2021 HIMSS Healthcare Cybersecurity Survey

2021 HIMSS Healthcare Cybersecurity Survey

Table of Contents

Overview

The **2021 HIMSS Healthcare Cybersecurity Survey** provides insight into the state of healthcare cybersecurity based upon the feedback from **167** healthcare cybersecurity professionals. Healthcare organizations face a myriad of challenges, including tight budgets, aging infrastructure and an increase in social engineering and ransomware attacks.

The Most Significant Security Incident:

- 🐟 **Phishing is still king.** Phishing leads the pack.
- 💲 **Financial information is the main target.** Threat actors typically go where the money is.
- 🎣 **Initial hook is by phishing.** Phishing tends to be the initial point of compromise.
- 💧 **Disruption is a typical impact.** Disruption is typical—whether organizations are prepared is another question.

Cybersecurity budgets:

- 📊 **Overall, budgets are still tight.** Six percent or less of the information technology budget is typically allocated for cybersecurity.
- 📈 **Increases in budget for some.** Cybersecurity budgets are modestly increasing compared to the previous year. But tight budgets still mean that one has to pick and choose which security solutions to acquire or implement.
- 📉 **Decreases in budget for others.** Cybersecurity budgets are decreasing for a few. This leads to less robust cybersecurity programs as a whole.

Threat landscape and security challenges:

- 🔎 **The usual suspects.** Ransomware and phishing attacks are top threats.
- ☁️ **Many challenges.** Budget & compliance with policies and procedures top the list.
- ▲ **Legacy systems are the norm.** Unsupported legacy operating systems are commonplace in healthcare organizations and the footprint is growing.
- ✹ **Slow to patch.** Many organizations are slow to patch, but patching is quicker in response to an active security incident.

Implemented security solutions:

- ✔ **Patchwork progress.** Many basic security controls are not fully implemented, while some advanced controls are being implemented.

Bug bounties:

- 🎥 Most healthcare organizations do not have bug bounty programs.

Methodology and Demographics

The **2021 HIMSS Healthcare Cybersecurity Survey** reflects the responses of **167** healthcare cybersecurity professionals. These professionals had at least some responsibility for day-to-day cybersecurity operations or oversight.

The **majority of respondents** (**61%**) had **primary responsibility** over healthcare cybersecurity programs at their respective organizations. **Others** had at **least some responsibility** (**23%**) or sometimes **as needed** (**16%**).

Organization Profile:

Most respondents either worked for **healthcare provider organizations** (**54%**) or **vendor/consulting organizations** (**28%**). The remainder of respondents worked for **other types of organizations** (**18%**).

Figure 1: Organization Type
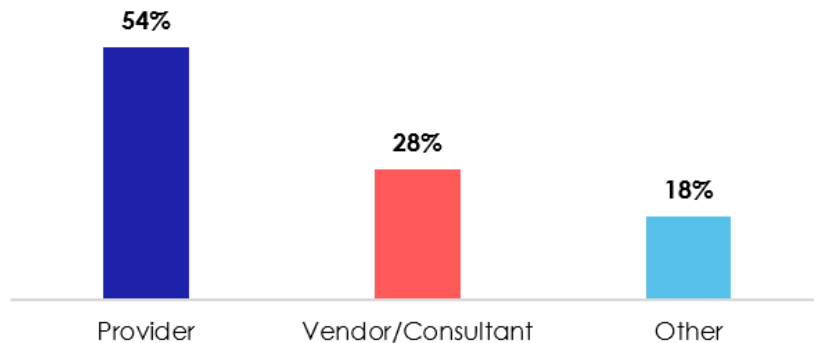
Professional Profile:

The **majority of respondents** (**90%**) reported having a management role in healthcare cybersecurity. More respondents had roles in **executive management** (**52%**) compared to **non-executive management** (**38%**). The **remainder** of respondents had **non-management roles** (**10%**).

Figure 2: Roles
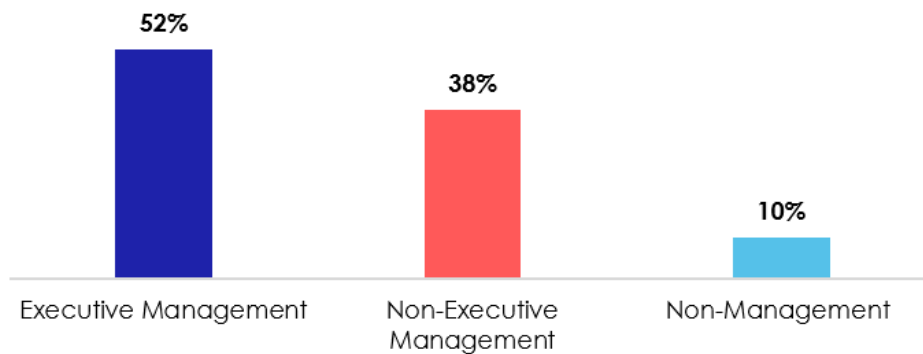
Findings

Section #1: The Most Significant Security Incident in the Past 12 Months

A. Significant Security Incidents are the Norm

Significant security incidents continue to plague healthcare organizations of all types and sizes. The data collection for this survey occurred during the COVID-19 pandemic and healthcare organizations of all types are clearly affected by significant security incidents. In this survey, **sixty-seven percent** of respondents indicated that their healthcare organizations experienced **significant security incidents in the past twelve months**.

We asked each respondent about the **most significant security incident that occurred in the past twelve (12) months**. The **severity level** of the most significant security incident in the past twelve months has typically been **medium** (**35%**) or **high** (**32%**), but some have been characterized as **critical** (**12%**) or **low** (**20%**). Respondents rated the severity level based upon their own criteria, including the perceived impact to the organization.

Figure 3: Severity Levels of the Most Significant Security Incident in the Past 12 Months
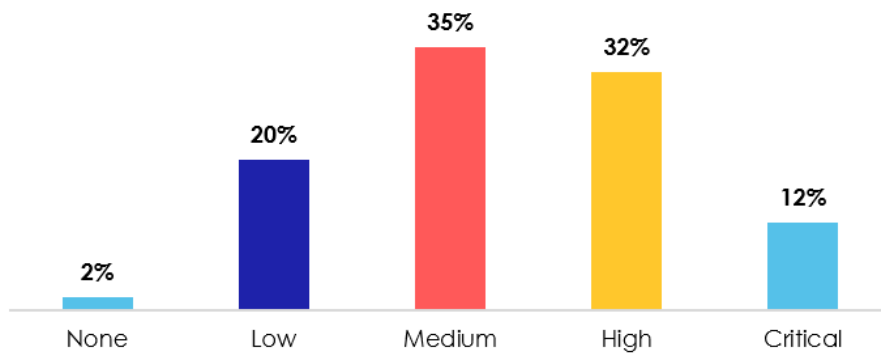
B. Phishing Attacks and Ransomware are Typically the Most Significant Security Incidents

The **most significant security incident** was typically either a **phishing attack** (**45%**) or **ransomware attack** (**17%**). Ransomware and phishing attacks frequently make the headlines when healthcare organizations experience a significant cyber-attack. It could be, though, that healthcare organizations are looking more for phishing and ransomware attacks compared to other types of significant security incidents. For example, our previous research has indicated that healthcare organizations often do not have robust insider threat management programs.[1] Thus, negligent insider activity and other types of significant security incidents may be underreported.

Figure 4: Most Significant Security Incident in the past 12 Months

Phishing attack	45%
Ransomware attack	17%
Breach or data leakage	7%
Negligent insider activity	5%
Social engineering attack	5%
Fire, flash flood, or natural hazard	4%
Credential harvesting attack	4%
Website or web application attack	2%
Distributed denial of service attack	2%
Theft or loss	2%
Supply chain compromise or attack	2%
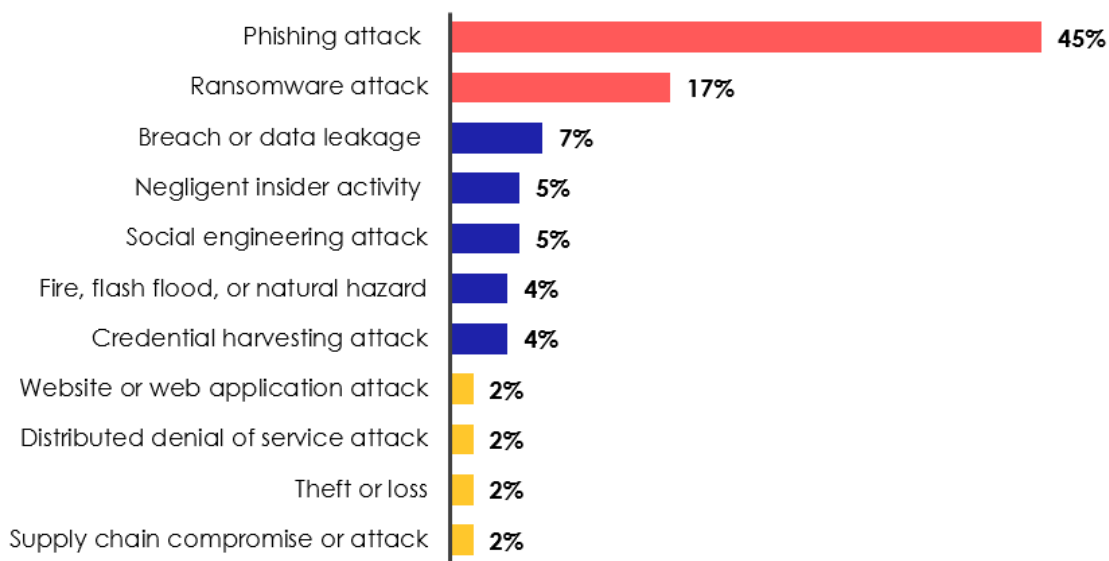
[1] 2018 HIMSS Cybersecurity Survey and 2017 HIMSS Cybersecurity Survey - almost half of respondents report either having an informal insider threat management program or no program at all.

C. *Phishing Typically Plays a Role in the Most Significant Security Incident*

A majority of respondents (**57%**) reported that the **most significant security incident** typically involved **phishing**. Specifically, the types of phishing reported included the following: **general email phishing** (**71%** of respondents), **spear-phishing** (**67%**), voice phishing/vishing (27%), whaling (27%), business e-mail compromise (23%), SMS phishing (21%), phishing websites (20%) and social media phishing (16%).

Figure 5: Types of Phishing Involved in Most Significant Security Incident

General email phishing	71%
Spear-phishing	67%
Voice phishing/vishing	27%
Whaling	27%
Business e-mail compromise	23%
SMS phishing	21%
Phishing website	20%
Social media phishing	16%
Pharming	3%
Deepfakes	2%
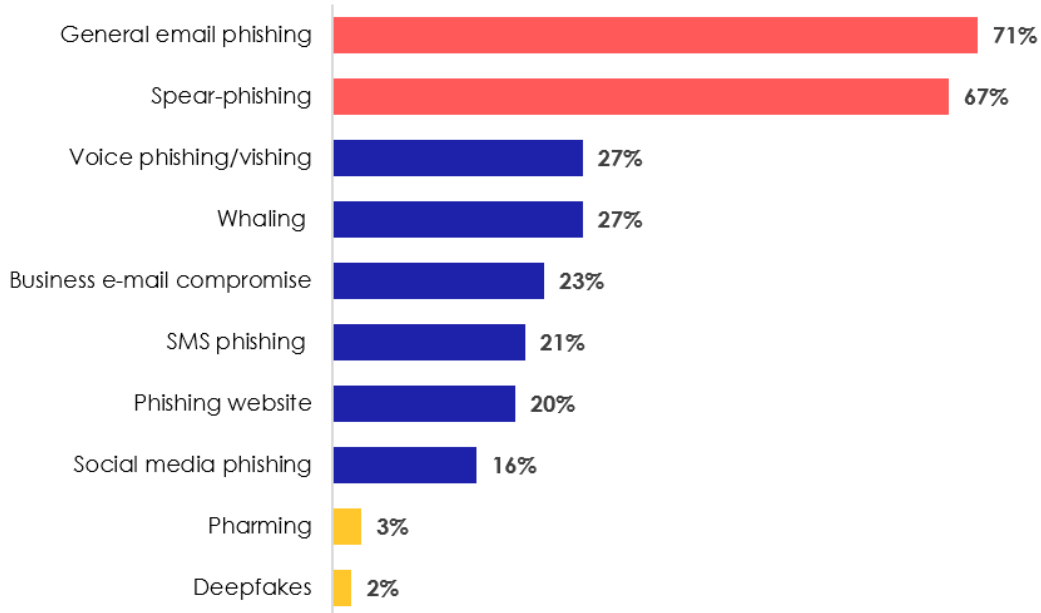
D. Initial Point of Compromise for the Most Significant Security Incident

(i)   Phishing is the Typical Initial Point of Compromise

The **initial point(s) of compromise** were typically **phishing** (**71%** of respondents) as well as human error (19%), social engineering (15%) and legacy software (15%). Accordingly, greater emphasis needs to be placed on security awareness programs (e.g., phishing and other types of social engineering), insider threat detection and mitigation and replacing or upgrading legacy (unsupported) software, if feasible.

Figure 6: Initial Point(s) of Compromise for the Most Significant Security Incident

Initial Point of Compromise	Percentage
Phishing	71%
Human error	19%
Social engineering	15%
Legacy (unsupported) software	15%
Website	11%
Remote access server	10%
Laptop, tablet or device	10%
Legacy (unsupported) operating system	9%
Cloud provider/service	9%
Shadow IT	8%
Unpatched (supported) software	7%
Unpatched (supported) operating systems	7%
...ardware or software infected with malware "off the shelf"	4%
Electronic health record system	4%
Picture Archiving and Communication System (PACS)	4%
Virtual private network (VPN)	4%
...lding automation system or other industrial control system	3%
Medical device	2%
Office productivity software	1%

E. Target(s) of Threat Actors for the Most Significant Security Incident

Respondents were asked to identify the **target(s) of the threat actors**. Similar to the findings in the 2020 HIMSS Cybersecurity Survey, this 2021 survey found that **financial information (52%)**, **employee information (43%)** and **patient information (39%)** were the primary targets of threat actors.

Figure 7: Target(s) of Threat Actors for Most Significant Security Incident
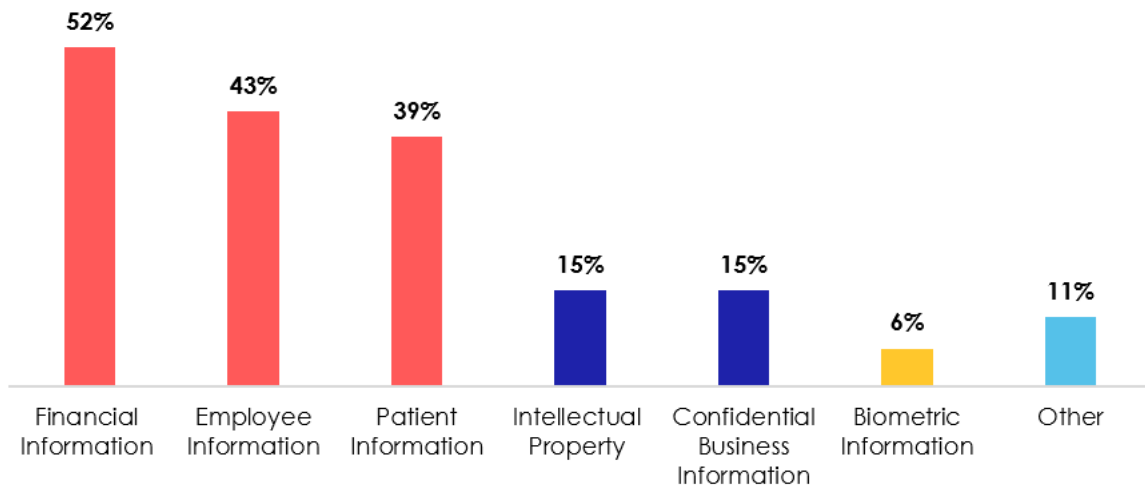
F. *Impact(s) of Most Significant Security Incident*

(i) Disruption, data breaches and leakages, disruption of clinical care systems/devices and monetary loss are top impacts

Respondents were asked to describe the perceived impact(s) of the security incident. Interestingly, **44%** of respondents reported **no impact or negligible impact**. It is possible that some respondents were unaware of the extent of the impact (e.g., latent harm).

Nonetheless, for respondents who did report an **actual impact**, the following occurred: (1) **disruption of systems/devices impacting business operations** (**32%**) or **IT operations** (**26%**), (2) **data breach or data leakage** (**22%**), (3) **disruption of systems/devices impacting clinical care** (**21%**) and (4) **monetary loss** (e.g., business e-mail compromise, wire fraud, ransom, etc.) (**17%**). Other impacts were reported, such as damage/destruction of systems/devices. Whether healthcare organizations are prepared for adverse impacts, such as disruption, damage or destruction is yet another issue. Business continuity and disaster recovery processes are typically weak at many healthcare organizations.

Figure 8: Significant Security Incidents – Impact of Incident
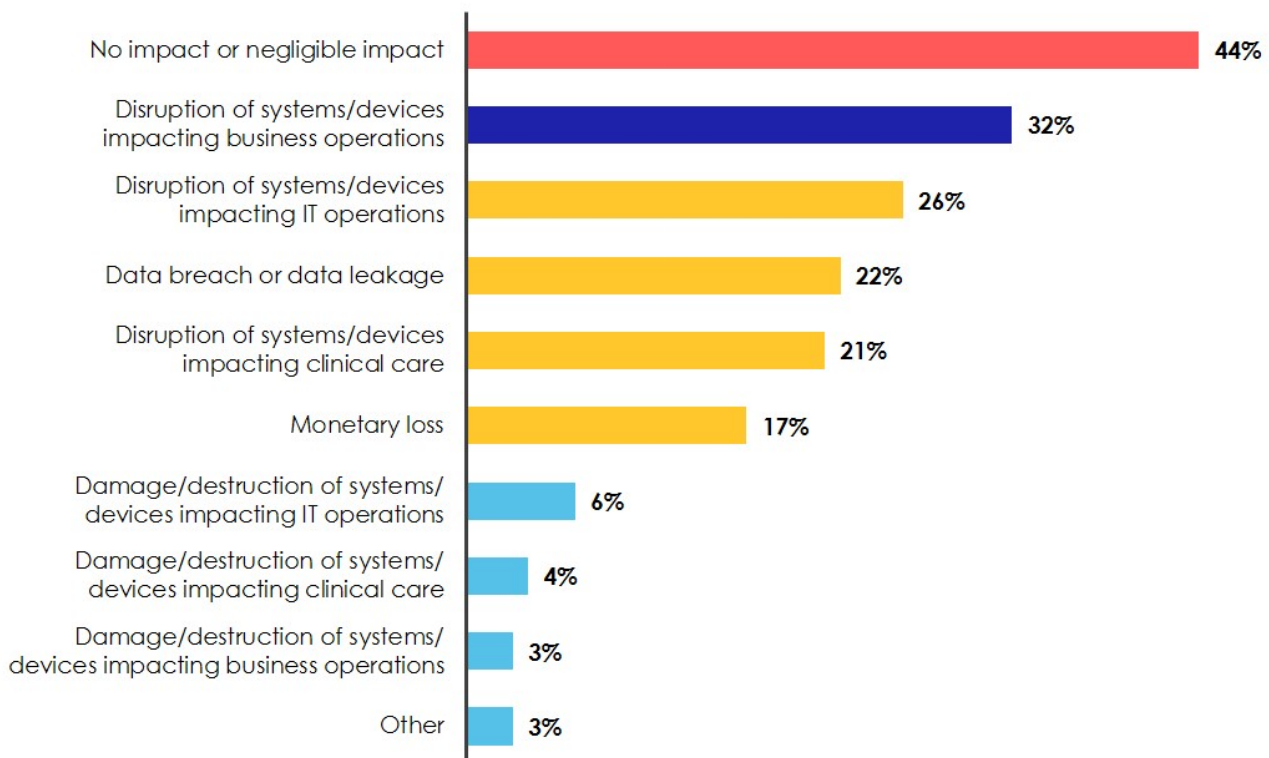
Section #2: Cybersecurity Budgets

A. Cybersecurity budgets are slim overall

A number of respondents (**24%**) reported that their cybersecurity budgets have **no specific carve out**. Notwithstanding this, **the majority of the other respondents (40%)** reported that **six percent or less of the information technology budget was allocated to cybersecurity**. This finding of six percent or less is consistent with the results of the 2018, 2019 and 2020 HIMSS Cybersecurity Survey.

Figure 9: Percent of Organization's IT Budget Allocated to Cybersecurity for 2021
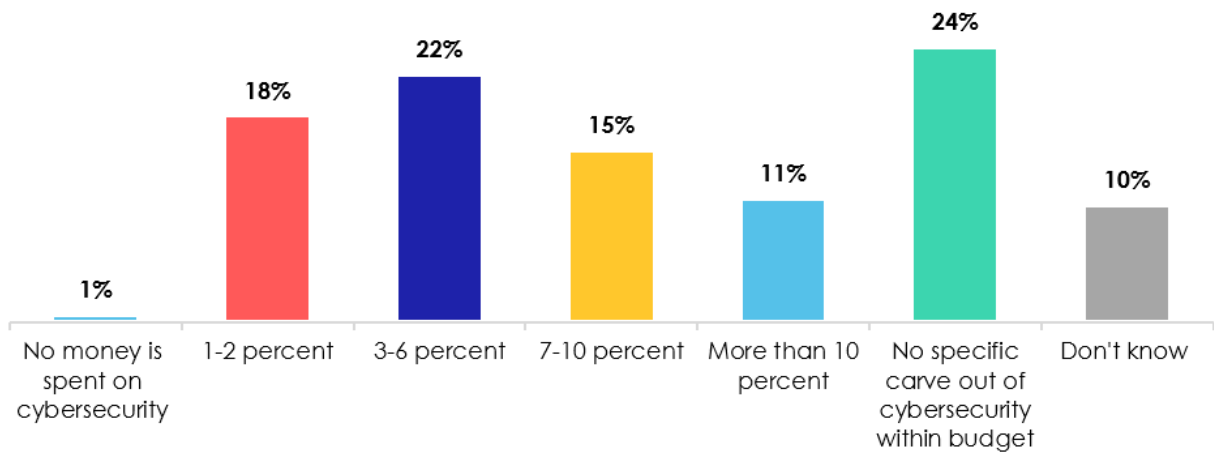
Table 1: Amount of IT Budget Allocated to Cybersecurity 2018-2021

Budget Allocation	2018 %	2019 %	2020 %	2021 %
No money is spent on cybersecurity	3%	1%	1%	1%
1 to 2 percent	**21%**	**9%**	**18%**	**18%**
3 to 6 percent	**21%**	**25%**	**24%**	**22%**
7 to 10 percent	7%	11%	10%	15%
More than 10 percent	7%	10%	6%	11%
Money spent on cybersecurity but no specific carve out in IT budget	27%	26%	23%	24%
Do not know	15%	18%	18%	10%

(i)   Better Cybersecurity Budgets for Some, While Leaner for Others

Collectively, a majority of respondents (**59%**) reported an increase in cybersecurity budgets in 2021 when compared to 2020. However, the remainder of respondents (**40%**) reported either a decreased budget or a budget that did not substantially change. Overall, the cybersecurity budgets are better for some.

Table 2: Change in Cybersecurity Budget 2020 to 2021

Budget Allocation	Percentage
Increased by 25% or more	**14%**
Increased by 10-24%	**17%**
Increased by 5-9%	**28%**
Did not substantially change	**34%**
Decreased by 5-9%	2%
Decreased by 10-24%	3%
Decreased by 25% or more	1%
Don't know	2%

(ii)   Increase in Cybersecurity Budgets: Better Security Postures in 2021

An **increase** in the cybersecurity budget at healthcare organizations from 2020 to 2021 typically led to the following outcomes: **more upgrades of security solutions** (**63%** of respondents), **more acquisitions of new security solution**s (**56%**), **increases in cybersecurity staffing (53%)**, **more maintenance of existing infrastructure (48%)**, **more security risk assessments or more comprehensive security risk assessments (48%)** and **more robust security risk management** (**47%**).

While an increase in cybersecurity budget is a positive trend, these figures indicate that healthcare cybersecurity budgets are still slim. In reality, what is needed is for more healthcare organizations to be able to do all of these necessary things. Instead, some tasks are prioritized over others. For example, increased cybersecurity training for IT and IT security staff stands only at **28%**. If anything, our cybersecurity staff needs to be more informed and not less.

Table 3: Impact of Cybersecurity Budget Increases - 2020 to 2021

Outcomes	Percentage
More upgrades of security solutions	**63%**
More acquisitions of new security solutions	**56%**
Increase in cybersecurity staffing	**53%**
More maintenance of existing infrastructure	**48%**
More security risk assessments or more comprehensive security risk assessments	**48%**
More robust security risk management	**47%**
Increased security awareness training	34%
More frequent penetration testing	31%
Increased cybersecurity training for IT & IT security staff	28%
Other (please specify)	2%

(iii) Decrease in Cybersecurity Budgets Lowers Security Postures in 2021

Relatively **few respondents** (**6%**) indicated a **decrease in cybersecurity budgets from 2020 to 2021**.[2] A decrease in cybersecurity budgets typically resulted in the following outcomes: **less acquisition of new security solutions** (**67%** of respondents), **less robust security risk management** (**67%**), **decrease in cybersecurity staffing** (**50%**) and **less maintenance of existing infrastructure** (**50%**). Accordingly, there is no upside to decreasing cybersecurity budgets.

Decreases in cybersecurity budget can significantly weaken the security posture of healthcare organizations. Aging or outdated security solutions may mean that the security solutions currently in use may not be able to keep up with new and emerging threats. Less robust security risk management may mean that risks are not adequately managed. Having fewer dollars to operate a cybersecurity program rarely translates into anything positive for the organization. If anything, cybersecurity programs should be more of a priority at organizations and not less.

Table 4: Impact of Cybersecurity Budget Decreases 2020 to 2021

Outcomes	Percentage
Less acquisition of new security solutions	**67%**
Less robust security risk management	**67%**
Decrease in cybersecurity staffing	**50%**
Less maintenance of existing infrastructure	**50%**
Less cybersecurity training for IT & IT security staff	33%
Fewer upgrades of security solutions	17%
Fewer security risk assessments or less comprehensive risk assessments	17%
Less security awareness training	17%
Less frequent penetration testing	17%

[2] Please see Table 2.

(iv)   Cybersecurity Budgets are Stagnant for Others in 2021

34% of respondents reported that their cybersecurity budgets did not substantially change from 2020 to 2021.[3] With price increases and inflation, it is likely that many healthcare organizations will have an à la carte situation in terms of having to pick and choose what they can afford and forego what they cannot.

B. *Looking ahead to 2022 – Change is Positive for Many, Worse for a Few*

In the aggregate, **most respondents** (**59%**) reported an **increase in cybersecurity budgets for 2022**. It is likely that this increase in budgets will lead to more positive growth within healthcare cybersecurity programs.

However, **35%** of respondents reported that their budgets are **not anticipated to change,** and a slim minority of respondents (3%) indicated that their budget will decrease. Accordingly, many of these healthcare organizations will likely not see marked improvement in their cybersecurity programs.

Table 5: Anticipated Change in Cybersecurity Budget – 2021 to 2022

Amount of Anticipated Change	Percentage
Increase by 25% of more	**11%**
Increase by 10-24%	**15%**
Increase by 5-9%	**33%**
Will not substantially change	**35%**
Decrease by 5-9%	1%
Decrease by 10-24%	2%
Decrease by 25% or more	0%
Don't know	4%

---

[3] See Table 2.

Section #3: *Threat Landscape & Security Challenges*

A. *Too Many Threats, Too Little Time*

Respondents rated potential threats to their healthcare organizations. These responses were rated on a scale from 1 to 5 (none=1, low=2, medium=3, high=4, critical=5). Based upon these responses, the following are rated as medium to high threats: **phishing attacks (3.72), ransomware attacks (3.50) and breaches or data leakage (3.38)**. These are the biggest concerns for healthcare cybersecurity professionals. Yet, there are many other concerns as well. It is likely that many healthcare organizations are not able to have robust plans of action regarding all of their concerns.

Figure 10: Concern Regarding Potential Future Threats

Threat	Rating
Phishing attack	3.72
Ransomware attack	3.50
Breach or data leakage	3.38
Social engineering attack	3.11
Credential harvesting attack	3.07
Negligent insider activity	3.01
Advanced persistent threat attack	2.95
Website or web application attack	2.84
Supply chain compromise or attack	2.83
Distributed denial of service attack	2.70
Malicious insider activity	2.68
Fire, flash flood, or natural hazard	2.60
Theft or loss	2.59

B. Many Challenges

The following are the biggest security challenges for healthcare cybersecurity programs: **budget** (**47%** of respondents), **staff compliance with policies and procedures** (**43%**), **legacy technology** (**39%**) and **patch and vulnerability management** (**34%**). While these are top challenges, there are many more challenges that continue to plague healthcare organizations. These challenges are discussed in more detail below.

Figure 11: Biggest Security Challenges

Challenge	Percentage
Budget	47%
Staff compliance with policies & procedures	43%
Legacy technology	39%
Patch and vulnerability management	34%
Employees	32%
Device management	29%
Identity and access management	28%
Organization's cybersecurity culture	27%
Data leaks or breaches	27%
Shadow IT (unauthorized IT solutions)	26%
Contractors / consultants	19%
Vendors	17%
Policies & procedures	14%
Cloud services/providers	11%
Wireless networks	10%
Threat information sharing	7%
Managed security service providers	4%
Other	2%

(i)   Budget

Budgets are still the **biggest security challenges** for many respondents (**47%**). This results in many healthcare organizations having to pick and choose what to maintain, upgrade or acquire. Typically, better security postures require more money.

(ii)   Staff compliance with policies & procedures

Staff compliance with policies and procedures is another headache for respondents (**43%**). Whether it is out of date policies and procedures or onerous policies and procedures that hinder day-to-day workflow and tasks, compliance with an organization's policies and procedures can be difficult. If there are numerous exceptions granted to policies and procedures or if such policies and procedures are inconsistently applied and enforced, this can significantly weaken the security posture of any healthcare organization.

(iii)   Legacy technology

Legacy technology can indeed be a significant security challenge for many respondents (**39%**).[4] Whether we are dealing with legacy devices, applications or operating systems, the inherent challenge is that these are no longer supported by the manufacturer and, typically, security patches and other upgrades are unavailable.

(A) Legacy technology: Legacy Operating Systems in Place

The **majority of respondents** (**73%**) reported having **legacy operating systems**. The typical legacy operating systems (OS) are **Windows Server 2008 (35%)**, **Windows 7 (34%)**, **legacy medical device OS (25%)**, **industrial control system OS (21%)**, **Windows XP (20%)** and **Windows Server 2003 and 2003 R2 (19%)**. Some healthcare organizations may not necessarily be planning for obsolescence of these operating systems. Every asset has a useful life, and it is important for organizations to plan for its end of life.

Figure 12: Legacy (Unsupported) Operating Systems in Place

---
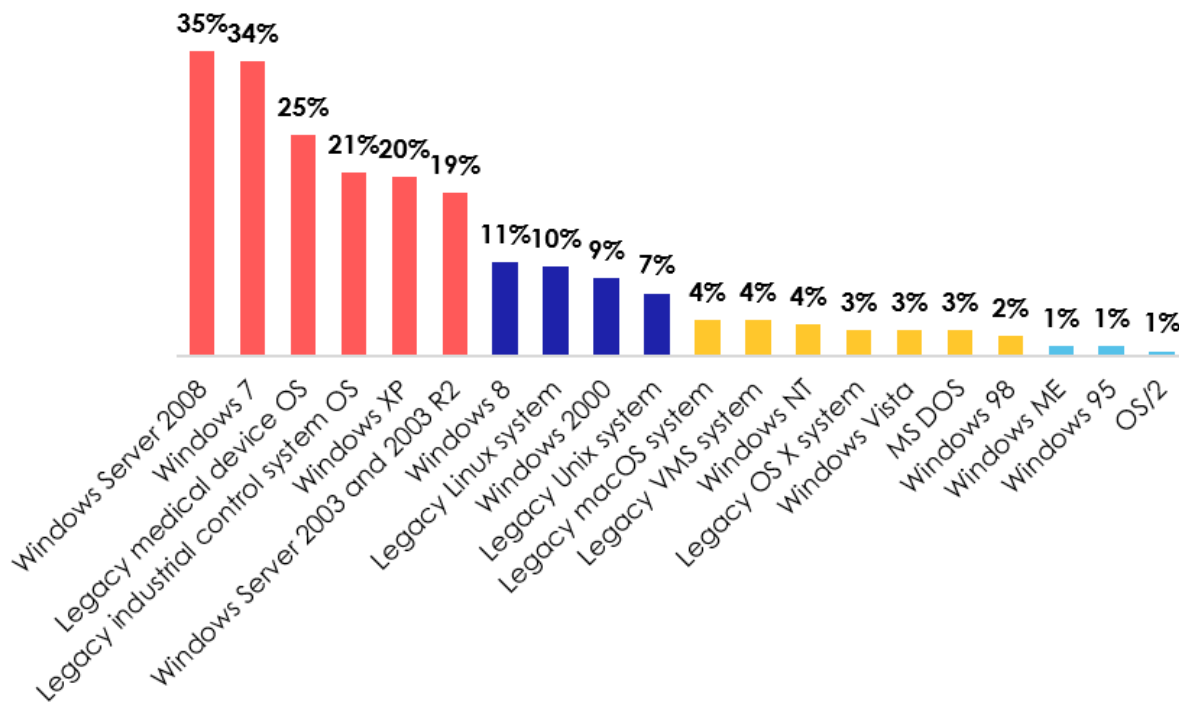
[4] See Figure 11.

(B) Legacy technology: Legacy System Footprints are Increasing

Respondents reported having **legacy operating system footprints** across healthcare organizations that typically range from either **1-10%** (**53%** of respondents) or **11-20%** (**23%**). The pervasiveness of legacy systems is a concern. Except in certain special circumstances, there are typically no patches available for legacy systems. Additionally, in the absence of compensating controls, legacy systems are truly vulnerable targets.

Table 6: Legacy Operating System Footprint

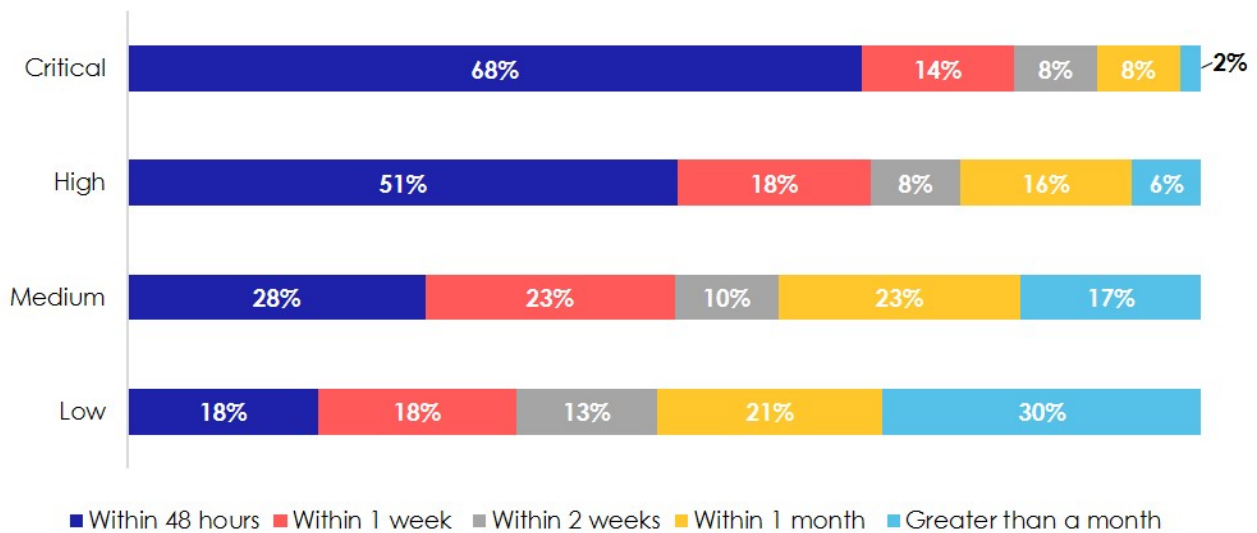| Amount of Legacy OS Footprint	Percentage
1-10%	**53**%
11-20%	**23**%
21-30%	11%
31-40%	4%
41-50%	3%
More than 50%	6%

(iv)   Patch and vulnerability management

Patch and vulnerability management is also a challenge for some respondents (**34%**).[5] Additionally, there can be a significant amount of time that passes before vulnerabilities are patched, whether under normal conditions or in response to a significant security incident. The longer it takes to patch, the greater opportunity there is for threat actors to potentially compromise a healthcare organization's infrastructure and assets. Absent a robust patch and vulnerability management program, there may be various entry points into a healthcare organization's systems and networks.

(A) Patch and vulnerability management: Normal state

Under **normal circumstances** (i.e., in the absence of an active security incident), respondents report that their organizations are patching vulnerabilities within **1 month** for vulnerabilities that are rated **low** in severity (**70%**), within **2 weeks** for **medium** severity (**61%**), within **1 week** for **high** severity (**69%**) and within **48 hours** for **critical** severity (**68%**).

Figure 13: Average Time to Patch - Normal Circumstances

Severity	Within 48 hours	Within 1 week	Within 2 weeks	Within 1 month	Greater than a month
Critical	68%	14%	8%	8%	2%
High	51%	18%	8%	16%	6%
Medium	28%	23%	10%	23%	17%
Low	18%	18%	13%	21%	30%

---

[5] *See* Figure 11.

(B) Patch and vulnerability management: Active Incident Response

In response to an **active security incident**, most respondents report that their organizations are generally responding within **1 week** for **low** (**58%** of respondents) and medium severity (**72%**) vulnerabilities, within **48 hours** for high severity vulnerabilities (**73%**) and critical severity vulnerabilities (**83%**). Essentially, the more severe the vulnerability, the quicker it is to patch. On average, the time to patch is faster, compared with the normal state.

Figure 14: Average Time to Patch – In Response to a Security Incident

Within 48 hours ■ Within 1 week ■ Within 2 weeks ■ Within 1 month ■ Greater than a month
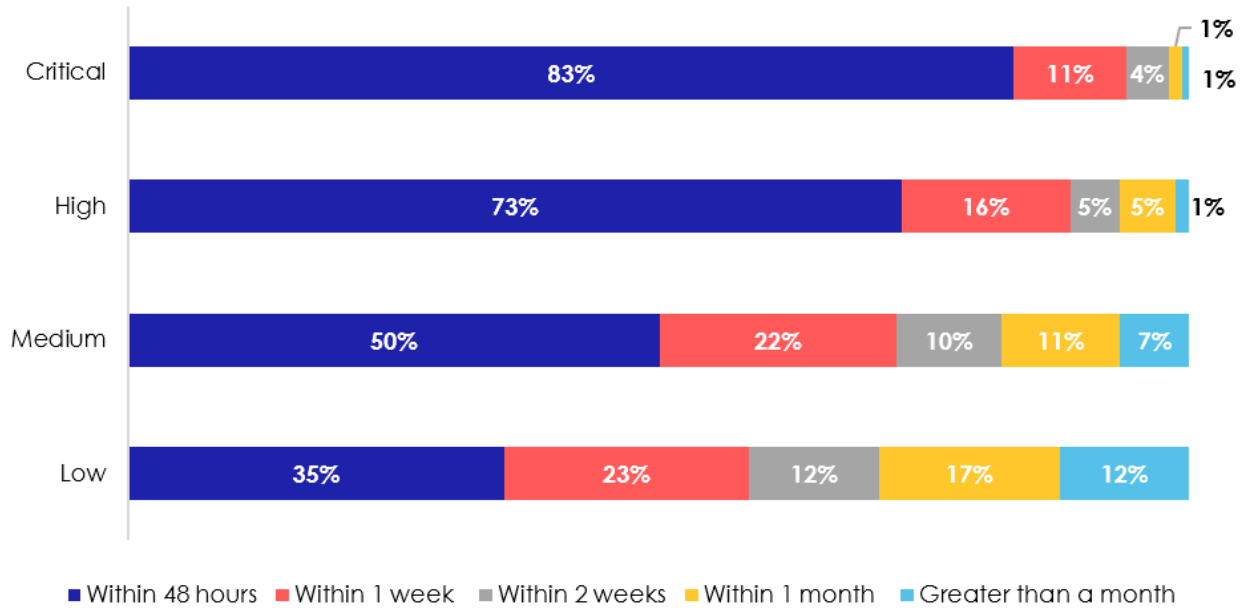
Section #4: *Implemented Security Solutions at Healthcare Organizations*

Robust cybersecurity programs require robust security controls. *A strong foundation of basic security controls is essential.* Without the basics, advanced security controls (such as zero tru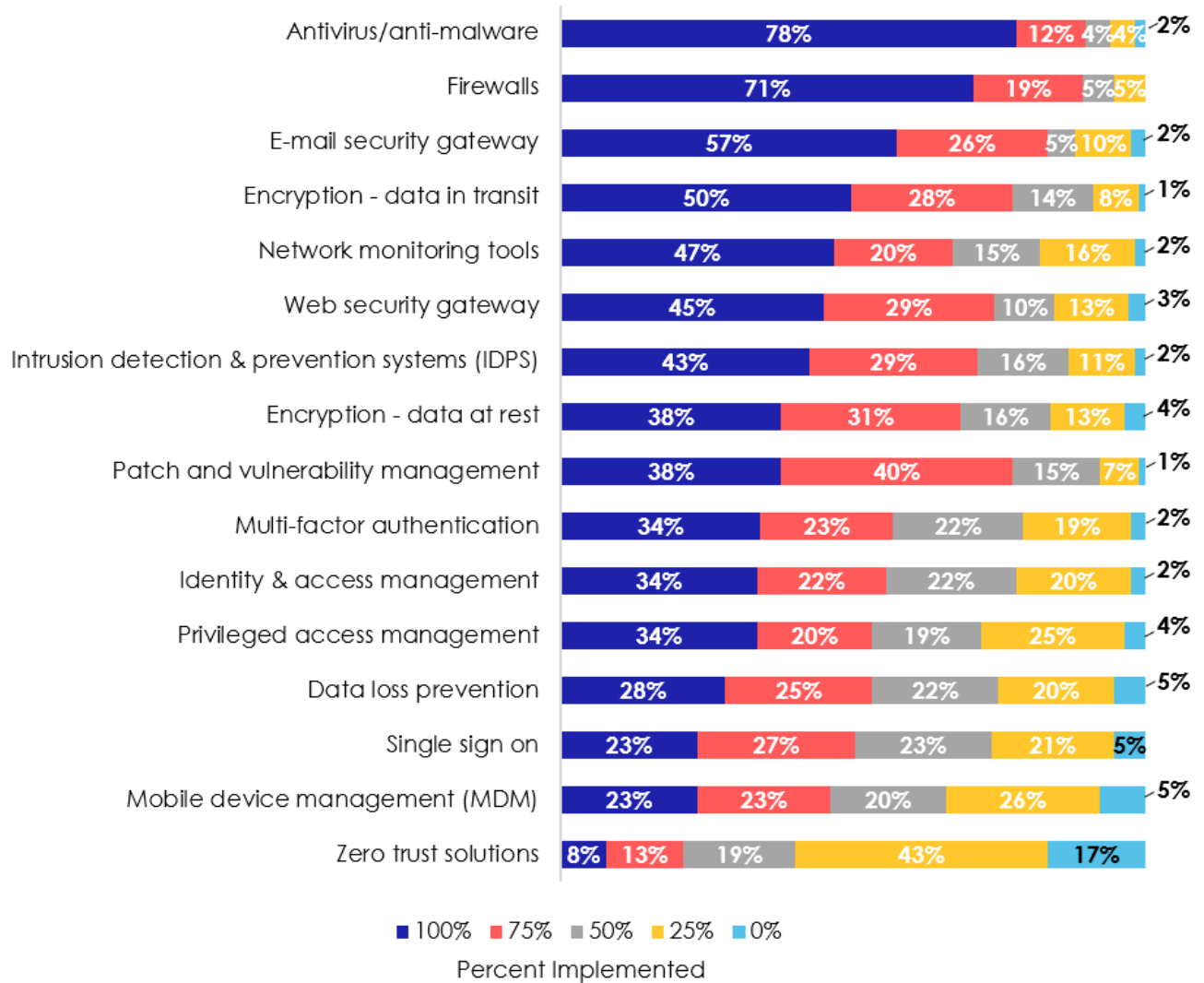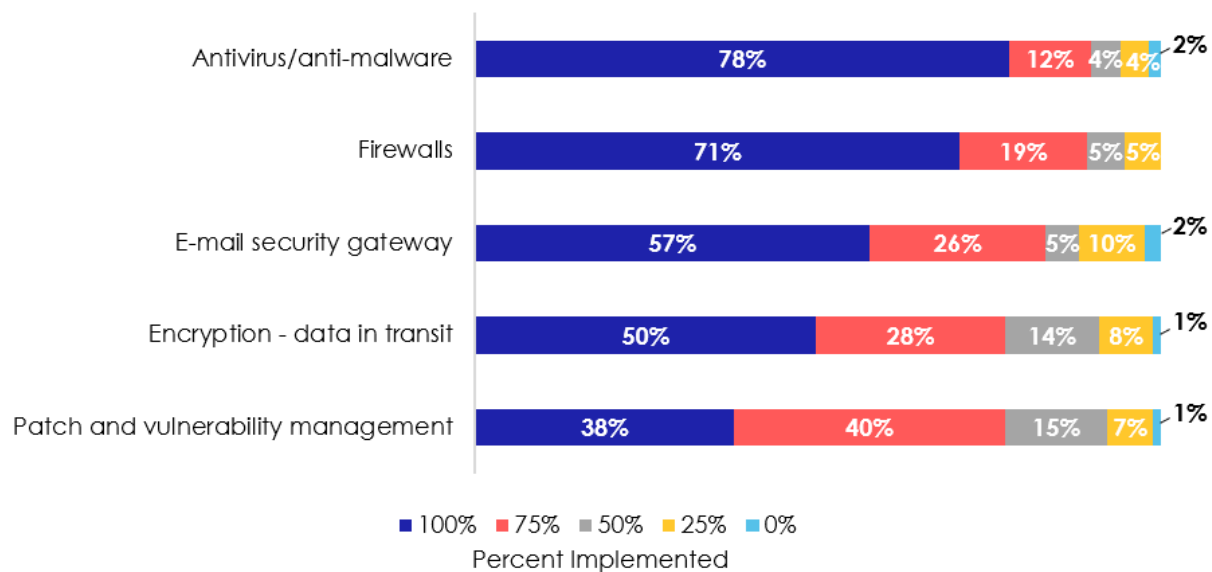st) will not realize their full potential. We asked respondents to specify the degree of implementation of these security controls within their healthcare organizations, as noted below.

Figure 15: Implemented Security Controls

Security Control	100%	75%	50%	25%	0%	(end)
Antivirus/anti-malware	78%	12%	4%	4%	2%	
Firewalls	71%	19%	5%	5%		
E-mail security gateway	57%	26%	5%	10%	2%	
Encryption - data in transit	50%	28%	14%	8%	1%	
Network monitoring tools	47%	20%	15%	16%	2%	
Web security gateway	45%	29%	10%	13%	3%	
Intrusion detection & prevention systems (IDPS)	43%	29%	16%	11%	2%	
Encryption - data at rest	38%	31%	16%	13%	4%	
Patch and vulnerability management	38%	40%	15%	7%	1%	
Multi-factor authentication	34%	23%	22%	19%	2%	
Identity & access management	34%	22%	22%	20%	2%	
Privileged access management	34%	20%	19%	25%	4%	
Data loss prevention	28%	25%	22%	20%	5%	
Single sign on	23%	27%	23%	21%	5%	
Mobile device management (MDM)	23%	23%	20%	26%	5%	
Zero trust solutions	8%	13%	19%	43%	17%	

■ 100% ■ 75% ■ 50% ■ 25% ■ 0%

Percent Implemented

A. Top Tier – Basic Security Controls

Figure 16: Top Tier Implemented Controls

	100%	75%	50%	25%	0%
Antivirus/anti-malware	78%	12%	4%	4%	2%
Firewalls	71%	19%	5%	5%	
E-mail security gateway	57%	26%	5%	10%	2%
Encryption - data in transit	50%	28%	14%	8%	1%
Patch and vulnerability management	38%	40%	15%	7%	1%

Percent Implemented

(i)   Antivirus/anti-malware solutions

Only **78%** of respondents reported that **anti-virus/anti-malware solutions** were implemented **comprehensively** (100%) across the enterprise. Yet other respondents indicated that antivirus/anti-malware solutions were implemented to a lesser degree. Without basic controls such as antivirus/anti-malware solutions, healthcare organizations are ill equipped in terms of truly basic security defenses.

(ii)   Firewalls

Only **71%** of respondents reported that **firewalls** were implemented **comprehensively** (100%) across the enterprise. Yet other respondents indicated that firewalls were implemented to a lesser degree. In the absence of firewalls, this leaves many healthcare organizations with significant gaps in network security.

(iii)   E-mail security gateways

Only **57%** of respondents reported that **e-mail security gateways** were implemented comprehensively (100%) across the enterprise. Yet other respondents indicated that e-mail security gateways were implemented to a lesser degree. In the absence of e-mail security gateways, e-mail phishing attacks and other compromises may be of greater concern.

(iv)   Encryption-Data in Transit

Only **50%** of respondents have implemented **encryption for data in transit** comprehensively (100%) across the enterprise. Yet other respondents indicated that encryption for data in transit was implemented to a lesser degree. In the absence of encrypting data in transit, the confidentiality and integrity of data may be especially at risk.

(v)   Patch and Vulnerability Management

Only **38%** of respondents have implemented **patch and vulnerability management** comprehensively (100%) across the enterprise.[6] Yet other respondents indicated that patch and vulnerability management was implemented to a lesser degree. In the absence of a robust patch and vulnerability management program, healthcare organizations may be leaving their systems, networks and assets in a vulnerable state.

---

[6] See Figure 16.

B. Second Tier – Basic Security Controls

Figure 17: Moderately Implemented Controls
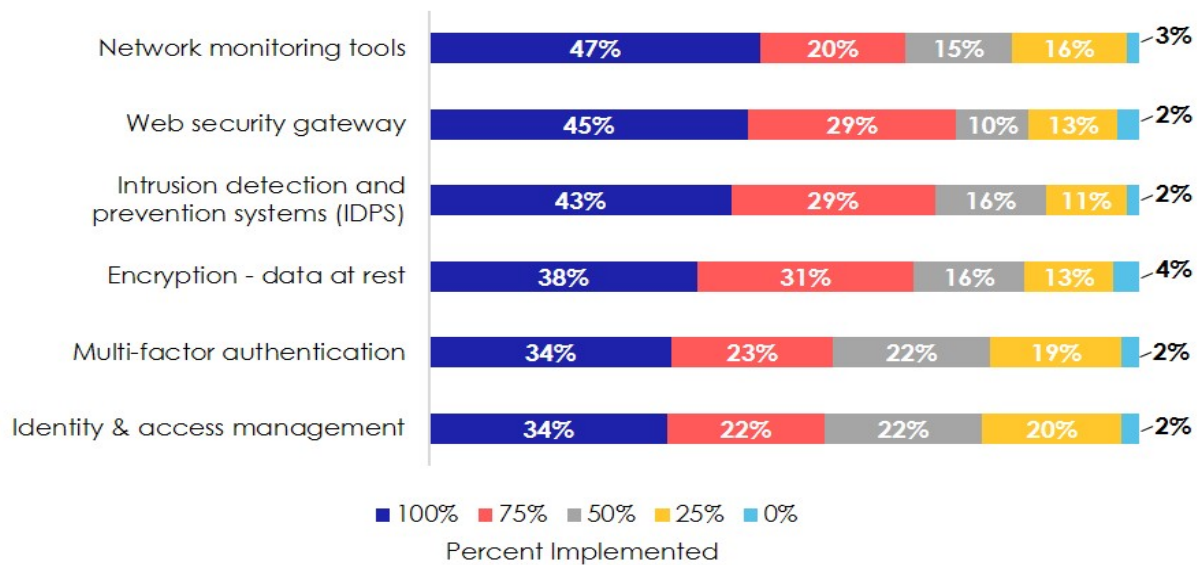
(i)   Network Monitoring Tools

Only **47%** of respondents have implemented **network monitoring tools** comprehensively (100%) across the enterprise. Yet other respondents indicated that network monitoring tools were implemented to a lesser degree. Inadequate or non-existent network monitoring tools can lead to blind spots. What healthcare organizations don't know about what may be going on inside their networks will likely hurt them.

(ii)   Web Security Gateways

Only **45%** of respondents have implemented **web security gateways** comprehensively (100%) across the enterprise. Yet other respondents indicated that web security gateways were implemented to a lesser degree. In the absence of web security gateways, this may leave organizations wide open to compromise. So much of what we do day to day is dependent upon the web.

(iii)   Intrusion detection and prevention systems (IDPS)

Only **43%** of respondents have implemented **intrusion detection and prevention systems** (IDPS) comprehensively (100%) across the enterprise. Yet other respondents indicated that intrusion detection and prevention systems were implemented to a lesser degree. A lack of IDPS implementation may mean a delayed response to active security incidents. This can lead to greater harm to healthcare organizations.

(iv)   Encryption-Data at Rest

Only **38%** of respondents have implemented **encryption for data at rest** comprehensively (100%) across the enterprise. Yet other respondents indicated that encryption for data at rest was implemented to a lesser degree. Without the implementation of encryption for data at rest, data that is either stored or archived remains vulnerable. The volumes of stored and archived data grow by the day.

(v)   Multi-factor Authentication

Only **34%** of respondents have implemented **multi-factor authentication** comprehensively (100%) across the enterprise.[7] Yet other respondents indicated that multi-factor authentication was implemented to a lesser degree. In the absence of multi-factor authentication, **unauthorized** individuals and entities may be able to access sensitive information, resources and assets. The confidentiality, integrity and availability of information may be unnecessarily put at risk.

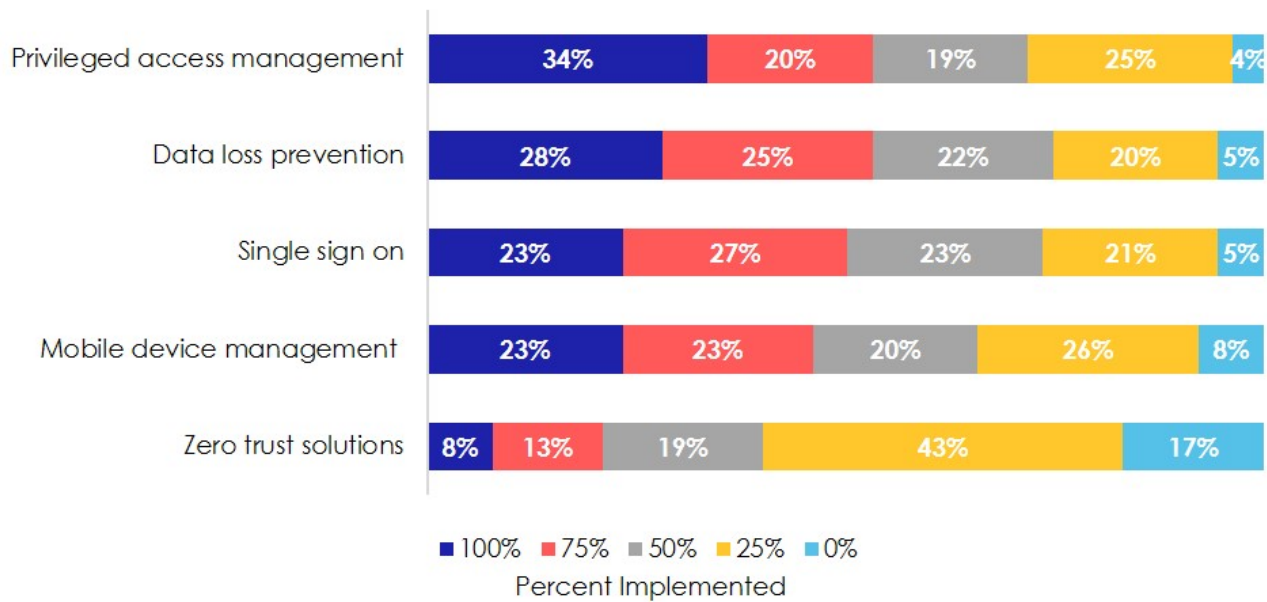### (vi)   Identity and Access Management

Only **34%** of respondents have implemented **identity and access management** comprehensively (100%) across the enterprise. [8] Yet other respondents indicated that identity and access management was implemented to a lesser degree. In the absence of identity and access management, manual processes may need to be relied upon to audit and control user access. This can lead to misuse of user accounts as well as user accounts that have been kept active long after an individual has left the organization.

---

[7] *See* Figure 17.
[8] *See* Figure 17.

C. Third Tier – Basic and Advanced Security Controls

Figure 18: Poorly Implemented Controls

Control	100%	75%	50%	25%	0%
Privileged access management	34%	20%	19%	25%	4%
Data loss prevention	28%	25%	22%	20%	5%
Single sign on	23%	27%	23%	21%	5%
Mobile device management	23%	23%	20%	26%	8%
Zero trust solutions	8%	13%	19%	43%	17%

Percent Implemented

(i) Privileged Access Management

Only **34%** of respondents have implemented **privileged access management** comprehensively (100%) across the enterprise. Yet other respondents indicated that privileged access management was implemented to a lesser degree. In the absence of privileged access management, governance of privileged user accounts may be haphazard, and some users may be granted more access than warranted.

(ii) Data Loss Prevention

Only **28%** of respondents have implemented **data loss prevention** comprehensively (100%) across the enterprise. Yet other respondents indicated data loss prevention was implemented to a lesser degree. In the absence of data loss prevention tools, there may be a greater risk of data leakage and breaches.

(iii) Single Sign On

Only **23%** of respondents have **single sign on** solutions comprehensively (100%) across the enterprise. Yet other respondents indicated single sign on solutions were implemented to a lesser degree. In the absence of single sign on solutions, there may be a significant risk of password reuse and other poor password management practices.

(iv) Mobile Device Management

Only **23%** of respondents have **mobile device management** solutions comprehensively (100%) across the enterprise. Yet other respondents indicated that mobile device management solutions were implemented to a lesser degree. In the absence of mobile device management solutions, there is a greater risk of data leakage, breaches and other compromise due to lost, stolen and compromised devices.

(v)   Zero Trust Solutions

Only **8%** of respondents have **zero trust solutions** comprehensively (100%) across the enterprise.[9] Yet other respondents indicated that zero trust solutions were implemented to a lesser degree. Zero trust solutions are still gaining traction within the healthcare sector. Zero trust solutions require a strong foundation of basic security controls to be in place, such as robust identity and access management. Nonetheless, the appropriate implementation of zero trust solutions can lead to significantly heightened security postures for healthcare organizations.

---

[9] *See* Figure 18.

Section #5: Bug Bounty Programs

A. Bug bounty programs are rare in healthcare

Bug bounty programs provide incentives for security researchers to identify, detect and report vulnerabilities to an organization. Within the bug bounty program, organizations define the scope of what is permitted and other rules of engagement. The organization providing a bug bounty may give a monetary reward, recognition or other remuneration to the researcher, if the vulnerability is confirmed.

We asked respondents if their **healthcare organizations participate in bug bounty programs**. The vast majority of respondents (**89%**) reported that their healthcare organizations **do not participate in bug bounty program**, whereas **11%** reported that their organizations **do participate in a bug bounty program**. Participants in bug bounty programs may be able to discover vulnerabilities that developers and security teams might otherwise overlook.

Figure 19: Healthcare Organizations Participating in a Bug Bounty Program
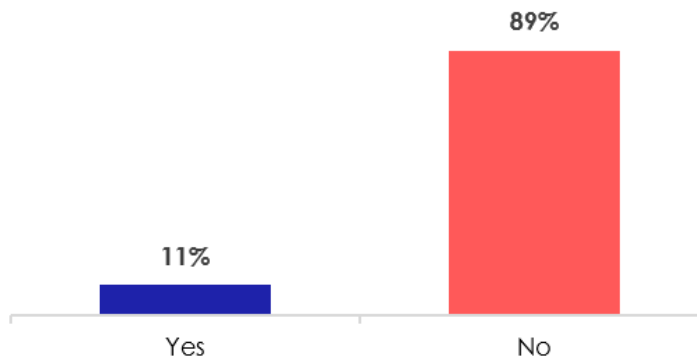
Conclusion

The findings of the **2021 HIMSS Healthcare Cybersecurity Survey** suggest that healthcare organizations still have significant challenges to overcome. These barriers to progress include tight security budgets, growing legacy footprints and the growing volume of cyber-attacks and compromises. Additionally, basic security controls have not been fully implemented at many organizations. But perhaps the largest vulnerability is the human factor. Healthcare organizations should do more to support healthcare cybersecurity professionals and their cybersecurity programs.

About HIMSS

The Healthcare Information and Management Systems Society (HIMSS) is a global advisor, thought leader and member association committed to transforming the health ecosystem. As a mission-driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research and analytics to advise leaders, stakeholders and influencers from across the ecosystem on best practices. With a community-centric approach, our innovation engine delivers key insights, education and engaging events to healthcare providers, payers, governments, startups, life sciences and other health services organizations, ensuring they have the right information at the point of decision. HIMSS has served the global health community for more than 60 years, with focused operations across North America, Europe, the United Kingdom, the Middle East and Asia-Pacific. Our members include more than 100,000 individuals, 480 provider organizations, 470 non-profit partners and 650 health services organizations.

How to Cite this Survey

Individuals are encouraged to cite this report and any accompanying graphics in printed matter, publications or any other medium, as long as the information is attributed to the **2021 HIMSS Healthcare Cybersecurity Survey**.

For More Information

Morgan Searles
Strategic Communications Manager
Marketing & Communications
HIMSS
350 N. Orleans St., Suite S10000
Chicago, IL 60654
312-915-9540
morgan.searles@himss.org