LevelBlue

US SLED

Futures™ Report 2024

Cyber Resilience

LevelBlue Futures™ Report

Beyond the barriers to cyber resilience

About the Research

In March 2024, we engaged FT Longitude to survey 1,050 C-suite and senior executives across 18 countries and seven industries: energy and utilities, financial services, healthcare, manufacturing, retail, transportation, and US SLED (state and local government, and higher education), to understand better their cybersecurity resilience strategies and how they were handling cyber resilience across the business. The total number surveyed in US SLED is 150. This is the US SLED report for 2024.

As part of this research, we use the following definitions:

Cyber resilience: focuses on the entire IT estate and includes the business as it pertains to computing and its ability to recover from an unexpected interruption, from a cyber incident to natural and man-made disasters.

Cybersecurity resilience: focuses purely on the cybersecurity estate and the ability to withstand and recover from cyber-specific threats and attacks.

Boundaryless computing: computing that takes place beyond the perimeter or outside the organization's four walls. We used this term to simplify the research. In this report, we call this *dynamic computing*.

Special thank you to FT Longitude, our research partner, and Altitude Management, our design partner, who made this report possible.

Contents

Welcome to the 2024 US SLED Report

What are the barriers to cyber resilience today in US SLED?

Why is it so difficult? And what is coming next, that will generate resilience challenges further down the line?

With this research, we sought to uncover the barriers to cyber resilience and how business leaders tackle these challenges. After five years of exploring the immediate future of cybersecurity and edge computing, we focused on the long-term obstacles and the strategies to overcome them.

The findings reveal a daunting yet exciting landscape. As the Internet of Things (IoT) and 5G technologies dissolve traditional perimeters and enable data collection and analysis at the source, state and local governments and educational institutions have entered the era of dynamic computing. This presents incredible opportunities for technology innovation within the US SLED sector, including improved data management and enhanced access to critical information. However, expanding computing and storage capabilities brings new security challenges as traditional methods become inadequate to protect sensitive public and educational data.

Our survey results tell an important story: 83% of US SLED respondents anticipate that dynamic computing will enhance operational performance within the next three years. Yet, a similar number acknowledge the increased exposure to risk.

In this area, optimism surrounds dynamic computing's potential, especially in AI strategy development and leveraging sophisticated supply chains. Nearly three-quarters (74%) of respondents believe computing innovation's benefits outweigh the cybersecurity risks. However, the industry remains cautious about AI adoption.

This highlights the daily paradox for cyber leaders: balancing technological innovation with cybersecurity and business resilience while facing ever-evolving threats from cybercriminals weaponizing the latest technologies.

Our report delves into the proactive measures executives can take to protect their organizations and their concerns about balancing innovation with risk mitigation. We assess their preparedness and readiness for the future.

We hope you find this report insightful and look forward to discussing its conclusions and recommendations with you in greater detail.

Theresa Lanowitz, Chief Evangelist

01

Cyber Resilience: Essential for Business Security

The rapid evolution of computing has thrust US SLED organizations into a perpetual struggle between innovation and risk. The stark reality is that cyber resilience remains a distant aspiration—something we can envision but is exceedingly difficult to attain.

Computing evolved so quickly that most IT leaders in US SLED no longer have visibility into their IT estate. As both proprietary and open sources of software are combined with legacy solutions, cloud computing, and digital transformation, US SLED leaders anticipate positive outcomes. However, 86% acknowledge the one thing they are trading off is risk (Figure 3).

The good news is that 79% of US SLED leaders expect earlier involvement of cybersecurity in computing projects, indicating a shift towards proactive measures. This positive trend, coupled with the cautious adoption of AI and a slightly lower concern for risk, suggests a moderate level of preparedness.

Meanwhile, cybercriminals are just getting started.

Today's US SLED organizations operate in a climate where vital systems can be disrupted within hours, compromising public services and sensitive data.

The task is to achieve broadscale cyber resilience and prepare the whole enterprise to recover from interruptions to the networks, systems, and data that underpin US SLED.

An adaptive computing strategy is how organizations will survive.

The inconvenient truth is that the escalation of the cyber threat coincides with an explosion in computing power—including AI and edge computing.

This creates unprecedented innovation opportunities. IT supports computing services with targeted app development, real-time data collection and analysis, and more (see our 2023 report to learn more).

At the same time, securing dynamic computing requires new thinking. Organizations need cyber resilience strategies to recover from attacks such as large-scale DDoS, business email compromise, and ransomware.

We evaluated the research through four lenses.

Our research reveals deep-seated barriers and inconsistencies in how US SLED leaders prioritize resilience issues. In this report, we look at the current landscape through four lenses:

Big picture: what's preventing cyber resilience

Drill down: what's preventing cybersecurity resilience

Business context: how organizations respond with money and resources

What's on the horizon: threats, innovation and AI

Finally, we provide a list of key initiatives for US SLED organizations to help remove roadblocks, reduce risk, and include security from the start.

Four Key Lenses

02

Critical Barriers to Cyber Resilience

Fast Facts

86% say computing innovation is increasing risk.

72% say regulation compliance requires unattainable information.

69% acknowledge cyber resilience is not a whole-organization priority.

67% cite a lack of clarity over responsibility as a resilience barrier.

Cyber resilience in US SLED involves securing the entire IT infrastructure and ensuring the ability to recover from unexpected disruptions, whether caused by a cyber attack, extreme weather event, or other emergencies.

It is a critical initiative for US SLED entities, as they balance internal demands for agility, flexibility, innovation, and cost management with external pressures for data protection, public safety, and operational predictability.

Added to this mix is technology innovation, what we call dynamic computing. This includes computing beyond the perimeter, as edge and the IoT move data collection closer to the source.

While US SLED leaders continue to face barriers and internal challenges, this study found opportunities for business leaders to remove roadblocks and understand where to focus resources for the most significant impact (see Figure 1).

Dynamic computing fuels innovation.

US SLED leaders are committed to investing in the technologies that drive dynamic computing. By processing data closer to the source, they can develop innovative services and applications based on real-time data transfer, enabling new ways of interacting with citizens and enhancing public services.

Improvements in computing give organizations a competitive edge.

Figure 3 shows how US SLED respondents expect dynamic computing to alter their businesses within the next three years. Most predict continued enterprise change within that timeframe. Specifically, 83% anticipate improvements to revenue and operations, and 60% expect to start working with a more sophisticated supply chain.

Risk increases as businesses favor innovation over resilience.

The downside is that 86% of SLED respondents agree that dynamic computing increases their risk exposure. Indeed, 73% indicate that it's impossible for them to assess how an attack might impact their organization—introducing a level of uncertainty that hampers their cyber resilience.

At a time of new opportunity and innovation, organizations may not be as opposed to risk as they were before. A whopping 74% of respondents confirmed that the opportunity of computing innovation outweighs the corresponding increase in cybersecurity risk. Such trade-offs make cyber resilience nearly impossible to achieve.

What's preventing cyber resilience?

There's no easy answer, but there are indicators that help clarify why business leaders are making decisions that undermine their resilience. Computing complexity forces businesses to make tough decisions and trade-offs based on business priorities. In the complex, often under-resourced US SLED environment, essential security considerations are often overlooked:

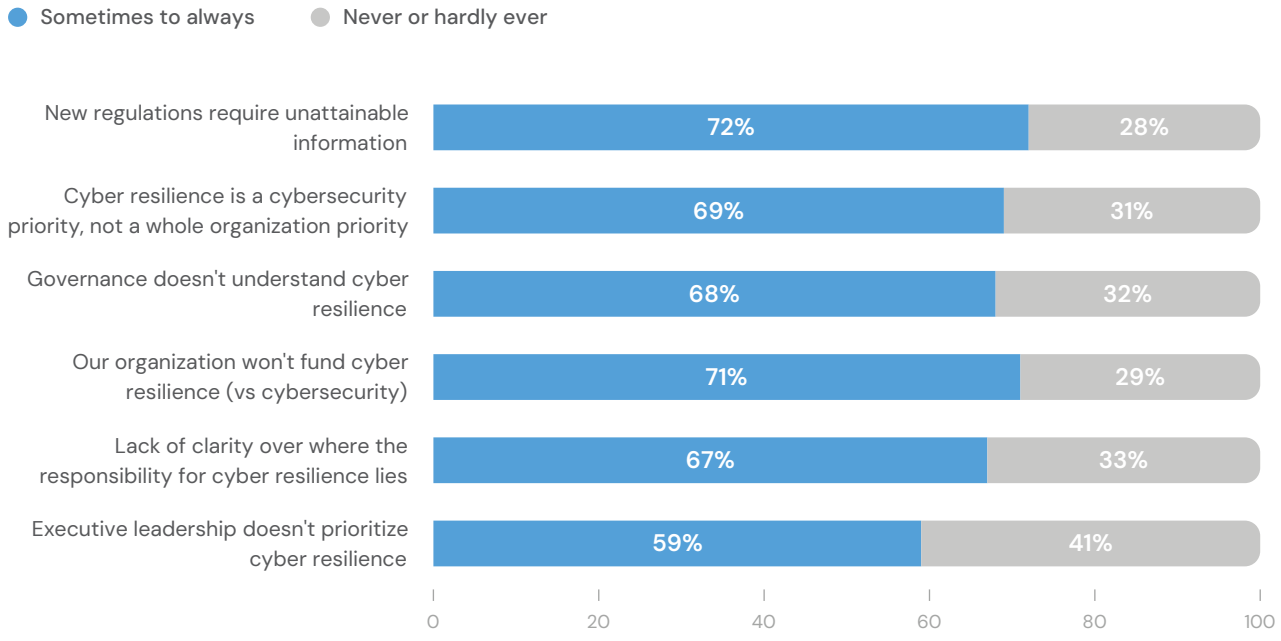
- unsecured vulnerabilities in both the software and physical supply chains
- apps launched without built-in data, compromising user privacy
- data migrated to the cloud without proper configuration settings
- widely distributed endpoints not being properly secured or mapped to the network.

Figure 1

Organizations lack organizational support for cyber resilience

Q: Which of the following options are barriers to cyber resilience in your organization?

% of respondents
N=150



Looking at the big picture, even as attacks increase and the associated costs skyrocket, cyber resilience is still not prioritized as a critical business initiative.

Cyber resilience is not embraced by executives as a whole-organization problem.

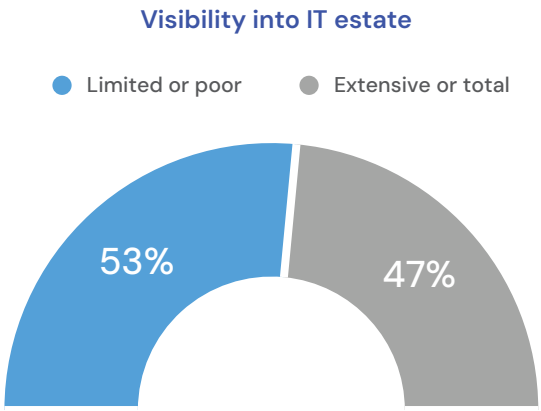
69% of our US SLED respondents report cyber resilience is primarily the responsibility of cybersecurity teams and is not an organization-wide priority. This is a cause for concern.

Figure 2

Dynamic computing has reduced visibility into the IT estate

Q: Please indicate where your organization is positioned as it relates to boundaryless computing.

% of respondents N=150



Cyber resilience requires executive and board support. A majority, 59% of respondents, say leadership doesn't prioritize cyber resilience, and 68% admit that their governance team doesn't understand it. Without executive support, silos in IT will continue to exist.

Accepting a certain amount of risk is a decision every CIO or CISO must embrace. Unfortunately, with 71% saying their organizations do not specifically invest in cyber resilience beyond cybersecurity, we can infer that leadership underestimates the harm a major cyber incident could create.

Few have a clear view of vulnerabilities.

Our research reinforces the need for visibility of the IT estate and its associated vulnerabilities. However, 53% of US SLED respondents indicate that they have little to zero visibility into the IT estate (Figure 2).

A full mapping of mature organizations will likely yield custom applications written with outdated tooling or mainframe datasets destined to exist for "business reasons." Couple these legacy necessities with emerging technologies, and a lack of visibility increases the possibility of a catastrophic attack.

Visibility is limited in a dynamic computing environment.

For 72% of respondents, the lack of visibility is compounded by new regulations requiring detailed information that is frequently unattainable.

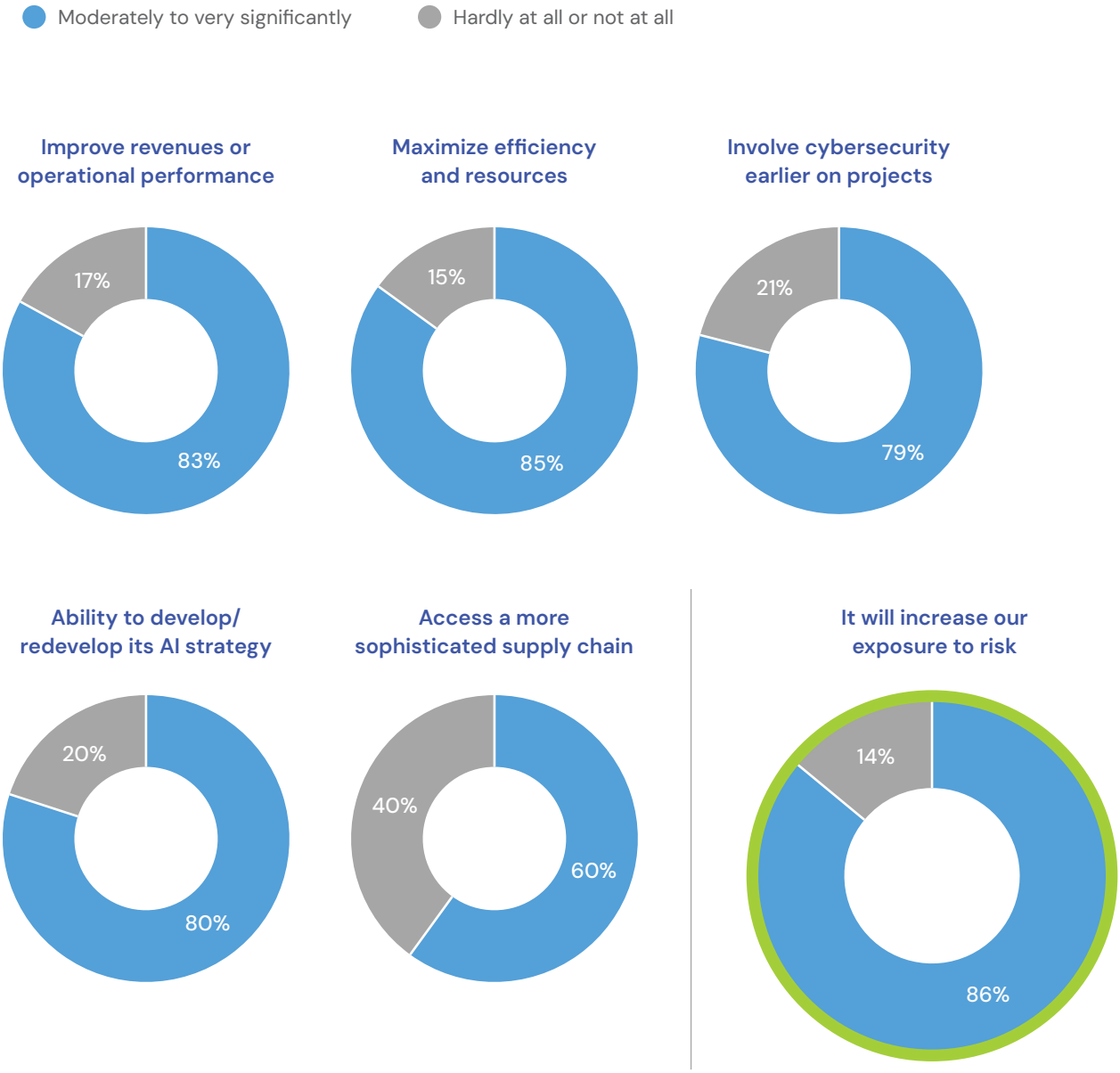
Balancing risk and innovation while understanding exposure is necessary to reap the rewards of dynamic computing. Without visibility, organizations cannot objectively understand the problem domain and where the acceptable risk threshold lies. IT needs leadership to support their efforts and prioritize resilience.

Figure 3

Dynamic computing brings significant benefits and risk

Q: How do you expect boundaryless (dynamic) computing to alter your business within the next three years?

% of respondents
N=150



03

Challenges Impacting Cybersecurity Resilience

Fast Facts

69% reveal their organizations are at risk due to barriers impacting their cybersecurity resilience strategies.

47% are most likely to seek cybersecurity expertise for strategy and planning.

66% indicate that digital transformation is an ongoing barrier to cybersecurity resilience.

72% are struggling to find the external guidance they need.

Cybersecurity resilience, different from cyber resilience, is critical as threats grow in frequency and complexity. With digital innovation driving business, cybersecurity resilience is essential for maintaining stakeholder trust. US SLED organizations can prioritize this by fortifying defenses, mitigating risks, and ensuring long-term viability in an evolving threat landscape.

Leaders also need to acknowledge that risk is running rampant. US SLED organizations know this vulnerability, with 86% recognizing their exposure to cyber threats. Meanwhile, 76% acknowledge their organizations accept some uncertainty regarding these threats. 69% of US SLED respondents agree that barriers impact their cybersecurity resilience strategy (Figure 4).

Figure 4

Cybersecurity issues are also preventing resilience

To what extent do you agree or disagree with the following statement?

% of respondents N=150

Barriers to cybersecurity resilience put my organization at risk

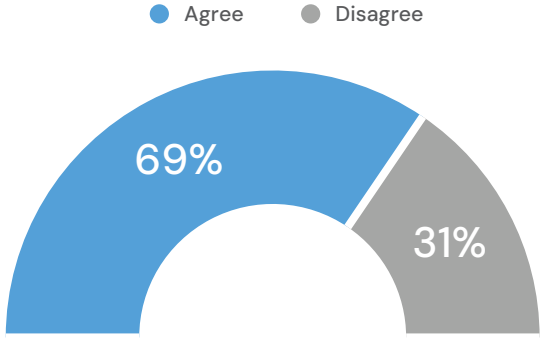


Figure 5

Barriers to cybersecurity resilience

Q: Now, thinking just about cybersecurity, to what extent do the following issues currently present a barrier to cybersecurity resilience?

% of respondents
N=150

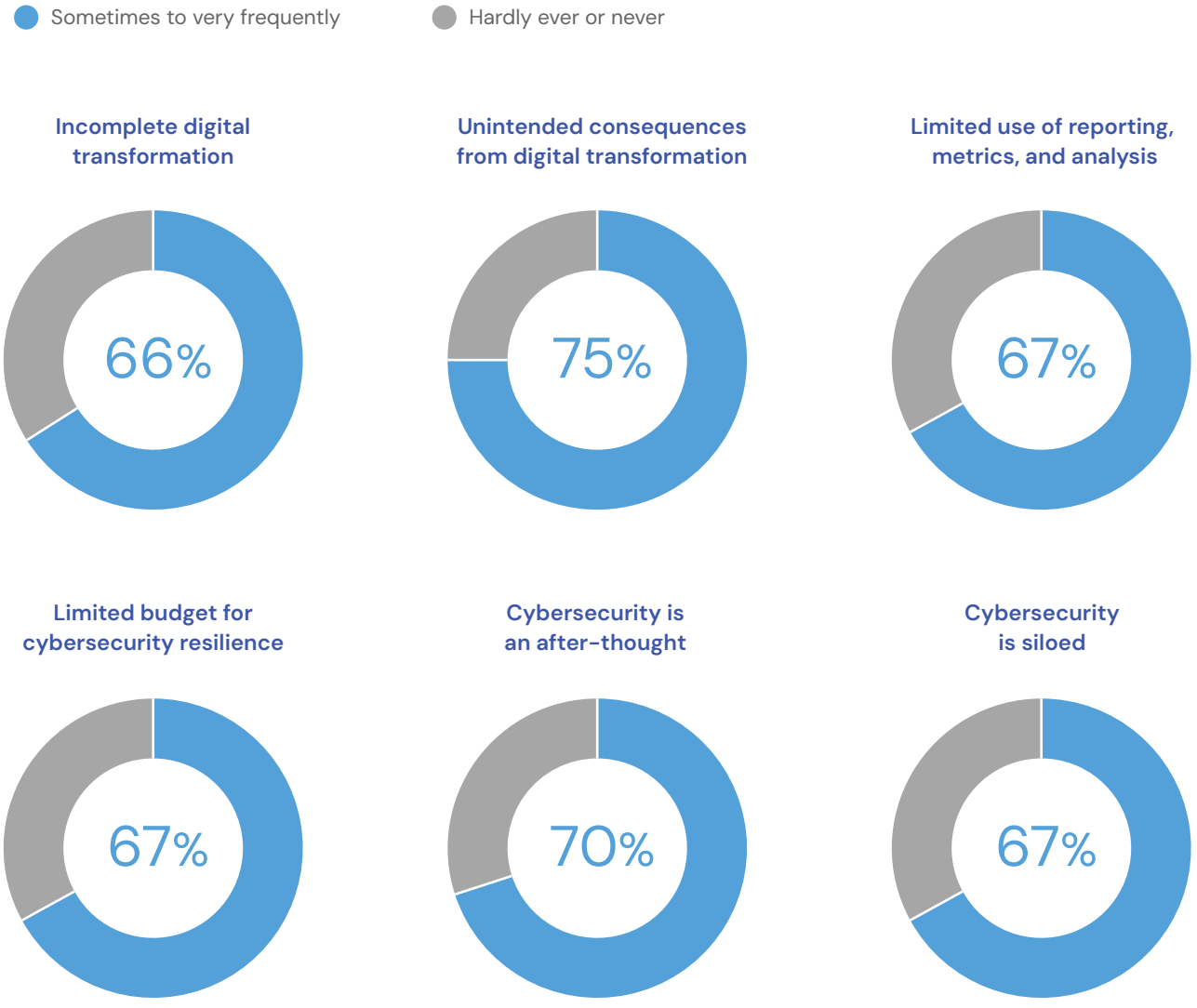
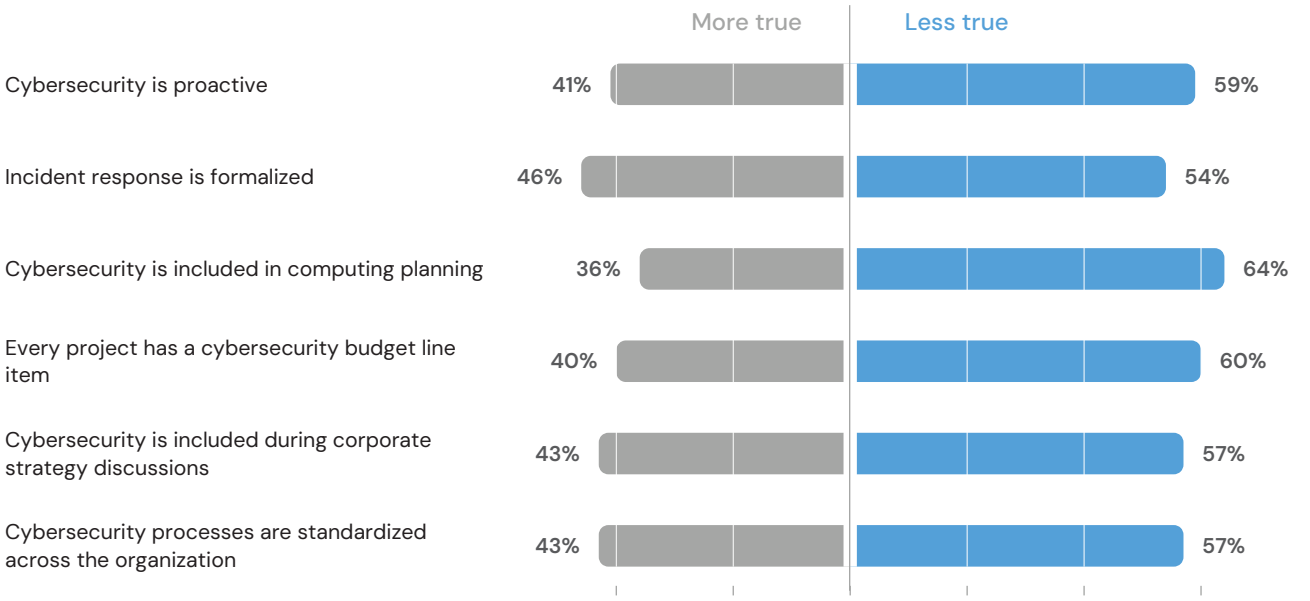


Figure 6

Cybersecurity has not yet been integrated into business strategy

Q: Which of the following best apply to your organization's cybersecurity strategy?

% of respondents
N=150



Respondents report a lack of executive engagement and proactivity.

A lack of engagement from senior executives poses a significant barrier to cybersecurity resilience in US SLED (Figures 5 and 6). Respondents indicate that cybersecurity is often excluded from high-level decision-making despite the devastating potential of cyber-attacks, leading to financial strains for US SLED organizations and disruptions to critical public services.

Just 36% of US SLED respondents say cybersecurity is typically included in computing planning, while 43% say it is included in corporate strategy discussions.

Improving cybersecurity to boost resilience across the organization.

Most US SLED respondents believe cybersecurity is an afterthought in their organizations (70%), and confirm efforts are often siloed, hindering comprehensive protection (67%). Additionally, there is a significant lack of visibility of the supply chain, with 54% of respondents indicating this as a major concern. This lack of visibility poses significant risks in US SLED organizations' physical and software supply chains.

Funding and resource allocation are also critical issues. A majority (67%) indicate that cybersecurity resilience initiatives are not sufficiently factored into the organization's budget. Furthermore, 54% of US SLED organizations lack formalized incident response plans, making them susceptible to prolonged disruptions and data breaches. Only 40% have a cybersecurity budget line item for every project, meaning many projects are not adequately protected.

More than half (57%) of US SLED organizations do not have standardized cybersecurity processes, which risks sensitive data and operational integrity. Addressing these barriers will help US SLED organizations enhance their cybersecurity resilience and better safeguard against growing threats.

04

Business Context Reveals Operational Issues

Fast Facts

69% of US SLED organizations report budgets are reactive rather than proactive.

69% say that measuring cybersecurity investments based on return on investment (ROI) is outdated.

55% reveal there's a lack of understanding about cybersecurity at the board level.

45% identify compliance as the driver most likely to unlock the cybersecurity budget.

Buy-in from US SLED business leaders, not just IT, is key to understanding the profound connection between the institution's survival and cyber resilience.

Cyber resilience is a comprehensive business initiative integral to organizational excellence. Every strategic business plan should include it as a top three priority, empowering leaders to steer the organization towards a secure future.

It starts with prioritizing IT and building security into everything you do.

One of the significant challenges faced by organizations within the State and Local Government and Higher and Education (US SLED) sector is the difficulty in finding adequate external expertise to support cybersecurity resilience. A striking 72% of US SLED respondents agree that this issue presents a substantial barrier. Given the complexities and evolving nature of cybersecurity threats, nearly half (47%) of US SLED organizations have turned to Cybersecurity-as-a-Service (CSaaS) as a solution.

This approach allows them to leverage specialized expertise that may not be available in-house, ensuring that security is integrated into every facet of their operations. By prioritizing IT and embedding cybersecurity into all aspects of their infrastructure, US SLED organizations can better protect themselves against the increasing cyber threats they face.

Figure 7

Finding the right outside expertise can be difficult

Q: Which of the following are barriers to cybersecurity resilience in your organization?

% of respondents N=150

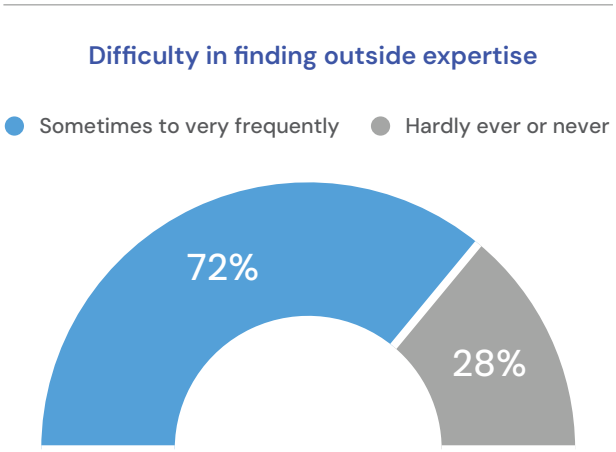


Figure 8

Compliance and breaches are driving spending

Q: Which drivers are most likely to unlock the budget for cybersecurity within your organization?

% of respondents
N=150

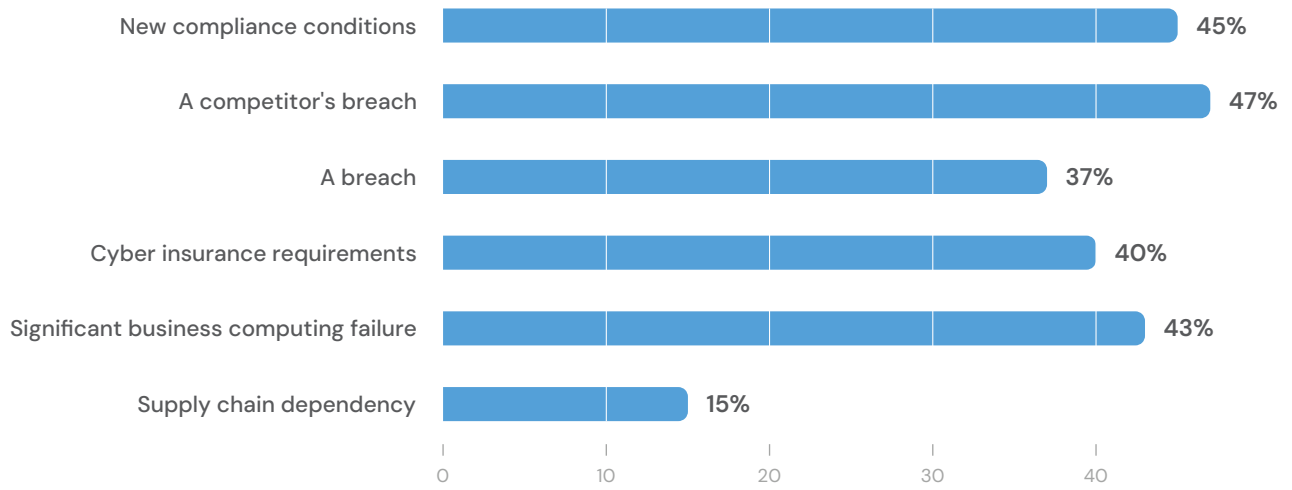


Figure 9

Security spending has increased in 2024

Q: How does your organization typically allocate resources across the entirety of a project?

% of respondents
N=150

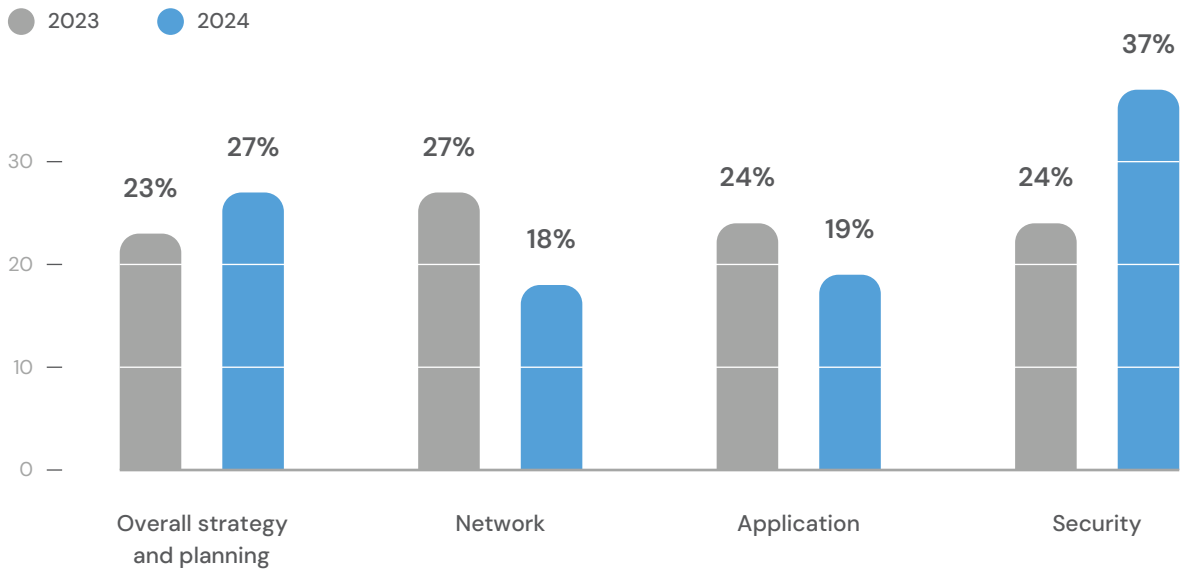
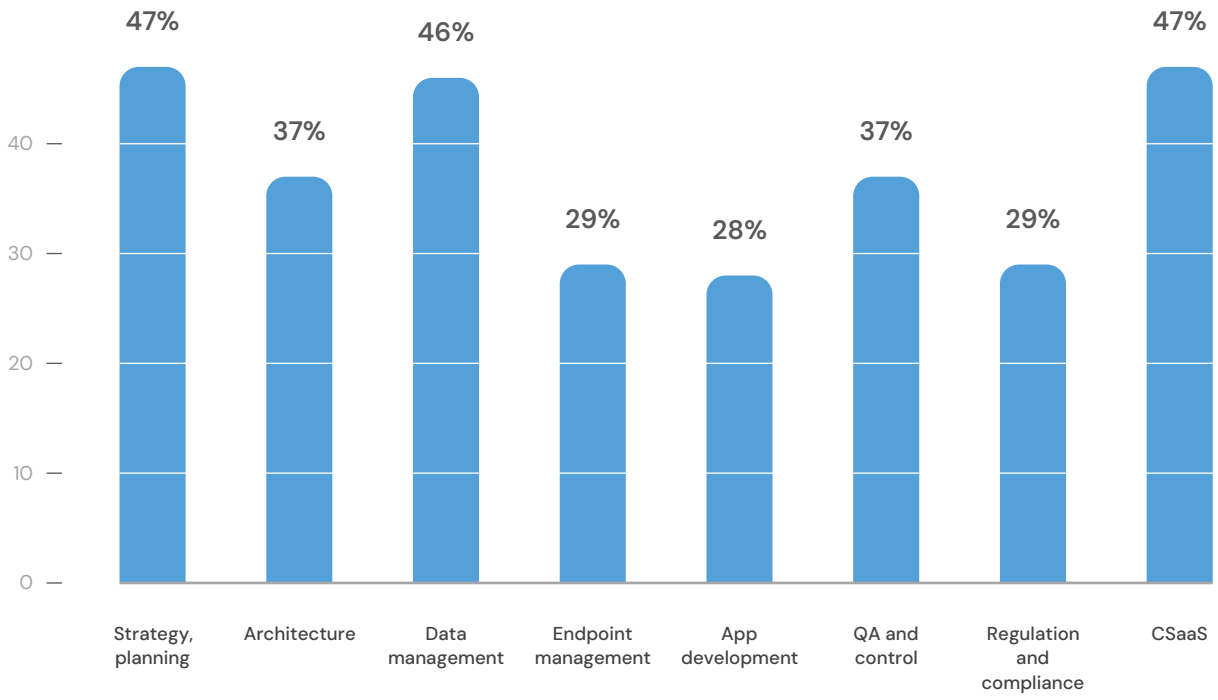


Figure 10

Outside expertise helps build a foundation for success

Q: When is your organization most likely to seek cybersecurity expertise from external vendors?

% of respondents
N=150



Budget allocations are shifting in a positive direction.

Compared to our 2023 research, there's a notable increase in resources dedicated to cybersecurity. This shift is significant, reflecting a move towards aligning resource allocation with evolving regulatory requirements and the demands of dynamic computing.

More broadly, our analysis comparing this year's responses to last year's research reveals a marked change in resource allocation trends. There's a notable increase in resources allocated to strategy and planning, and security, while networking and applications seem to operate more predictably in terms of costs. The integration of open source, coupled with new regulations mandating deeper reporting on software bill of materials (SBOMs), likely contributes to this shift. Additionally, budgeting for external support may play a role in driving this positive change.

Leveraging external expertise is not just beneficial; it's integral to success.

Outside expertise is crucial for many aspects of business, including cyber resilience. US SLED relies on external experts for many things, but strategic planning (47%), cybersecurity-as-a-service (47%), and data management (46%) are the top priorities.

The adoption of Cybersecurity-as-a-Service (CSaaS) is on the rise, with 47% opting to outsource their cybersecurity needs rather than manage them in-house. US SLED is using 15% more outside

resources than any other industry. This reflects the benefits of strategically extending cybersecurity teams with specialized service providers.

Achieving organizational excellence in cybersecurity requires a fundamental shift in mindset and approach.

Our findings underscore the critical need for *business leaders*, not just IT professionals, to recognize the strategic importance of cyber resilience. It's not a technical issue; cyber resilience is a comprehensive business imperative.

As organizations navigate the complexities of dynamic computing, they must prioritize cyber resilience. However, our study reveals a concerning gap between cybersecurity investments and broader business goals, with budgets often reactive and misaligned. This reactive approach and outdated practices undermine effective cyber resilience efforts. Notably, 69% of respondents report that measuring cybersecurity investments based on ROI is outdated.

To address these challenges, organizations must adopt proactive strategies, leverage external expertise, and align cybersecurity investments with strategic business objectives.

"Our findings underscore the critical need for *business leaders*, not just IT professionals, to recognize the strategic importance of cyber resilience. It's not a technical issue; cyber resilience is a comprehensive business imperative."

05

Looking Ahead – What's on the Horizon

From threats to supply chain security to the ultimate use of the cloud to artificial intelligence, based on the core of Moore's Law, the rate of change is only likely to increase.

Threat management needs to be better aligned with probability

Just 36% of US SLED respondents integrate cybersecurity into their computing planning. This stops them keeping up with emerging technologies and leaves their organizations vulnerable and unprepared to harness the potential of dynamic computing.

Here, we delineate key intersections where cybersecurity converges with strategic corporate initiatives, emphasizing the criticality of elevating cyber resilience to a whole business priority. Figure 12 outlines the most likely attacks to occur within respondents' organizations. While 40% recognize distributed denial-of-service (DDoS) as a probable attack vector, 42% admit to lacking confidence in handling it.

From an industry perspective, our data shows that organizations across all industries are ill-prepared for DDoS, business email compromise, or nation-state attacks.

The supply chain delivers unintended consequences.

Supply chain attacks continue to dominate headlines, serving as a stark reminder of the vulnerability of every organization.

Our supply chains, encompassing the processes involved in software development and physical products, expose us to many security risks.

Vulnerabilities stemming from third-party sources rank among the top threat factors for any organization. In fact, over half of respondents (68%) reveal difficulty in assessing supply chain risk, with only 21% stating that their supply chain is completely or almost completely secure.

Figure 11

Many organizations don't have supply chain visibility

Q: Which of the following options are barriers to cybersecurity resilience in your organization?

% of respondents N=150

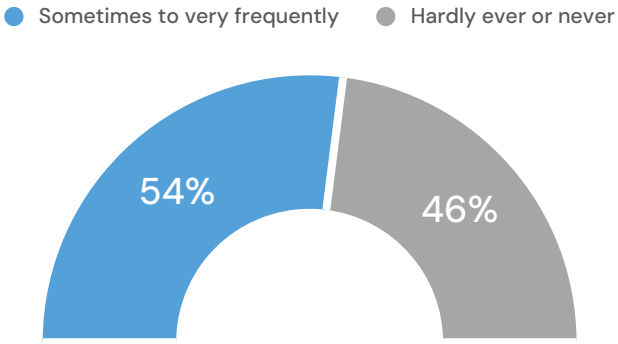
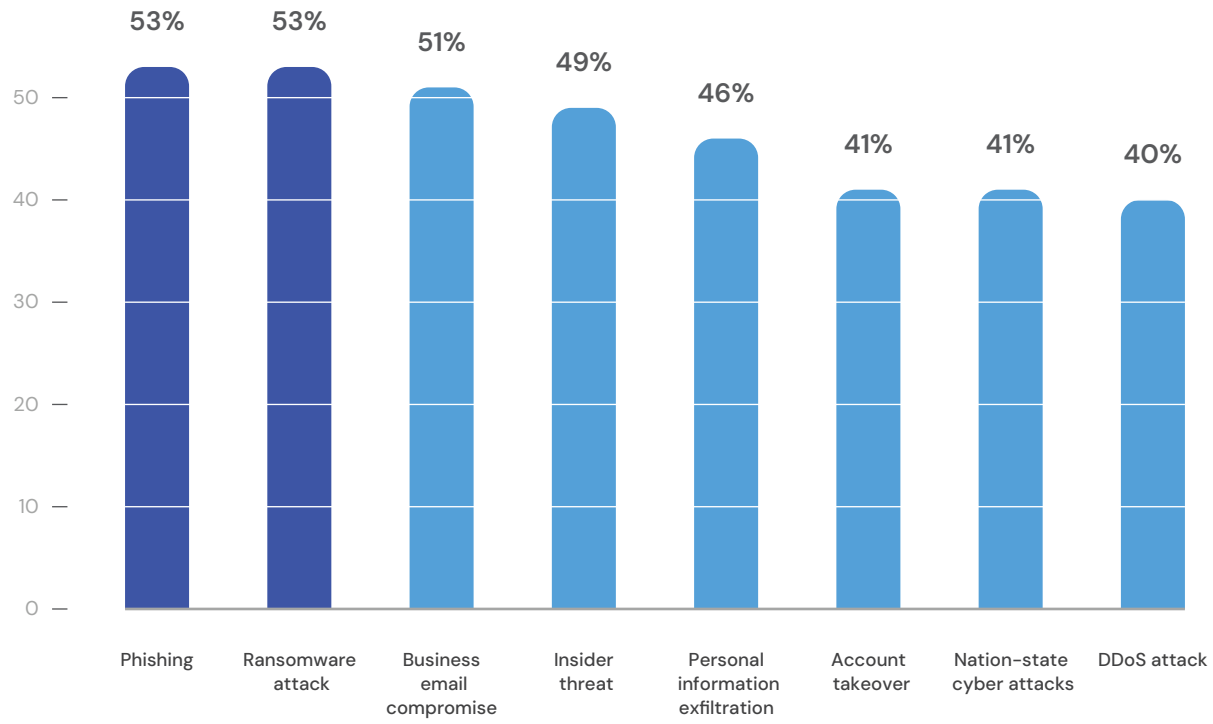


Figure 12

Anticipated top threats

Q: Which attacks are most likely to occur in your organization?

% of respondents
N=150



However, strategies and solutions are available to address these vulnerabilities, and with the right approach, businesses can significantly reduce the risk.

Infrastructure ownership is changing in US SLED.

When US SLED organizations transitioned to remote operations during the pandemic, many were compelled to adopt cloud technologies. The shift to the cloud has brought several benefits, such as breaking down departmental silos, boosting on-site computational capabilities, and providing enhanced scalability to meet the growing demands of remote work and digital services.

Today, 75% express confidence that cloud computing provides sufficient cybersecurity resilience for their organizations.

Artificial Intelligence is on everyone's agenda, but it brings risk.

Today, AI is a ubiquitous topic, yet its implementation also entails risk. The pressure to adopt AI strategies sometimes results in sidelining other crucial initiatives. In US SLED, 63% acknowledge they are a cautious or late adopter of AI. (Figure 14). 18% report using Generative AI, 25% use machine learning, and 20% use deep learning (Figure 15).

Figure 13

Most want infrastructure on-premise, but some choose non-ownership

Q: Please indicate where your organization is positioned on the following dimension: on-premise infrastructure or cloud with no desire to own infrastructure.

% of respondents N=150

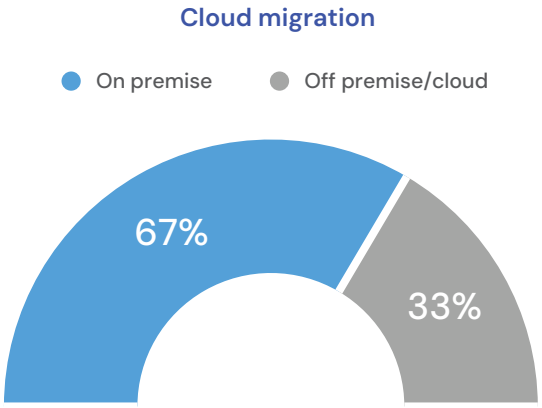
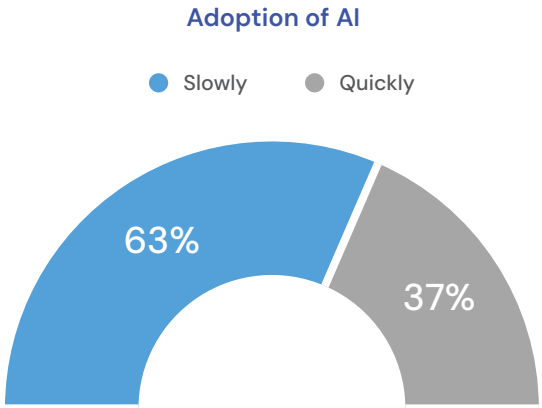


Figure 14

Dynamic computing is helping AI move quickly into the IT estate

Please indicate where your organization is positioned on the following dimension: how fast are you adopting AI?

% of respondents N=150



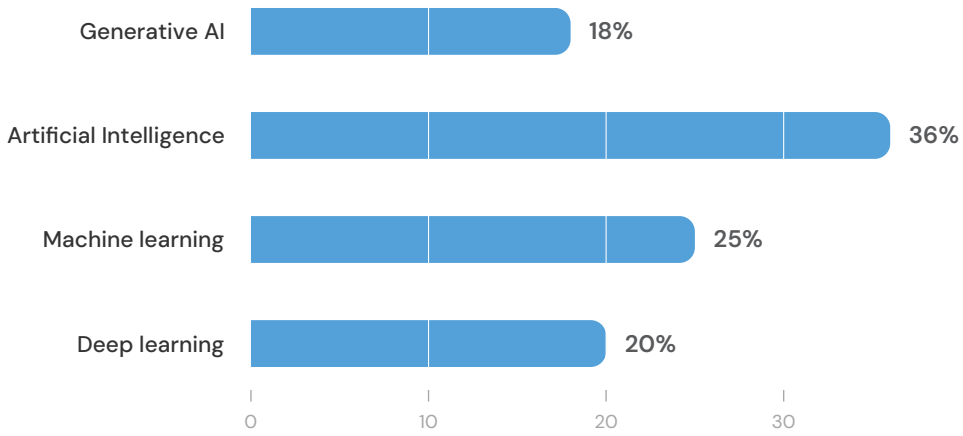
AI capabilities will permeate various solutions, from business tool stacks to cybersecurity platforms, becoming inherent components rather than separate entities. However, skilled human intervention remains critical for effectively utilizing AI tools.

Figure 15

AI has emerged with momentum to help with cybersecurity

Q: How will your use of AI in cybersecurity break down across the following technologies over the next two years?

% of respondents
N=150



06

Prioritizing Cyber Resilience in a Changing Landscape

Balancing innovation with cyber risk is crucial in today's rapidly changing US SLED environment. While embracing dynamic computing offers substantial advantages, it also brings about new vulnerabilities that must be proactively managed to safeguard sensitive data and protect critical public assets.

Identifying and overcoming cybersecurity barriers, standardizing processes, and integrating cybersecurity into every facet of the organization's operations are essential to building a resilient framework. By prioritizing cybersecurity as a fundamental business dependency and embracing a proactive approach to risk management, businesses can navigate the complexities of the digital landscape with confidence and agility.

As we look to the future, the top priority of every organization is to protect its intellectual property and digital assets. That's why cyber resilience remains essential for organizations seeking to thrive in an increasingly interconnected world. By staying vigilant, adaptive, and collaborative, businesses can mitigate emerging threats and safeguard their digital assets for years.

We are your advocates for a proactive and holistic approach to cyber resilience. We believe organizations can navigate the digital landscape with confidence and agility by implementing the following steps and prioritizing cybersecurity as an integral aspect of all business operations.

"Understanding the obstacles to cyber resilience is the first step towards fortifying your organization's defenses."

"Proactive allocation of cybersecurity budgets in alignment with overall business strategy is key to effective risk management."

Five Steps to Future Cyber Resilience

Achieving cyber resilience is paramount for businesses striving to safeguard their operations against the relentless onslaught of cyber threats. Here, we outline five essential steps to navigate this challenging terrain and emerge stronger in the face of adversity.

By implementing these five steps, organizations can better allocate resources, align with business goals, and effectively manage their ecosystems and supply chains. Armed with a deeper understanding of their risk landscape, they can harness the latest technologies and embrace a more cyber-resilient future.

01

Identify the Barriers

Conduct a thorough assessment to pinpoint risk areas and understand how your physical and software supply chain influences decision-making processes. Clear identification of barriers lays the groundwork for effective resilience strategies.

02

Be Secure by Design

Assess your organization's next-generation computing needs and embed security measures from the outset to ensure compliance and mitigate future risks.

03

Align Cyber Investments with the Business

Break down silos and allocate resources strategically to align cybersecurity initiatives with overarching business objectives.

04

Build a Support Ecosystem

Forge partnerships with external collaborators to augment your organization's expertise and enhance real-time decision-making processes.

05

Transform the Cybersecurity Strategy

Adaptability is key in the ever-changing landscape of cyber threats. Regularly update tools and capabilities to meet the demands of an evolving attack surface.

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, enabling 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.

LevelBlue. Cybersecurity. Simplified.

© 2024 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. | FRSL 11-2024

LevelBlue

Achieving cyber resilience is paramount to safeguarding US SLED from the relentless onslaught of cyber threats.