RESEARCH REPORT

Spotlight Report: Cyber Resilience and Business Impact in Healthcare

LevelBlue

LevelBlue

Contents

1. Cyber Resilience: A Proactive Stance Builds Business Confidence
2. Business Impact: Aligning Cybersecurity with Strategic Goals
3. Silo Breakthrough: Alignment and Collaboration for a Proactive Healthcare Culture
4. Evolving Vectors: Preparing for More Sophisticated Attacks
5. Software Supply Chain: Risks and Resilience in Healthcare Organizations
6. Four Steps to Cyber Resilience

About the Research
We wanted to better understand enterprise cyber resilience strategies and how they are being handled throughout an organization. To uncover this data, in January 2025 we engaged FT Longitude to survey 1,500 C-suite and senior executives across 14 countries and seven specific industries: energy and utilities, financial services, healthcare, manufacturing, retail, transportation, US state and local government and higher education (US SLED).

The total number surveyed in healthcare is 220. This is the Spotlight Report: Cyber Resilience and Business Impact in Healthcare for 2025.

We would like to thank FT Longitude, our research partner, and Altitude Management, our design partner, for making this report possible.

We use the following definition in this report:
Cyber resilience: This refers to the entire IT estate and includes the business as it relates to computing and its ability to recover from an unexpected interruption—from cyber incidents to natural and human-caused disasters.

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

1. Cyber Resilience: A Proactive Stance Builds Business Confidence

AI tools promise healthcare organizations unprecedented levels of efficiency, optimized processes, and enhanced automation. But the blazing speed of its evolution—far faster than governance and regulations can keep up—is a reason to be cautious.

In this year's Spotlight on healthcare, we uncover how the industry is protecting itself from increasingly numerous and sophisticated attacks.

Key findings include:

Healthcare organizations are being forced to take cybersecurity more seriously

Increasing risks and the fast-developing threat landscape are forcing cyber resilience up the C-suite's agenda:

- 32% of healthcare executives say their organization suffered a breach in the past 12 months
- 46% say they are experiencing a significantly higher volume of attacks
- 67% say that media reports of high-profile breaches elevated cybersecurity on the C-suite agenda

Most healthcare businesses are not ready for new attacks

Healthcare organizations expect AI-powered attacks, deepfakes, and synthetic identity attacks in 2025. But many are not prepared for them:

- 29% of healthcare executives say they are prepared for AI-powered threats, despite 41% believing they will happen
- 32% feel their organization is prepared for deepfake attacks, even though 49% are expecting them

Resilience in the software supply chain is low on the agenda

Healthcare organizations are underestimating how under-regulated AI tools could pose a risk to their extended ecosystem:

- 54% say they have very low to moderate visibility into the software supply chain
- 19% say that engaging with software suppliers about their security credentials is a priority in the next 12 months

Healthcare companies will thrive by becoming more proactive and more aligned

Responsibility for cyber-resilience measures is making its way into more areas of the business:

- 61% of executives say that their cybersecurity team is aligned with lines of business
- 59% say that leadership roles in their healthcare organization are measured against cybersecurity KPIs

We hope you enjoy reading this year's research and would be delighted to discuss its conclusions and recommendations with you in more detail.

Theresa Lanowitz, Chief Evangelist

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

2. Business Impact: Aligning Cybersecurity with Strategic Goals

Making an organization cyber-resilient both protects it from loss and, at the same time, creates an environment that fosters productivity and innovation.

An increasingly complex and concerning threat landscape is elevating cybersecurity up the agenda: 46% of healthcare executives say they have experienced a significantly higher volume of cyber attacks than 12 months ago, and 32% have experienced a breach in the past 12 months.

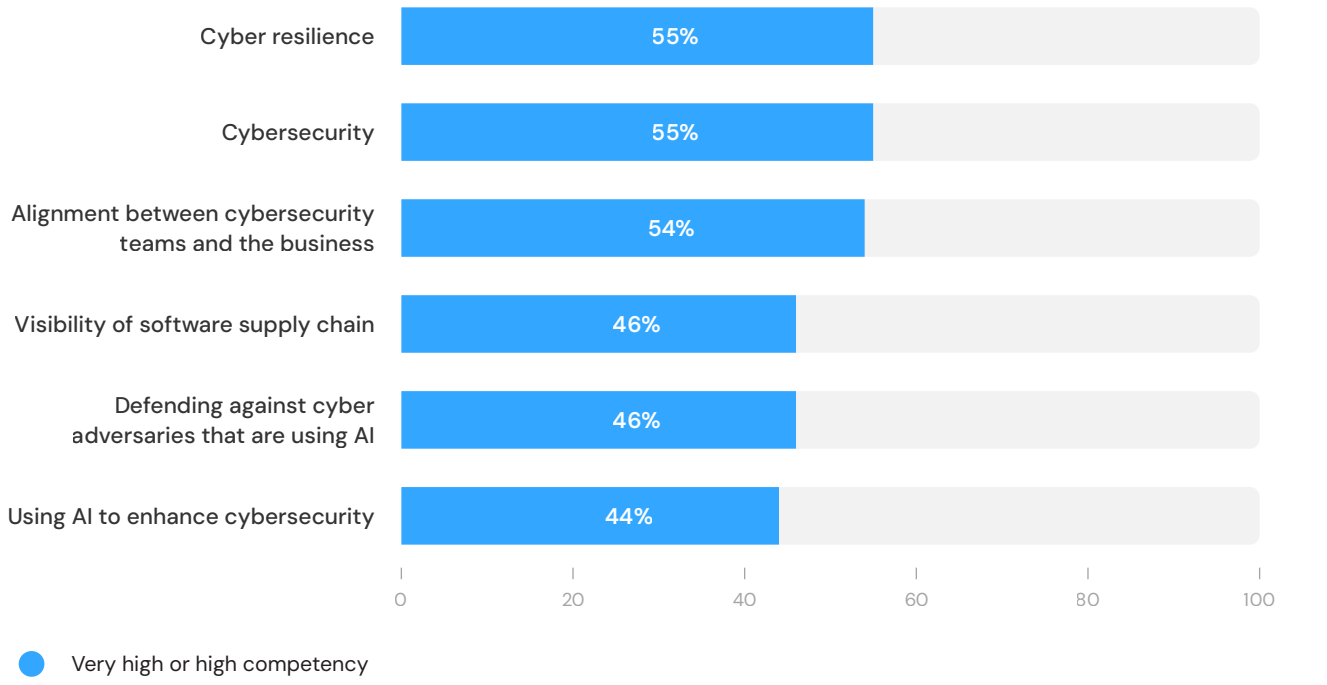
Some 67% of healthcare executives say that media reports of high-profile breaches have pushed cybersecurity up the C-suite agenda. And as AI-powered technologies make attacks more sophisticated, 62% of executives say that it is becoming more difficult for employees to identify real threats.

Figure 1

Healthcare executives report competence at defending against AI attacks and using AI for security

Q: How would you rate your organization's competence in the following areas?

% of respondents
N=220



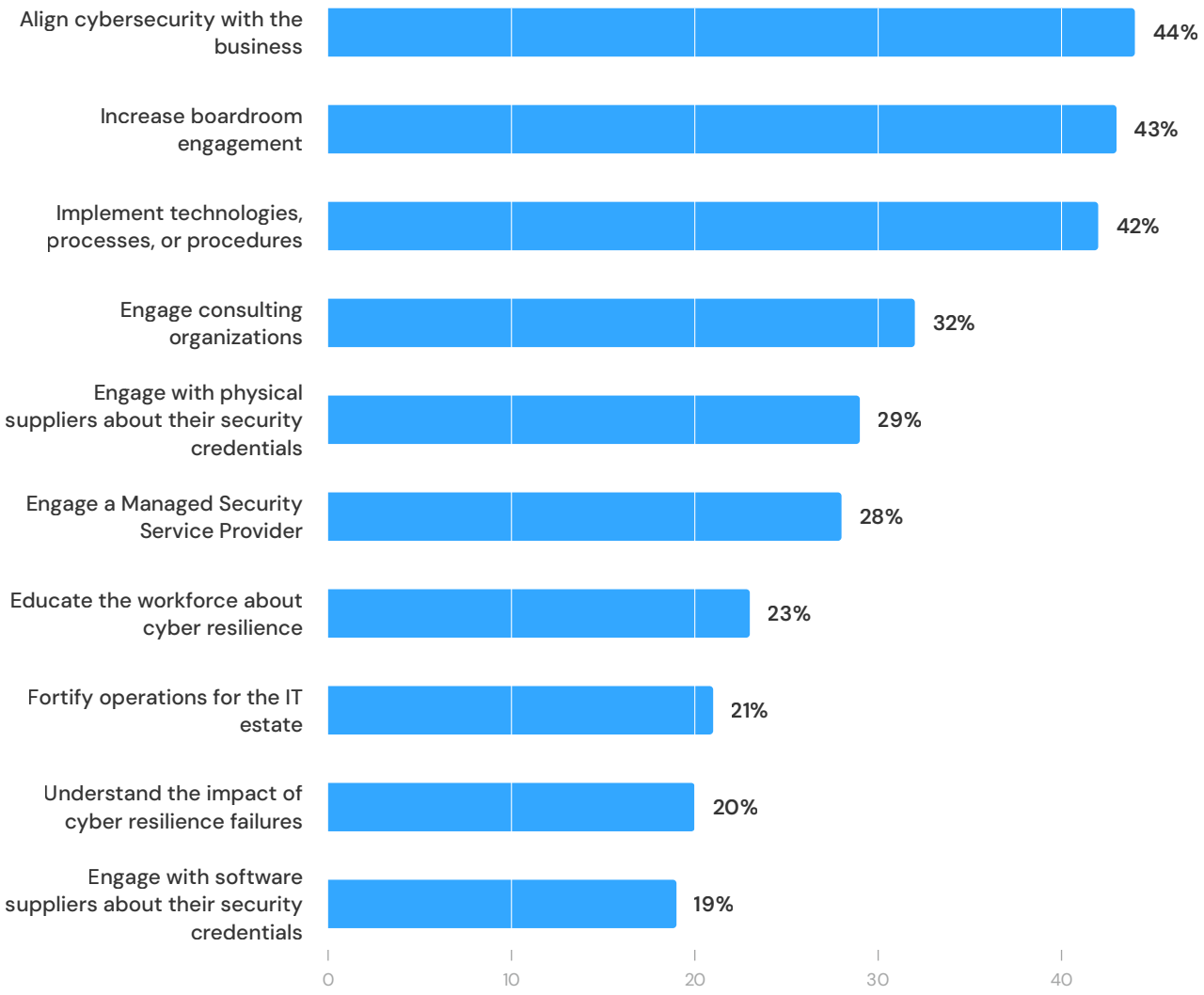
© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

Figure 2

Business impact of cybersecurity drives the healthcare leadership agenda in 2025

Q: Which of the following will be a priority for your organization over the next 12 months as it seeks to improve its cyber resilience?

% of respondents
N=220



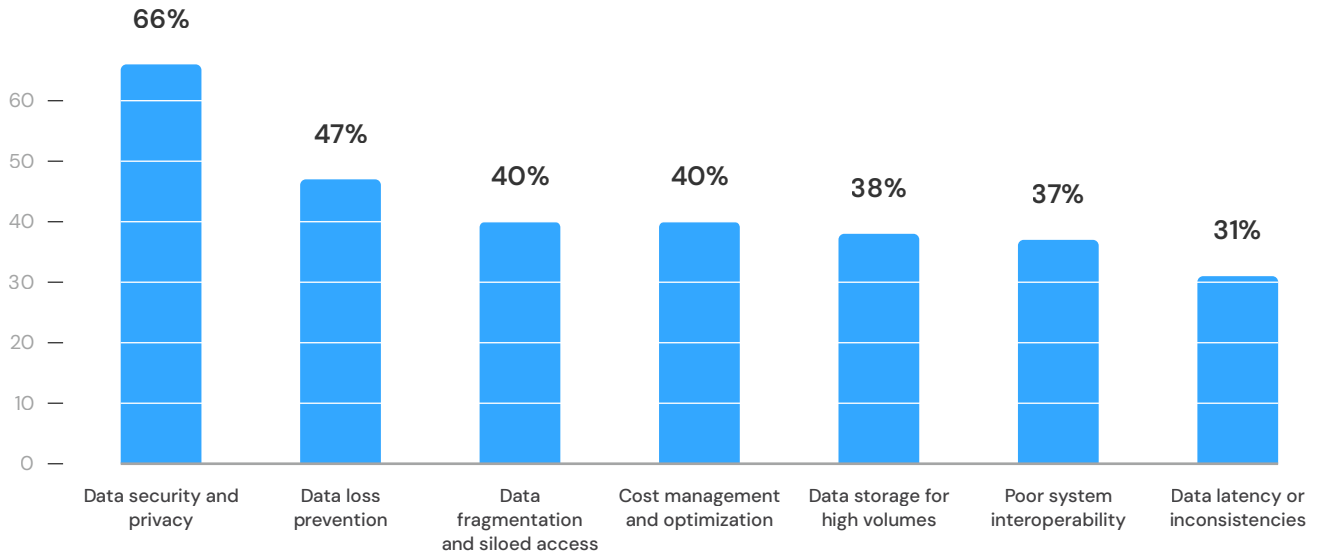
© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

Figure 3

Data security remains a leading concern in healthcare

Q: What are your organization's biggest data challenges as you move towards computing beyond the perimeter of your own organization?

% of respondents
N=220



Are healthcare organizations over-confident in the face of AI-related adversaries?

Despite their concerns, healthcare executives are feeling confident about defending themselves against AI-related adversaries and using AI to enhance defense (Figure 1). Almost half (46%) say they are highly or very highly competent at defending themselves against AI techniques, and in implementing and using AI to enhance cybersecurity (44%).

Healthcare organizations must push discussions to the highest level

Effective leaders see cyber resilience as a core business function. They integrate it into business decisions from the top and ensure that it is prioritized across the organization. Having a boardroom engaged with cyber issues means the organization is better prepared to handle incidents and minimize losses. Healthcare organizations recognize this: 43% say they are increasing boardroom engagement in cyber-resilience discussions, making it the second-highest priority for improving cyber resilience in the next 12 months (Figure 2).

Some healthcare organizations are balancing their approaches to risk and innovation

Cybersecurity not only protects assets, but it can also help healthcare organizations to access new revenue streams. By making their digitalization efforts cyber-resilient, organizations can build trust, while enhancing their reputations and confidence, which creates a robust and flexible environment for innovation and development.

To develop cyber resilience, cybersecurity teams need to be aligned with lines of business. This creates a more balanced approach to cybersecurity and innovation risk.

Nearly half of healthcare organizations are making good progress: 43% say they have effectively aligned

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

business risk appetites with cybersecurity risk management and the same number (43%) allocate a cybersecurity budget to new initiatives from the beginning.

Aligning cybersecurity with lines of business allows organizations to take bigger risks with innovation. Healthcare organizations are starting to see results: 55% say that an adaptive approach to cybersecurity enables them to take greater innovation risks.

But are organizations paying due attention to AI risks?

Higher levels of cybersecurity alignment also seem to reduce healthcare organizations' caution about implementing AI. Only 33% of healthcare executives say they are reluctant to implement AI tools and technologies because of cybersecurity ramifications.

AI adoption is happening too fast for regulations, governance, or mature cybersecurity controls to keep pace, which increases organizations' attack surface and risk exposure. Executive confidence about implementing AI despite the cybersecurity ramifications suggests a disconnect. They recognize the very real risks but are nevertheless enthusiastic about implementing the technology—possibly without adequate safeguards in place.

Healthcare businesses must move beyond data security to unlock business opportunities

Computing beyond the perimeter is standard practice in healthcare organizations, and businesses are having to move away from solely relying on traditional network perimeter security and toward a more comprehensive approach. In this context, concerns around data security and privacy are still the biggest challenge, according to 66% of executives (Figure 3). Healthcare organizations must get more comfortable with the cybersecurity measures they have put in place and move on to support the business with better-performing and higher-quality insights.

AI adoption is happening too fast for regulations, governance, or mature cybersecurity controls to keep pace, which increases attack surface and risk exposure.

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

3. Silo Breakthrough: Alignment and Collaboration for a Proactive Healthcare Culture

An organization with a cyber-resilient culture is a place where everyone, at every level, understands their role in cybersecurity and takes accountability for it—including protecting sensitive data and systems.

The barriers to cyber resilience are lessening as accountability grows

According to our research, understanding of and alignment on cyber issues is improving across healthcare (Figure 4).

The perception of cyber resilience as purely a cybersecurity issue, rather than a priority for the whole organization, is far less of a barrier this year (only 35% of identify this as a barrier, compared with 42% in 2024). And 35% now identify the governance team not understanding cyber resilience as a barrier, compared with 38% in 2024.

Cybersecurity is spreading throughout the organization, but there is work to do

Healthcare organizations are making good progress overall at integrating cybersecurity across their operations (Figure 5).

Healthcare organizations should consider engaging more with outside experts to improve enterprise awareness. The number expecting to use external support for training and awareness in the next two years (36%) is similar to that for the past 12 months (32%).

External expertise is especially important because some enterprise-wide cybersecurity measures are still falling short (Figure 6). Only 32% say that cybersecurity due diligence for mergers and acquisitions is effective. And there is room for organizations to foster more resilient cultures: less than half (41%) say they have an effective company-wide cybersecurity culture.

Understanding of and alignment on cyber issues is improving across healthcare.

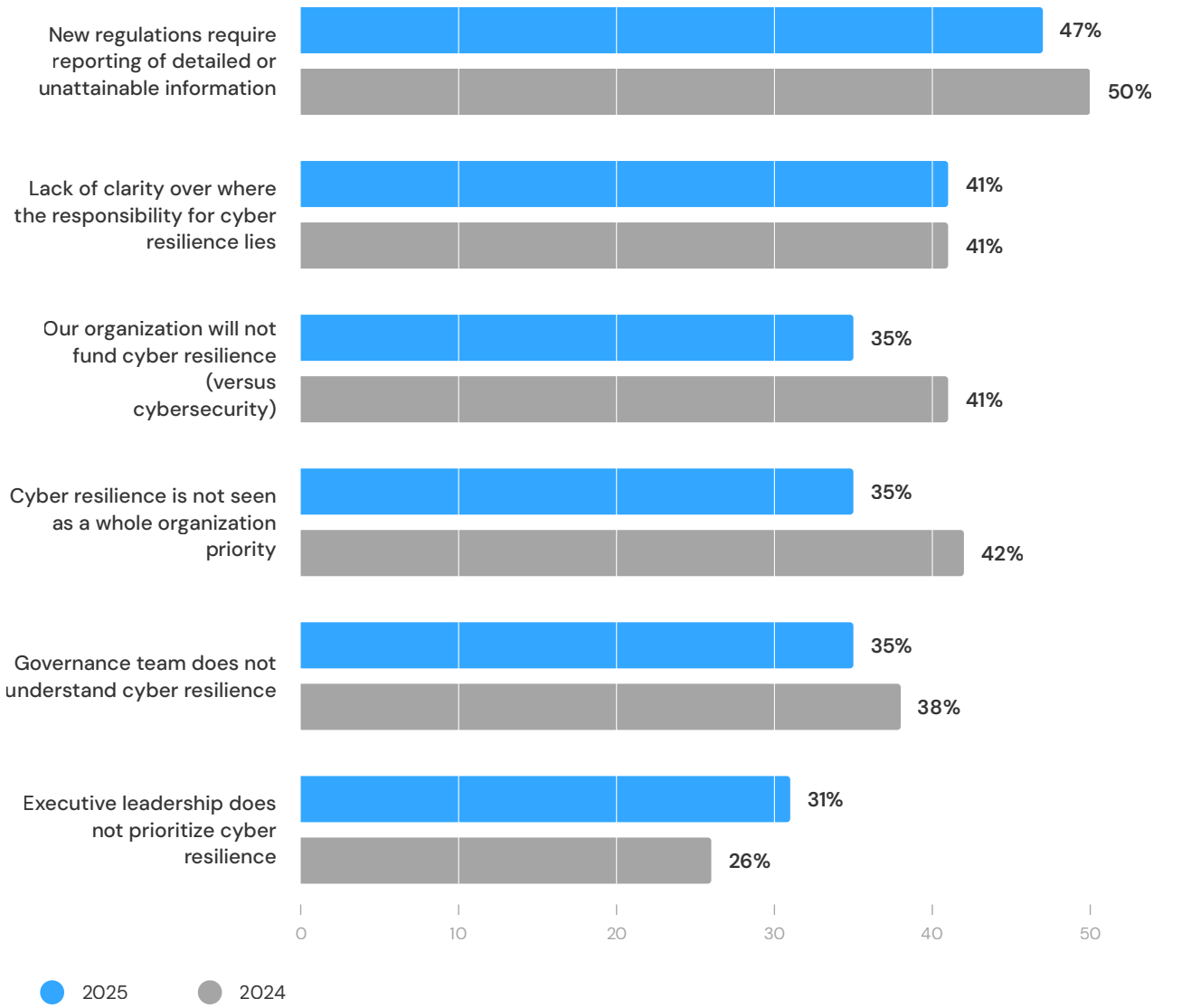
© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

Figure 4

Cyber resilience understanding and alignment have improved year over year

Q: To what extent are the following barriers to cyber resilience in your organization?

% of respondents
N=220



© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

Figure 5

Cybersecurity measures are visible across the organization

% of respondents
N=220

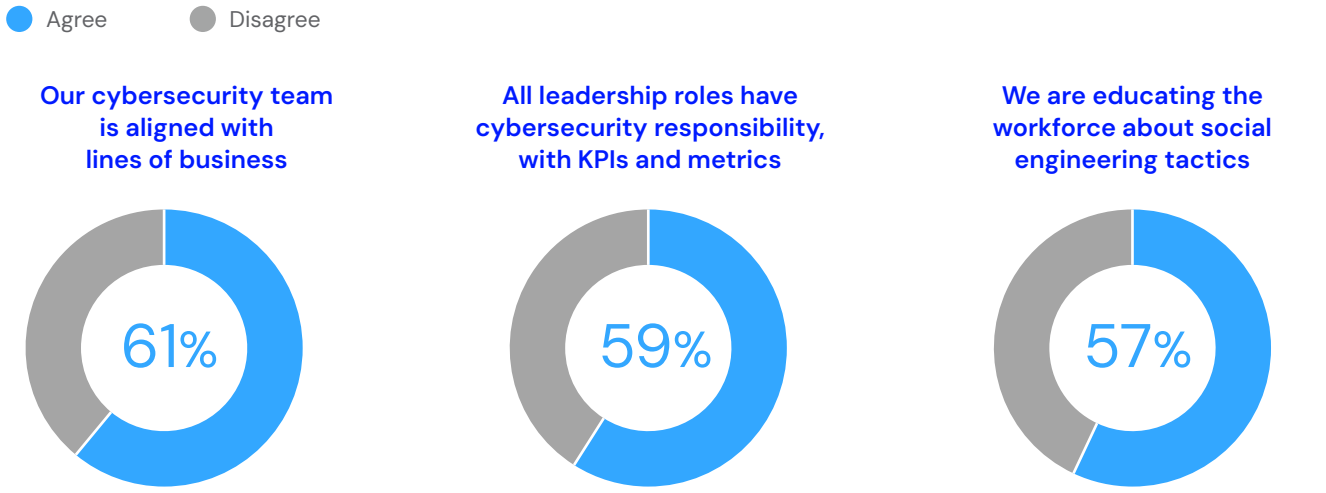
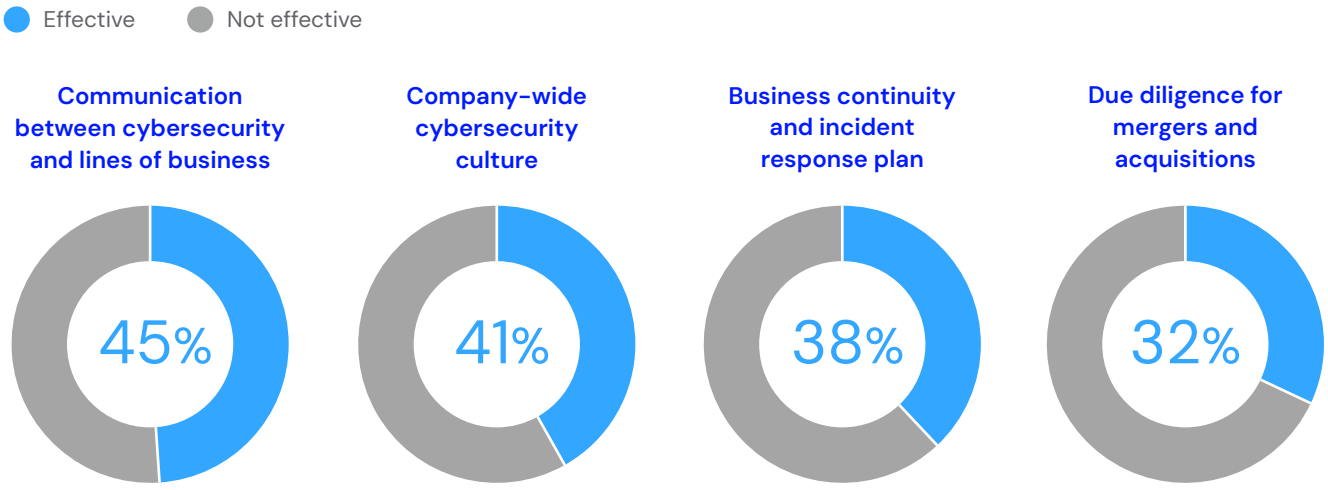


Figure 6

Some enterprise-wide cybersecurity measures are still falling short

Q: How effective are the following areas of cybersecurity within the wider organization?

% of respondents
N=220



© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

4. Evolving Vectors: Preparing for More Sophisticated Attacks

Healthcare organizations recognize that sophisticated attacks are imminent

AI tools are supercharging cyberattacks, allowing threat actors to rapidly identify and exploit vulnerabilities through automated large-scale ransomware and phishing campaigns (Figure 7). They can also use AI to craft more persuasive phishing messages, create deepfakes for fraud schemes, and develop malicious code and new variants of malware that cybersecurity systems are less likely to detect.

But the healthcare industry is not ready

Only 29% of healthcare organizations say they are prepared for AI-powered attacks, and 32% for deepfake and synthetic identity attacks.

Rising geopolitical tensions have led to an explosion of distributed denial of service (DDoS) attacks. "Hacktivists" and nation-state groups are using this technique of flooding a network or website with traffic to overwhelm the system in a bid to disrupt critical infrastructure. Attackers are also exploiting the increase in insecure IoT devices to build large botnets to scale attacks. DDoS attacks have existed for nearly three decades, which makes them one of the internet's most long-standing and prevalent threats, but only 38% of healthcare executives in our survey say they are expecting or are prepared for a DDoS attack.

Application security and cyber resilience are investment priorities

When asked to what extent their organization is investing in certain measures to prepare for new and emerging types of cyber threat (Figure 8), healthcare executives say they are most likely to invest moderately or significantly in:

- Application security (64%)
- Data encryption (63%)
- Cyber-resilience processes across the business (62%)

Surprisingly, only 38% are investing in Zero Trust Architecture (ZTA). An effective ZTA provides additional layers of protection against unpredictable threats. It can quickly identify suspicious behavior, implement defense measures, and respond to incidents. It can also help to encourage cyber-resilient behavior among users, which helps to extend the effectiveness of measures throughout the organization.

External support is a critical part of proactive cyber resilience

Healthcare organizations recognize that they cannot do this alone (Figure 9). Nearly half (44%) expect to enlist managed security service providers (MSSPs) in the next two years to help them manage the increasingly complex and dynamic threat landscape, an increase from 30% that have done so over the past 12 months.

Only 29% of healthcare organizations say they are prepared for AI-powered attacks, and 32% for deepfake and synthetic identity attacks.

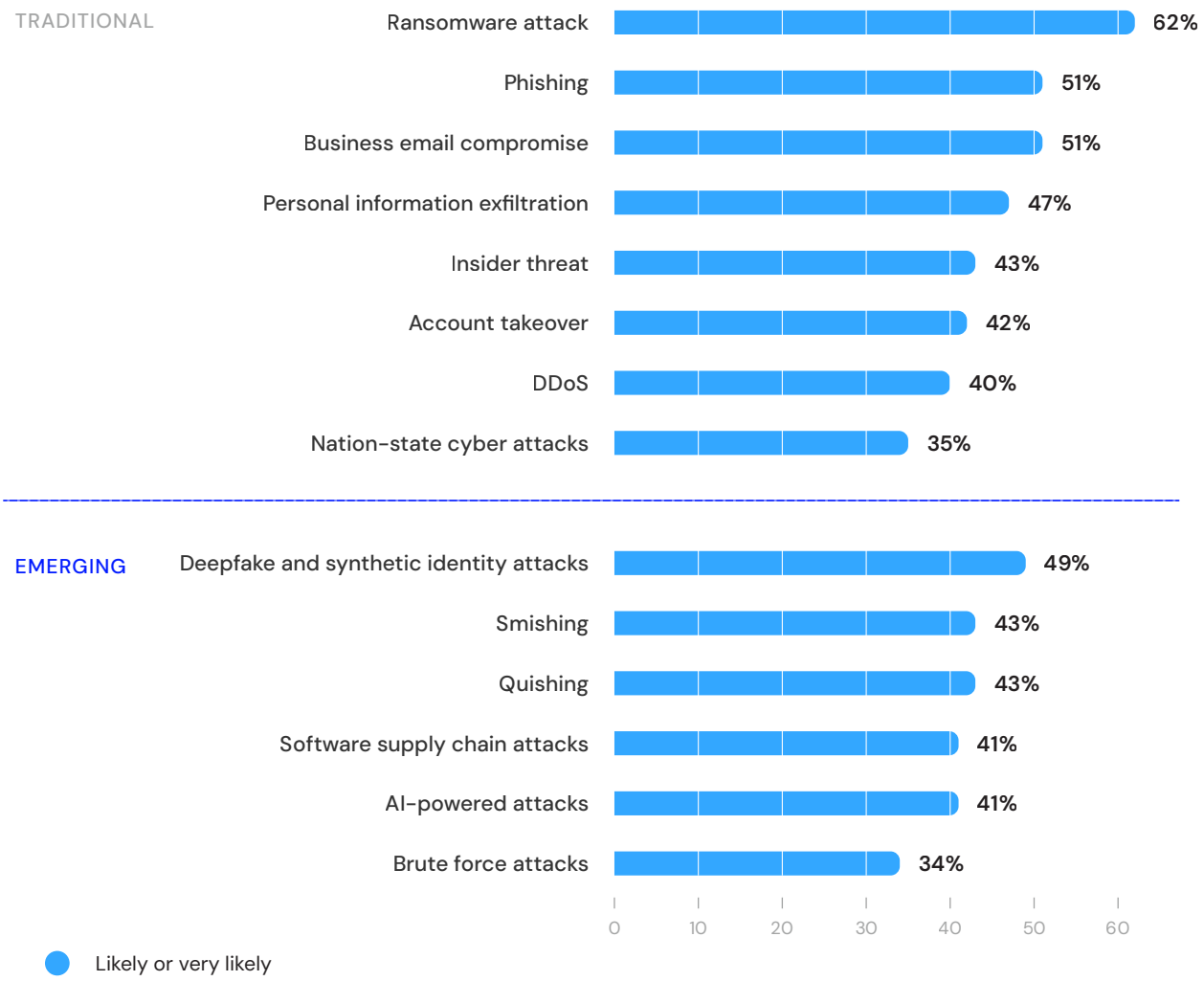
© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

Figure 7

Healthcare executives are expecting more varied types of cyber attacks

Q: How likely is it that the following attacks will occur in your organization over the next 12 months?

% of respondents
N=220



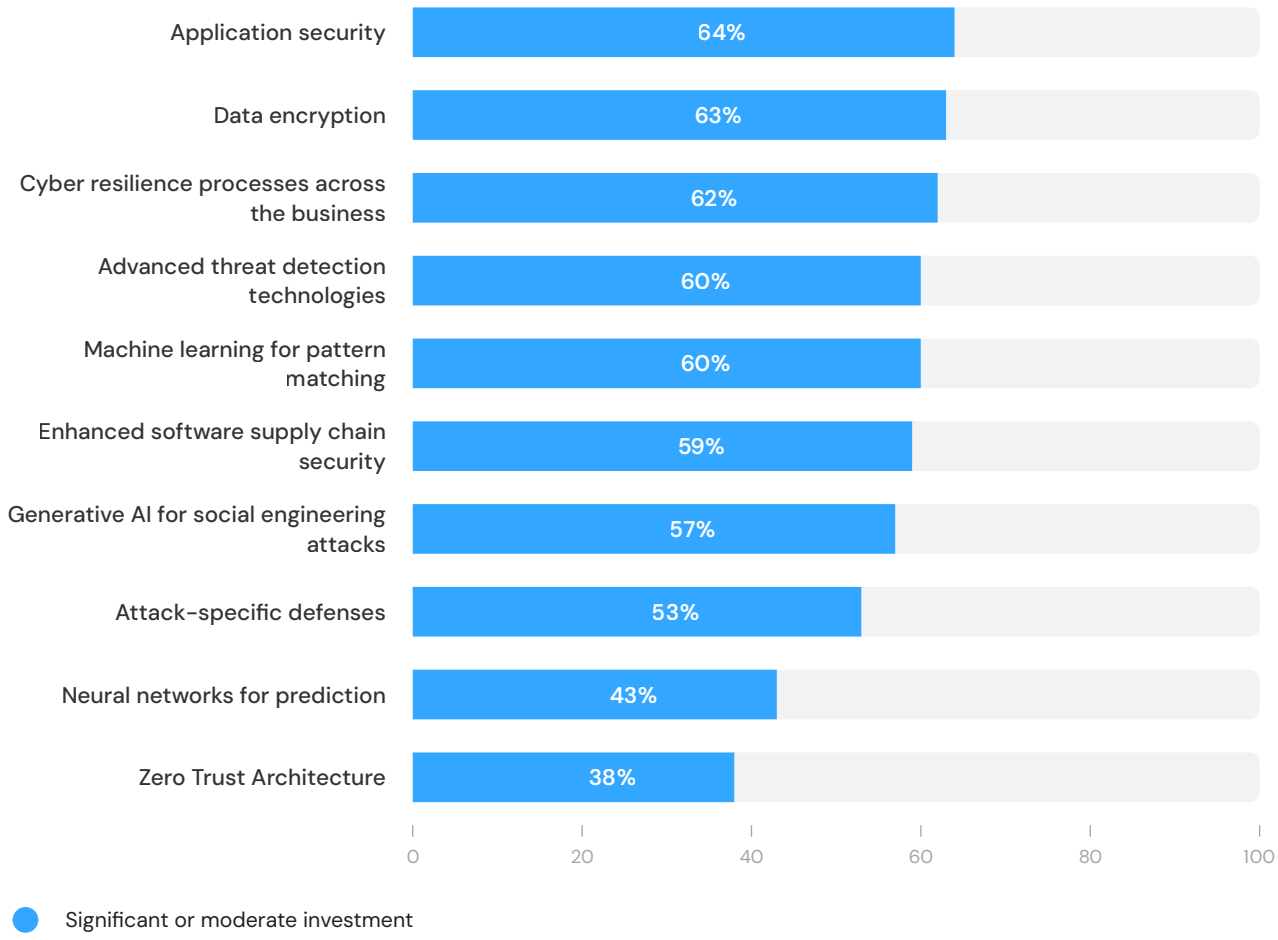
© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

Figure 8

Building cyber resilience, AI, and application security are investment priorities

Q: To what extent is your organization investing in the following measures to prepare for new and emerging types of cyber threats?

% of respondents
N=220



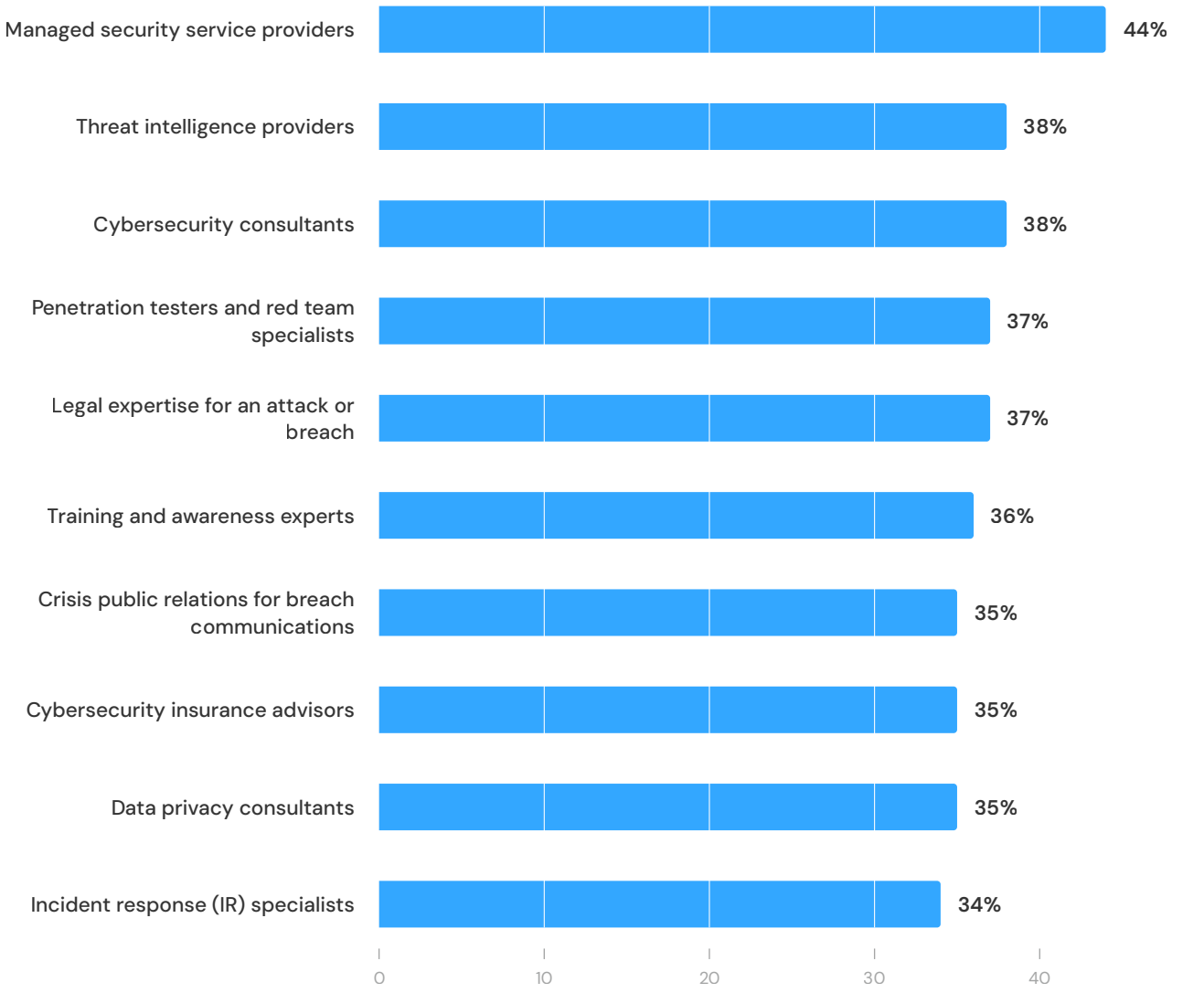
© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

Figure 9

External support is part of a more proactive future

Q: Which of the following external experts are you most likely to engage with over the next two years?

% of respondents
N=220



© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

5. Software Supply Chain: Risks and Resilience in Healthcare Organizations

If they are not properly secured, vulnerabilities in the software supply chain can provide entry points for threat actors.

Once in, hackers can move deeper into a network, stealing credentials, gaining control of valuable systems, and pushing out malware, potentially to thousands of victims. And attacks like this can often go undetected until compromised software has been widely distributed.

Many healthcare executives do not see the risk

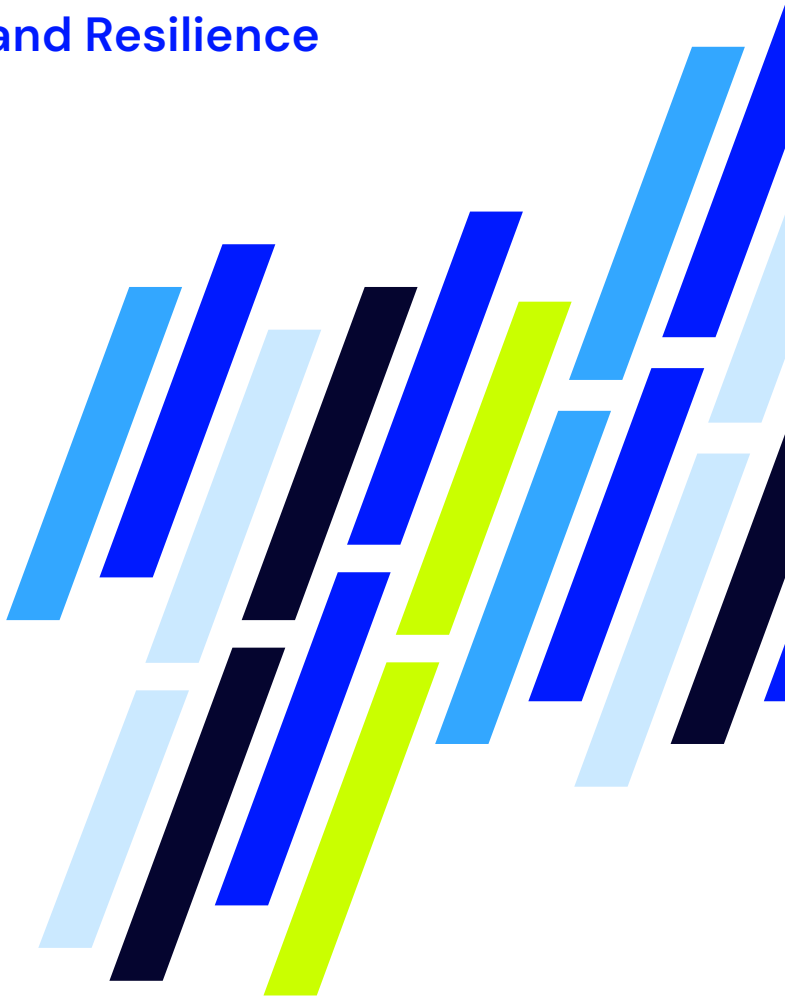
Our research finds that a minority of healthcare executives see any part of the software supply chain as high-risk. Only 16% rate open-source code, libraries, and frameworks as very high risk; 15% see unsupported software as very high risk; and only 15% consider insufficient visibility to conduct security assessments to be a very high risk.

Healthcare organizations are building a robust view of source code, but more progress is needed

Of the factors driving better software supply chain visibility (Figure 10), the highest percentage (42%) of organizations cited visibility of source code integration quality and 36% cited understanding of the origins of source code.

Only 29% say awareness of known vulnerabilities in source code and assigning or creating a confidence level of suppliers (24%) are top drivers of better visibility.

Healthcare organizations need to commit more investment: only 21% say they are investing significantly in software supply chain security.



Are organizations paying enough attention to software supply chain threats?

Overall, healthcare executives do not seem to be taking software supply chain threats as seriously as they should in the current technology and risk environment: 37% say that the biggest risk they face today is from within their software supply chain, but only 19% say that engaging with software suppliers about their security credentials is a priority for the next 12 months.

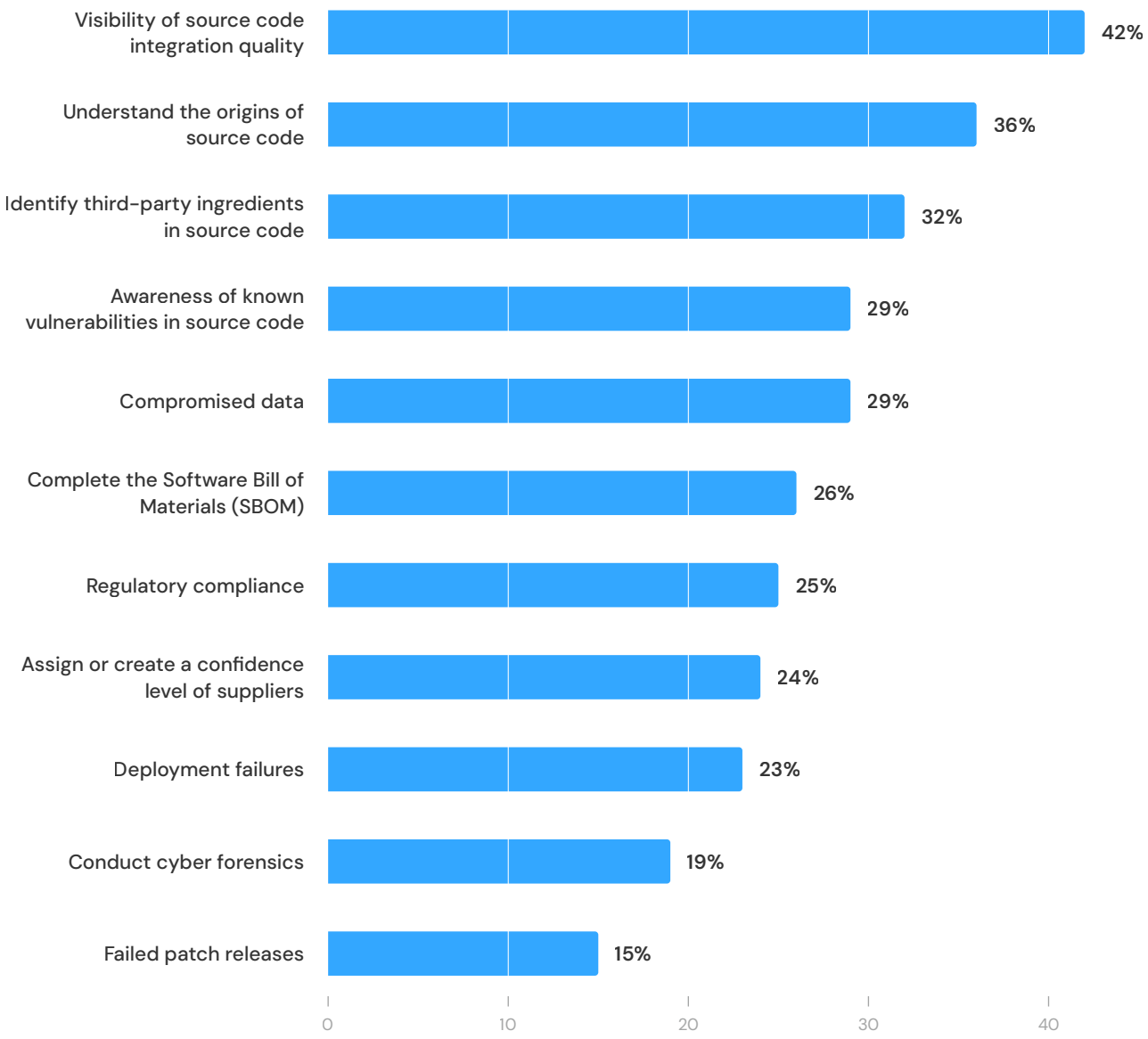
© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

Figure 10

Healthcare organizations prioritize source code integration quality as they seek to secure the software supply chain

Q: What are the most important factors driving a need for better software supply chain visibility within your organization?

% of respondents
N=220



© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

6. Four Steps to Cyber Resilience in Healthcare

Healthcare organizations are at a turning point with AI: it might be more mainstream, but it is still relatively new and unregulated. Threats can easily slip through the cracks and bad actors can take advantage. The way decision-makers respond in 2025 will be critical for the future of their businesses.

Elevate cyber resilience

- Increase engagement throughout leadership, including the board, to make cyber resilience a core business requirement
- Align cyber-resilience considerations with business decisions at the highest level
- Measure leadership roles against cybersecurity KPIs

Foster a cyber-resilient culture

- Practice safe online behaviors at every level
- Encourage everyone to report potential threats and make it easy to do so
- Implement regular cybersecurity training programs highlighting emerging threats and best practices

Be proactive and intentional

- Invest in cybersecurity measures to get ahead of risks, such as advanced threat detection and response, and exposure and vulnerability management technologies
- Engage external providers to enhance cybersecurity measures, advise on strategy, and provide you with training
- Move to a Zero Trust Architecture as a foundation for a multi-layered approach to network security

Prioritize software supply chain resilience

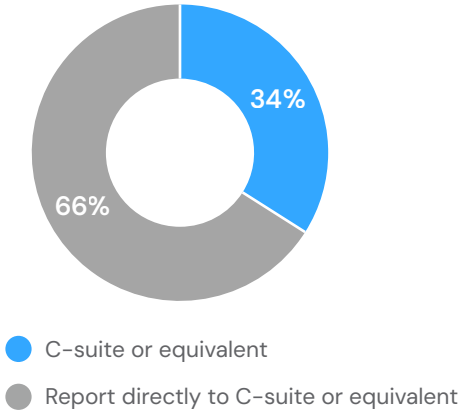
- Verify suppliers' cybersecurity credentials to help identify potential vulnerabilities in your software supply chain
- Create a confidence level of suppliers to improve supply chain visibility
- Carry out regular assessments to maintain resilience

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

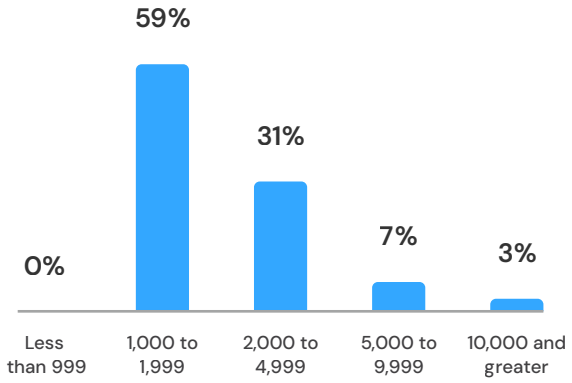
Healthcare Demographics

Survey Sample Sizes
Total sample N=1500
Healthcare respondents N=220

Respondent Seniority



Organization Size



Respondent Location

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Contact us today to learn more about how we can safeguard your organization's future.

© 2025 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 475SR 05-2025