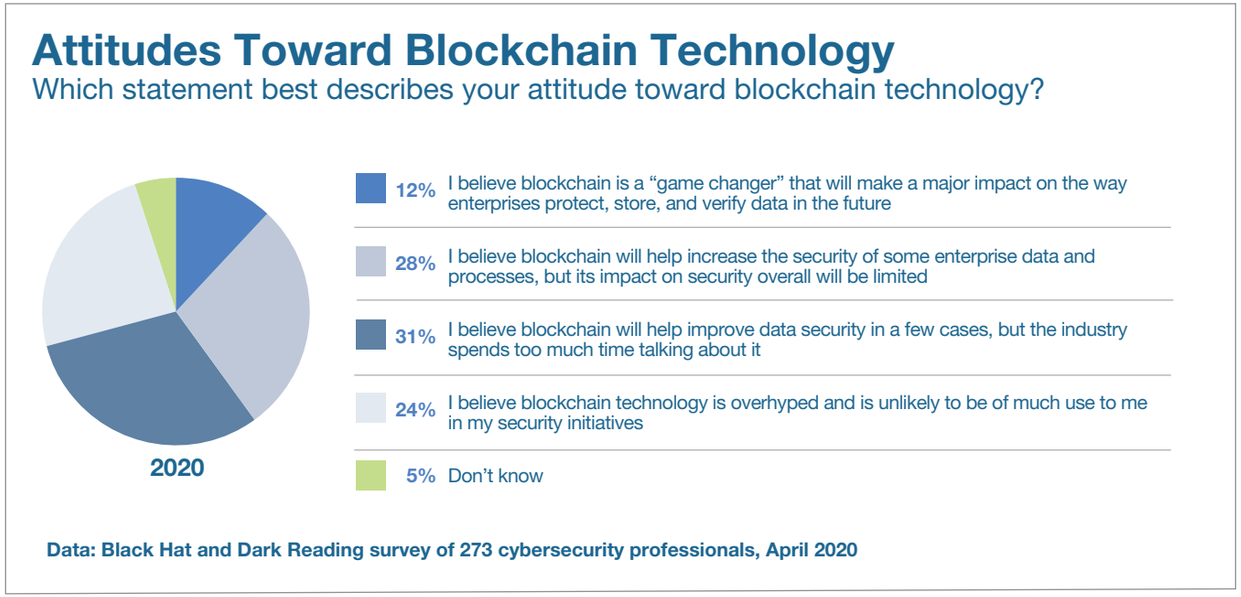
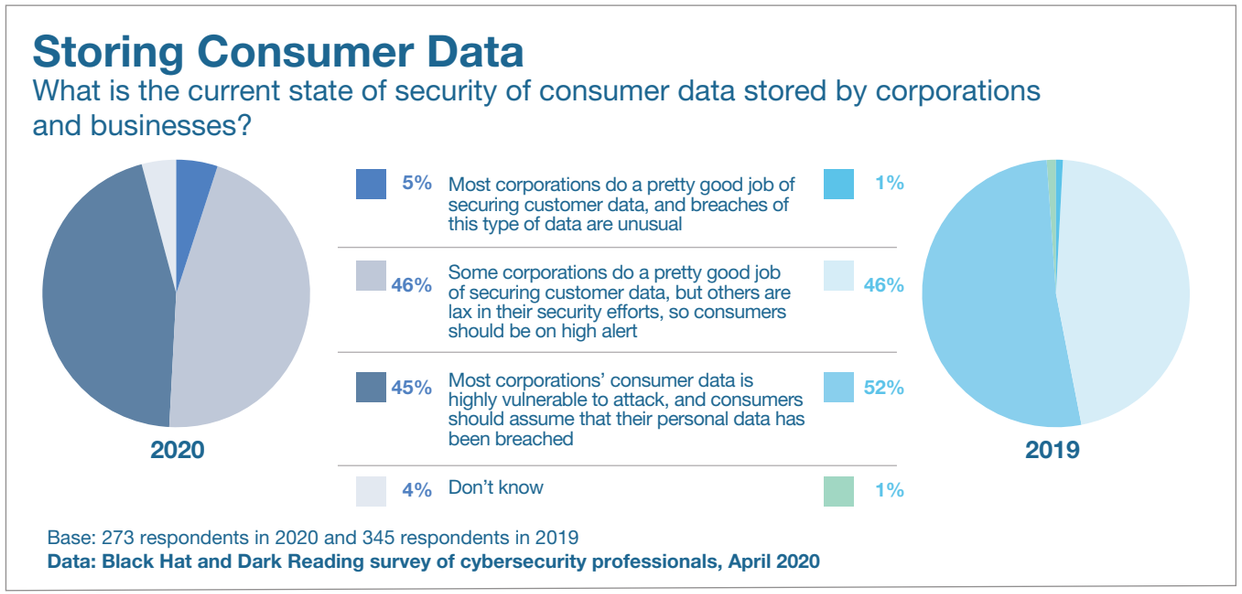


Figure 18



asked about artificial intelligence (AI) and machine learning (ML), for example, only 23% of survey respondents said they believe AI and ML will be game-changing technologies (**Figure 16**). Seventy-three percent said they believe the impact of AI and ML on security will be limited. Thirty percent said they think AI and ML are over-discussed or overhyped. Only 33% ranked these technologies as effective. Attitudes toward blockchain technology were even more cynical: Only 12% of Black Hat survey respondents rated the technology as game-changing; more than half (55%) believe it is overdiscussed, and of that, 24% said they believe the technology is "overhyped and unlikely to be of much use" to their organizations (**Figure 17**).

Many security experts also expressed serious concerns over the ability of corporations and consumers to protect the data and identity of individual users. Nearly half (45%) of respondents to the survey said they believe the consumer data stored by most corporations is highly vulnerable to attack and that consumers should assume that their personal data has been breached (**Figure 18**). Eighty-seven percent of cyber-

Figure 19

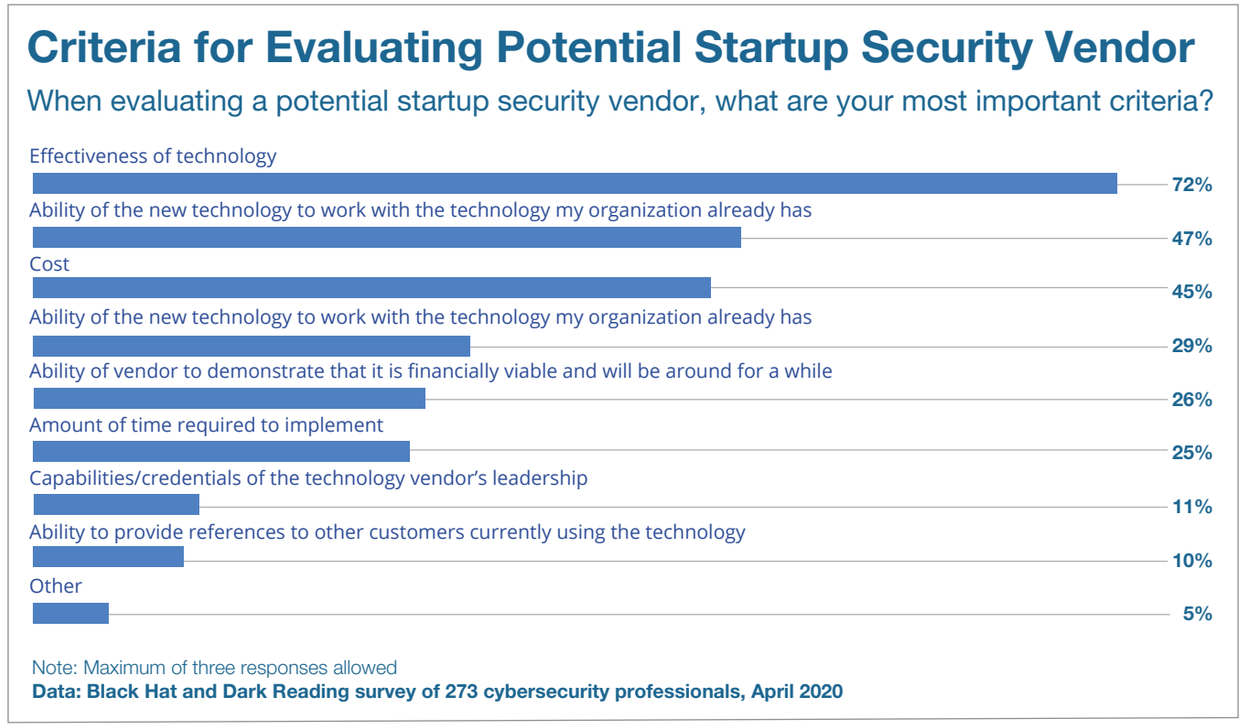
security pros believe that no matter how careful consumers are with their personal information, it's likely that their data and/or credentials are available to criminals online right now. Only 38% of respondents think that it will be possible for individuals to protect their online identity and privacy in the future.

Over the past year, many startups and new technology companies have launched security tools that promise to help solve enterprise cybersecurity problems. For most enterprises, however, it is difficult to find the time and the resources required to identify and evaluate startup vendors that might be able to provide the solutions they need.

In the Black Hat USA Attendee Survey, only 34% of respondents said that their organizations are consistently willing to consider solutions from all startup companies and/or that they have a test bed for evaluating them (**Figure 19**). Twenty-nine percent said they are willing to consider startups but simply don't have time to research and evaluate very many of them and end up choosing mostly well-known vendors. Twenty-eight percent of respondents said they generally do not even consider startup technology vendors unless the startup has a solid customer base, or they have no other choice.

For those enterprises that do evaluate startup security technology vendors, the effectiveness of their technology (72%) is by far the most important criterion for consideration (**Figure 20**). The ability of the startup's technology to work with legacy systems is No. 2 (47%). The cost of the new technology was the third-most important criterion (45%). Interestingly, the capabilities and credentials of the startup vendor's leadership — a central benchmark considered by venture capital investors — plays almost no role in the decision of enterprise security buyers (5%).

Figure 20



The State of the Cybersecurity Community

The outbreak of COVID-19 has put a great deal of stress on the cybersecurity community, which already was stretched to its limits by the constant stream of new vulnerabilities and exploits being discovered at a rapid pace. In open-ended responses, Black Hat USA Attendee Survey respondents called for better communication and sharing of information to help improve enterprise defenses.

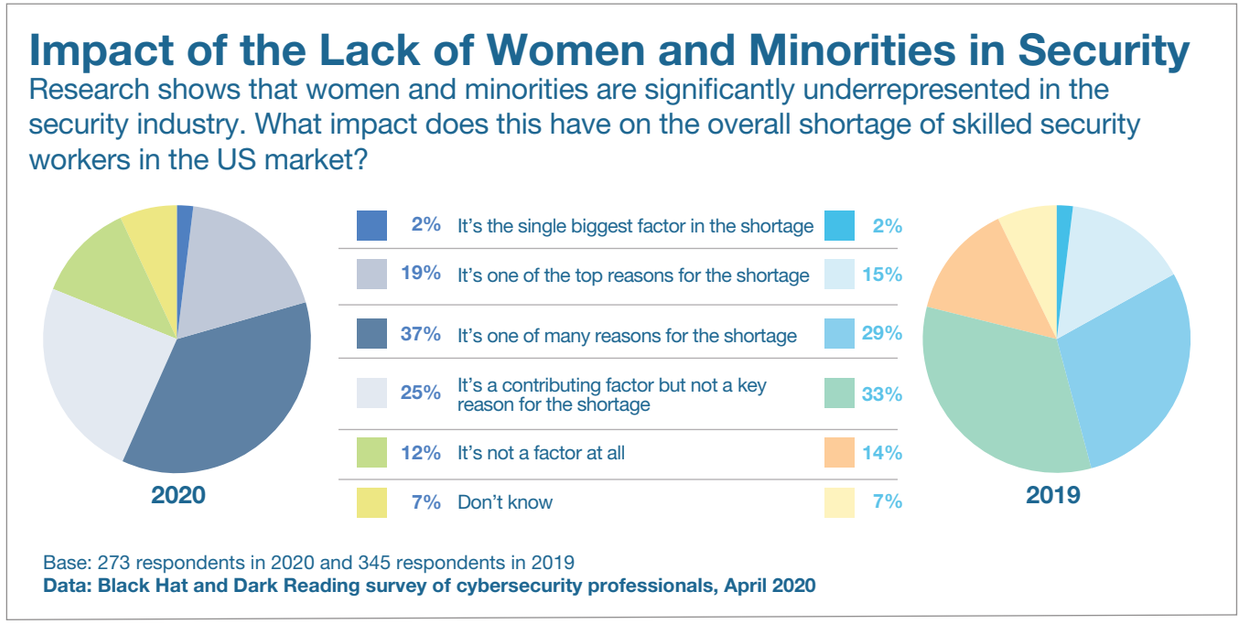
"I believe we need a better private and public sector system for sharing and disclosing cyber incidents," said one respondent. "Full disclosure of the perceived who, what, when, where, and how, and any remediations taken. This would warn and position others to leverage this info to protect each other."

Many respondents also suggested that the cybersecurity community needs more training, both to improve enterprise defenses and to help address the skills shortage. "We need to demystify security and make it easier for stakeholders to understand," said one respondent. "Then we need to use that knowledge to train a larger workforce."

Many cybersecurity professionals also expressed concern over the issue of diversity in hiring, pointing out the broader need for more qualified personnel. "I think the cybersecurity industry could do better at reaching out to certain demographics that are underrepresented in the community," said one respondent. "This would include outreach to kids at an earlier age to get them excited about the industry, but also to let them know that there's a viable and exciting career path."

In the Black Hat USA Attendee Survey, 62% of security pros said that the shortage of women and minorities in the profession

Figure 21



concerned them. Twenty-one percent said the lack of diversity is one of the top reasons for the skills shortage across the industry (**Figure 21**).

Many of the survey responses indicate that cybersecurity professionals are under more pressure than ever before, and that this pressure is taking its toll — not only on enterprise networks but on IT security pros themselves.

When asked about their current level of "burnout," in which professionals lose effectiveness because they are over-stressed and oversubscribed, 38% of security professionals said they consider themselves burned out by their work (a rating of 7 to 10). This figure is up significantly from 30% in 2019 and suggests that burnout is now prevalent across the industry (**Figure 22**).

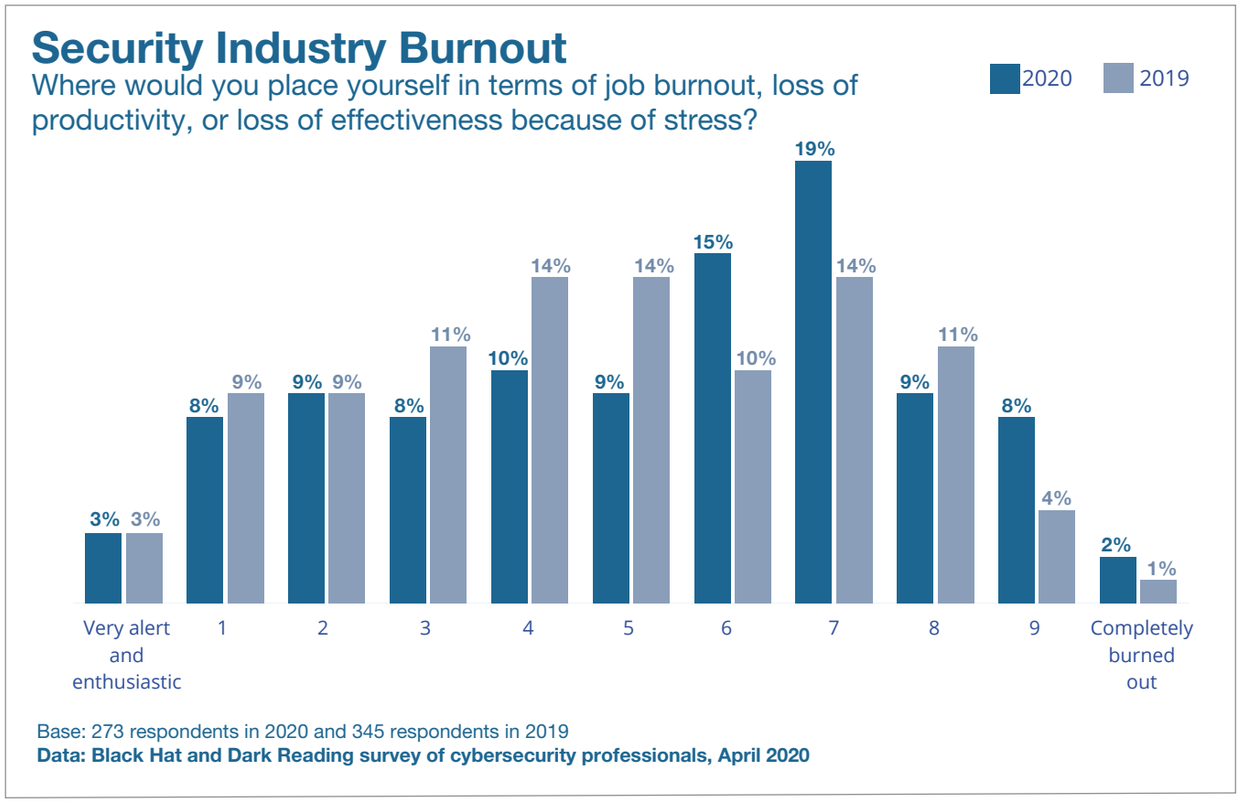
Conclusion

The rise of the global COVID-19 pandemic has made a huge impact on the cybersecurity industry, just as it has in other industries. A majority of cybersecurity professionals believe that the risk to enterprise data is greater than ever, particularly in remote access systems during the quarantine. Black Hat USA Attendee Survey respondents also are concerned about the rapid increase in new exploits built around vulnerabilities exposed during the crisis.

At the national level, cybersecurity professionals are raising a high level of concern around the integrity of the upcoming US elections, and particularly around disinformation campaigns that might affect voter decisions. In addition, security experts warned that attacks on critical infrastructure are more likely than ever, while expressing a lack of confidence that government and private industry are prepared for such attacks.

At the enterprise level, Black Hat USA Attendee Survey respondents think that they

Figure 22



do not have the staff, budget, or technology they need to handle the threats they expect to see in upcoming months. Many are frustrated by a lack of effectiveness in current security tools and an overabundance of hype surrounding technologies that are not delivering on their promises.

At the community level, cybersecurity professionals are increasingly feeling burned out and in need of greater help and support. They seek better information sharing, improved training and education, and greater opportunities for women and minorities.

APPENDIX

Figure 23

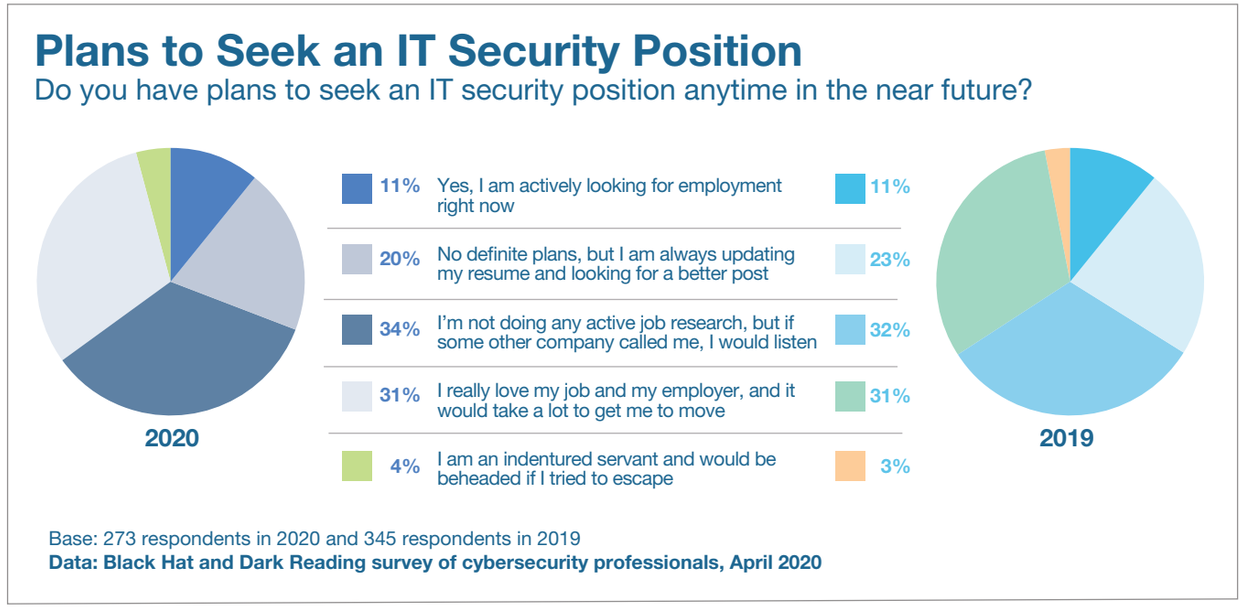


Figure 24

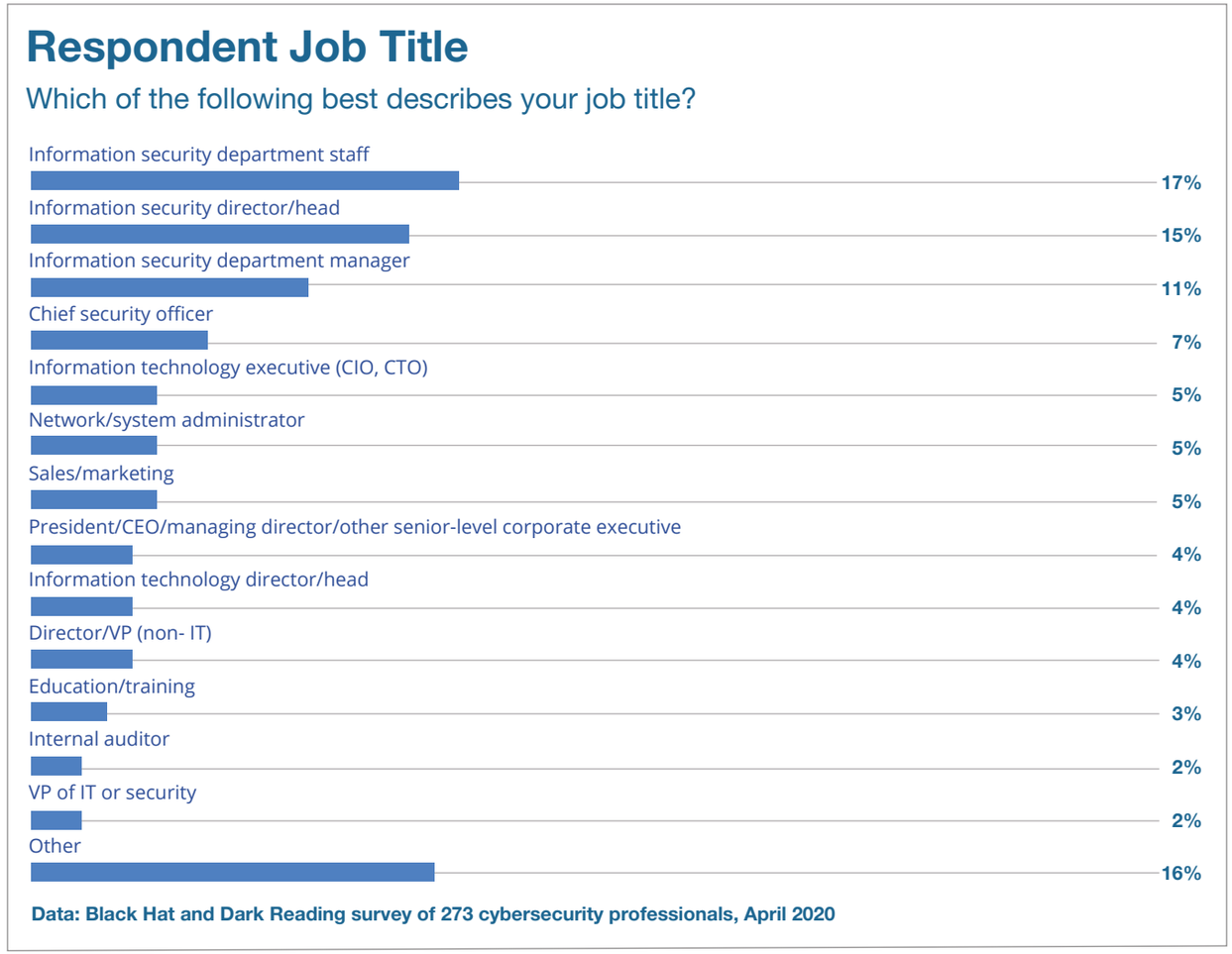

Respondent Job Title
Which of the following best describes your job title?
Information security department staff
17%
Information security director/head
15%
Information security department manager
11%
Chief security officer
7%
Information technology executive (CIO, CTO)
5%
Network/system administrator
5%
Sales/marketing
5%
President/CEO/managing director/other senior-level corporate executive
4%
Information technology director/head
4%
Director/VP (non- IT)
4%
Education/training
3%
Internal auditor
2%
VP of IT or security
2%
Other
16%
Data: Black Hat and Dark Reading survey of 273 cybersecurity professionals, April 2020

Figure 25

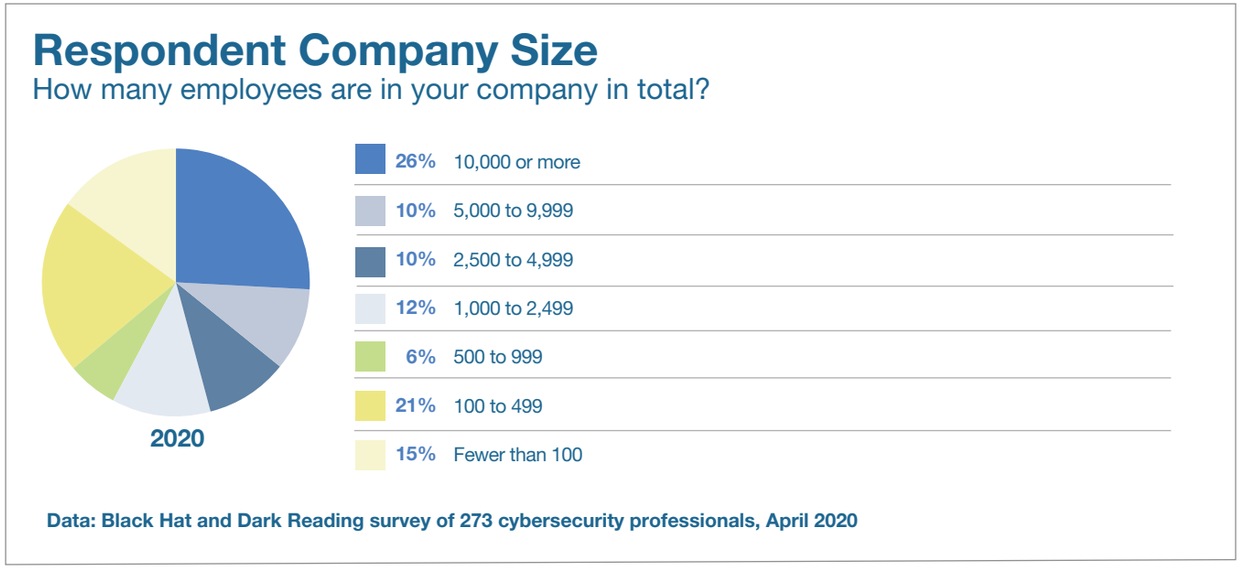

Respondent Company Size
How many employees are in your company in total?
2020
26% 10,000 or more
10% 5,000 to 9,999
10% 2,500 to 4,999
12% 1,000 to 2,499
6% 500 to 999
21% 100 to 499
15% Fewer than 100
Data: Black Hat and Dark Reading survey of 273 cybersecurity professionals, April 2020

Figure 26

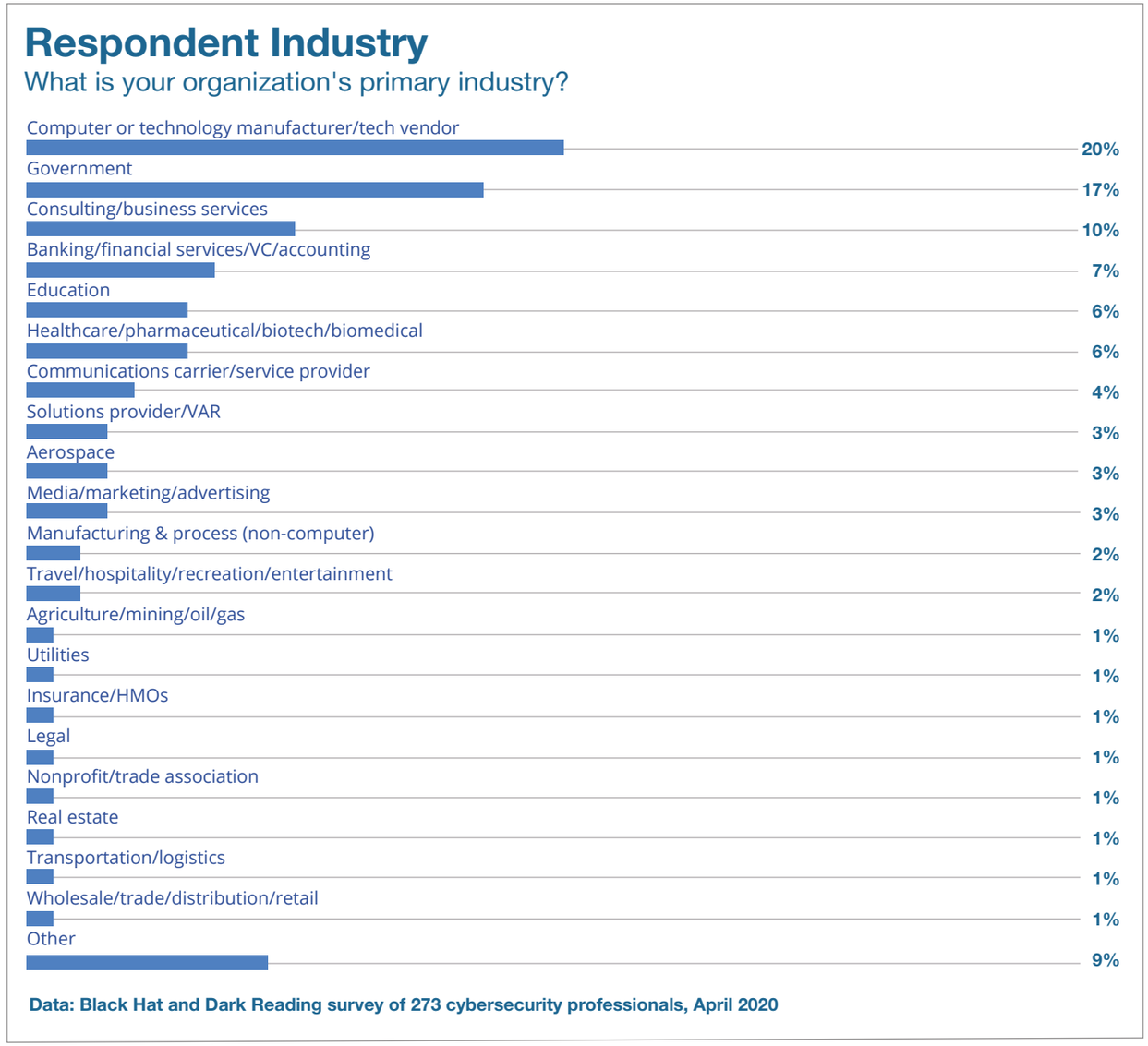
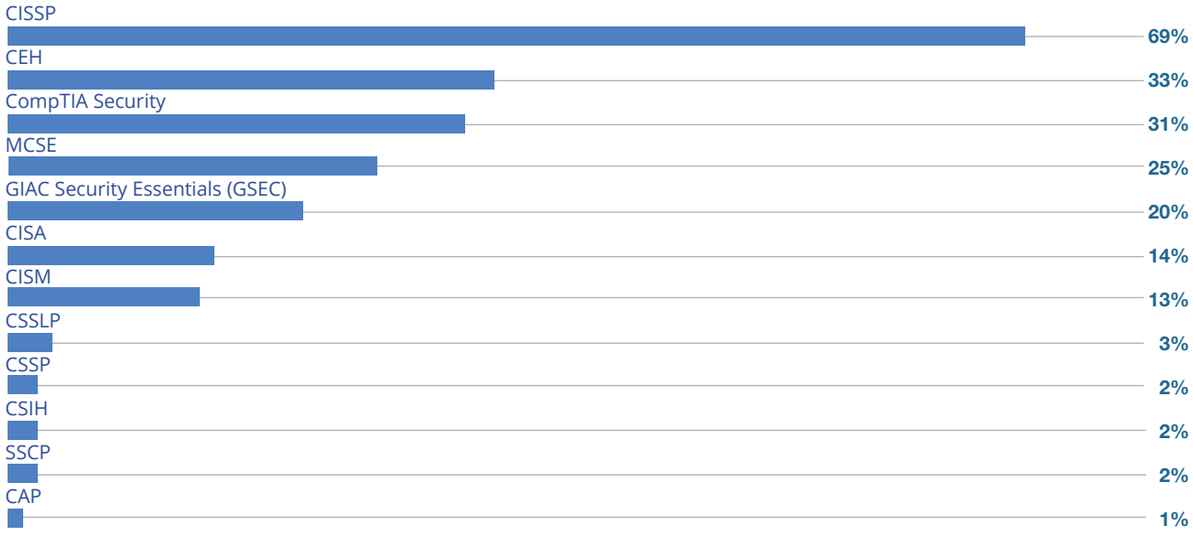

Respondent Industry
What is your organization's primary industry?
Computer or technology manufacturer/tech vendor 20%
Government 17%
Consulting/business services 10%
Banking/financial services/VC/accounting 7%
Education 6%
Healthcare/pharmaceutical/biotech/biomedical 6%
Communications carrier/service provider 4%
Solutions provider/VAR 3%
Aerospace 3%
Media/marketing/advertising 3%
Manufacturing & process (non-computer) 2%
Travel/hospitality/recreation/entertainment 2%
Agriculture/mining/oil/gas 1%
Utilities 1%
Insurance/HMOs 1%
Legal 1%
Nonprofit/trade association 1%
Real estate 1%
Transportation/logistics 1%
Wholesale/trade/distribution/retail 1%
Other 9%
Data: Black Hat and Dark Reading survey of 273 cybersecurity professionals, April 2020

Figure 27

Respondent Certifications

What security certifications/training certificates have you held, either now or in the past?



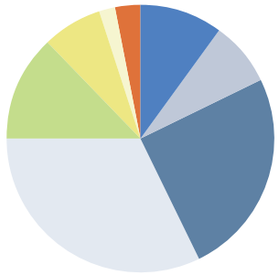
Note: Multiple responses allowed

Data: Black Hat and Dark Reading survey of 273 cybersecurity professionals, April 2020

Figure 28

Respondent Annual Salary

What is your current annual salary?



2020

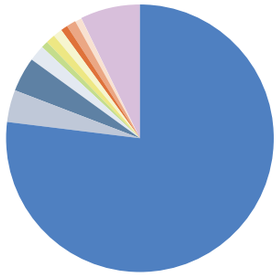
10%	$250,000 or more	13%	$75,000–$99,999
8%	$200,000–$249,999	7%	$50,000–$74,999
25%	$150,000–$199,999	2%	$30,000–$49,999
32%	$100,000–$149,999	3%	Under $30,000

Data: Black Hat and Dark Reading survey of 273 cybersecurity professionals, April 2020

Figure 29

Respondent Country of Residence

In what country do you live?



2020

77%	United States	1%	Japan
4%	Canada	1%	Singapore
4%	Germany	1%	Sweden
2%	Brazil	1%	United Kingdom
1%	France	7%	Other
1%	Israel		

Data: Black Hat and Dark Reading survey of 273 cybersecurity professionals, April 2020