Security and digital identity in the healthcare industry

How healthcare facilities can safeguard their systems with a holistic security strategy

INSIGHTS
Worldwide Business Research

Sponsored by:
imprivata

Table of contents

Executive summary

Healthcare organizations have been put under a significant amount of strain in recent years due to the ongoing COVID-19 pandemic. Many hospitals and clinics have found themselves at times overwhelmed with patients, and medical professionals are experiencing high levels of burnout and turnover. Unfortunately, these events haven't exempted them from being at risk from cyberattacks and data breaches.

According to Forbes, the number of hacking incidents reported in healthcare climbed for the fifth straight year, jumping 42% in 2020. Hacking incidents comprised more than half of 2021's patient data breaches—62% up from 2019.[1]

Healthcare organizations have taken significant steps to protect themselves from external threats, but to fully protect themselves, they must also successfully manage all of their digital identities, including third parties. Remotely accessible human interfaces, in-practice transactions, and on-site networks can all suffer breaches when the identities of users aren't effectively verified. High levels of burnout and turnover can also contribute to risk, as employees often leave the job with their login credentials still intact.

This report explores how healthcare organizations like hospitals, clinics, and medical systems are approaching security risks. It provides readers with cybersecurity benchmarking information about the industry and key suggestions on how to address some of the most pressing security challenges.

[1] Culbertson, Nick. "Increased Cyberattacks On Healthcare Institutions Shows The Need For Greater Cybersecurity." Forbes. June 7th, 2021. https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=7bfe6c785650

About the respondents

The WBR Insights research team surveyed 200 security leaders at healthcare companies across the U.S. and the UK to generate the results featured in this report.

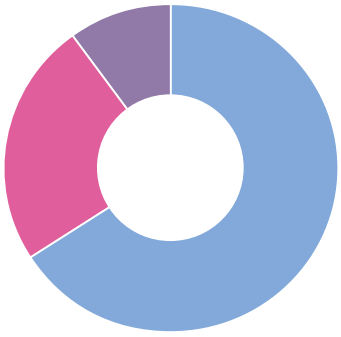
Most of the respondents (66%) represent a facility or facilities that have 500 to 1,000 beds. About one- quarter of the respondents (24%) are from a health system that has 1,000 to 2,500 beds, while 10% are from a system that has more than 2,500 beds.

At 57%, most of the respondents are directors. The remaining respondents are department heads (19%), C-suite executives (17%), and vice presidents (7%).

The respondents occupy roles in information security (44%), security (42%), and identity access (14%).

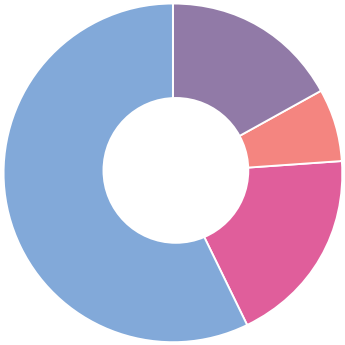
How many beds does your facility or do your facilities have?

- **66%** 500 – 1,000 beds
- **24%** 1,000 – 2,500 beds
- **10%** More than 2,500 beds



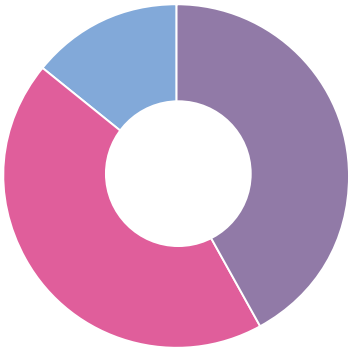
What is your seniority?

- **17%** C-suite
- **7%** Vice president
- **19%** Department head
- **57%** Director



What is your role?

- **42%** Security
- **44%** Information security
- **14%** Identity access



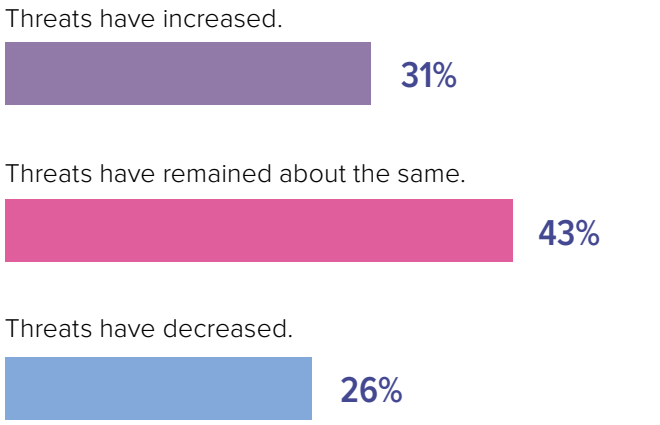
Healthcare facilities struggle with costly cyber incidents

Data and network security have been key investments for companies in a variety of industries over the past several years, especially since high-profile security breaches have revealed significant gaps in security at even the largest organizations. But if there was ever a time in which hospitals and clinics weren't a target for cybercrime, that time has passed.

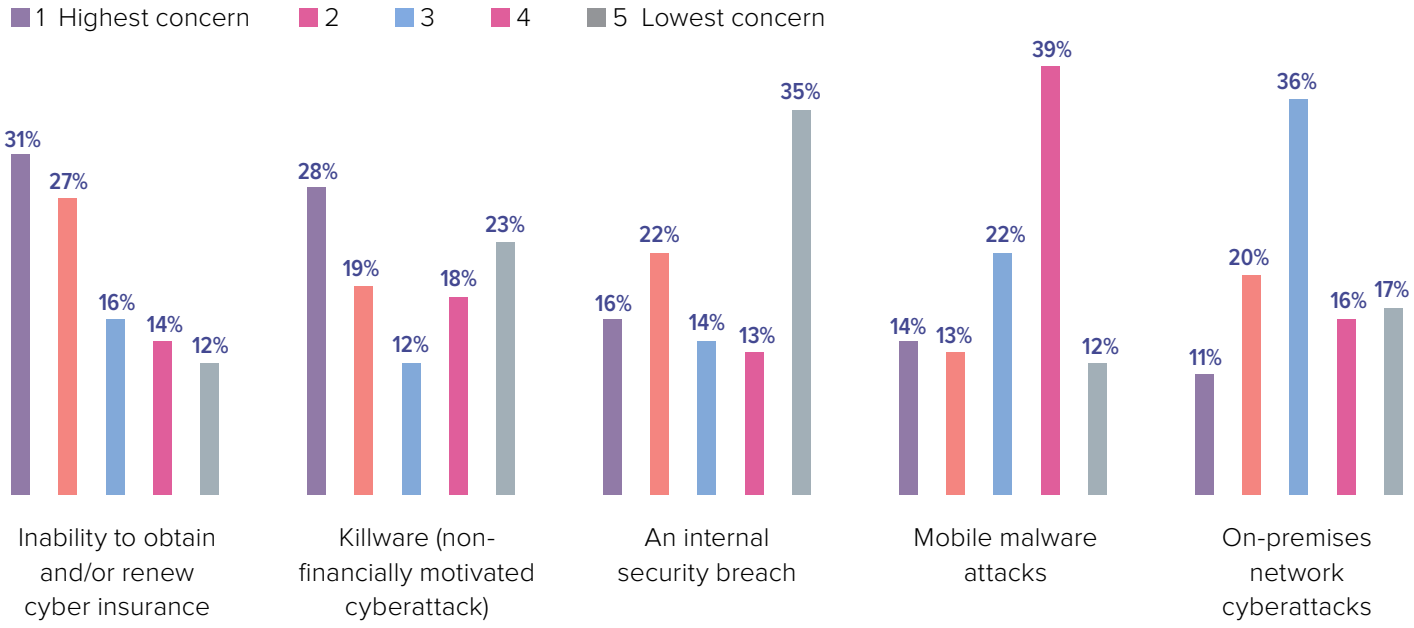
According to most of this study's respondents, cybersecurity risks have either remained about the same over the past two years (43%) or increased (31%).

Healthcare providers work with sensitive data daily. Data relating to transactions and patient identities are primary targets for hackers and other bad actors. Hospitals have also become attractive targets for non-financially motivated cyberattacks, as they are a key component of most regional infrastructures.

Based on your experience, have cybersecurity risks increased or decreased for your organization over the past two years?



What are your top security concerns for 2022?



The respondents' top security concerns for 2022 are an inability to maintain cyber insurance (31%), the risk of non-financially motivated cyberattacks, including "Killware" (28%), and internal security breaches (16%).

Significant portions of the respondents are also moderately concerned with on-premises network attacks and mobile malware attacks.

To address these challenges, healthcare providers are engaging in a range of security initiatives in 2022, with the intention of providing lasting security attacks this year and beyond.

Specifically, the respondent's highest-priority projects include updating legacy systems (51%), implementing multifactor authentication, or MFA (47%), and creating a cybersecurity response plan (43%).

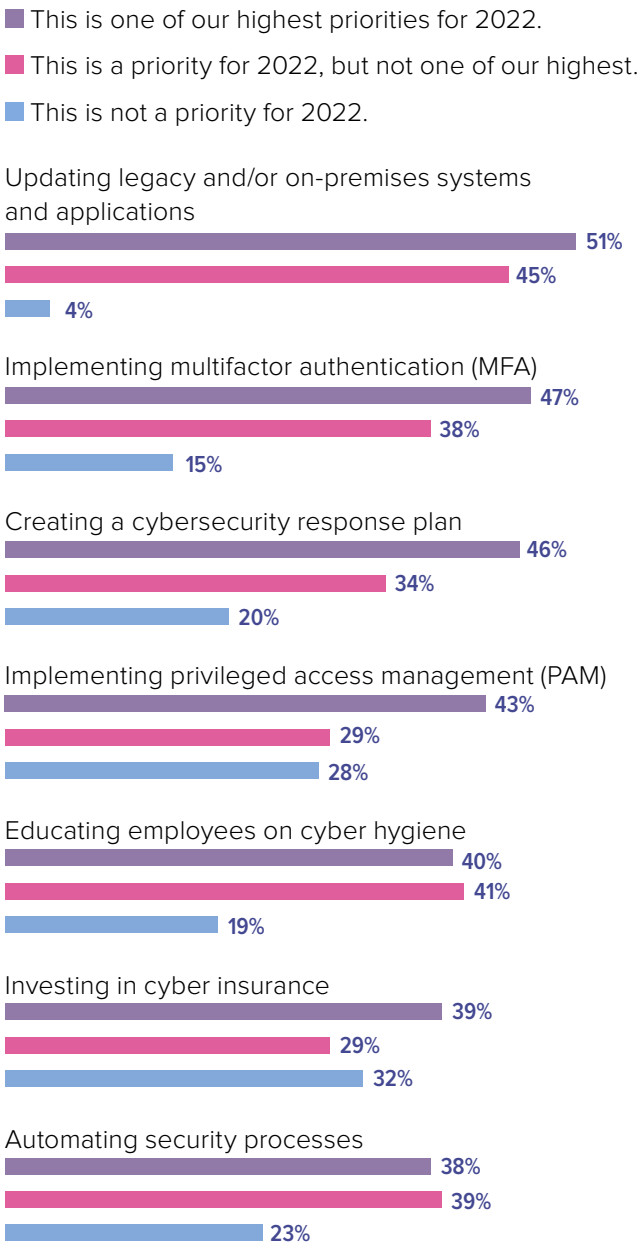
It is notable, however, that updating legacy systems is considered "high priority" by 51% of the respondents, and it is the only security initiative on the list that a majority of the respondents consider a high priority. This suggests that the respondents are placing a variety of security initiatives at "high priority," when they could benefit by a narrower focus.

For example, more than a quarter of the respondents (28%) say implementing privileged access management (PAM) is not a priority for 2022.

PAM helps healthcare facilities manage the digital identities of their privileged accounts. These users or accounts are those with the highest level of access and therefore pose a greater security risk than the average end user due to the degree of sensitive information that could be exposed.

It also helps security teams identify malicious activity, and it should be a priority for most healthcare organizations. Although this type of protocol requires an investment, it is often an essential defense function against security incidents.

Please rate the following security initiatives in terms of their priority for 2022.



Indeed, most of the respondents (51%) say their organizations have experienced a security incident in the past year. Whether this was a minor internal incident involving a single employee or a broad attack from outside the organization, either example could expose the facility's network and compromise the organization's data.

Among those respondents who have experienced a security incident in the past year, most (51%) say the incident involved the theft of personally identifiable information (PII). PII is any information that could be linked to the identity of an individual. Data like Social Security numbers, credit card information, and even names and birthdays can be used by cybercriminals to gain illicit access to systems like bank accounts.

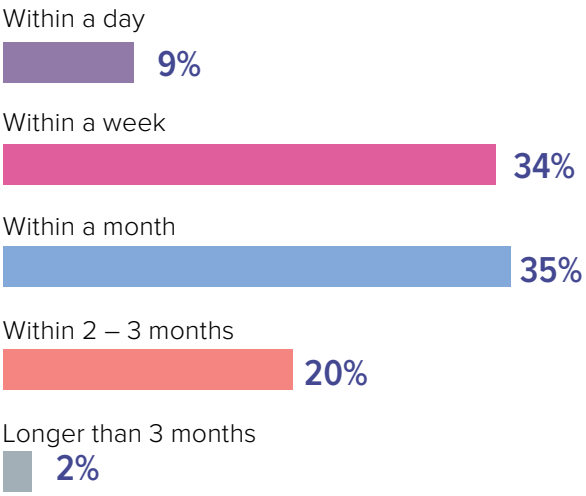
PII theft was the most prominent incident on record, as fewer than one-third of these respondents say they suffered from intellectual property theft (32%), theft of personal health information (28%), and others.

These respondents also indicate that it took their organizations a significant amount of time to recover from such incidents. Although 9% of the respondents recovered within a day and 34% recovered within a week, most of these respondents (57%) needed one month or more to recover.

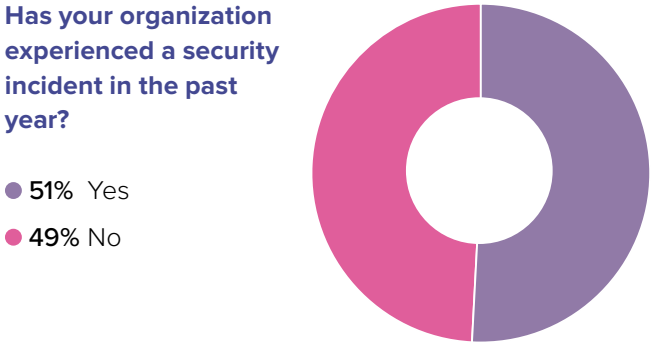
Not only are cybersecurity incidents becoming more frequent, but they are also becoming more costly. Healthcare providers that endure an incident can suffer financially due to the incident itself, but also due to the time it takes to recover. Cyber incidents also affect patient confidence, as it implies their information may not be safe with their local healthcare facility.

These organizations must take steps now to ensure they have identity protections in place as well as a robust cybersecurity program to ward off external threats. Ideally, within the next few years, most healthcare organizations will report that they haven't suffered a cybersecurity incident within the previous 12 months.

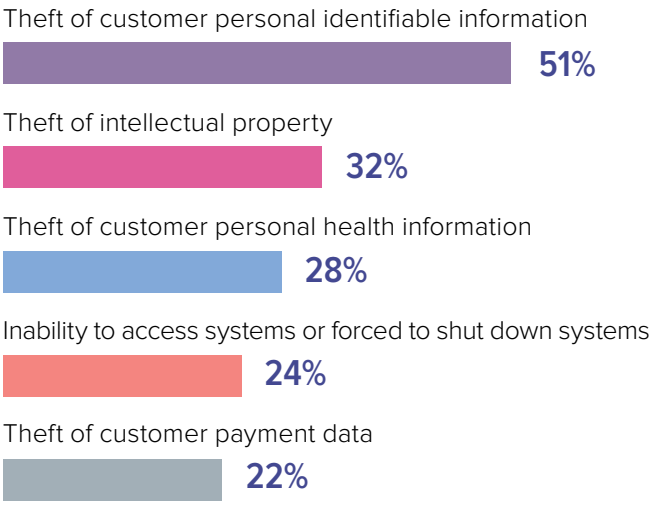
How long did it take you to identify and remediate these security incident(s) on average?



Has your organization experienced a security incident in the past year?



Since you said "Yes," please indicate which types of security incidents your organization experienced.



Security strategies becoming more robust among healthcare providers

Despite the challenges they must contend with, many healthcare providers have taken steps to safeguard their data. They've implemented robust cybersecurity suites to protect themselves from external threats. Many clinics and hospitals are also using advanced on-premises security features, such as biometrics, to safeguard information and access.

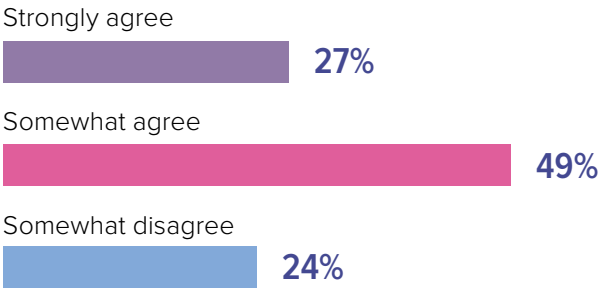
Most of the respondents either somewhat agree (49%) or strongly agree (27%) that their organizations' security strategies have become more robust and comprehensive over the past 12 months. However, almost one-quarter of the respondents (24%) somewhat disagree with this statement. They don't believe their security strategy has kept pace with what's needed in the industry.

Unfortunately, many organizations don't take the necessary steps to protect their data until they experience or witness an incident. This type of reactive security strategy is present in almost every industry, not just the healthcare sector.

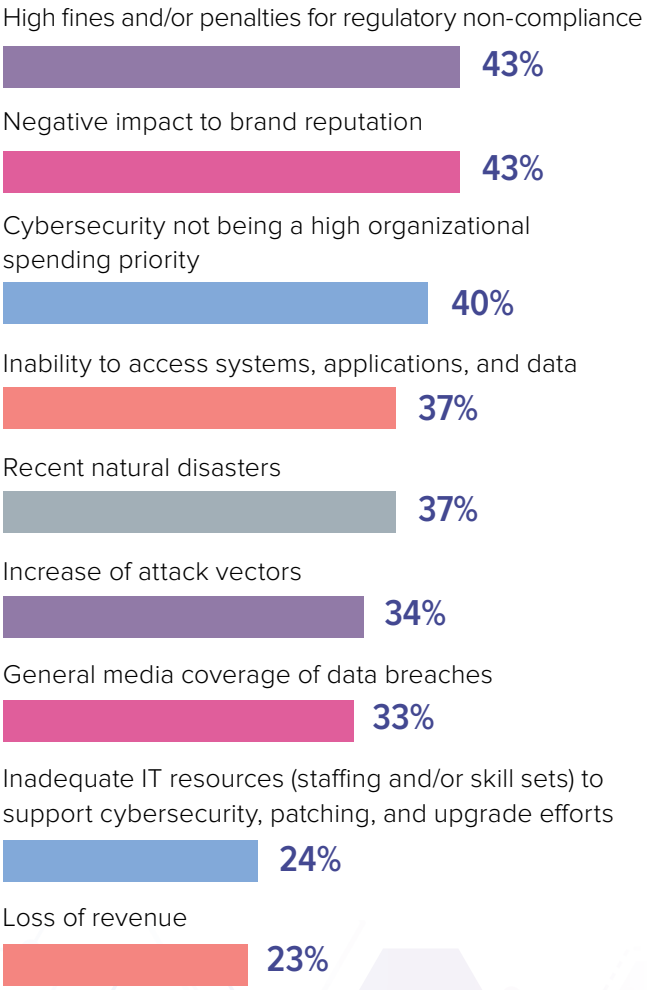
For example, in each case, 43% of the respondents say negative impacts to their brands' reputation and high fines or penalties have driven them to be concerned about their ability to safeguard data. Meanwhile, 40% say they've noticed that cybersecurity is not a high organizational spending priority. This could lead to a security deficit if not addressed quickly.

Over one-third of the respondents are concerned about other events or potential events, such as recent natural disasters (37%), the inability to access systems or data (37%), an increase in attack vectors (34%), and general media coverage of data breaches (33%).

Please choose the response that best fits with this statement: "I believe that my organization's security strategy has become more robust and comprehensive since this time last year."



Which of the following events have driven concern about your ability to safeguard sensitive data at your organization?



This suggests healthcare organizations are also searching for ways to safeguard their data from incidents that go beyond cyber threats. Other security incidents, including natural disasters, could significantly impact data security and can't be protected against by standard cybersecurity measures.

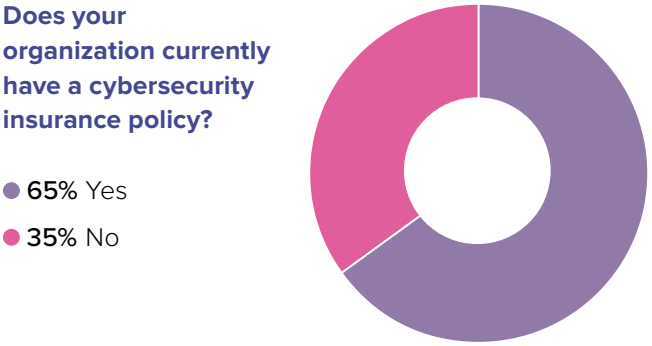
Most of the respondents also recognize the significant fallout that could occur due to a security incident. As such, 65% of them currently have a cybersecurity insurance policy in place. This type of insurance protects a business against losses due to cyber-related crimes and data breaches, and it's quickly becoming an important investment for companies that are the primary targets of cyberattacks.

Among those organizations that have a cybersecurity insurance policy, most say their insurance premiums have increased by at least 11% over the past year (77%). This includes 40% who say their premiums have increased by 26% to 50%, as well as 7% who say their premiums have increased by 51% to 75%.

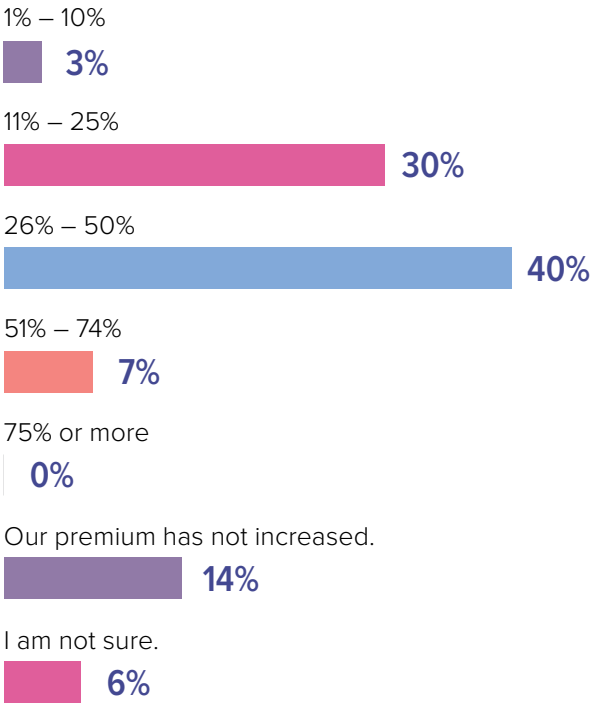
Insurance companies typically raise premiums on specific accounts if they suffer an incident. However, they may also raise premiums due to an overall increase in security risks.

Individually, healthcare organizations must implement security measures to ensure their premiums stay low. Digital identity verification, identity governance, access management, and protocols like MFA and PAM for internal and third parties are more frequently becoming requirements to even secure cyber insurance, let alone keep policy costs down.

Does your organization currently have a cybersecurity insurance policy?



Since you said "Yes," how much has your cybersecurity insurance premium increased over the past year?



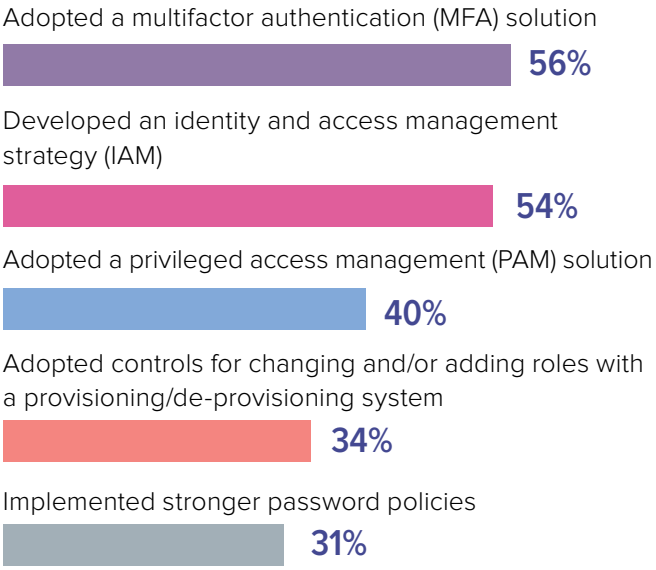
Most of the respondents who have an insurance policy have already implemented MFA (56%) and have developed an identity and access management (IAM) strategy (54%). However, with the current climate of cyber crimes, these numbers should be higher. At the very least, those organizations who have been able to secure cyber insurance may see decreased premiums, and at best, protect themselves from serious risk.

Fewer of these respondents are using a privileged access management solution (40%), a provisioning and de-provisioning system (34%), and strong password policies. These security strategies are especially important for protecting the organization against internal threats, such as disgruntled employees or employee negligence.

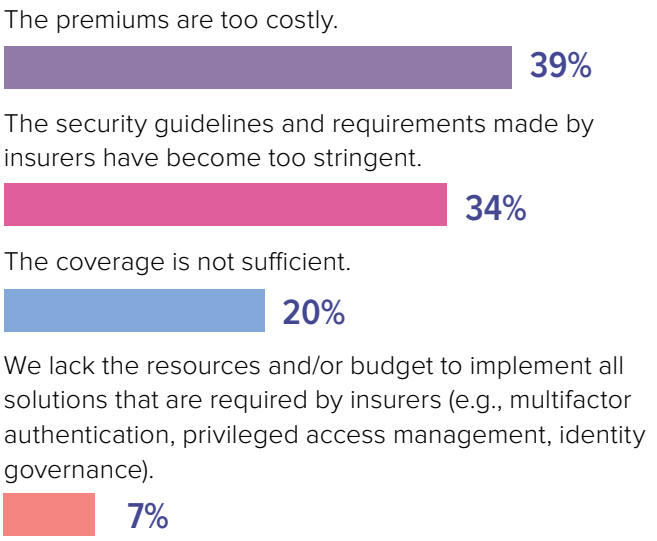
The respondents who don't have this type of insurance policy cite multiple reasons for going without one. However, most of the respondents are either concerned about the policies' high premiums (39%) or the stringent requirements made by insurers to carry them (34%).

These concerns are relevant, but insurance could be worth the investment considering the significant losses that could occur because of a cyber incident. To protect themselves, healthcare organizations should operate as if they are under constant threat from cyberattacks, and assume that they will experience an incident eventually.

Since you said "Yes," what measures have you put in place to reduce the increase of your insurance premiums?



Since you said, "No," what is the primary reason your organization does not have a cybersecurity insurance policy?



Healthcare security leaders recognize the importance of identity management

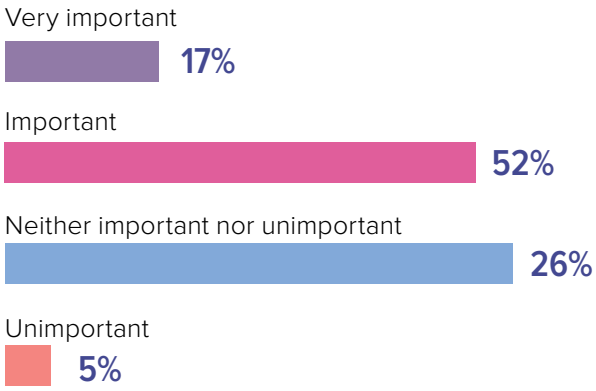
Despite some significant gaps in security and insurance, most security leaders at healthcare organizations understand the threats they face. However, they also have many challenges to driving their security efforts to fruition, such as interdepartmental hurdles, and misalignment in cost prioritization from other decision-makers.

Among the many security protocols recognized by healthcare security leaders as important or very important is digital identity management. Specifically, 52% of the respondents view digital identity management as important, while 17% view it as very important.

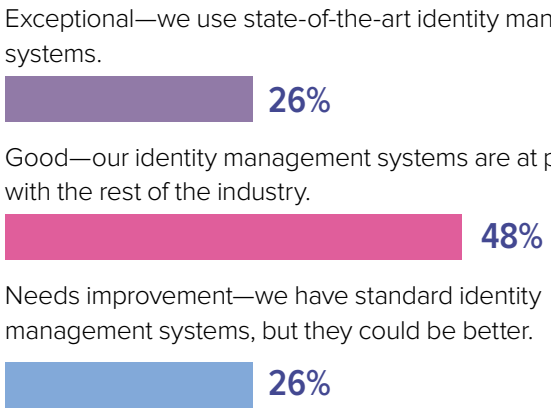
Additionally, most of the respondents believe they have strong identity management systems in place. Almost half (48%) say their identity management systems are at parity with the rest of the industry. Over one-quarter (26%) say they use state-of-the-art identity management systems.

Nonetheless, 26% also say their identity management systems need improvement. They have a standard system in place, but their protections could be better. These organizations need to make improvements to their current system or find one that provides easier and more frictionless access to users.

How important do you believe managing digital identities is to your security strategy?



How would you rate your organization's current identity management systems?

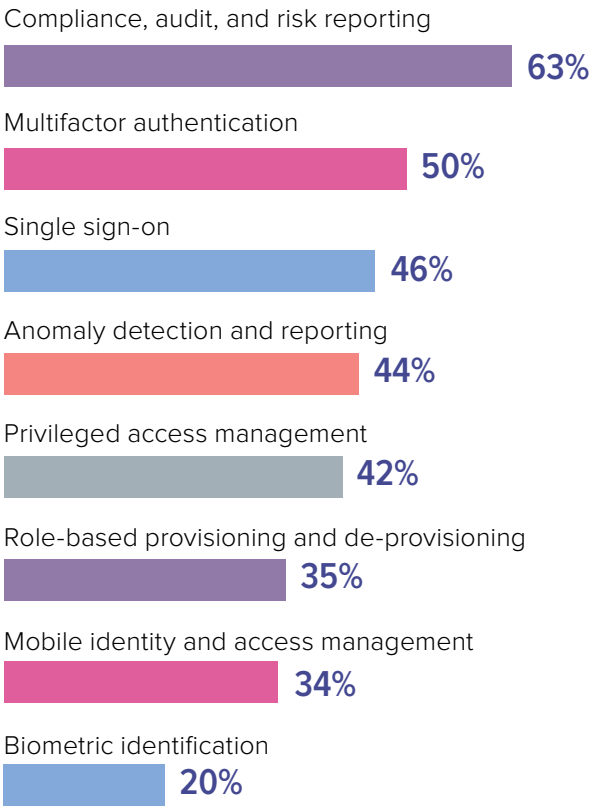


For example, only 46% of the respondents currently use single sign-on. This protocol not only reduces the number of attack surfaces in the system but also makes access easier for credentialed users, which avoids risky behavior like writing passwords down or sharing credentials. Instead of having to log into a system each time they need to accomplish a task, they only need to do so once per day or once per shift.

Although most of the respondents (63%) currently use compliance, audit, and risk reporting solutions, they need to implement other solutions to enhance security. Only 50% of the respondents are currently using MFA, which should be standard across the industry.

Similarly, only about one-third of the respondents (34%) are using mobile identity and access management. Going without this solution could put the organization at risk from mobile attacks, especially if employees can access the network via their personal devices.

Which of the following solutions do you currently use at your organization?

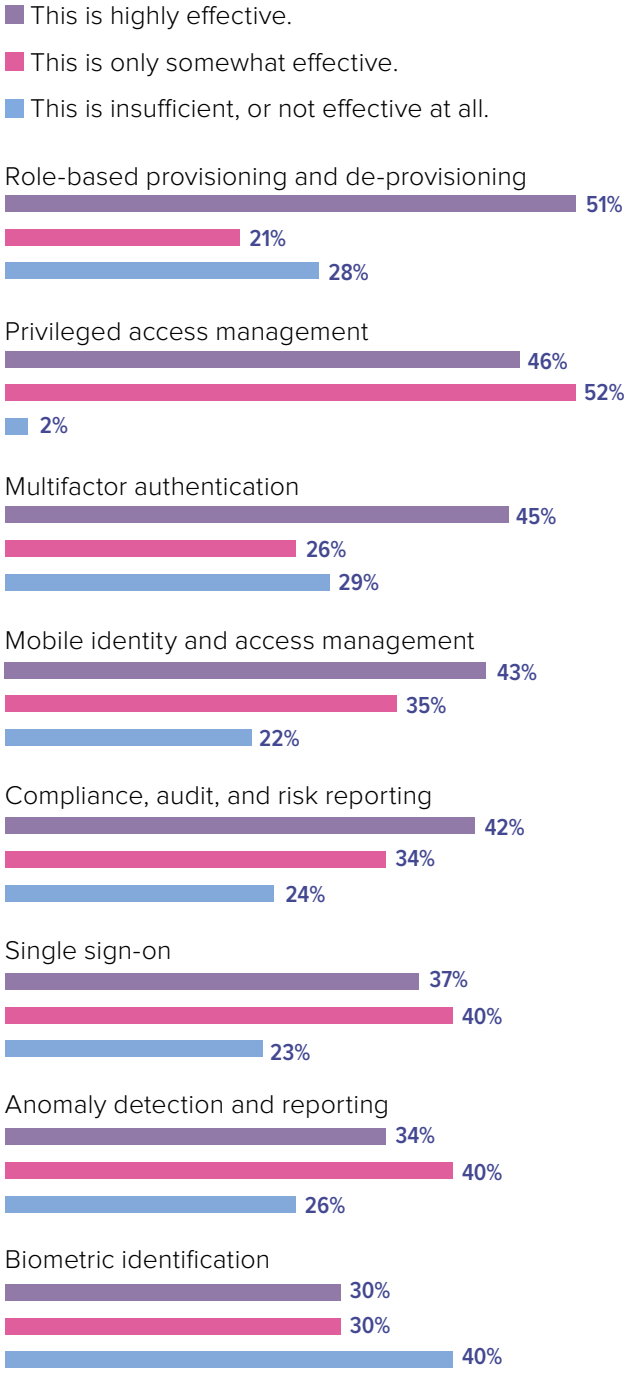


A majority of the respondents don't rate most of the security measures presented to them as highly effective. This suggests that respondents view individual security protocols as lacking on their own, requiring a layered approach that includes identity access, log-in access, and traditional cybersecurity solutions like anti-virus software for true risk mitigation.

In each case, over one-quarter of the respondents believe MFA (29%), role-based provisioning (28%), and anomaly detection and reporting (26%) are insufficient or not effective for preventing cyberattacks and data breaches. Meanwhile, 40% say biometric identification is not sufficient.

Nonetheless, most of the respondents (51%) say role-based provisioning is highly effective at preventing attacks. In each case, almost half of the respondents say the same thing about privileged access management (46%) and MFA (45%).

Please rate the following security measures in terms of their effectiveness for preventing cyberattacks and data breaches in 2022.



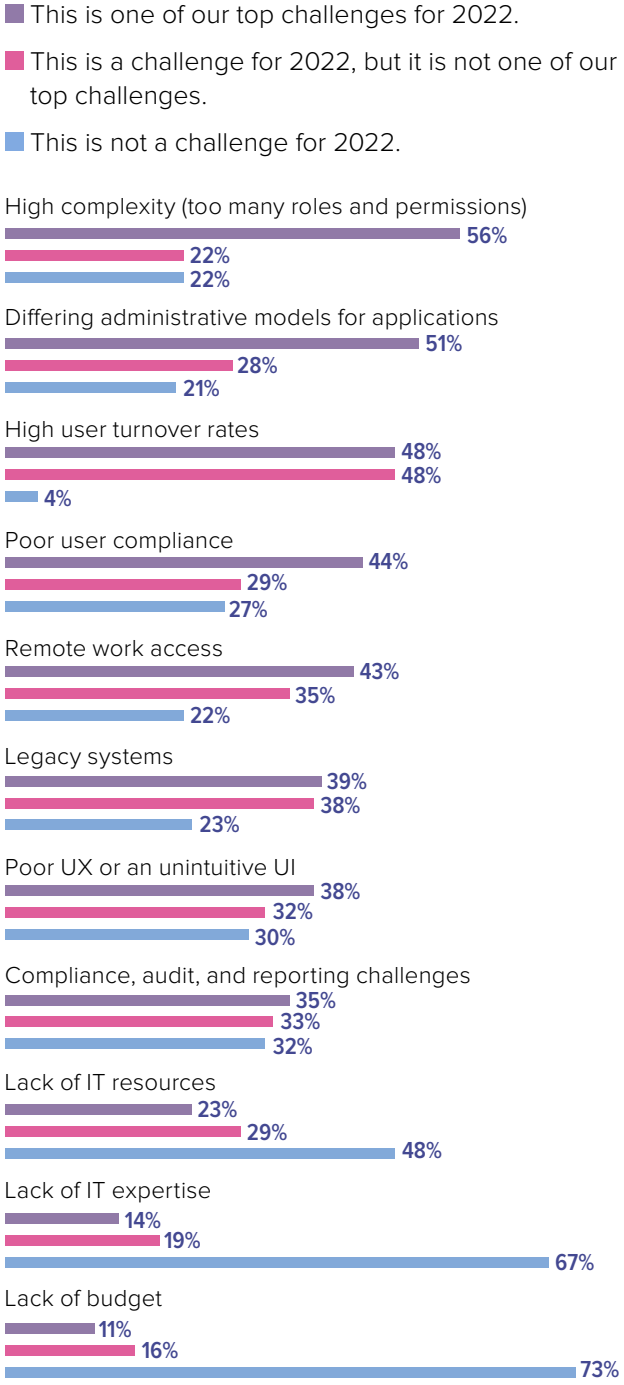
As we've learned, some of the gaps in these organizations' security measures are due to concerns about cost, but there are other barriers and roadblocks between healthcare security leaders and their cybersecurity goals. Identity management can be challenging to implement internally. Without the help of a seasoned security partner, some organizations may face setbacks when working to implement new policies.

At 56%, most of the respondents say high complexity, such as having to work with too many roles and permissions, is one of their top challenges in addressing identity management in 2022. A slight majority of the respondents (51%) say the same about differing administrative models for applications.

High turnover rates (48%)—common in the healthcare sector—are also a challenge for many, as are poor user compliance (44%) and challenges related to remote work access (43%).

Interestingly, 73% of the respondents say lack of budget is not a challenge for their identity management strategy in 2022. This suggests that most healthcare organizations have the means to initiate a robust identity management program, but they may be struggling with complexity, user adoption, legacy systems, and other internal obstacles.

Please rate the following roadblocks in terms of the challenge each poses to implementing and/or enforcing your identity management strategy.



Key suggestions

- **Healthcare organizations should take steps to obtain cyber insurance so they can recover from security incidents faster.** To reduce premiums and premium increases, they should enact a robust cybersecurity policy that includes external protections as well as internal defenses, such as identity access controls.
- **Multifactor authentication (MFA) should become standard for all applications, devices, and access points.** When paired with single sign-on (SSO), MFA can be implemented without causing significant problems for the user experience.
- **Hospitals, clinics, and other healthcare facilities must audit their current identity management systems to ensure they are sufficient for their security.** State-of-the-art, turnkey solutions are available from providers that specialize in serving the healthcare sector.
- **Healthcare organizations should partner with solution providers to overcome common roadblocks to implementing and enforcing their identity management strategy.** Many solution providers can assist with highly complex roles and permissions, poor user compliance, and legacy system integration.

Conclusion: Overcoming internal obstacles to identity management

Responses to the study imply that healthcare organizations have made some significant progress in protecting their systems from cyberattacks and data breaches. They are also aware of the risks inherent in the current threat landscape.

However, the fact that 51% of the organizations surveyed have suffered a security incident in the past 12 months should raise concern. Not only are security threats common, but they are also becoming more relentless and damaging. Even a small lapse in security could make a healthcare system and its data vulnerable.

The respondents indicate that they are concerned about the costs of cybersecurity insurance, but they say that budget isn't an issue when it comes to identity management. This suggests that most healthcare systems have the resources they need to create a robust identity management protocol. Afterward, insurance may be more attractive, as the identity management system could help them lower premiums.

Moving forward, hospitals, clinics, and healthcare systems must partner with identity management experts to enact more robust policies and encourage adoption among employees. With this help, security leaders will be able to demonstrate to both associates and decision-makers how this type of investment can protect the organization, help operations run more smoothly, and help the bottom line.

Key findings

Among the respondents:

- The inability to renew or obtain cyber insurance is their highest (31%) or second-highest (27%) security concern for 2022.
- 51% consider updating legacy or on-premises systems one of their highest priorities for 2022, while 47% consider multifactor authentication (MFA) a high priority.
- Although 43% say cybersecurity risks have not increased over the past two years, 31% claim risks have increased compared to just 26% who say risks have decreased.

- 51% claim their organizations have **experienced a security incident in the past year.**

- 76% agree that their organizations' security strategies have become more robust and comprehensive since this time last year.
- In each case, 43% say negative impacts to brand reputation and high fines for non-compliance have driven concern about their ability to safeguard sensitive data.

- 65% claim their organizations currently have a **cybersecurity insurance policy.**

- Those who do not currently have a cybersecurity insurance policy claim their primary reason is that the premiums are too costly (39%) or that the security requirements made by insurers have become too stringent (34%).
- 52% consider managing digital identities important and 17% consider it very important to their security strategies.
- 63% claim they currently use compliance, audit, and risk reporting solutions at their organizations and 50% claim they use MFA.
- 51% say role-based provisioning and de-provisioning will be highly effective at preventing cyberattacks in 2022, but this was the only security measure that a majority named highly effective.
- Their most significant roadblocks to implementing and/or enforcing identity management strategies are high complexity (56%) and differing administrative models for applications (51%).

About the authors

imprivata

We build healthcare's preferred platform for digital identity based on actual clinical workflows — ensuring frictionless user access to the right data and applications, for the right reasons. Always.

We make patient care easier by removing the barriers to user access and authentication. Our digital identity platform is developed with, and vetted by, clinicians who face these daily challenges. It's how we're able to deliver frictionless interactions across the entire healthcare ecosystem while ensuring workflow security.

For more information, please visit www.imprivata.com.

InfoSec Healthcare CONNECT

InfoSecurity Healthcare Connect is an invite-only forum for senior-level information and cybersecurity executives. Here, you can benchmark against other leaders in your industry, hear custom executive-level content, and evaluate solutions that meet your specific needs up close. This is a luxurious and exclusive experience you can't get anywhere else.

For more information, please visit cisohealthcare.wbresearch.com.

INSIGHTS Worldwide Business Research

WBR Insights is the custom research division of Worldwide Business Research (WBR), the world leader in industry-driven thought-leadership conferences. Our mission is to help inform and educate key stakeholders with research-based whitepapers, webinars, digital summits, and other thought-leadership assets while achieving our clients' strategic goals.

For more information, please visit www.wbrinsights.com.