



RESEARCH REPORT

2025 Futures Report:

Cyber Resilience and Business Impact

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).

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 definitions 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 man-made disasters.

Cyber-resilient organization: This is our characterization of an organization, based on our findings, that has put in place a significant number of resilience measures and strategies that are disseminated throughout the business. These organizations have not experienced a breach in the past year. For a full overview, see “**Five Characteristics of Cyber-Resilient Organizations.**” We use this term to show where businesses are on their journey to cyber resilience.

2025 LevelBlue Futures Report: Cyber Resilience and Business Impact

Contents

01

Cyber Resilience: A Proactive Stance
Builds Business Confidence 3

02

Business Impact: Aligning Cybersecurity
with Strategic Goals 5

03

Silo Breakthrough: Alignment and
Collaboration for a Proactive Culture 10

04

Evolving Vectors: Preparing
for More Sophisticated Attacks 14

05

Software Supply Chain:
Risks and Resilience 19

06

Four Steps to Cyber Resilience 22

Welcome to the 2025 Report

In our [2024 Futures Report](#) we learned that the old ways of securing businesses were no longer fit for purpose in the world of “boundaryless” computing characterized by technologies such as the internet of things (IoT), edge, and 5G – or beyond the proverbial perimeter. In this year’s report, we explore how another disruption—AI—is forcing organizations to pivot once again.

Generative AI went mainstream in 2024. Excitement about its transformative potential extended to AI’s broader capabilities, and more and more industries started to adopt it. AI is simultaneously creating the beginning of a new technology revolution and greater opportunities for adversaries.

AI tools promise us 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, prepared, and expand cybersecurity readiness.

Perhaps one of the most frightening possibilities is the use of readily available and affordable AI tools to supercharge cyberattacks. AI can increase the persistence and aggression of common types of attack, quickly generate new and sophisticated malicious code that is harder to trace, and create voice and image clones—deepfakes—for more persuasive fraud schemes.

Recent developments include a new open-source large language model (LLM) that is cheaper, more efficient, and more accessible than previous models. It allows users to download, copy, and build on its code with the help of comprehensive technical explanations. These open-source models are still in their infancy, but the development suggests that a new disruptive phase of AI is imminent. It might open up the technology to developers and offer organizations exciting opportunities to innovate, but it also opens it up to threat actors.

So how are organizations protecting themselves from increasingly numerous and sophisticated attacks? Are they enforcing cyber-resilience measures that extend throughout the organization? Are they prepared to face technological and cybersecurity uncertainty: the “unknown unknowns?”

Our latest research shows that this is a story of two halves. Leaders are taking notice of the threats, and organizations are starting to implement cyber-resilience measures. But they still underestimate the potential risk of AI-powered cyberattacks and have more to do to properly prepare and protect themselves.

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

AI tools promise us 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.

01

Cyber Resilience: A Proactive Stance Builds Business Confidence

Organizations are being forced to take cybersecurity more seriously

In 2024, our research found that cybersecurity teams were isolated, underfunded, and overlooked. This year, increasing risks and the fast-developing threat landscape are forcing business leaders to take cyber resilience more seriously, and are pushing it up the C-suite's agenda:

- 30% of executives say their organization suffered a breach in the past 12 months
- 41% say they are experiencing a significantly higher volume of attacks
- 68% say that media reports of high-profile breaches elevated cybersecurity on the C-suite agenda

Most businesses are not ready for new attacks

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

- 29% of executives say they are prepared for AI-powered threats, despite 42% believing they will happen
- 32% feel their organization is prepared for deepfake attacks, even though 44% are expecting them

Businesses are aware of the emerging threats, but only 24% of executives say their organization is committing significant investment in advanced threat detection technologies.

Resilience in the software supply chain is low on the agenda

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

- 30% of executives recognize that AI adoption has increased risks to the software supply chain
- 49% say they have very low to moderate visibility into the software supply chain
- 25% say that engaging with suppliers about their security credentials is a priority in the next 12 months

Companies will survive by becoming more proactive and more aligned

Enterprise alignment has been a core focus over the past 12 months: 45% of executives say that cyber resilience is recognized as a whole company priority rather than simply a cybersecurity issue—an increase from 27% last year. And responsibility for cyber resilience measures is making its way into more areas of the business:






- 66% of executives say that their cybersecurity team is aligned with lines of business
- 60% say that leadership roles in their organization are measured against cybersecurity KPIs

However, investment in more proactive security measures remains low: 25% are paying attention to security threats in the software supply chain. This is despite 53% recognizing that a cyber breach will be more costly if their organization's security strategy is not more proactive. CEOs are more concerned than other leadership roles that their organization's reactive approach to cybersecurity puts their business at risk (38% of CEOs compared with 22% of CIOs and CTOs, for example). ■

Five Characteristics of Cyber-Resilient Organizations

7%

of survey organizations are classified as cyber resilient

01	02	03	04	05
Defending against AI-powered attacks	Enhancing security using AI	Prepared for new threats	Aligning security with business goals	Preventing security breaches
 <p>They are competently defending against cyber adversaries that are using AI techniques</p>	 <p>They are proficiently implementing AI to enhance cybersecurity</p>	 <p>They are preparing for emerging AI-powered and software supply chain attacks</p>	 <p>Their cybersecurity team is aligned with lines of business</p>	 <p>Their organization has not experienced a breach in the past 12 months</p>

Cyber-resilient organizations are aligned and proactive



91%

are investing in advanced threat detection vs 63% overall



48%

plan to engage threat intelligence providers in the next two years vs 39% overall



94%

are investing in software supply chain security vs 62% overall

And they are confidently innovating

79%

of cyber-resilient organizations (vs 61% overall) say they can risk more with innovation because they take an adaptive approach to cybersecurity

02

Business Impact: Aligning Cybersecurity with Strategic Goals

Fast Facts



5

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

A significant cyber incident can severely affect operations, finances and reputation, with ramifications across entire business ecosystems and both physical and software supply chains. As a protective control, cyber resilience reduces the likelihood of these incidents and helps the organization bounce back when an incident does happen.

While leaders are aware of the growing risk of cyber incidents and the subsequent potential damage to the organization, they do not feel fully prepared for the onslaught. However, our research does find areas where organizations are extending cyber-resilient measures across the enterprise. It also explores how aligning cyber teams with the line of business helps organizations press ahead with their transformation and innovation efforts.

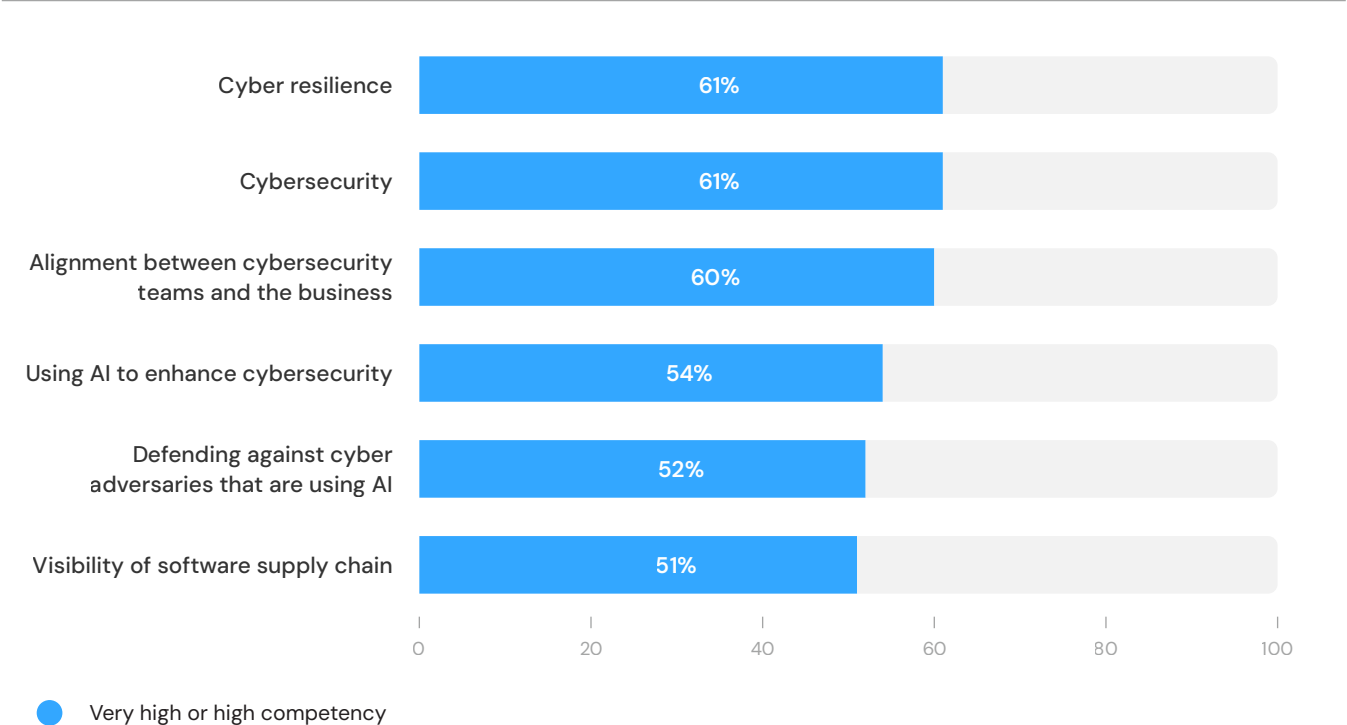
An increasingly complex and concerning threat landscape is pushing cybersecurity up the agenda: 41% of executives say they have experienced a significantly higher volume of cyberattacks than 12 months ago, and 30% have experienced a breach in the past 12 months.

Figure 1

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=1500



Some 68% of executives say that media reports of high-profile breaches elevated cybersecurity up the C-suite agenda. And as AI-powered technologies make attacks more sophisticated, 59% of executives say that it is becoming more difficult for employees to identify real threats.

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

Despite their concerns, executives are feeling confident about defending themselves against AI-related adversaries and using AI to enhance defense. More than half (52%) say they are highly or very highly competent at defending themselves against AI techniques, and in implementing and using AI to enhance cybersecurity (54%).

The growing accessibility and affordability of AI tools such as open-source LLMs are making it cheaper

and easier for threat actors to identify and exploit vulnerabilities in networks, automate far-reaching ransomware and phishing campaigns, and develop new forms of malware that are less likely to be caught by cybersecurity controls. They can also use AI to create deepfakes for fraud schemes—and the executives in the survey say these types of attacks are increasingly difficult for employees to detect.

Our cyber-resilient organizations are better placed to navigate these emerging AI threats, and they can prove it: none of them have experienced a cyber breach in the past 12 months.

Cyber-resilient organizations are pushing discussions to the highest level

Leadership plays an important role in cyber resilience, and cyber-resilient organizations are more likely to recognize this: 43% say they are increasing

Figure 2

Business impact of cybersecurity drives the leadership agenda

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=1500

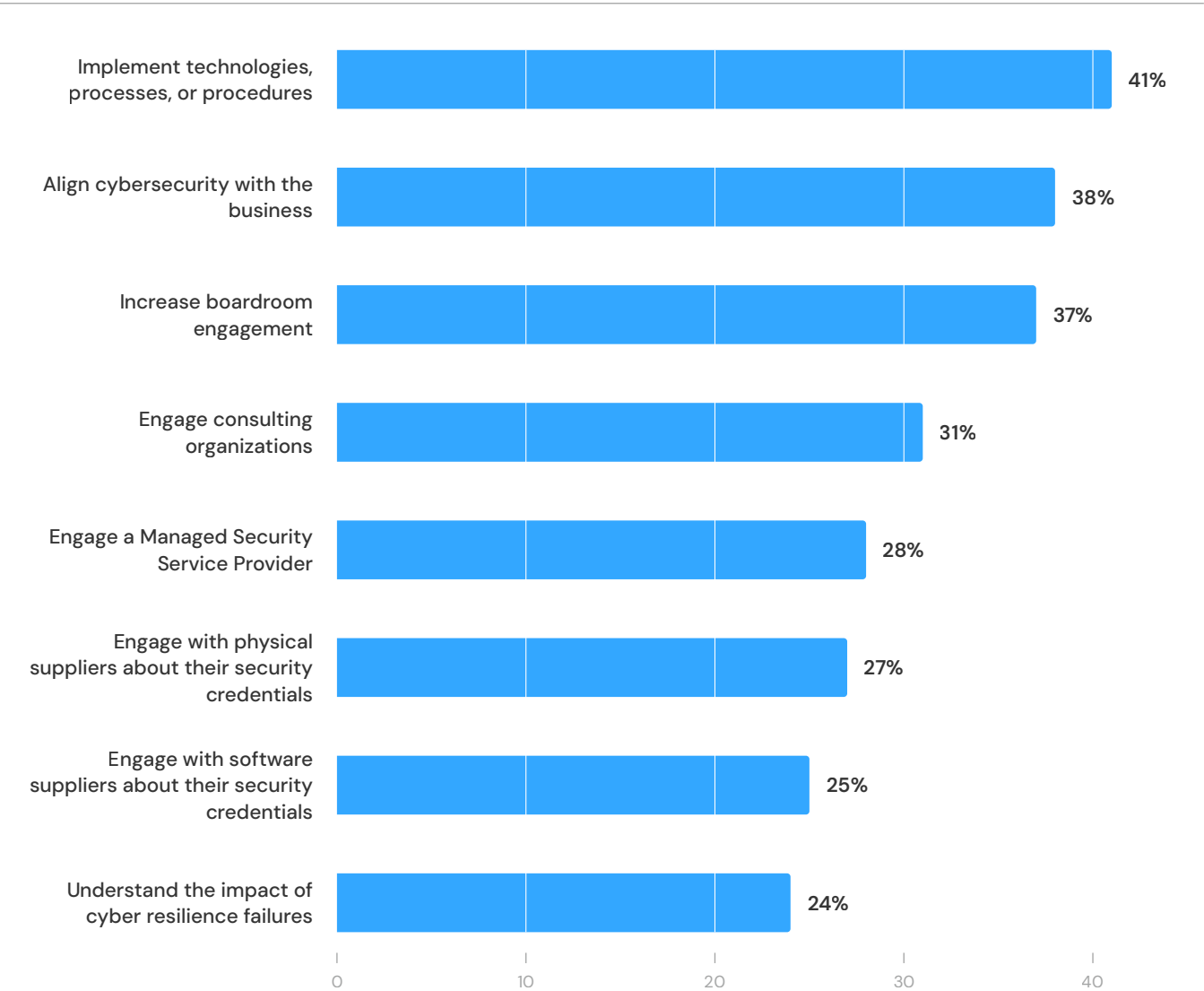
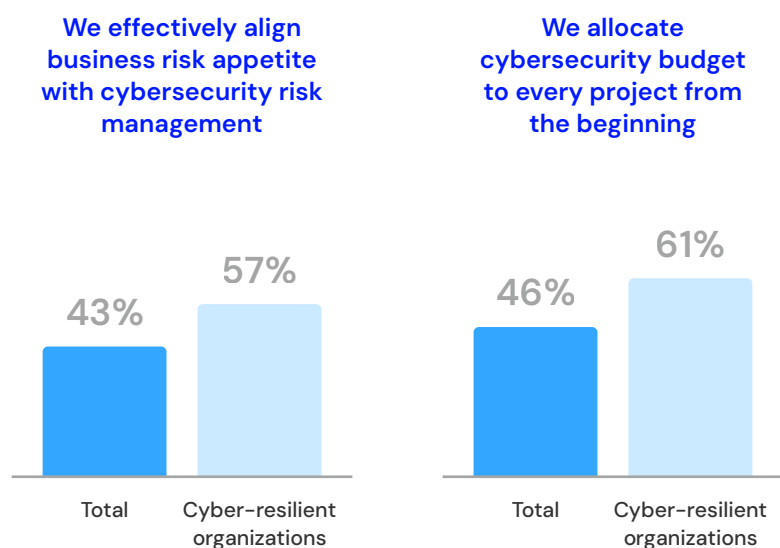


Figure 3

Cyber teams are becoming more aligned with lines of business

% of respondents N=1500



boardroom engagement in cyber-resilience discussions, compared with 37% of the executives overall.

Effective leaders see cyber resilience as a core business function. They align cyber resilience with business decisions from the top and ensure that it is prioritized across the organization. Having a boardroom engaged in cyber issues means the organization is better prepared to handle incidents and minimize losses.

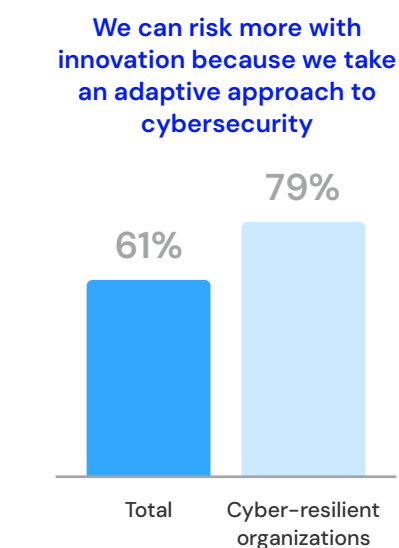
Some organizations are balancing their approach to risk and innovation

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

Figure 4

Organizations are balancing cybersecurity and innovation risk

% of respondents N=1500



To develop a cyber-resilient organization according to our criteria, cybersecurity teams need to be aligned with lines of business. This creates a more balanced approach to cybersecurity and innovation risk.

Cyber-resilient organizations are more likely to say they have effectively aligned business risk appetites with cybersecurity risk management (57% compared with 43% of executives overall) and to have allocated a cybersecurity budget to new initiatives from the beginning (61% compared with 46%).

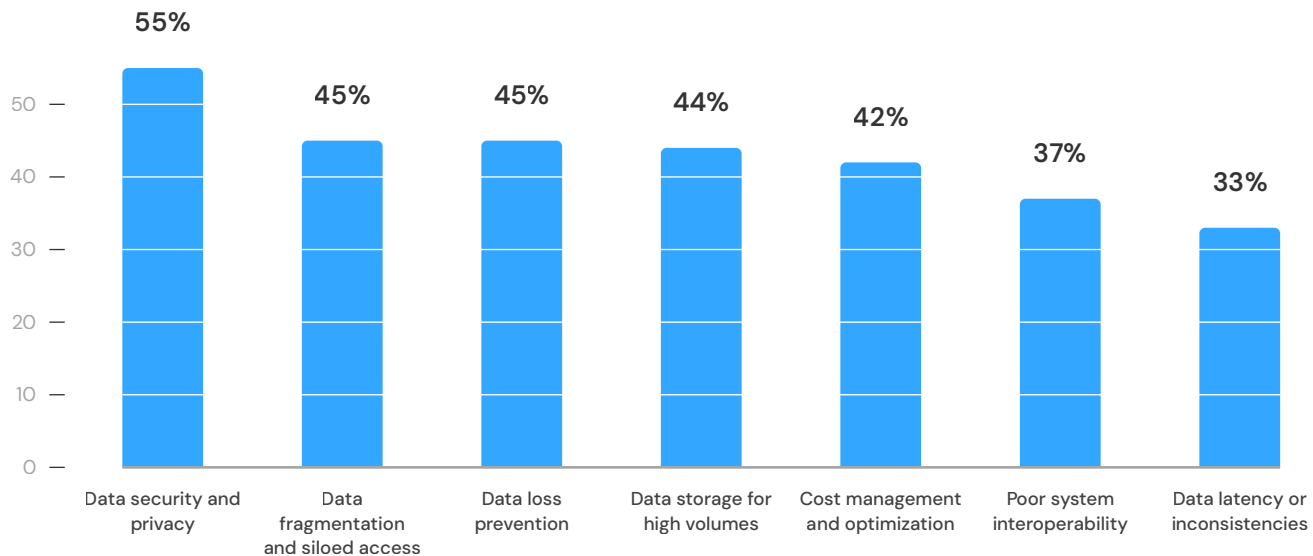
Aligning cybersecurity with lines of business also allows cyber-resilient organizations to take bigger risks with innovation. An impressive 79% say that an adaptive approach to cybersecurity enables their company to take greater innovation risks. Encouragingly, executives overall are not far behind (61%), which suggests there is widespread recognition of the importance of cybersecurity at all levels of the organization.

Figure 5

Data security remains a leading concern

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

% of respondents
N=1500



This level of cybersecurity alignment also seems to reduce organizations' caution about implementing AI. Only 29% of executives overall—and none of the cyber-resilient organizations—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 an organization's attack surface and risk. Executives' confidence about implementing AI despite the cybersecurity ramifications again suggests a disconnect. They recognize the very real risks but are enthusiastic about implementing the technology in any way—possibly without adequate safeguards in place.

Some businesses are moving beyond data security to unlock business opportunities

Computing beyond the perimeter is standard practice in most organizations, and businesses are moving 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 55% of executives overall.

Notably, cyber-resilient organizations are more comfortable with the cybersecurity measures they have in place, and they are supporting the business with better-performing and higher-quality insights. Data fragmentation and siloed access, and data loss prevention (DLP) are greater concerns for cyber-resilient organizations than they are for businesses overall. ■

03

Silo Breakthrough: Alignment and Collaboration for a Proactive Culture

Fast Facts


66%

of executives say their cybersecurity team is aligned with lines of business

60%

of all leadership roles are measured against cybersecurity KPIs

53%

say a cyber breach will be more costly than necessary unless their security strategy becomes more proactive

38%

of CEOs say their organization's reactive approach to cybersecurity puts their business at risk

39%

of CEOs say their organization's leadership team is too slow to make decisions relating to cybersecurity strategy

83%

of cyber-resilient organizations are educating the workforce about social engineering tactics

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. To create this kind of culture, leaders need to foster a collective mindset across the organization, where every employee actively practices safe online behaviors and is encouraged to report any potential threats. Regular cybersecurity training programs tailored to each role are a crucial way to keep

employees updated on emerging threats and best practices.

The barriers to cyber resilience are lessening as accountability grows

According to our research, understanding of and alignment on cyber issues improved year-over-year, which suggests that cyber issues are being taken seriously at all levels of the organization—not just siloed in cybersecurity or IT teams. This year, organizations see a lack of accountability across the business as less of a barrier to cyber resilience than they did in 2024.

The perception of cyber resilience as a cybersecurity issue instead of a priority for the whole organization is

Figure 6

Cyber 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=1500

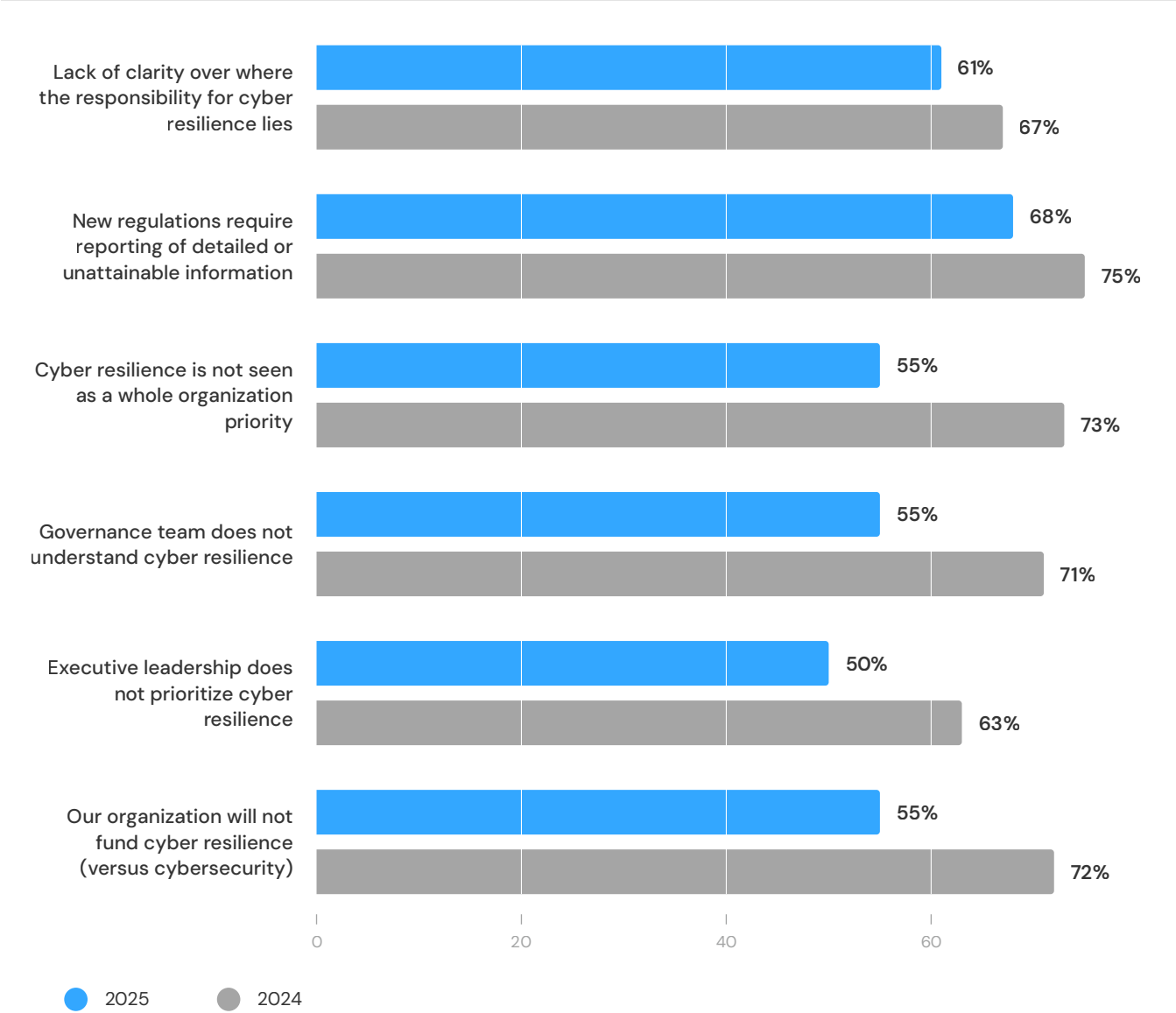


Figure 7

Cybersecurity measures are visible across the organization

% of respondents who agreed

% of respondents
N=1500

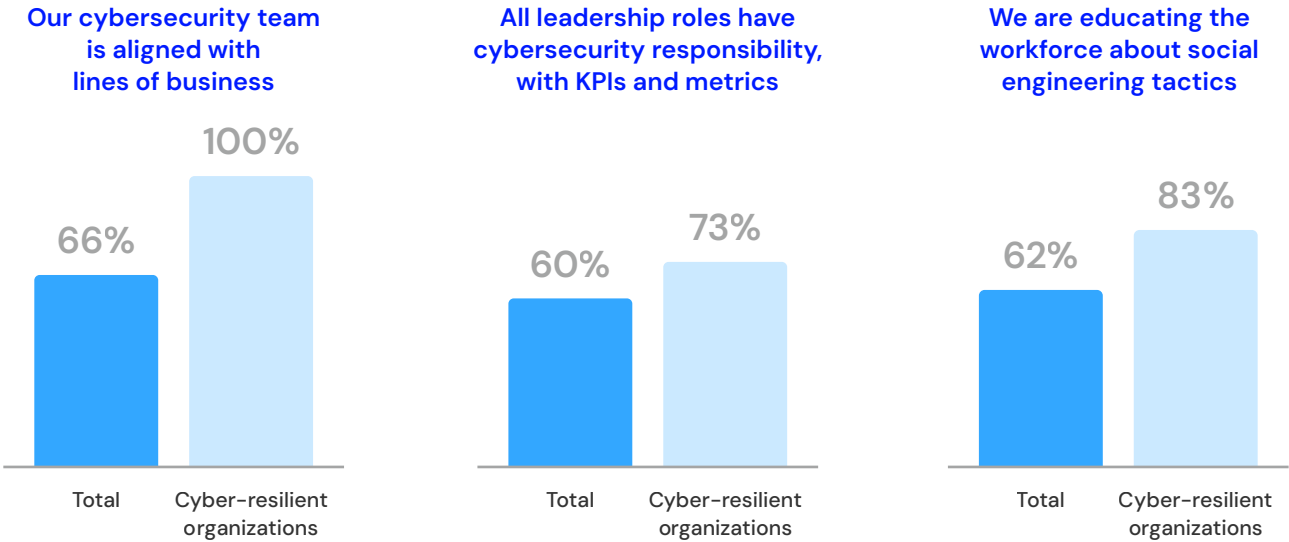


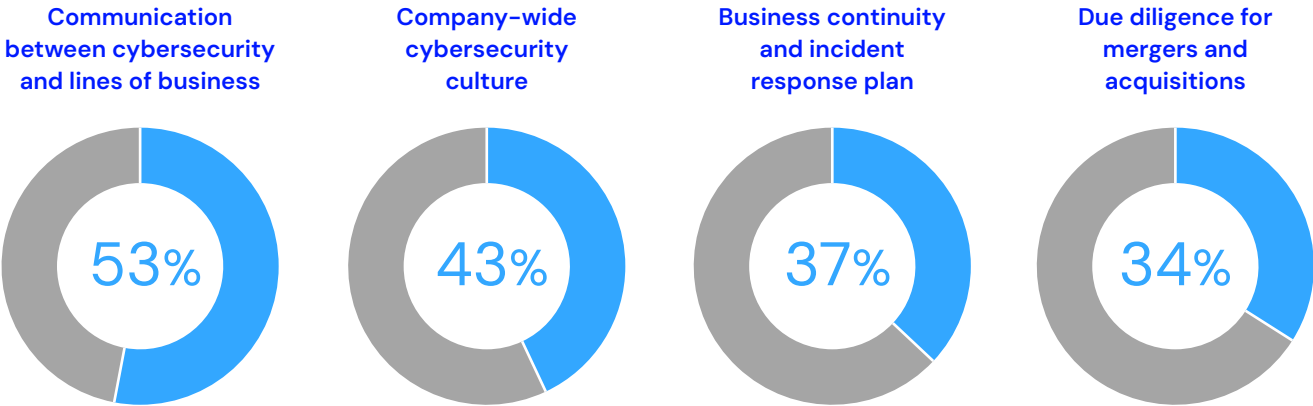
Figure 8

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=1500

Effective Not effective



far less of a barrier this year (55% of executives say it is sometimes, frequently, or very frequently a barrier, compared with 73% in 2024). And only 55% now say that the governance team not understanding cyber resilience is a barrier, compared with 71% in 2024.

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

Organizations overall are making good progress at integrating cybersecurity across the whole organization. They are running only slightly behind the cyber-resilient organizations.

But cyber-resilient organizations are more likely than businesses overall to be:

- Aligning cybersecurity with lines of business (100% compared with 66%)
- Making cybersecurity the responsibility of all leadership roles with KPIs and metrics (73% compared with 60%)
- Implementing a workforce education strategy (83% compared with 62%)

Slightly more cyber-resilient organizations are also expecting to engage external support from training and awareness experts in the next two years (44% compared with 38% of businesses overall) than in the past 12 months (35% and 32% respectively).

Some enterprise-wide cybersecurity measures are still falling short. Communication between cybersecurity and line-of-business teams is seen as effective by 53% of respondents, but just 34% 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 (43%) say they have an effective company-wide cybersecurity culture. The effectiveness of business continuity and incident response plans remains low (37%).

CEOs believe that current cyber postures are too reactive

Taking a more proactive stance to cyber resilience is still a challenge for many, and CEOs are worried about it. They are more likely than CIOs and CTOs, for instance, to say that:

- Their reactive approach to cybersecurity is putting the organization at risk (38%, compared with 22%)
- The leadership team is too slow to make decisions relating to cybersecurity strategy (39% compared with 23% of CIOs and 22% of CTOs) ■

Organizations overall
are making good
progress at integrating
cybersecurity across
the whole organization.
They are running
only slightly behind
the cyber-resilient
organizations.

04

Evolving Vectors: Preparing for More Sophisticated Attacks

Fast Facts



42%

of executives expect AI-powered attacks in their organization in the next year

44%

say deepfake and synthetic identity attacks will happen in their organization in the next year

63%

of all organizations are investing in advanced threat detection technologies

29%

believe their organization is prepared for AI-powered attacks

32%

believe their organization is prepared for deepfake and synthetic identity attacks

91%

of cyber-resilient organizations are investing in advanced threat detection

Organizations recognize that sophisticated attacks are imminent.

AI tools are supercharging cyberattacks, allowing threat actors to rapidly identify and weaponize vulnerabilities and automate large-scale ransomware and phishing campaigns. 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 are less likely to be detected by cybersecurity systems.

And executives say that these emerging types of attacks are likely in the next 12 months:

- 46% expect quishing (credential theft via QR codes)
- 44% expect software supply chain attacks and smishing (credential theft via text message)
- 44% expect deepfake and synthetic identity attacks
- 42% expect AI-powered attacks

But businesses are not ready

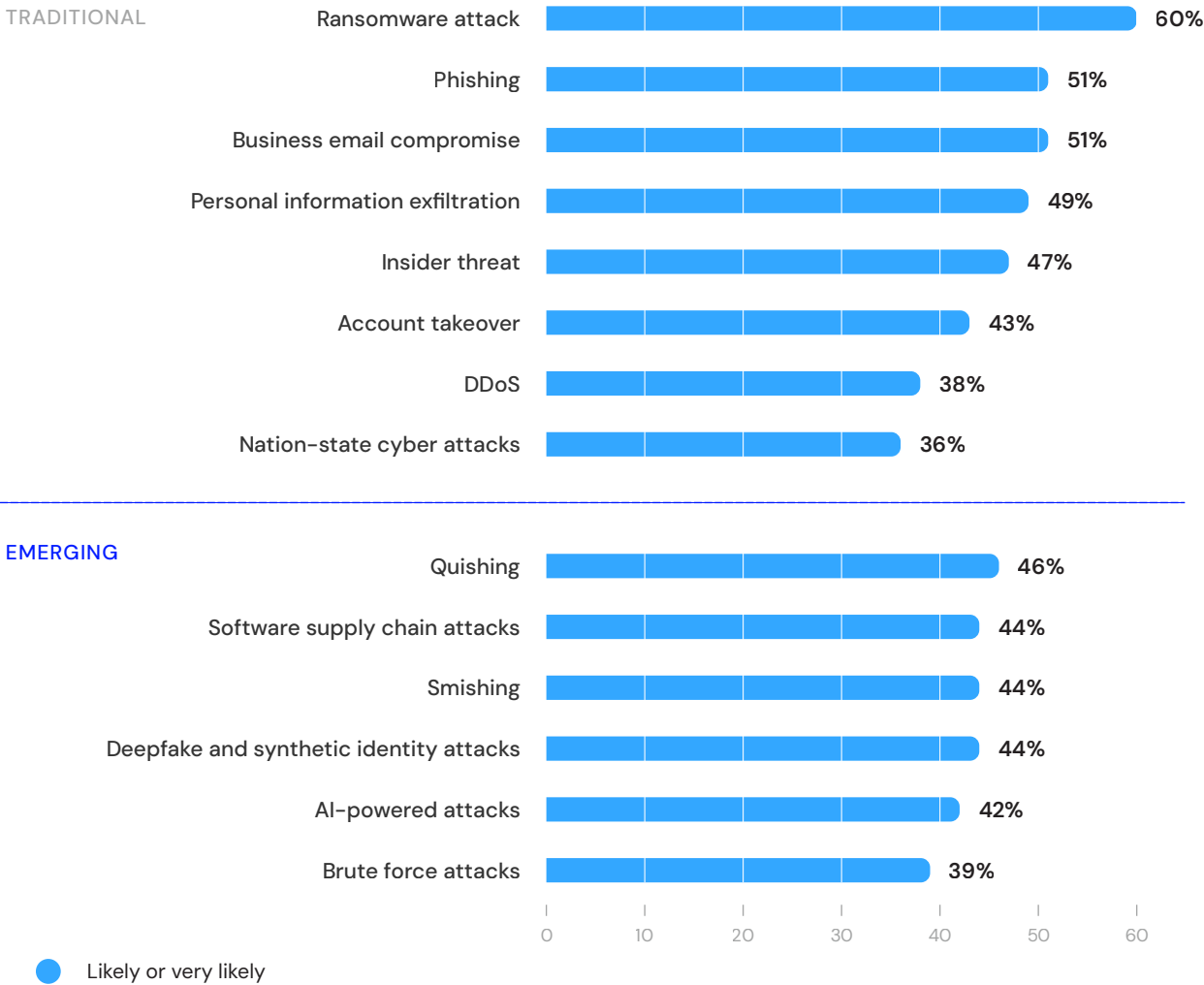
Only 29% of organizations say they are prepared for AI-powered attacks, and 32% for deepfake and synthetic identity attacks.

Figure 9

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=1500



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 of insecure IoT devices to build large botnets to scale attacks. DDoS attacks have existed

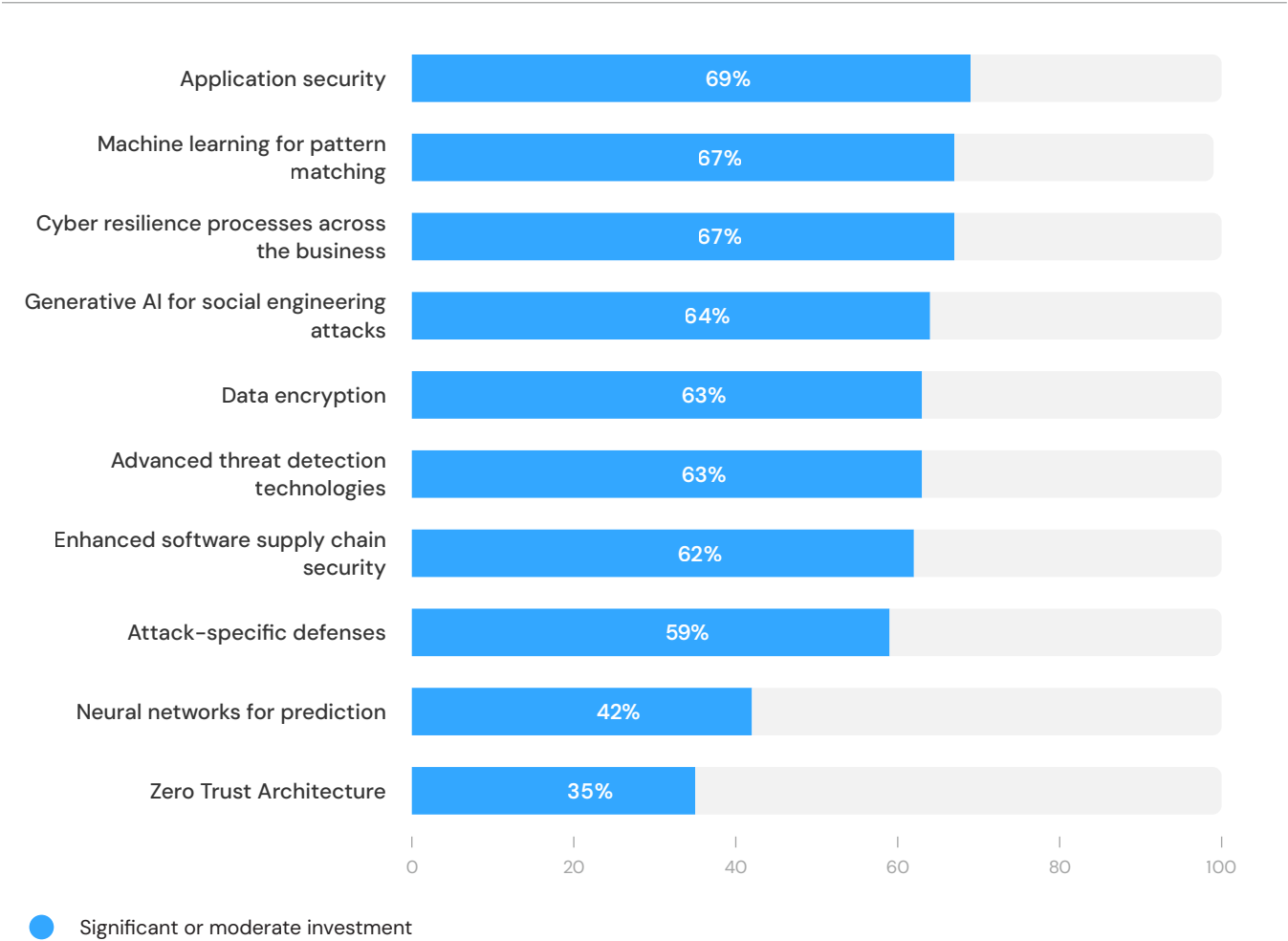
For deeper analysis and understanding of dominant cyber threat activity observed by LevelBlue security operations centers (SOCs) and LevelBlue Labs, see our [2025 LevelBlue Threat Trends Report, Edition One](#).

Figure 10

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=1500



for nearly three decades, which makes them one of the internet’s most long-standing and prevalent threats, but just 38% of executives in our survey say they are expecting or are prepared for a DDoS attack.

Application security, AI, 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 threats, executives say they are most likely to invest moderately or significantly in:

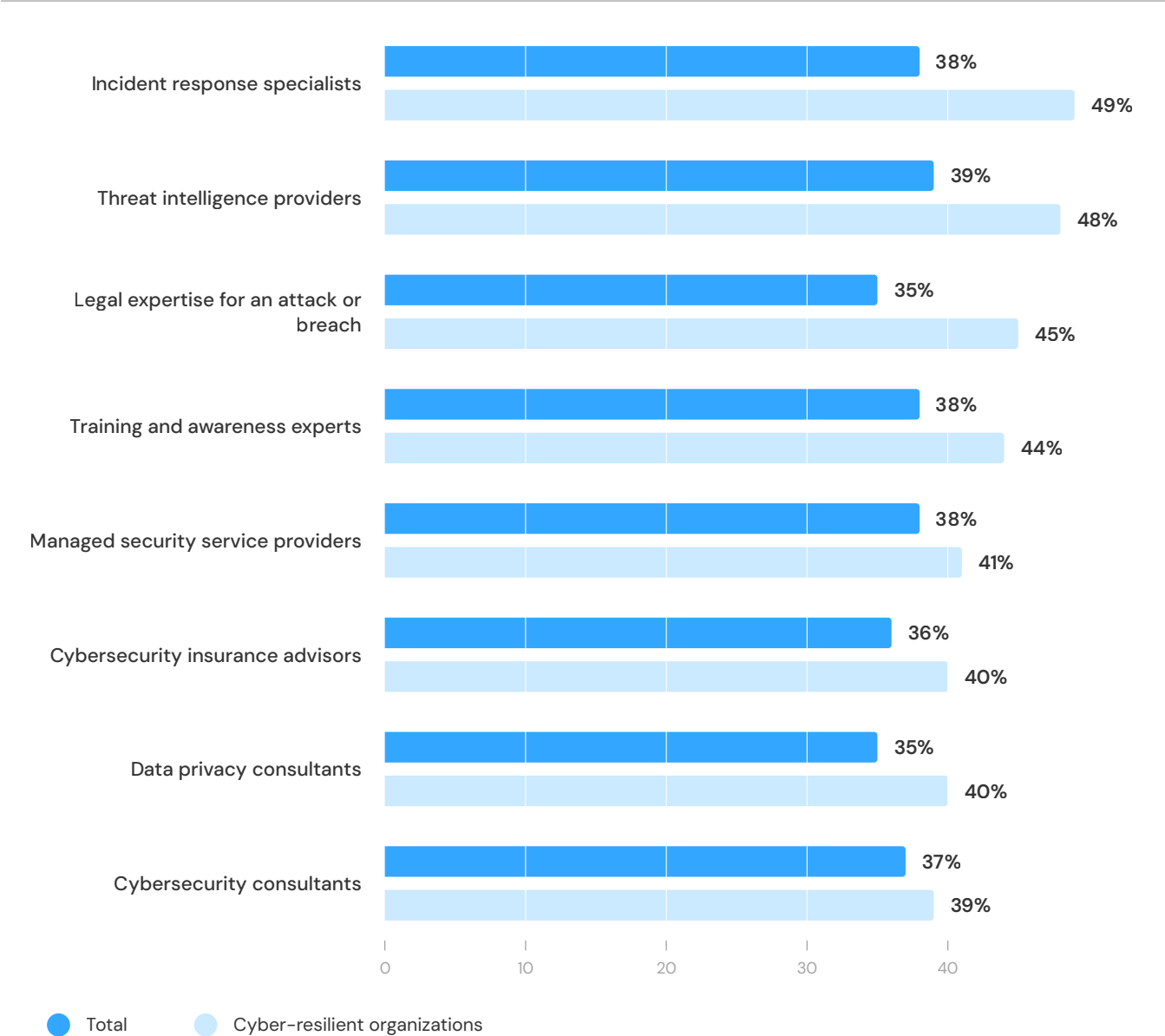
- Application security (69%)
- Machine learning for pattern matching (67%)
- Cyber-resilience processes across the business (67%)
- Generative AI for social engineering attacks (64%)

Figure 11

For cyber-resilient organizations, 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=1500



Surprisingly, only 35% are investing in Zero Trust Architecture (ZTA). An effective zero trust framework provides additional layers of protection against unpredictable threats. An effective ZTA 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 measures throughout the organization.

The cyber-resilient organizations in our research are more committed to taking a proactive approach to improving their cybersecurity. Far more are investing in cyber-resilience processes across the business and generative AI for protection against social engineering attacks. But even among the cyber-resilient organizations, only 45% say they are moderately or significantly investing in a Zero Trust Architecture.

Cyber-resilient organizations are also more likely to invest in advanced threat detection technologies (91% compared with 63%) and enhanced software supply chain security (94% compared with 62%).

Cyber-resilient organizations are more committed to taking a proactive approach to improving their cybersecurity.

External support is becoming a critical part of proactive cyber resilience

Organizations cannot do this alone. To manage the increasingly complex and dynamic threat landscape they need experts, including consultants and managed security service providers (MSSPs), who can advise, guide, and implement effective strategies and systems.

- **Cyber-resilient organizations** are more likely to seek this kind of support, and over the next two years they are most likely to be investing in incident response specialists (49%) and threat intelligence providers (48%)
- Organizations **overall** are also prioritizing incident response (38%) and threat intelligence (39%), along with training and awareness experts and MSSPs (both 38%) ■

05

Software Supply Chain: Risks and Resilience

Fast Facts

**30%**

of executives agree that AI adoption has increased risks to the software supply chain

62%

of CEOs consider their organization's custom-developed source code to be somewhat risky or high risk

49%

of organizations have very low to moderate visibility into the software supply chain

25%

of executives say that engaging with suppliers about their security credentials in the next 12 months will be a priority

34%

of cyber-resilient organizations prioritize building confidence in their suppliers' cybersecurity

94%

of cyber-resilient organizations are investing in software supply chain security, compared with 62% of businesses overall

If 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 to potentially thousands of victims. And attacks like this can often go undetected until compromised software has been distributed widely.

Many executives do not see the risk, but CEOs and CTOs are more cautious

Our research finds that only a minority of executives see any part of the software supply chain as high risk. Only 14% 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.

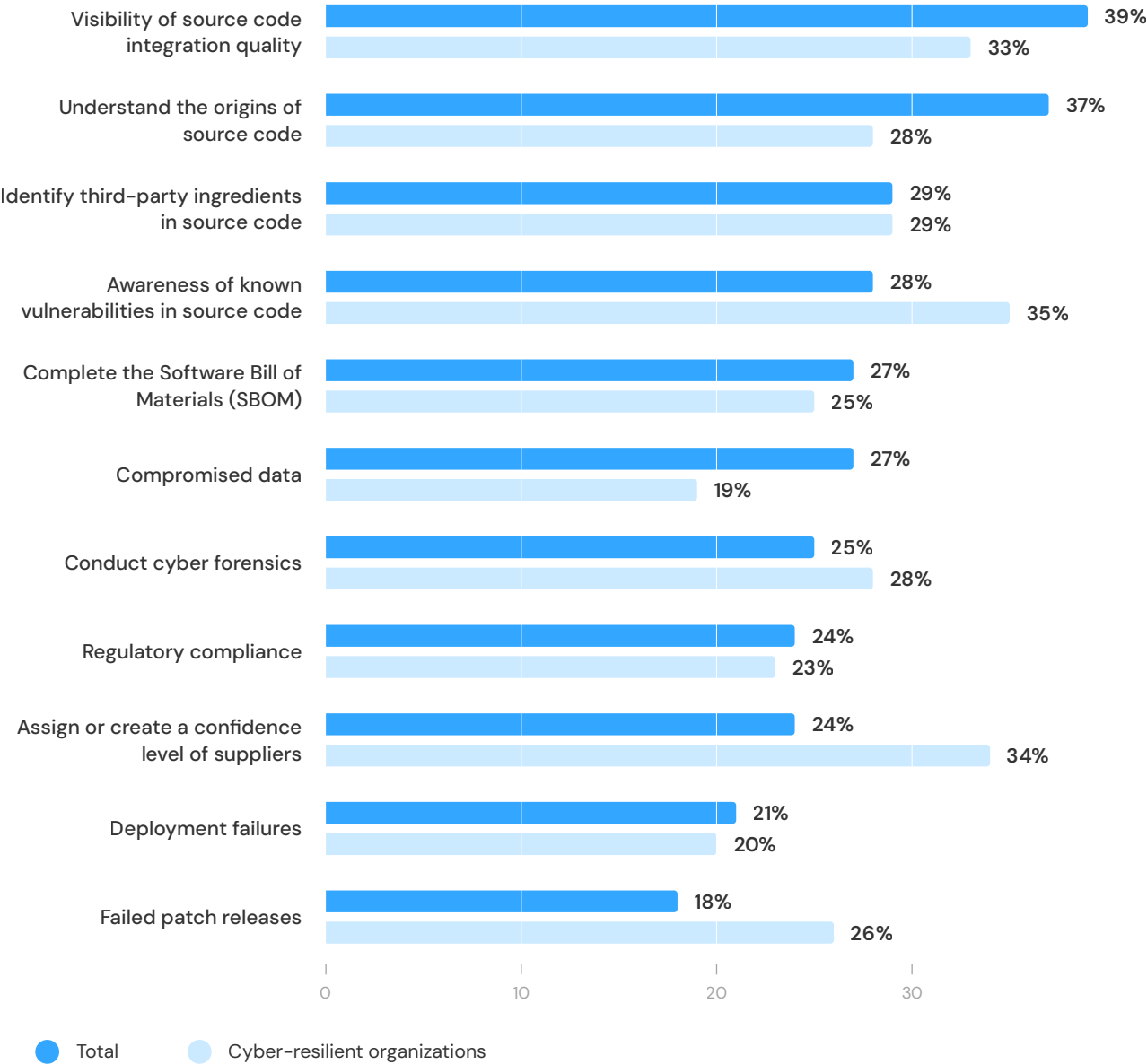
CEOs are far more concerned with software supply chain risk than some of the other C-suite roles, possibly because they have an overarching view of the whole organization and the impact of a breach.

Figure 12

Cyber-resilient leaders take a more holistic approach to securing their software supply chains

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

% of respondents
N=1500



- 62% of CEOs consider their organization's custom-developed source code as somewhat risky or high risk, compared with just 37% of CISOs, for example
- 60% of CEOs consider application programming interfaces (APIs) to be risky, compared with just 38% of CISOs
- CEOs and CTOs are equally nervous about third-party software distribution channels (both 60%) and unsupported software (both 59%)

Organizations are building a robust view of source code, but cyber-resilient organizations are more advanced

Of the factors driving better software supply chain visibility in their organizations, the highest percentage (39% of the total respondents) cited visibility of source code integration quality and 37% cited understanding the origins of source code.

For cyber-resilient organizations, the most important ways to increase supply chain visibility are awareness of known vulnerabilities in source code (selected by 35%) and assigning or creating a confidence level of suppliers (34%). This suggests that these organizations already understand that better visibility of their software supply chain is critical.

These cyber-resilient organizations are backing this up with investment: 50% say they are significantly investing in software supply chain security, compared with just 24% of businesses overall. ■

Are organizations paying enough attention to software supply chain threats?

Overall, executives do not seem to be taking software supply chain threats as seriously as they should in the current technology and risk environment:



30%

say that AI adoption has caused greater risk to the software supply chain



49%

say the visibility into their supply chain needs improvement



32%

say that the biggest risk they face today is from within their software supply chain



25%

say that engaging with software suppliers about their security credentials is a priority for the next 12 months

Four Steps to Cyber Resilience

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 business.

01

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

02

Foster a cyber-resilient culture

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

03

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 training
- / Move to a Zero Trust Architecture as a foundation for a multi-layered approach to network security

04

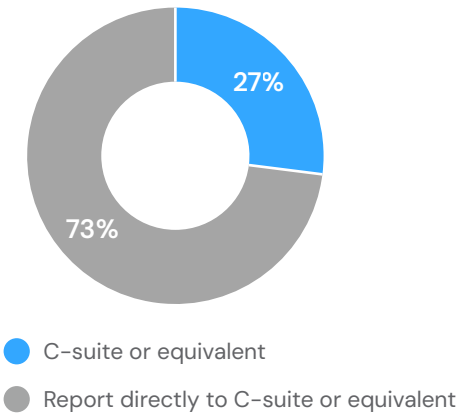
Prioritize software supply chain resilience

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

Demographics

Respondent Seniority

Total sample

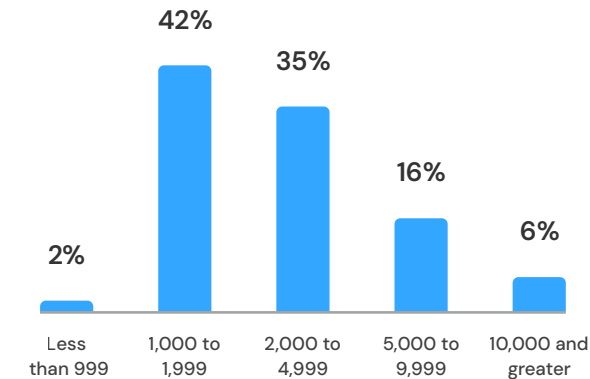


Survey Sample Sizes

Total sample N=1500
Cyber-resilient organizations N=109

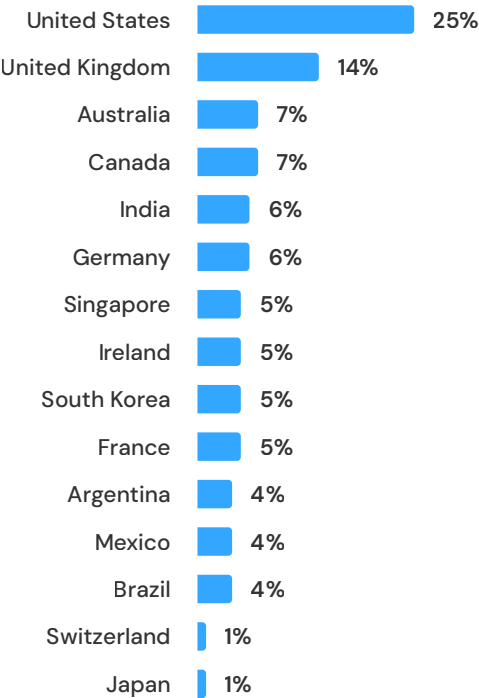
Organization Size

Total sample



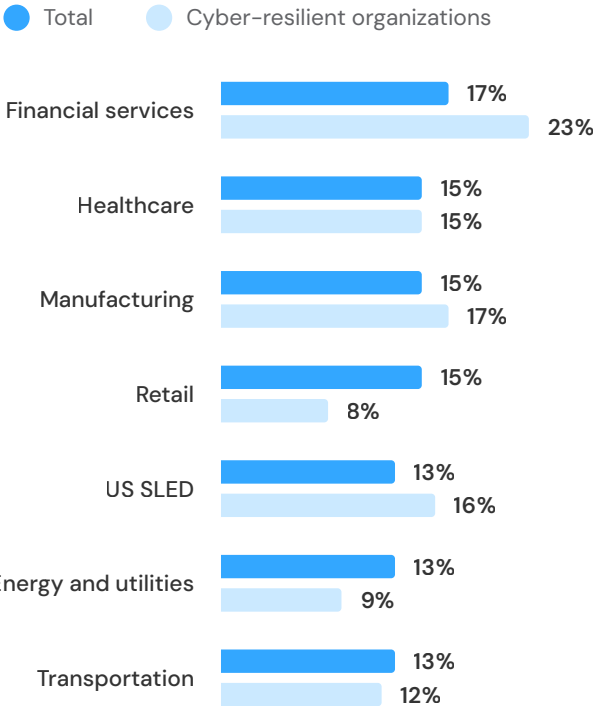
Location

Total sample



Industry

Total sample vs cyber-resilient organizations



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.

<https://levelblue.com/contact>



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