CYBER INSECURITY IN HEALTHCARE:

THE COST AND IMPACT ON PATIENT SAFETY AND CARE

Independently conducted by:

Ponemon INSTITUTE

Sponsored by:

proofpoint.

TABLE OF CONTENTS

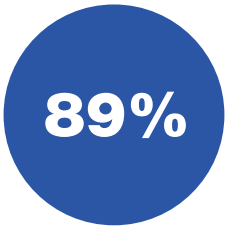
EXECUTIVE SUMMARY

THE PURPOSE OF THIS RESEARCH IS TO UNDERSTAND THE CYBERSECURITY THREATS TARGETING HEALTHCARE ORGANIZATIONS AND THE COST OF RESPONDING TO ATTACKS THAT CAN ENDANGER PATIENT SAFETY AND CARE DELIVERY.

With sponsorship from Proofpoint, Ponemon Institute surveyed 641 IT and IT security practitioners in healthcare organizations who are responsible for participating in cybersecurity strategies including setting IT cybersecurity priorities, managing budgets and selecting vendors and contractors.

According to the research, 89 percent of organizations in this research experienced cyberattacks in the past 12 months. For organizations in that group, the average number of attacks was 43. We asked respondents to estimate the single most expensive cyberattack in the past 12 months from a range of less than $10,000 to more than $25 million. Based on the responses, the average total cost for the most expensive cyberattack experienced was $4.4 million. This included all direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs and lost business opportunities.

At an average cost of $1.1 million, lost productivity was the most significant financial consequence from the cyberattack. However, despite the connection between cyberattacks and patient safety, the least amount of cost following a cyberattack was the time required to ensure the impact on patient care was corrected ($664,350).



of organizations in this research had at least one cyberattack over the past 12 months

The average total cost for the single most expensive cyberattack experienced over the past 12 months

in lost productivity was on average the most significant financial consequence from the cyberattack

The report analyzes four types of cyberattacks and their impact on healthcare organizations, patient safety and patient care delivery:

Cloud compromise. Seventy-five percent of respondents say their organizations are vulnerable to a cloud compromise. In the past two years 54 percent of respondents say their organizations experienced at least one cloud compromise. Organizations within this group experienced an average of 22 such compromises in the past two years.

Ransomware. Seventy-two percent of respondents believe their organizations are vulnerable to a ransomware attack. When asked what cybersecurity threats their organizations are most concerned about ransomware is the number one (60% of respondents). In the past two years, organizations that had ransomware attacks (41 percent of respondents) experienced an average of three such attacks.

Supply chain attacks. Seventy-one percent of respondents say their organizations are vulnerable to a supply chain attack. Fifty percent of respondents say their organizations experienced at least one attack against the supply chain in the past two years. Organizations represented in this group had an average of four supply chain attacks in the past two years.

Business email compromise (BEC)/spoofing phishing.[1] BEC attacks encompass a wide range of impersonation tactics such as spoofing, phishing and social engineering. Sixty-four percent of respondents say their organizations are vulnerable to a BEC incident. Fifty-one percent of respondents said they experienced at least one BEC incident in the past two years. Organizations in this group had an average of 3.5 BEC attacks in the past two years.

An important part of the research is exploring how cyberattacks affect patient safety and care delivery. Following are highlights on how cyberattacks have affected patient safety and care delivery.

- Fifty percent of respondents say their organizations had an attack against its supply chain. Seventy percent of those respondents say it disrupted patient care. The consequences included the delay of procedures and tests that resulted in poor outcomes such as an increase in the severity of an illness (54 percent). Another consequence was a longer length of stay (51 percent). Twenty-three percent of respondents say there was an increase in mortality rate.
- Sixty-seven percent of respondents say a BEC attack and/or a ransomware attack against their organizations disrupted patient care. Twenty-one percent of respondents say a BEC incident and 24 percent of respondents say ransomware increased the mortality rate.
- Ransomware attacks are more likely than the other types of attacks to hurt patient safety and care delivery. Sixty-four percent of respondents in organizations that experienced a ransomware attack say it caused delays in procedures and tests that resulted in poor outcomes. Fifty-nine percent of respondents say it resulted in longer lengths of stay, which strains resources.
- Technologies such as cloud, mobile, big data and IoT increase the risks to patient information and safety, according to 67 percent of respondents.

[1] In the survey, BEC and spoofing phishing were combined in the questions. In the context of this research, spoofing and phishing are tactics used to cause the BEC compromise.

Other key takeaways include the following.

Insecure medical devices and mobile apps are considered among the top cybersecurity concerns in healthcare. On average, organizations have more than 26,000 network-connected devices. Sixty-four percent of respondents say they are concerned about the security of these medical devices and 59 percent of respondents say they are concerned about insecure mobile apps. Examples of medical devices that potentially could be vulnerable to an attack include pacemakers and infusion pumps.

Organizations use a combination of approaches to user access and identity management in the cloud. Sixty percent of respondents say their organizations use a combination of solutions. These include separate identity management interfaces for the cloud and on-premises environments, unified identity management interface for both the cloud and on-premises environments and deployment of single sign-on.

The lack of preparedness puts healthcare organizations and patients at risk. While insecure medical devices are considered the top cybersecurity threat, only about half (51 percent) of respondents say their organizations include prevention and response to an attack on these devices as part of their cybersecurity strategy. Less than half of respondents say they have documented the steps to prevent and respond to a BEC attack (48 percent) and/or attacks to the supply chain (44 percent of respondents). Most organizations focus on steps to prevent and respond to cloud compromises (63 percent of respondents) and/or ransomware (62 percent of respondents).

Lack of in-house expertise, staffing and collaboration with other functions are challenges to having an effective cybersecurity posture. Fifty-three percent of respondents say their organizations lack in-house expertise and 46 percent of respondents say insufficient staff are challenges. Working in silos and lack of collaboration with other functions also affects the effectiveness of their organizations' cybersecurity strategy.

Ensuring security without diminishing user productivity is considered essential to organizations' cybersecurity strategy. It is critical in healthcare organizations to have a productive workforce while effectively securing highly sensitive and confidential patient information. Lost productivity is also the highest cost incurred when responding to a cyberattack ($1.1 million). The three most essential steps are to use adaptive access controls to protect users most at risk while not reducing the productivity of other users (79 percent of respondents), have strong authentication controls in place prior to accessing data and applications in the cloud (78 percent of respondents) and support multiple identity federation standards, including security assertion markup language (SAML) (74 percent of respondents).

Training and awareness programs and monitoring employees are the top two steps taken to reduce the insider risk. Negligent employees pose a significant risk to healthcare organizations. Fifty-nine percent of respondents say their organizations take steps to address the risk of employees' lack of awareness about cybersecurity threats, especially BEC. Of these respondents, 63 percent of respondents say they conduct regular training and awareness programs and 59 percent of respondents say their organizations monitor the actions of employees.

As part of the cybersecurity strategy, 60 percent of respondents say their organizations use threat intelligence. The types of threat intelligence commonly used are network traffic (57 percent of respondents), firewall/IPS traffic (53 percent of respondents), dark web data (46 percent of respondents) and user behavior (44 percent of respondents).

KEY FINDINGS

IN THIS SECTION, WE PROVIDE AN ANALYSIS OF THE RESEARCH.

The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following topics.

- Cloud compromise, ransomware, supply chain and business email compromise (BEC) in healthcare
- The impact of cyberattacks on patient care
- The cost of cyber insecurity
- Vulnerabilities in the cloud
- Solutions and response to healthcare cyber insecurity

FIGURE 1.

Healthcare organizations are vulnerable to cyberattacks

Healthcare organizations recognize how vulnerable they are to the four cyberattacks featured in this research. Respondents were asked to rate their organizations' vulnerability to specific types of threats on a scale from 1 = not vulnerable to 10 = highly vulnerable. Figure 1 presents the vulnerable and highly vulnerable responses (7+ on the 10-point scale). As shown, almost all respondents recognize the threat of cloud compromises (75 percent) followed by ransomware attacks (72 percent) and supply chain attacks (71 percent). Also high is healthcare organizations' vulnerability to BEC/ spoofing phishing (64 percent of respondents).

On a scale from 1 = not vulnerable to 10 = highly vulnerable, 7+ responses presented

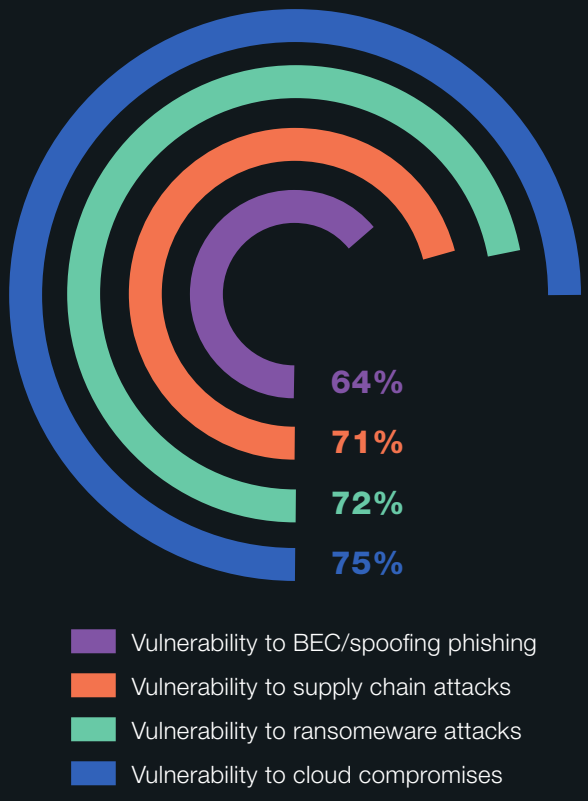


FIGURE 2.

The top six cybersecurity threats of greatest concern

Insecure medical devices and mobile devices are among the top cybersecurity concerns in healthcare. On average, organizations have more than 26,000 network-connected devices. As shown here, 64 percent of respondents say they are concerned about the security of their medical devices, which can have a significant impact on patient safety. Examples of medical devices are pacemakers and insulin pumps. Fifty-nine percent of respondents say they are concerned about insecure mobile apps. Ransomware is the number two threat (60 percent of respondents).

More than one response permitted

Cloud compromises and attacks in the supply chain were the most frequent types of attacks against healthcare organizations.

Figure 3 on Page 9 shows the frequency of each attack. Cloud compromise results from criminals obtaining access to credentials (user IDs and passwords). The consequence is typically an account takeover where criminals then use those validated credentials to takeover accounts, commit fraud and transfer sensitive data to systems under their control. Fifty-four percent of respondents say their organizations experienced a cloud compromise in the past two years. The average number of cloud compromises for these organizations was 22 in the past two years.

Forty-one percent of respondents say their organizations had an average of three ransomware attacks in the past two years.

Ransomware is a sophisticated piece of malware that blocks the victim's access to files. While there are many strains of ransomware, they generally fall into two categories. Crypto ransomware encrypts files on a computer or mobile device making them unstable. Crypto ransomware essentially takes the files hostage, demanding a ransom in exchange for the decryption key needed to restore the files. Locker ransomware is a virus that blocks basic computer functions, essentially locking the victim out of their data and files located on the infected device. Instead of targeting files with encryption, cybercriminals demand a ransom to unlock the device.

Fifty percent of respondents say their organizations had an attack against their supply chain in the past two years. The average number of attacks was four in the past two years.

Supplier impersonation and compromise attacks occur when a malicious actor impersonates or successfully compromises an email account in the supply chain. The attacker then observes, mimics and uses historical information to craft scenarios to spoof employees in the supply chain.

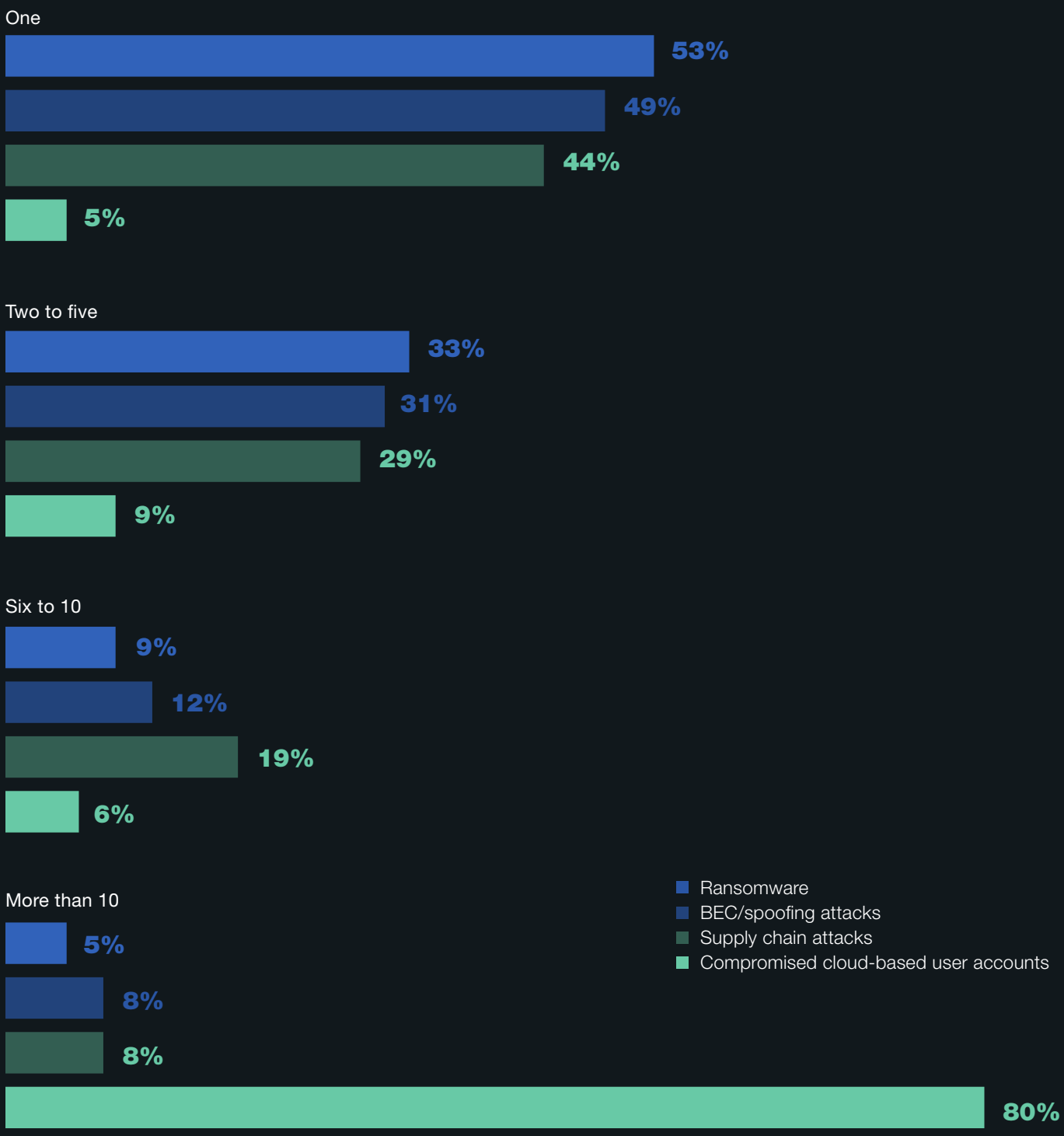
Fifty-one percent of healthcare organizations in this study experienced at least one BEC attack in the past two years. Organizations in this group had an average of 3.5 BEC attacks in the past two years.

BEC attacks are a form of cybercrime which uses email fraud to attack healthcare organizations to achieve a specific outcome which negatively impacts the targeted organization. Examples include invoicing fraud, extortion, payroll redirects and advance-fee fraud.

FIGURE 3.

Frequency of attacks in the past two years

Extrapolated averages for attacks: Ransomware 3 attacks, Supply chain 4 attacks, BEC/spoofing 3.5, Cloud compromises 21



[2] An extrapolated value is a weighted average. Respondents were asked to report the number of attacks within a range. The extrapolated value is used to explain the average median value based on the frequency of responses. These values can reveal trends within complex sets of data.

CYBERATTACKS HAVE DISRUPTED CARE, INCREASING THE RISK TO PATIENTS.

FIGURE 4.

Did these cyber attacks disrupt patient care?

Figure 4 shows the four types of cyberattacks featured in this research and if they hurt patient safety and care delivery. Of those organizations that experienced these attacks, more respondents (70 percent) believe the supply chain attacks disrupted patient care followed by the BEC and ransomware attacks (67 percent of respondents).

Such disruptions include delays in procedures and tests that have resulted in poor outcomes, longer length of stay, increase in patients transferred or diverted to other facilities, increase in complications from medical procedures and an increase in mortality rate.

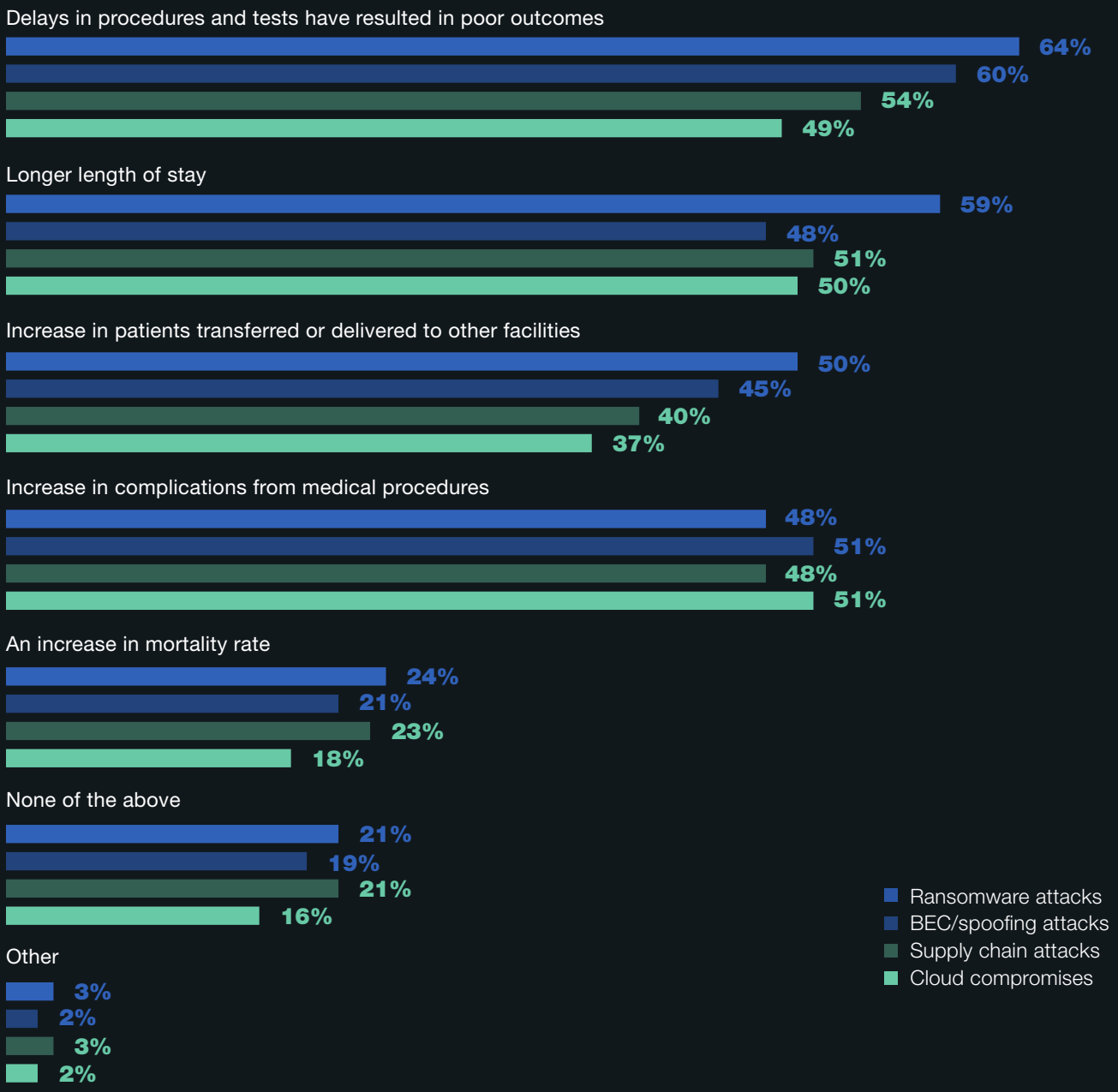
Yes responses presented

FIGURE 5.

If your organization experienced these cyberattacks, what impact did they have on patient care?

Ransomware attacks are more likely to hurt patient safety and care delivery than other cyberattacks. As shown here, 64 percent of respondents in organizations that had a ransomware attack say it caused delays in procedures and tests that resulted in such poor outcomes as the increase in the severity of the illness. Fifty-nine percent of these respondents say patients had longer lengths of stay because of ransomware, which puts a burden on healthcare organizations.

More than one response permitted



LOST PRODUCTIVITY IS THE MOST SIGNIFICANT FINANCIAL CONSEQUENCE FROM A CYBERSECURITY COMPROMISE.

TABLE 1.

Five average costs of a healthcare cybersecurity compromise

According to the research, 89 percent of organizations in this research experienced cyberattacks in the previous 12 months. For organizations in that group, the average number of attacks was 43. We asked respondents to estimate the single most costly cyberattack in the past 12 months from a range of less than $10,000 to more than $25 million. Based on the responses, the average total cost for the most expensive cyberattack experienced was $4.4 million. This includes all direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs and lost business opportunities.

As shown here, respondents estimated that the highest cost ($1.1 million) was caused by users' idle time and lost productivity because of downtime or system performance delays. This is followed by disruption to normal healthcare operations because of system availability problems ($1 million), damage or theft of assets and infrastructure ($930,090) and remediation & technical support activities, including forensic investigations, incident response activities, help desk and delivery of services to patients ($708,640).

Despite the connection between cyberattacks and patient safety, the least amount of cost was due to the time required to ensure impact on patient care is corrected.

COMPROMISE RESULT	PERCENTAGE	AVERAGE COST
Users' idle time and lost productivity because of downtime or system performance delays	25%	$1,107,250
Disruption to normal healthcare operations because of system availability problems	23%	$1,018,670
Damage or theft of IT assets and infrastructure	21%	$930,090
Remediation & technical support activities, including forensic investigations, incident response activities, help desk and delivery of services to patients	16%	$708,640
Time required to ensure impact on patient care is corrected	15%	$664,350
		$4,429,000

VULNERABILITIES IN THE CLOUD

AS HEALTHCARE ORGANIZATIONS MOVE SENSITIVE PATIENT DATA TO THE CLOUD, RESPONDENTS RECOGNIZE THE RISKS.

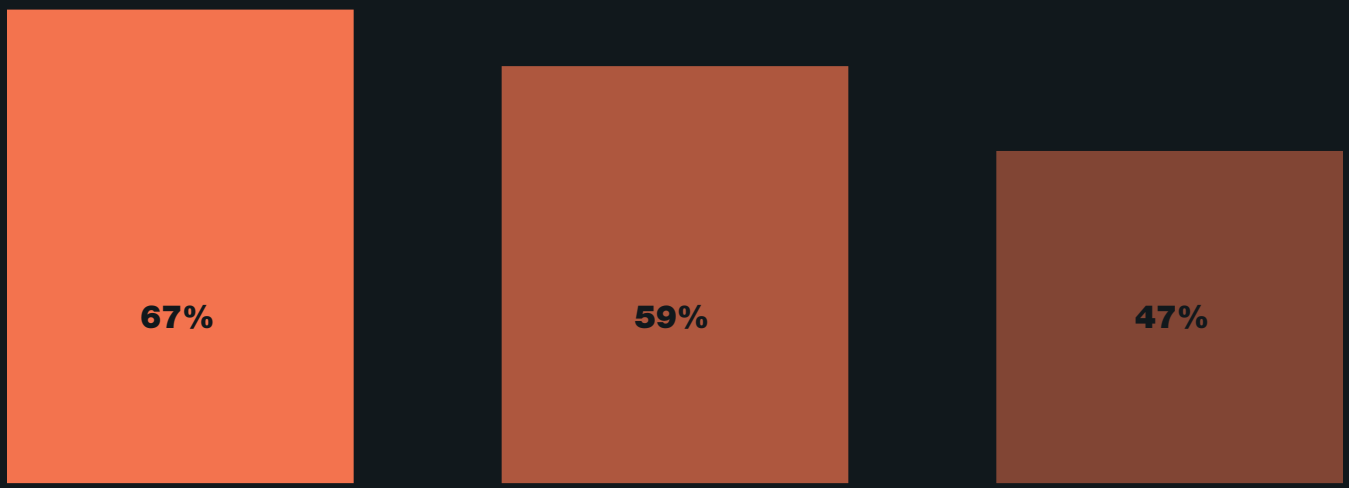
FIGURE 6.

Vulnerabilities in the cloud

As discussed, organizations that had a cloud compromise experienced an average of 22 such incidents in the past two years.

Sixty-seven percent of respondents say the cloud, mobile, big data and IoT increase threats to patient information and safety. Fifty-nine percent of respondents say cloud account takeovers present a significant security risk.

Strongly agree and Agree responses presented



Technologies such as cloud, mobile, big data and the Internet of Things increase the vulnerability of and threats to patient information and safety

Cloud account takeovers present a significant security risk for my organization

Internal phishing results in more compromised cloud accounts

FIGURE 7.

How does your organization protect confidential or sensitive information in the cloud?

Encryption, tokenization or other cryptographic tools are used to protect data in the cloud. As shown here, the primary technologies used are encryption, tokenization or other cryptographic tools followed by premium security services provided by the cloud provider.

More than one response permitted

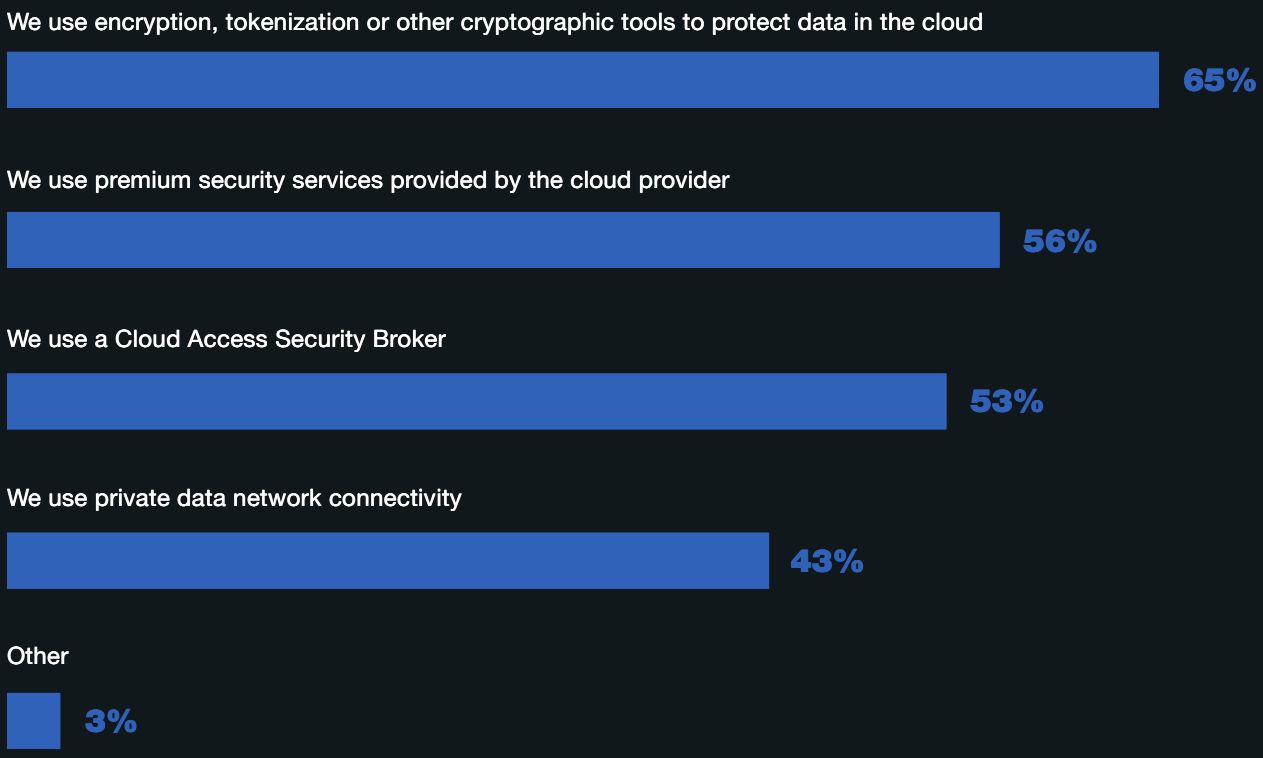
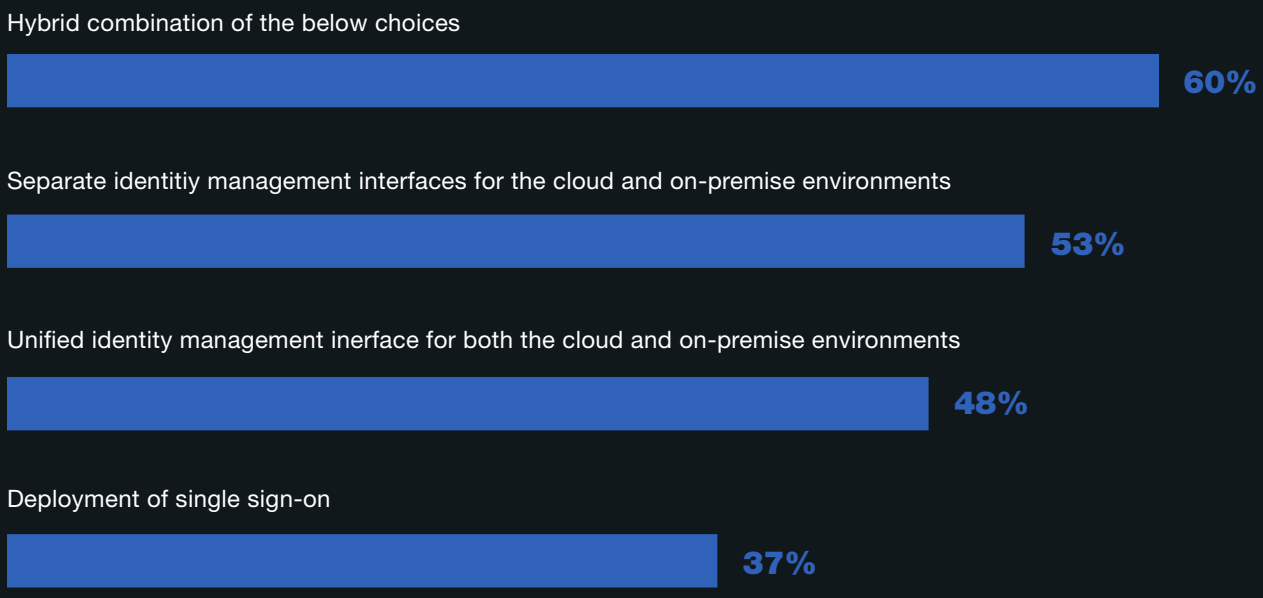


FIGURE 8.

What best describes your organization's approach to user access and identity management in the cloud?

Organizations use a combination of several approaches to user access and identity management in the cloud. To secure access to patient data in the cloud there are specific methods to pursue. As shown here, 60 percent of respondents say their organizations use a combination of approaches. This is followed by separate identity management interfaces for the cloud and on-premises environments (53 percent) and unified identity management interface for both the cloud and on-premises environments (48 percent).

More than one response permitted



THE LACK OF PREPAREDNESS PUTS HEALTHCARE ORGANIZATIONS AND PATIENTS AT RISK.

FIGURE 9.

Does your organization include the prevention and response to the following threats as part of its cybersecurity strategy?

While insecure medical devices are considered the top cybersecurity threat to healthcare organizations only about half (51 percent) of respondents say their organizations include prevention and response to an attack on these devices as part of their cybersecurity strategy. Less than half of respondents say they have documented the steps to prevent and respond to a BEC attack (48 percent) and/or attacks to the supply chain (44 percent). Most organizations focus on steps to prevent and respond to cloud compromises (63 percent of respondents) and/or ransomware (62 percent of respondents).

More than one response permitted

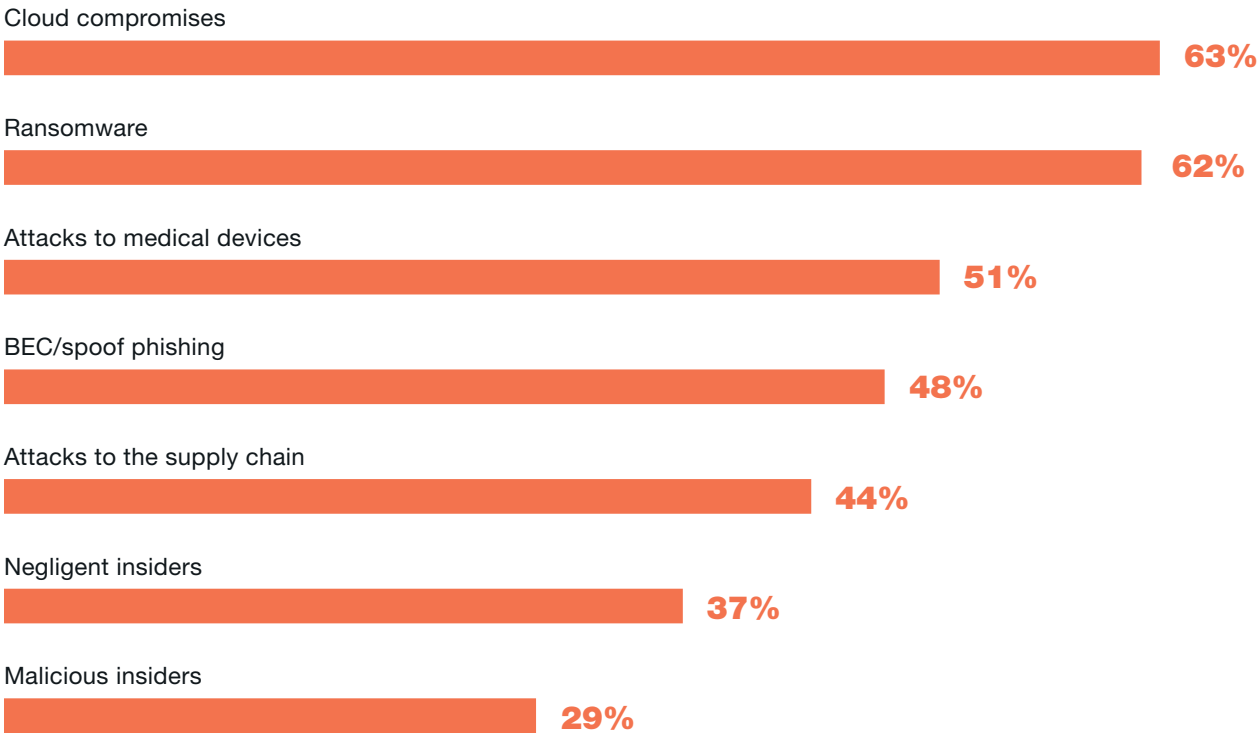


FIGURE 10.

What challenges keep your organization's cybersecurity posture from being fully effective?

Lack of in-house expertise, staffing and collaboration with other functions are challenges to having an effective cybersecurity posture. As shown here, 53 percent of respondents say their organizations lack in-house expertise and another 46 percent of respondents say insufficient staff are challenges. Working in silos and lack of collaboration with other functions also impact the effectiveness of their organizations' cybersecurity strategy.

Three responses permitted

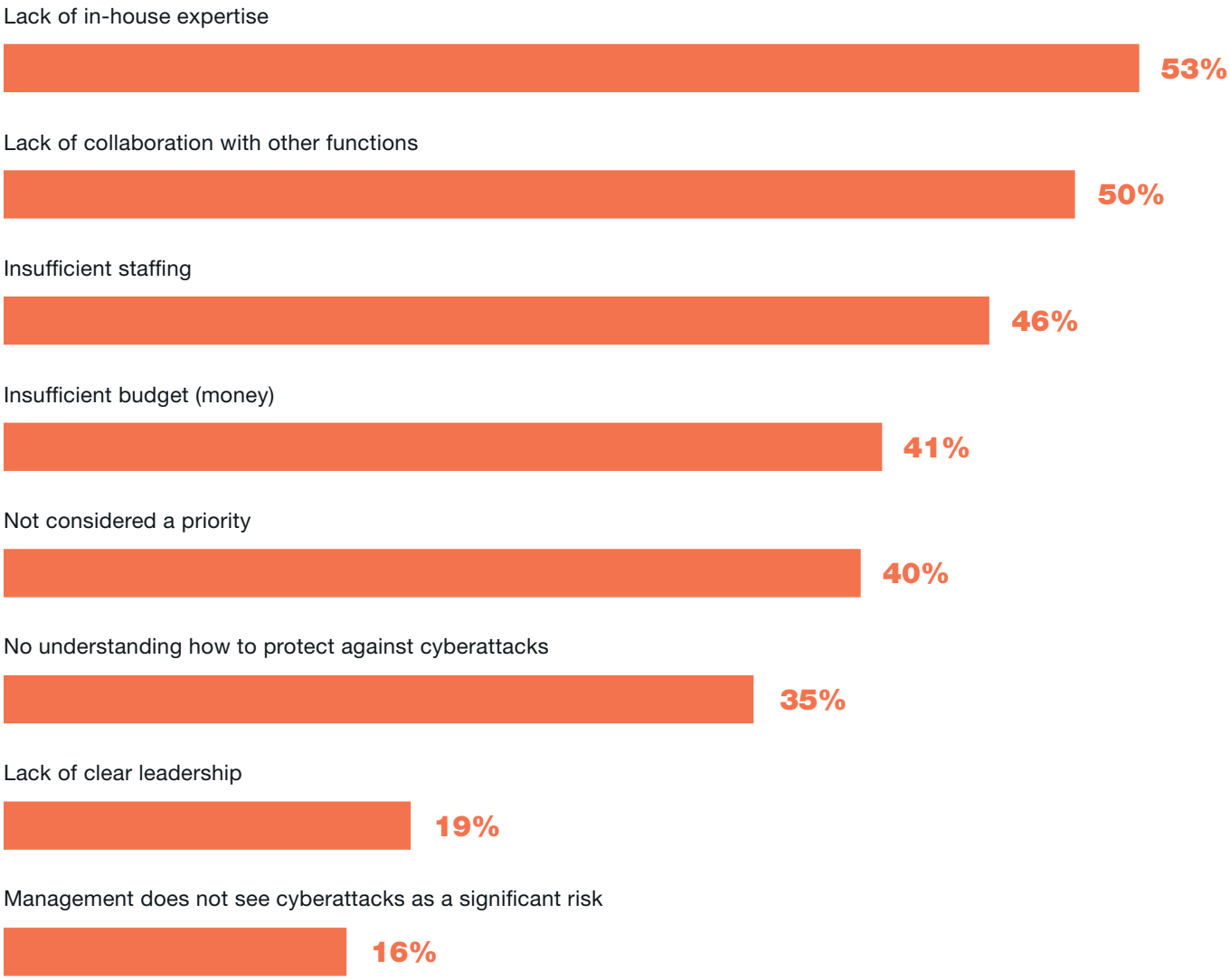


FIGURE 11.

Essential steps and solutions to reducing cybersecurity threats without diminishing productivity

Ensuring security without diminishing user productivity is considered essential to organizations' cybersecurity strategy. It is critical in healthcare organizations to have a productive workforce while effectively securing highly sensitive and confidential patient information. Lost productivity is also the highest cost incurred when responding to a cyberattack ($1.1 million).

Respondents were asked to rate how essential specific steps and solutions are to reducing cybersecurity threats on a scale from 1 = not essential to 10 = very essential. This chart presents the essential and very essential responses (7+ on the 10-point scale).

As shown, the three most essential steps are to use adaptive access controls to protect users most at risk while not reducing the productivity of other users (79 percent of respondents), have strong authentication controls in place prior to accessing data and applications in the cloud (78 percent of respondents) and support multiple identity federation standards, including security assertion markup language (SAML) (74 percent of respondents).

On a scale from 1 = not essential to 10 = very essential, 7+ responses presented

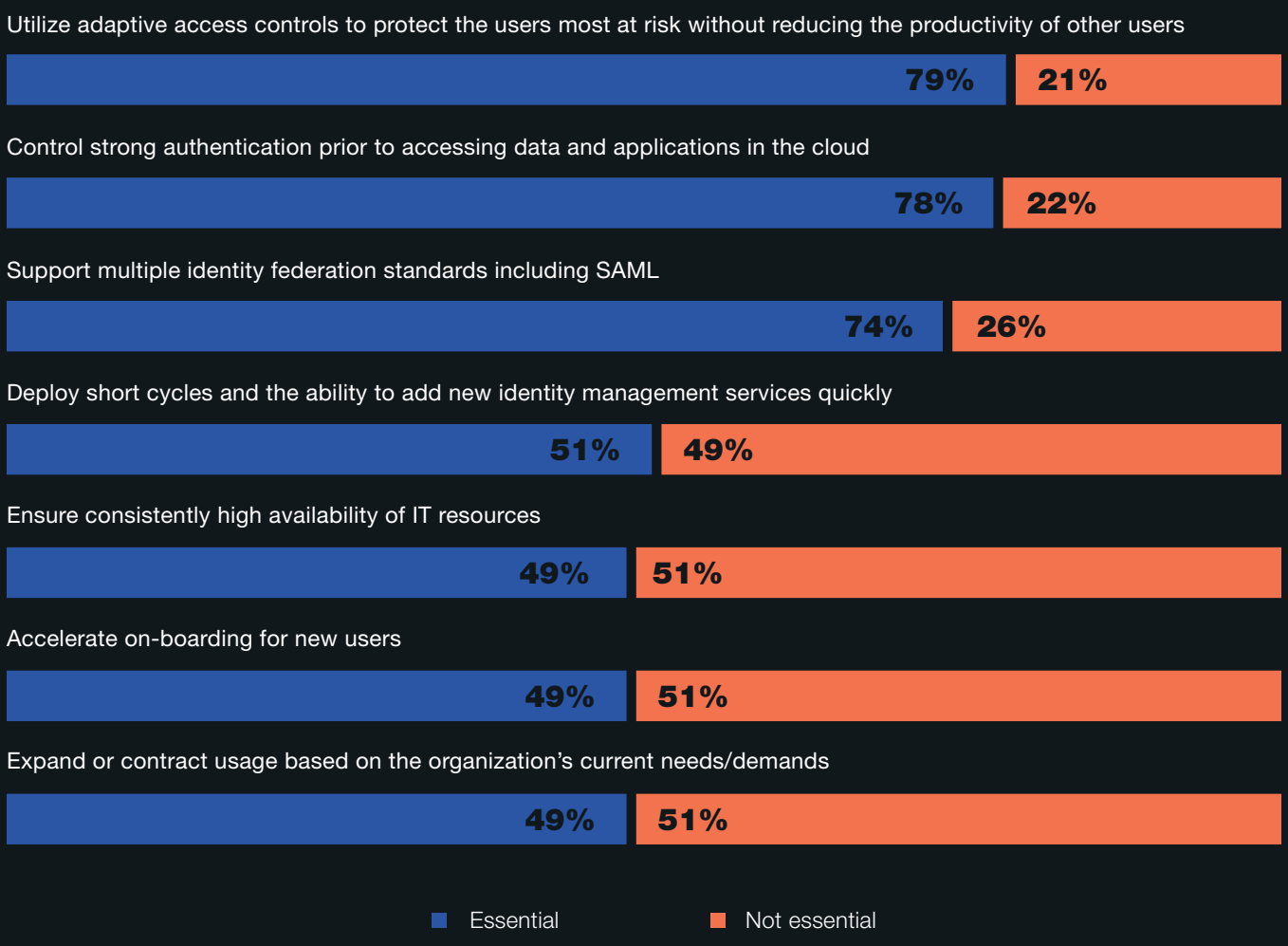


FIGURE 12.

Steps taken to reduce the risk of employees' lack of awareness

Training and awareness programs and monitoring employees are the top two steps taken to reduce the insider risk. Negligent employees pose a significant risk to healthcare organizations. Fifty-nine percent of respondents say their organizations take steps to address the risk of employees' lack of awareness about cybersecurity threats, especially BEC. As shown in Figure 12, of these respondents, 63 percent of respondents say their organizations conduct a regular training and awareness program and 59 percent of respondents say their organizations monitor the actions of employees.

More than one response permitted

FIGURE 13.

Technologies used to reduce phishing and email-based attacks

To reduce phishing and BEC attacks, organizations are using identity and access management (56 percent of respondents), multi-factor authentication (56 percent of respondents) and email data loss prevention (52 percent of respondents), as shown in Figure 13.

More than one response permitted

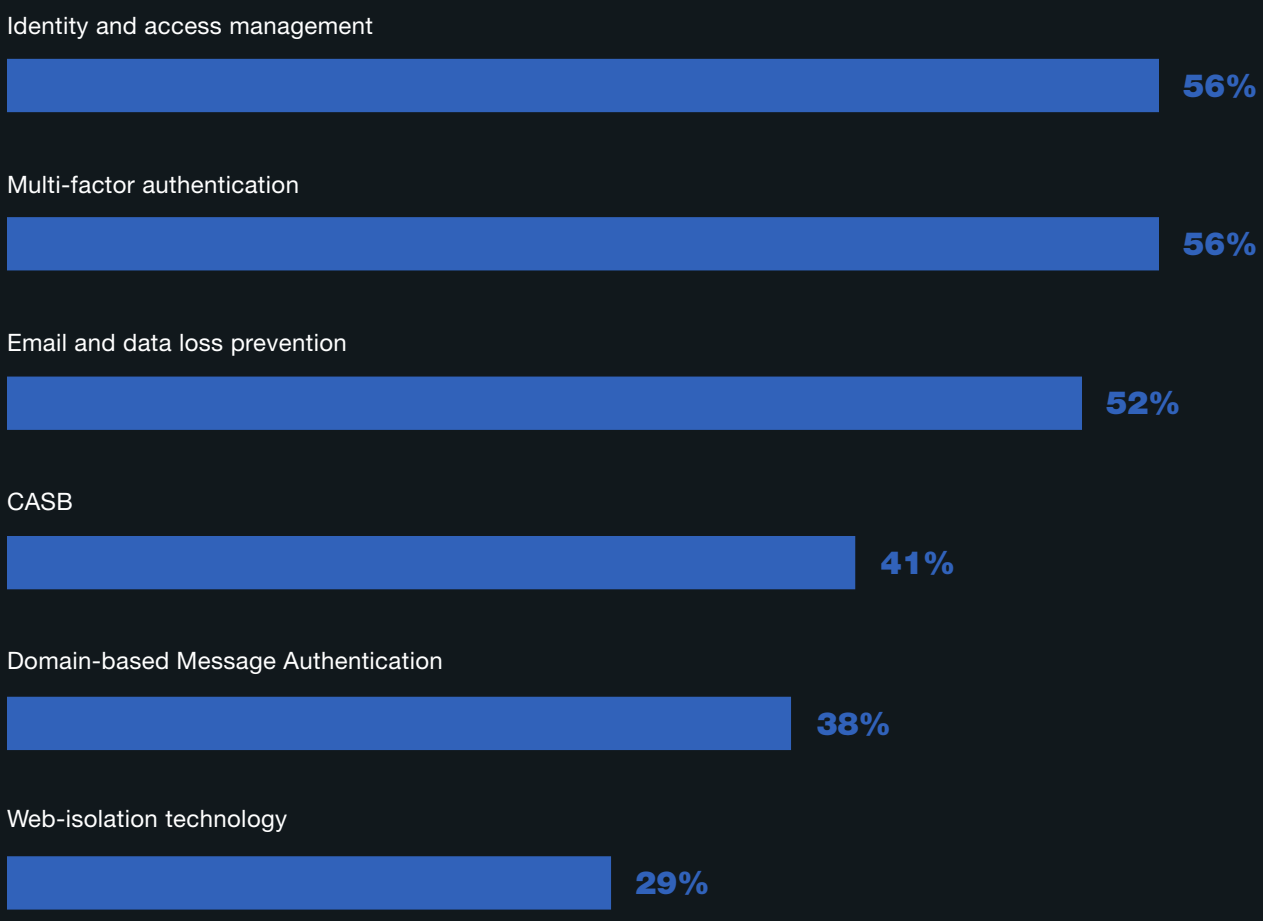


FIGURE 14.

Threat intelligence used in organization's cybersecurity strategy

As part of its cybersecurity strategy, 60 percent of respondents say their organizations use threat intelligence. As shown here, the types of threat intelligence most used are network traffic (57 percent of respondents), firewall/IPS traffic (53 percent of respondents), dark web data (46 percent of respondents) and user behavior (44 percent of respondents).

More than one response permitted

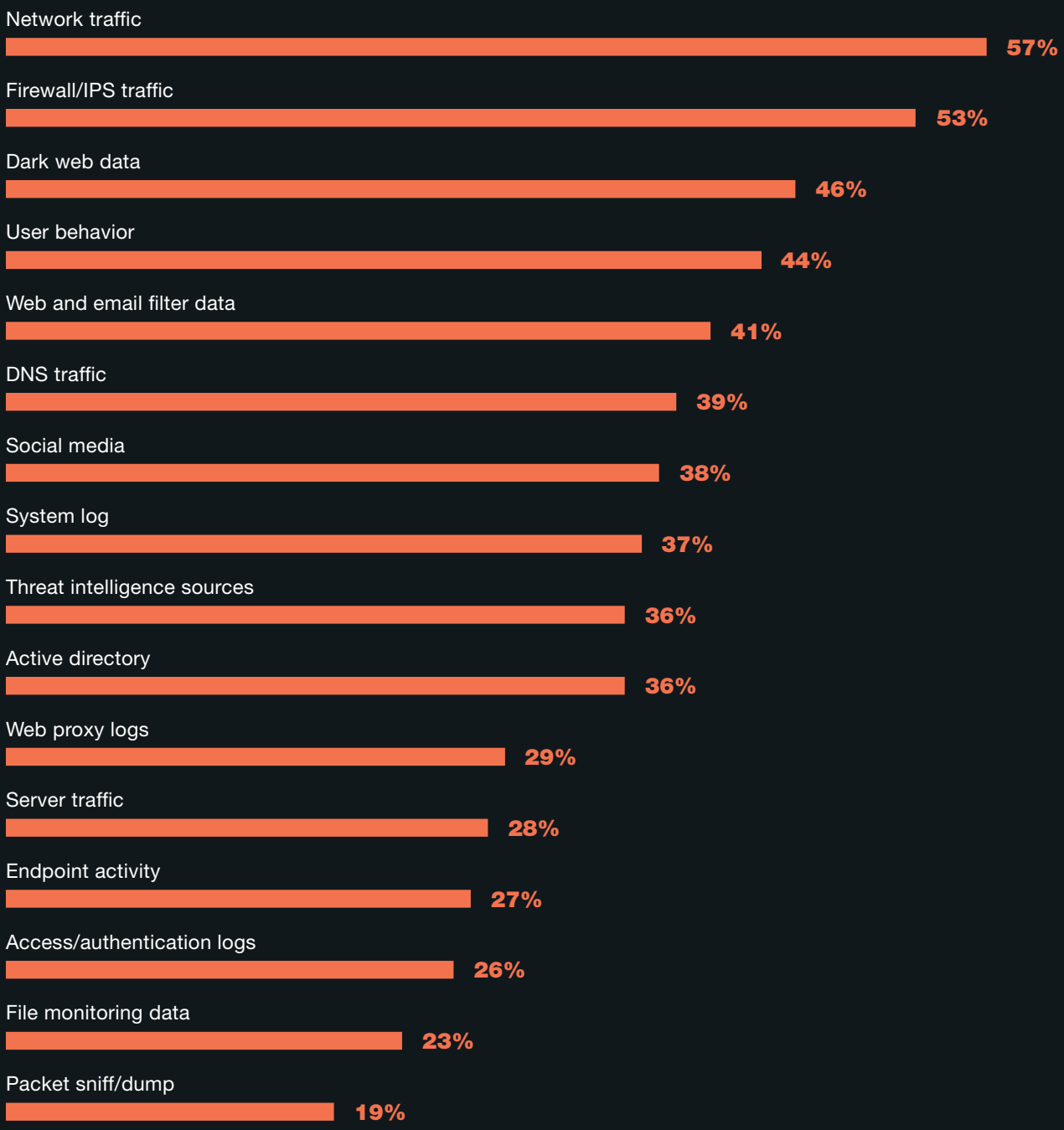
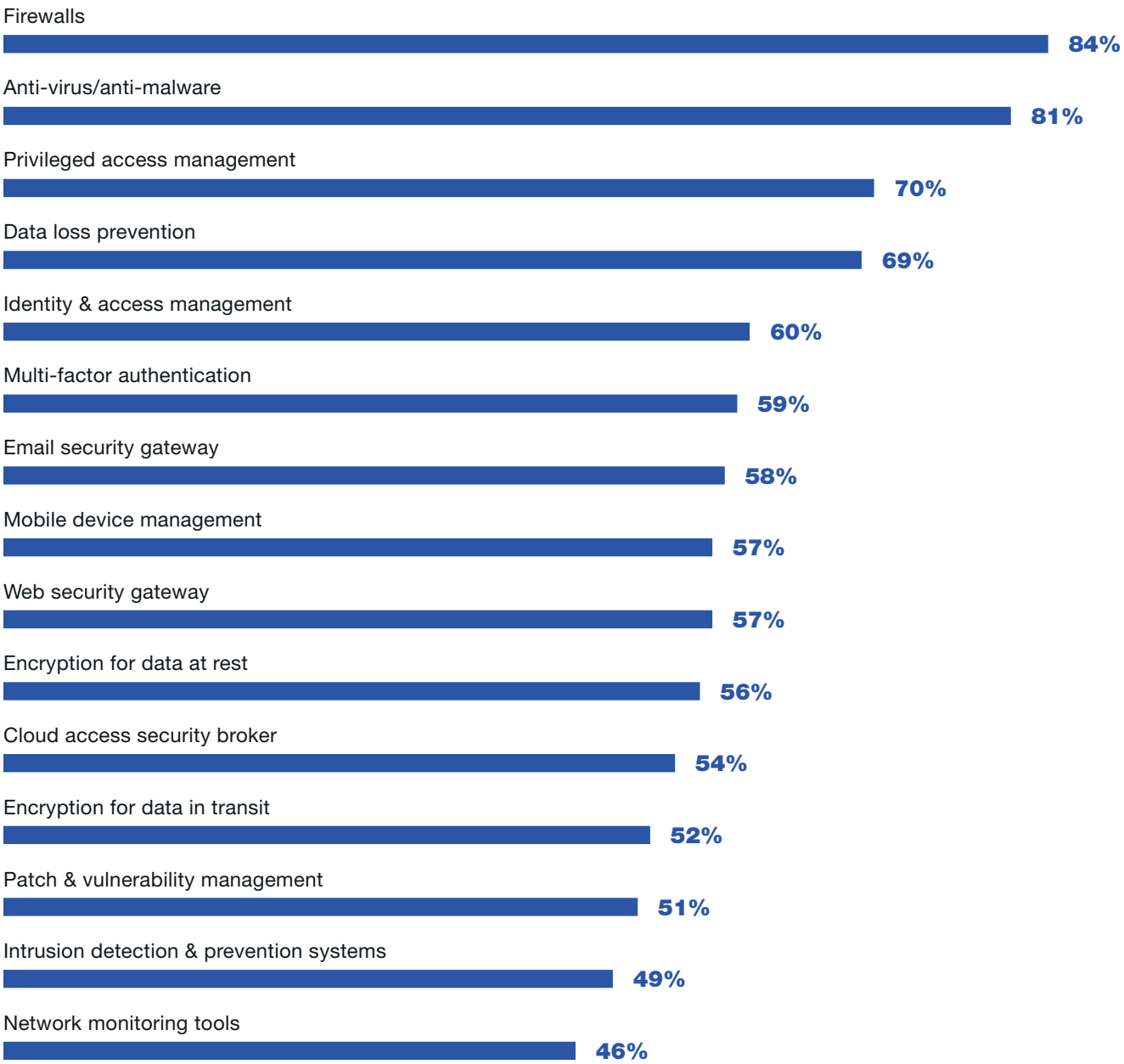


FIGURE 15.

The top technologies fully deployed to stop cyberattacks

The top technologies that organizations have fully implemented are shown here. As part of their cybersecurity strategy, the technologies most fully deployed are firewalls (84 percent of respondents), anti-virus/anti-malware (81 percent of respondents) and privileged access management (70 percent of respondents).

More than one response permitted



OUR FINAL SAMPLE CONSISTED OF 641 SURVEYS OR A 3.9 PERCENT RESPONSE.

A sampling frame of 16,451 IT and IT security practitioners in healthcare organizations who are responsible for participating in cybersecurity strategies including setting IT cybersecurity priorities, managing budgets and selecting vendors and contractors were selected as participants to this survey. Table 2 shows 698 total returns. Screening and reliability checks required the removal of 57 surveys. Our final sample consisted of 641 surveys or a 3.9 percent response.

TABLE 2.

SAMPLE RESPONSE	FREQUENCY	PERCENTAGE
Sampling frame	16,451	100%
Total returns	698	4.2%
Rejected or screened surveys	57	0.3%
Final sample	641	3.9%

FIGURE 16.

Current position within the organization

This figure reports the respondent's organizational level within participating organizations. By design, more than half (62 percent) of respondents are at or above the supervisory levels. The largest category at 33 percent of respondents is technician or staff for security.

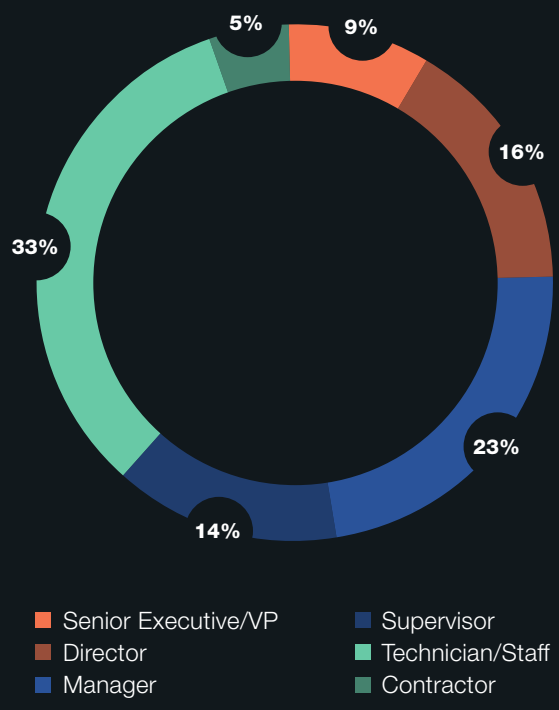


FIGURE 17.

Direct reporting channel

As shown here, 21 percent of respondents report to the chief information officer, 19 percent of respondents report to the chief information security officer, 12 percent of respondents report to cloud administration, 10 percent of respondents data center management and 9 percent of respondents report to the compliance officer.

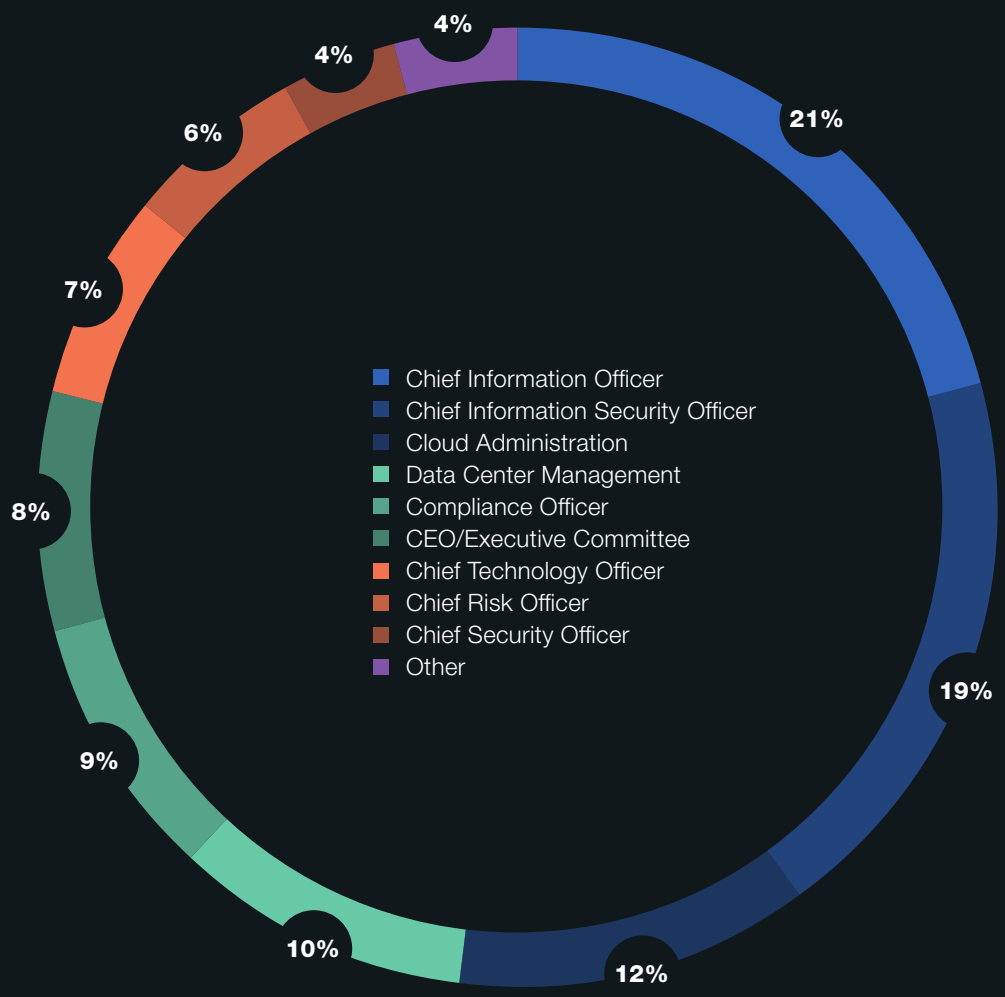
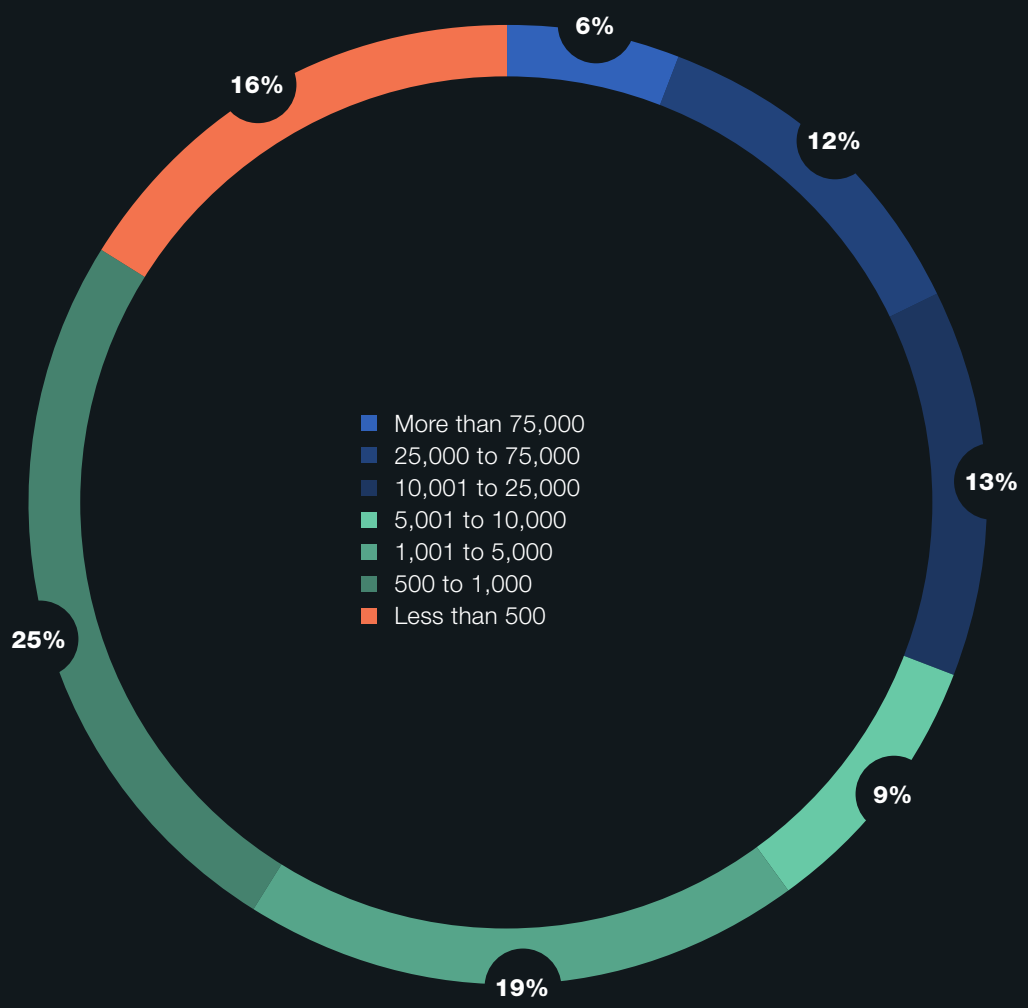


FIGURE 18.

Global full-time headcount

As shown here, 59 percent of respondents are from organizations with a global headcount of more than 1,000 employees.



CAVEATS TO THIS STUDY

THERE ARE INHERENT LIMITATIONS TO SURVEY RESEARCH THAT NEED TO BE CAREFULLY CONSIDERED BEFORE DRAWING INFERENCES FROM FINDINGS.

The following items are specific limitations that are germane to most web-based surveys.

Non-response bias

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

Sampling-frame bias

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

Self-reported results

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

APPENDIX WITH THE DETAILED AUDITED FINDINGS

THE FOLLOWING TABLES PROVIDE THE FREQUENCY OR PERCENTAGE FREQUENCY OF RESPONSES TO ALL SURVEY QUESTIONS CONTAINED IN THIS STUDY.

All survey responses were captured in March 2022.

SURVEY RESPONSE	FREQUENCY
Total sampling frame	16,451
Total returns	698
Rejected returns	57
Total sample	641
Response rate	3.9%

WHICH OF THE FOLLOWING BEST DESCRIBES YOUR ROLE IN IT OR IT SECURITY WITHIN YOUR ORGANIZATION? (Check all that apply)	PERCENTAGE
Setting IT cybersecurity priorities	46%
Managing IT security budgets	42%
Selecting vendors and contractors	47%
Participating in IT cybersecurity strategies	51%
Evaluating and measuring effectiveness of cybersecurity strategies	34%
Managing cybersecurity risk	36%
Overseeing governance and compliance	29%
None of the above	0%

ORGANIZATIONAL CHARACTERISTICS

Q1 WHAT BEST DESCRIBES YOUR ORGANIZATION? (Select one best choice)	PERCENTAGE
Public healthcare provider	19%
Private healthcare provider	22%
Healthcare insurer	13%
Payer	15%
Healthcare insurance	9%
Life sciences	8%
Biotech	5%
Pharma	9%
Total	100%

Q2 HOW MANY NETWORK-CONNECTED DEVICES DOES YOUR ORGANIZATION HAVE?	PERCENTAGE
Less than 500	2%
501 to 1,000	3%
1,001 to 2,500	5%
2,501 to 5,000	9%
5,001 to 7,500	12%
7,501 to 10,000	12%
10,001 to 25,000	15%
25,001 to 50,000	17%
More than 50,000	25%
Total	100%
Extrapolated value	26,208

CYBERSECURITY THREATS TO HEALTHCARE ORGANIZATIONS

Q3	PLEASE RATE THE FOLLOWING STATEMENTS FROM STRONGLY AGREE TO STRONGLY DISAGREE USING THE SCALE BELOW EACH ITEM. (Strongly Agree and Agree responses combined)	PERCENTAGE
	Technologies such as cloud, mobile, big data and the Internet of Things increase the vulnerability of and threats to patient information and safety.	67%
	Legacy systems increase the vulnerability and threats to patient information and safety.	63%
	More attacks use social engineering in place of conventional threats such as vulnerable URLs and malware.	59%
	Traditional VPN does not reduce the risks created by remote access.	41%
	Regular training and simulated BEC and phishing attacks are effective in informing users on how to stop many attacks and reveal who is most vulnerable in the organization.	55%
	Internal phishing results in more compromised cloud accounts.	47%
	Cloud account takeovers present a significant security risk for my organization.	59%
	Phishing is the most frequent method attackers use to acquire legitimate credentials.	60%

Q4	WHAT CYBERSECURITY THREATS IS YOUR ORGANIZATION MOST CONCERNED ABOUT? (Please select the top six)	PERCENTAGE
	Insecure medical devices	64%
	Ransomware	60%
	Insecure mobile apps (eHealth)	59%
	Employee negligence or error	58%
	Cloud compromises	57%
	BEC/ spoof phishing	46%
	Supply chain risks	43%
	Malicious insiders	37%
	Process failures	36%
	System failures	36%
	Employee-owned mobile devices or BYOD	34%
	Third-party misuse of patient data	33%
	Use of public cloud services	18%
	Nation state attacks	17%
	Other (please specify)	2%
	Total	600%

Q5	WHAT TYPES OF INFORMATION DO YOU BELIEVE CYBER ATTACKERS ARE MOST INTERESTED IN STEALING? (Please select all that apply)	PERCENTAGE
	Patient medical records	65%
	Login credentials	56%
	Passwords and other authentication credentials	53%
	Employee information including payroll data	45%
	Email content and attachments	34%
	Clinical trial and other research information	26%
	Patient billing information	24%
	Administrative and scheduling information	23%
	Accounting and financial information	21%
	Intellectual property	19%
	Productivity applications	15%
	Other (please specify)	4%
	Total	385%

Q6	DOES YOUR ORGANIZATION INCLUDE THE PREVENTION AND RESPONSE TO THE FOLLOWING THREATS AS PART OF ITS CYBERSECURITY STRATEGY? (Please check all that apply)	PERCENTAGE
	Attacks to medical devices	51%
	Attacks to the supply chain	44%
	BEC/spoof phishing	48%
	Cloud compromises	63%
	Malicious insiders	29%
	Negligent insiders	37%
	Ransomware	62%
	Total	334%

Q7	WHAT CHALLENGES KEEP YOUR ORGANIZATION'S CYBERSECURITY POSTURE FROM BEING FULLY EFFECTIVE? Please select the top three (3) challenges)	PERCENTAGE
	Insufficient budget (money)	41%
	Insufficient staffing	46%
	Lack of in-house expertise	53%
	Lack of clear leadership	19%
	No understanding how to protect against cyberattacks	35%
	Management does not see cyberattacks as a significant risk	16%
	Lack of collaboration with other functions	50%
	Not considered a priority	40%
	Total	300%

Q8	USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S VULNERABILITY TO BEC/SPOOFING PHISHING (from 1 = not vulnerable to 10 = highly vulnerable)	PERCENTAGE
	1 or 2	11%
	3 or 4	13%
	5 or 6	12%
	7 or 8	24%
	9 or 10	40%
	Total	100%
	Extrapolated value	6.88

Q9	USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S VULNERABILITY TO SUPPLY CHAIN ATTACKS (from 1 = not vulnerable to 10 = highly vulnerable)	PERCENTAGE
	1 or 2	5%
	3 or 4	8%
	5 or 6	16%
	7 or 8	23%
	9 or 10	48%
	Total	100%
	Extrapolated value	7.52

Q10	USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S VULNERABILITY TO RANSOMWARE ATTACKS (from 1 = not vulnerable to 10 = highly vulnerable)	PERCENTAGE
	1 or 2	6%
	3 or 4	9%
	5 or 6	13%
	7 or 8	25%
	9 or 10	47%
	Total	100%
	Extrapolated value	7.46

Q11	USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE YOUR ORGANIZATION'S VULNERABILITY TO CLOUD COMPROMISES (from 1 = not vulnerable to 10 = highly vulnerable)	PERCENTAGE
	1 or 2	0%
	3 or 4	9%
	5 or 6	16%
	7 or 8	30%
	9 or 10	45%
	Total	100%
	Extrapolated value	7.72

Q12	DID YOUR ORGANIZATION EVER EXPERIENCE A RANSOMWARE ATTACK?	PERCENTAGE
	Yes	41%
	No (please skip to Q16a)	52%
	Unsure (please skip to Q16a)	7%
	Total	100%

Q13	HOW MANY RANSOMWARE INCIDENTS DID YOUR ORGANIZATION EXPERIENCE OVER THE PAST TWO YEARS?	PERCENTAGE
	One	53%
	Two to five	33%
	Six to 10	9%
	More than 10	5%
	Total	100%
	Extrapolated value	3.01%

Q14A	DID YOUR ORGANIZATION PAY THE RANSOM?	PERCENTAGE
	Yes	51%
	No	49%
	Total	100%

Q14B	IF YES, HOW MUCH WAS THE RANSOM? (If your organization has had more than one ransomware attack, please select the costliest ransom paid)	PERCENTAGE
	Less than $10,000	2%
	$10,000 to $25,000	9%
	$25,001 to $50,000	7%
	$50,001 to $75,000	10%
	$75,001 to $100,000	17%
	$100,001 to $250,000	19%
	$250,001 to $500,000	18%
	$500,001 to $1,00,000	8%
	$1,00,001 to $5,000,000	5%
	$5,00,001 to $10,000,000	3%
	More than $10,000,000	2%
	Total	100%
	Extrapolated value	$ 771,905

Q15A	DID THE RANSOMWARE ATTACK RESULT IN A DISRUPTION IN PATIENT CARE?	PERCENTAGE
	Yes	67%
	No	30%
	Unsure	3%
	Total	100%

Q15B	IF YES, WHAT IMPACT DID THE RANSOMWARE ATTACK HAVE ON PATIENT CARE?	PERCENTAGE
	An increase in mortality rate	24%
	Delays in procedures and tests have resulted in poor outcomes	64%
	Increase in complications from medical procedures	48%
	Increase in patients transferred or diverted to other facilities	50%
	Longer length of stay	59%
	None of the above	21%
	Other (please specify)	3%
	Total	269%

Q16A	DID YOUR ORGANIZATION EVER EXPERIENCE A BEC/SPOOFING PHISHING ATTACK?	PERCENTAGE
	Yes	51%
	No (please skip to Q18a)	40%
	Unsure (please skip to Q18a)	9%
	Total	100%

Q16B	IF YES, HOW MANY BEC/SPOOFING ATTACKS DID YOUR ORGANIZATION EXPERIENCE OVER THE PAST TWO YEARS?	PERCENTAGE
	One	49%
	Two to five	31%
	Six to 10	12%
	More than 10	8%
	Total	100%
	Extrapolated value	3.50

Q17A	DID THE BEC/SPOOFING ATTACK RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS?	PERCENTAGE
	Yes	67%
	No	30%
	Unsure	3%
	Total	100%

Q17B	IF YES, WHAT IMPACT DID THE BEC/SPOOFING ATTACK HAVE ON PATIENT CARE? (Please select all that apply)	PERCENTAGE
	An increase in mortality rate	21%
	Delays in procedures and tests have resulted in poor outcomes	60%
	Increase in complications from medical procedures	51%
	Increase in patients transferred or diverted to other facilities	45%
	Longer length of stay	48%
	None of the above	19%
	Other (please specify)	2%
	Total	246%

Q18A	DID YOUR ORGANIZATION EVER EXPERIENCE ATTACKS AGAINST ITS SUPPLY CHAIN?	PERCENTAGE
	Yes	50%
	No (please skip to Q20a)	44%
	Unsure (please skip to Q20a)	6%
	Total	100%

Q18B	IF YES, HOW MANY SUPPLY CHAIN ATTACKS DID YOUR ORGANIZATION EXPERIENCE OVER THE PAST TWO YEARS?	PERCENTAGE
	One	44%
	Two to five	29%
	Six to 10	19%
	More than 10	8%
	Total	100%
	Extrapolated value	3.94

Q19A	DID THE SUPPLY CHAIN ATTACKS RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS?	PERCENTAGE
	Yes	70%
	No	24%
	Unsure	6%
	Total	100%

Q19B	IF YES, WHAT IMPACT DID THE SUPPLY CHAIN ATTACKS HAVE ON PATIENT CARE? (Please select all that apply)	PERCENTAGE
	An increase in mortality rate	23%
	Delays in procedures and tests have resulted in poor outcomes	54%
	Increase in complications from medical procedures	48%
	Increase in patients transferred or diverted to other facilities	40%
	Longer length of stay	51%
	None of the above	21%
	Other (please specify)	3%
	Total	240%

PROTECTING THE CLOUD

Q20A	DID YOUR ORGANIZATION EVER EXPERIENCE CLOUD COMPROMISES?	PERCENTAGE
	Yes	54%
	No (please skip to Q22)	41%
	Unsure (please skip to Q22)	5%
	Total	100%

Q20B	HOW MANY TIMES HAVE ATTACKERS COMPROMISED CLOUD-BASED USER ACCOUNTS WITHIN YOUR ORGANIZATION OVER THE PAST TWO YEARS?	PERCENTAGE
	Once	5%
	2 to 5	9%
	6 to 10	6%
	11 to 15	14%
	16 to 20	22%
	21 to 25	17%
	26 to 50	18%
	More than 50	9%
	Total	100%
	Extrapolated value	21.7

Q21A	DID THE CLOUD COMPROMISES RESULT IN A DISRUPTION IN PATIENT CARE OPERATIONS	PERCENTAGE
	Yes	64%
	No	32%
	Unsure	4%
	Total	100%

Q21B	IF YES, WHAT IMPACT DID THE CLOUD COMPROMISES HAVE ON PATIENT CARE? (Please select all that apply)	PERCENTAGE
	An increase in mortality rate	18%
	Delays in procedures and tests have resulted in poor outcomes	49%
	Increase in complications from medical procedures	51%
	Increase in patients transferred or diverted to other facilities	37%
	Longer length of stay	50%
	None of the above	16%
	Other (please specify)	2%
	Total	223%

Q22	HOW DOES YOUR ORGANIZATION PROTECT CONFIDENTIAL OR SENSITIVE INFORMATION IN THE CLOUD? (Please select all that apply)	PERCENTAGE
	We use private data network connectivity	43%
	We use premium security services provided by the cloud provider	56%
	We use encryption, tokenization or other cryptographic tools to protect data in the cloud	65%
	We use a Cloud Access Security Broker (CASB)	53%
	Other (please specify)	3%
	Total	220%

Q23	WHAT BEST DESCRIBES YOUR ORGANIZATION'S APPROACH TO USER ACCESS AND IDENTITY MANAGEMENT IN THE CLOUD ENVIRONMENT? (Please select all that apply)	PERCENTAGE
	Separate identity management interfaces for the cloud and on-premise environments	53%
	Unified identity management interface for both the cloud and on-premise environments	48%
	Deployment of single sign-on (SSO)	37%
	Hybrid combination of the above choices	60%
	Total	198%

STEPS AND SOLUTIONS TO REDUCING CYBERSECURITY THREATS

HOW IMPORTANT ARE EACH OF THE FOLLOWING FEATURES TO YOUR ORGANIZATION'S ABILITY TO CONTROL AND SECURE ACCESS (from 1 = not essential to 10 = very essential)

Q24A	SUPPORT MULTIPLE IDENTITY FEDERATION STANDARDS INCLUDING SAML (1 = not essential to 10 = very essential)	PERCENTAGE
	1 or 2	6%
	3 or 4	5%
	5 or 6	15%
	7 or 8	33%
	9 or 10	41%
	Total	100%
	Extrapolated value	7.46

Q24B	CONTROL STRONG AUTHENTICATION PRIOR TO ACCESSING DATA AND APPLICATIONS IN THE CLOUD (from 1 = not essential to 10 = very essential)	PERCENTAGE
	1 or 2	6%
	3 or 4	9%
	5 or 6	7%
	7 or 8	29%
	9 or 10	49%
	Total	100%
	Extrapolated value	7.62

Q24C	UTILIZE ADAPTIVE ACCESS CONTROLS TO PROTECT THE USERS MOST AT RISK WITHOUT REDUCING THE PRODUCTIVITY OF OTHER USERS (from 1 = not essential to 10 = very essential)	PERCENTAGE
	1 or 2	0%
	3 or 4	3%
	5 or 6	18%
	7 or 8	31%
	9 or 10	48%
	Total	100%
	Extrapolated value	7.98

Q24D	EXPAND OR CONTRACT USAGE BASED ON THE ORGANIZATION'S CURRENT NEEDS/DEMANDS (from 1 = not essential to 10 = very essential)	PERCENTAGE
	1 or 2	6%
	3 or 4	13%
	5 or 6	32%
	7 or 8	21%
	9 or 10	28%
	Total	100%
	Extrapolated value	6.54

Q24E	DEPLOY SHORT CYCLES AND THE ABILITY TO ADD NEW IDENTITY MANAGEMENT SERVICES QUICKLY (from 1 = not essential to 10 = very essential)	PERCENTAGE
	1 or 2	11%
	3 or 4	15%
	5 or 6	23%
	7 or 8	21%
	9 or 10	30%
	Total	100%
	Extrapolated value	6.38

Q24F	ACCELERATE ON-BOARDING PROCESS FOR NEW USERS (from 1 = not essential to 10 = very essential)	PERCENTAGE
	1 or 2	10%
	3 or 4	18%
	5 or 6	23%
	7 or 8	18%
	9 or 10	31%
	Total	100%
	Extrapolated value	6.34

Q24G	ENSURE CONSISTENTLY HIGH AVAILABILITY OF IT RESOURCES (from 1 = not essential to 10 = very essential)	PERCENTAGE
	1 or 2	6%
	3 or 4	13%
	5 or 6	32%
	7 or 8	21%
	9 or 10	28%
	Total	100%
	Extrapolated value	6.54

Q25A	DOES YOUR ORGANIZATION TAKE STEPS TO ADDRESS THE RISK OF EMPLOYEES' LACK OF AWARENESS ABOUT CYBERSECURITY THREATS, ESPECIALLY BEC/SPOOFING PHISHING?	PERCENTAGE
	Yes	59%
	No	35%
	Unsure	6%
	Total	100%

Q25B	IF YES, WHAT STEPS DOES IT TAKE? (Please select all that apply)	PERCENTAGE
	Regular training and awareness programs	63%
	Simulations of phishing attacks	41%
	Monitoring of employees	59%
	Audits and assessments of areas most vulnerable to employees' lack of awareness	39%
	Include user's compliance with privacy and security policies in performance evaluations	35%
	Other (please specify)	3%
	Total	240%

Q26	WHAT TECHNOLOGIES DOES YOUR ORGANIZATION USE TO REDUCE PHISHING AND EMAIL-BASED ATTACKS? (Please select all that apply)	PERCENTAGE
	Domain-based Message Authentication (DMARC)	38%
	Web-isolation technology	29%
	Multi-factor authentication	56%
	Email data loss prevention	52%
	CASB	41%
	Identity and access management (IAM)	56%
	Total	272%

Q27A	DOES YOUR ORGANIZATION USE THREAT INTELLIGENCE IN ITS CYBERSECURITY PROGRAM?	PERCENTAGE
	Yes	60%
	No	40%
	Total	100%

Q27B	IF YES, WHAT THREAT INTELLIGENCE DATA DOES YOUR ORGANIZATION CONSUME? (Please select all that apply)	PERCENTAGE
	DNS traffic	39%
	Web and email filter data	41%
	Network traffic	57%
	Firewall/IPS traffic	53%
	Server traffic	28%
	Packet sniff/ dump	19%
	File monitoring data	23%
	User behavior	44%
	Endpoint activity	27%
	Active directory	36%
	Access/authentication logs	26%
	System log	37%
	Threat intelligence sources	36%
	Web proxy logs	29%
	Dark web data	46%
	Social media	38%
	Total	579%

Q28	TO WHAT EXTENT HAS YOUR ORGANIZATION FULLY IMPLEMENTED THE FOLLOWING SECURITY TECHNOLOGIES? (Please select all that apply)	PERCENTAGE
	Anti-virus/anti-malware	81%
	Firewalls	84%
	Email security gateway	58%
	Encryption for data in transit	52%
	Network monitoring tools	46%
	Web security gateway	57%
	Intrusion detection & prevention systems (IDPS)	49%
	Encryption for data at rest	56%
	Patch & vulnerability management	51%
	Multi-factor authentication	59%
	Identity & access management	60%
	Privileged access management	70%
	Data loss prevention	69%
	Mobile device management (MDM)	57%
	Cloud Access Security Broker (CASB)	54%
	Total	903%

CYBERATTACK EXPERIENCE

Q29	HOW MANY CYBERATTACKS HAS YOUR ORGANIZATION EXPERIENCED OVER THE PAST 12 MONTHS?	PERCENTAGE
	None (please skip to Part 6)	11%
	1 to 5	12%
	6 to 10	15%
	11 to 25	13%
	26 to 50	11%
	51 to 100	23%
	More than 100	15%
	Total	100%
	Extrapolated value	43.3

Q30	APPROXIMATELY, HOW MUCH WAS THE TOTAL COST FROM THE ONE MOST SIGNIFICANT CYBERSECURITY ATTACK? (Please note that the cost estimate should include all direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs and lost business opportunities.)	PERCENTAGE
	Less than $10,000	0%
	50,001 to $100,000	6%
	100,001 to $250,000	12%
	250,001 to $500,000	18%
	500,001 to $1,000,000	16%
	1,000,001 to $5,000,000	21%
	5,000,001 to $10,000,000	13%
	10,000,001 to $25,000,000	12%
	More than $25,000,000	2%
	Total	100%
	Extrapolated value	$4,429,000

Q31	TO UNDERSTAND THE RELATIONSHIP OF EACH OF THE FIVE CATEGORIES TO THE TOTAL COST OF A CYBER SECURITY COMPROMISE, PLEASE ALLOCATE POINTS TO EACH CATEGORY FOR A TOTAL OF 100 POINTS.	100 POINTS
	Remediation & technical support activities, including forensic investigations, incident response activities, help desk and delivery of services to patients	16.00
	Users' idle time and lost productivity because of downtime or system performance delays	25.00
	Disruption to normal healthcare operations because of system availability problems	23.00
	Damage or theft of IT assets and infrastructure	21.00
	Time required to ensure impact on patient care is corrected	15.00
	Total Points	100.00

SECURITY SPENDING & INVESTMENT

Q32	WHAT IS YOUR ORGANIZATION'S APPROXIMATE ANNUAL BUDGET FOR IT?	PERCENTAGE
	Less than $1,000,000	0%
	1,000,000 to $5,000,000	2%
	5,000,001 to $10,000,000	6%
	10,000,001 to $25,000,000	10%
	25,000,001 to $50,000,000	23%
	$50,000,001 to $100,000,000	28%
	$100,000,000+	36%
	Total	105%
	Extrapolated value	$75,200,000

Q33	WHAT PERCENTAGE OF YOUR ORGANIZATION'S IT BUDGET IS DEDICATED TO INFORMATION SECURITY?	PERCENTAGE
	Less than 5%	3%
	5 to 10%	7%
	11 to 15%	23%
	16 to 20%	35%
	21 to 30%	21%
	More than 30%	11%
	Total	100%
	Extrapolated value	19%

YOUR ROLE AND ORGANIZATION

D1	WHAT ORGANIZATIONAL LEVEL BEST DESCRIBES YOUR CURRENT POSITION?	PERCENTAGE
	Senior Executive/VP	9%
	Director	16%
	Manager	23%
	Supervisor	14%
	Technician/Staff	33%
	Contractor	5%
	Other (please specify)	0%
	Total	100%

D2	CHECK THE PRIMARY PERSON YOU OR YOUR IT SECURITY LEADER REPORTS TO WITHIN THE ORGANIZATION.	PERCENTAGE
	CEO/Executive Committee	8%
	Chief Information Officer	21%
	Chief Information Security Officer	19%
	Chief Risk Officer	6%
	Chief Security Officer	4%
	Chief Technology Officer	7%
	Compliance Officer	9%
	Data Center Management	10%
	Cloud Administration	12%
	Other (please specify)	4%
	Total	100%

D1 WHAT IS THE HEADCOUNT OF YOUR ORGANIZATION?	PERCENTAGE
Less than 500	16%
500 to 1,000	25%
1,001 to 5,000	19%
5,001 to 10,000	9%
10,001 to 25,000	13%
25,001 to 75,000	12%
More than 75,000	6%
Total	100%
Extrapolated value	14,548

Ponemon INSTITUTE

Advancing Responsible Information Management

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

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

proofpoint.

About Proofpoint

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.