LogRhythm®

2024 State of the Security Team

Navigating Constant Change

Contents

Executive Summary

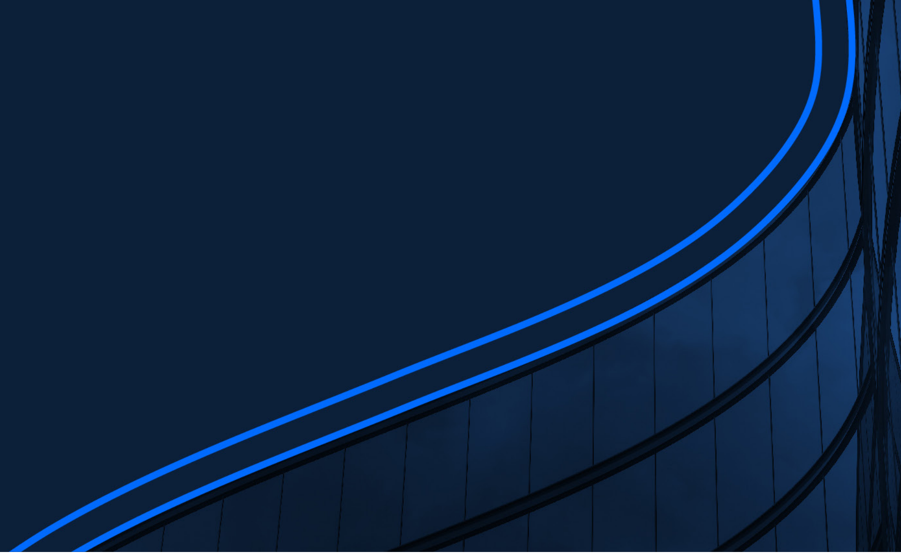
In cybersecurity, 2024 is marked by significant transformations. Businesses worldwide have faced an unprecedented rate of change in the threat environment evidenced by 95% of companies reporting security strategy adjustments within just the past year. This continual adjustment to strategies is primarily driven by the relentless pace of regulatory shifts, AI adoption and customer expectations regarding data protection and privacy.

The necessity for organizations to remain agile and adaptive in their security approaches has never been more critical. The 2024 cybersecurity environment is dynamic, with traditional defense mechanisms continuously being challenged by innovative threats, particularly those powered by advancements in artificial intelligence (AI). This environment demands a proactive and flexible strategy that can respond to current threats and anticipate future challenges.

At the heart of these strategic shifts is the role of leadership within organizations. The accountability for security breaches has risen to the highest levels, with 78% of professionals pointing to the cybersecurity leader or CEO — or both — as bearing the ultimate responsibility for protecting against and responding to cyber incidents. The perception of cybersecurity has changed from a purely technical issue to a central component of business strategy and corporate governance.

The alignment between business objectives and security protocols is improving, as evidenced by the decrease in deals lost due to security concerns — from 67% to 38% in just one year. This achievement reflects a growing understanding and collaboration between security teams and business executives, ensuring security strategies are robust and aligned with broader business goals.

As organizations progress through 2024 and beyond, the emphasis on executive leadership, alongside the development of adaptive and forward-thinking security strategies, will be paramount. This alignment is essential for fostering a secure and resilient digital environment that supports ongoing business success and protects against cyberthreats.



01

Key Findings

The 2024 cybersecurity research reveals pivotal insights into organizational adaptation amidst digital challenges, highlighting the need for ongoing evolution, strategic alignment, and strong communication. Key takeaways include:

95%

of companies reported altering their cybersecurity strategies in the past year.

Reasons:

- The dynamic threat landscape
- Emerging technologies and threats

29%

fewer business deals were lost over 12 months because of inadequate security strategies.

Reason:

- Improved management of business cybersecurity risks

Impact of AI and Regulatory Changes

- The adoption of AI and the shifting regulatory landscape are significant drivers of change in security practices.
- 98% of companies cite regulatory requirements as a factor in their cybersecurity approaches, resulting in 25% removing revenue generating products or services from the market.
- AI utilization has prompted strategy adjustments for 65% of organizations.

Increased Allocation of Resources

- A notable increase in confidence exists among security professionals regarding the sufficiency of their resources.
- 92% of companies adjusted or maintained their cybersecurity budgets in response to evolving threats.
- Most adjustments took the form of increased resource allocation.

Communication and Reporting Challenges

- Despite improvements, effective communication between security teams and non-security executives remains a significant gap.
- 59% of professionals report difficulties explaining the necessity of specific security solutions, indicating there is a pressing need for enhanced reporting mechanisms to facilitate better decision-making.

Improved Confidence Among Security Teams

- 78% of teams are confident they have the right resources to defend the company from cyberattacks.
- 79% of companies rate their security defense as good or excellent, while 89% adjust their security strategies to satisfy customers.

Strategic Approaches to Cybersecurity

- 78% of companies believe security breach responsibilities reside at the top leadership level.
- Organizations employ strategic approaches to overcome resource limitations, such as leveraging cloud infrastructure, prioritizing high-risk items, and outsourcing security functions.

These key findings illustrate the complex interplay between technological advancements, regulatory pressures, resource allocation, and the imperative for clear communication within cybersecurity. They highlight the critical need for organizations to adopt flexible, informed, and strategic approaches to cybersecurity, ensuring they can effectively protect against and respond to the evolving digital threats of today and tomorrow.

02

The Evolving Cybersecurity Landscape

Cybersecurity is more fluid and pressured than ever, shaped by technological advancements, evolving threats, and changing societal expectations. This dynamic environment presents unique challenges and opportunities for businesses aiming to safeguard their digital assets and maintain trust with stakeholders.

Catalysts for Change in Cybersecurity Strategies

Cybersecurity strategies are changing at an unprecedented pace, as shown by **95%** of companies reporting having **altered their security strategies** within the last 12 months. Drivers of these changes include:

- Technological evolution, such as the rise of AI-driven threats and solutions
- Shifts in the cyberthreat landscape, including the emergence of new types of attacks

95% of Companies Have Changed Their Security Strategy in the Last 12 Months

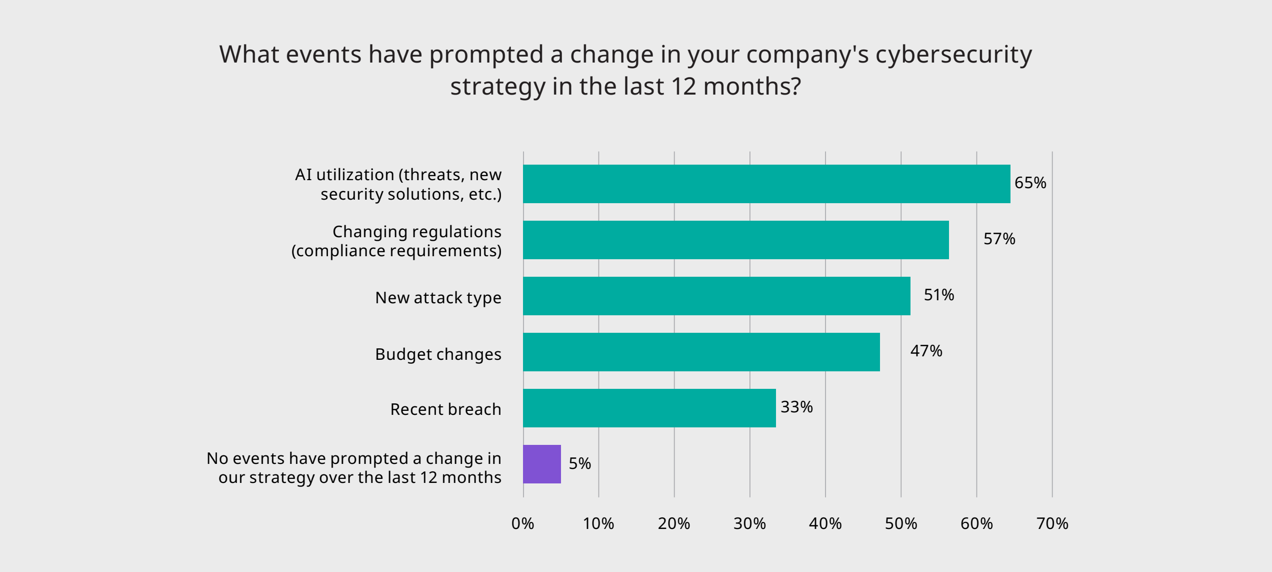


Figure 1

These developments compel organizations to continuously reassess and adapt their cybersecurity measures to keep pace with potential vulnerabilities and threats.

The Impact of Regulatory Requirements and Customer Demands on Security Practices

Regulatory requirements are a significant factor in cybersecurity, with 98% of organizations indicating that regulatory demands are a primary force driving changes in their security protocols. This regulatory pressure mandates adjustments in processes and staffing and, for 25% of businesses, has led to the discontinuation of some products or services to comply with legal standards.

98% State Regulatory Requirements Are Forcing Change, with 25% Removing Products or Services from the Market

What changes has your organization made in response to regulatory requirements?

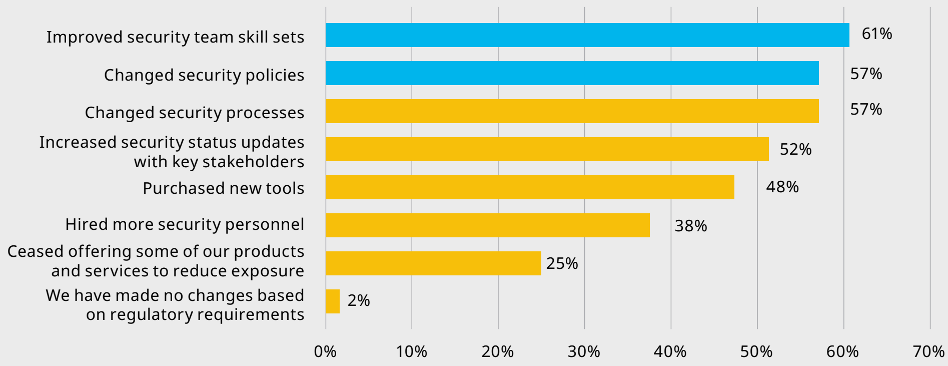
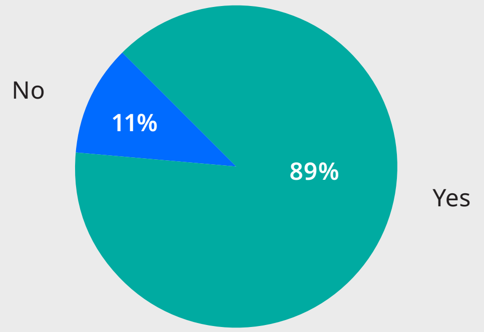


Figure 2

Alongside regulatory pressures, customer demands are crucial in shaping security strategies. The need to meet customer expectations for data protection has driven 89% of companies to modify their security approaches, highlighting the importance of security as a competitive differentiator and trust builder with consumers.

89% of Companies Adjust Security Strategies to Satisfy Customers

Has your organization changed its security strategy as a direct result of losing deals from a lack of confidence in your company security strategy?



*Companies that had lost deals due to poor security strategy

Figure 3

Shifting Responsibility to the Top: CEO and Cybersecurity Leaders

In an era where cybersecurity stakes continue to rise, the role of executive leadership in guiding cybersecurity initiatives is increasingly critical. Notably, 78% of professionals now view cybersecurity as a responsibility that rests at the top, with CEOs and cybersecurity leaders held accountable either jointly or individually for breaches. Executives now actively lead and shape security initiatives, influencing operational strategies and the organization's culture and decision-making ethos.

78% State Security Breach Responsibilities Reside at the Top Leadership Levels

In your opinion, who should be responsible for a security breach?

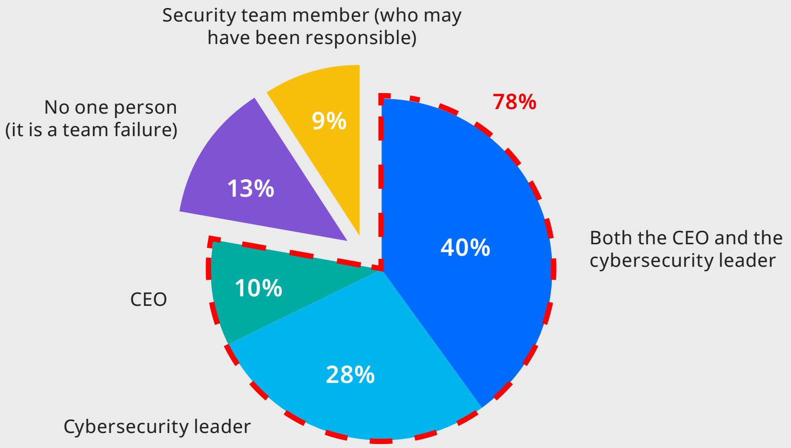


Figure 4

The reasons behind the shift are twofold:

1. The impact of cybersecurity incidents extends beyond IT departments, affecting every facet of a business, from operational continuity to brand reputation.
2. The strategic decisions involved in managing cybersecurity (such as investment in new technologies, balancing risk, and compliance) require a level of oversight and understanding that should reside with top executives.

This reflects a broader trend from recognizing cybersecurity as merely a technical issue to a critical business leadership and risk management component. Almost half (49%) of executives meet either daily or weekly to discuss their company's security status.

49% of Executives Meet Weekly or Daily to Discuss Security Status

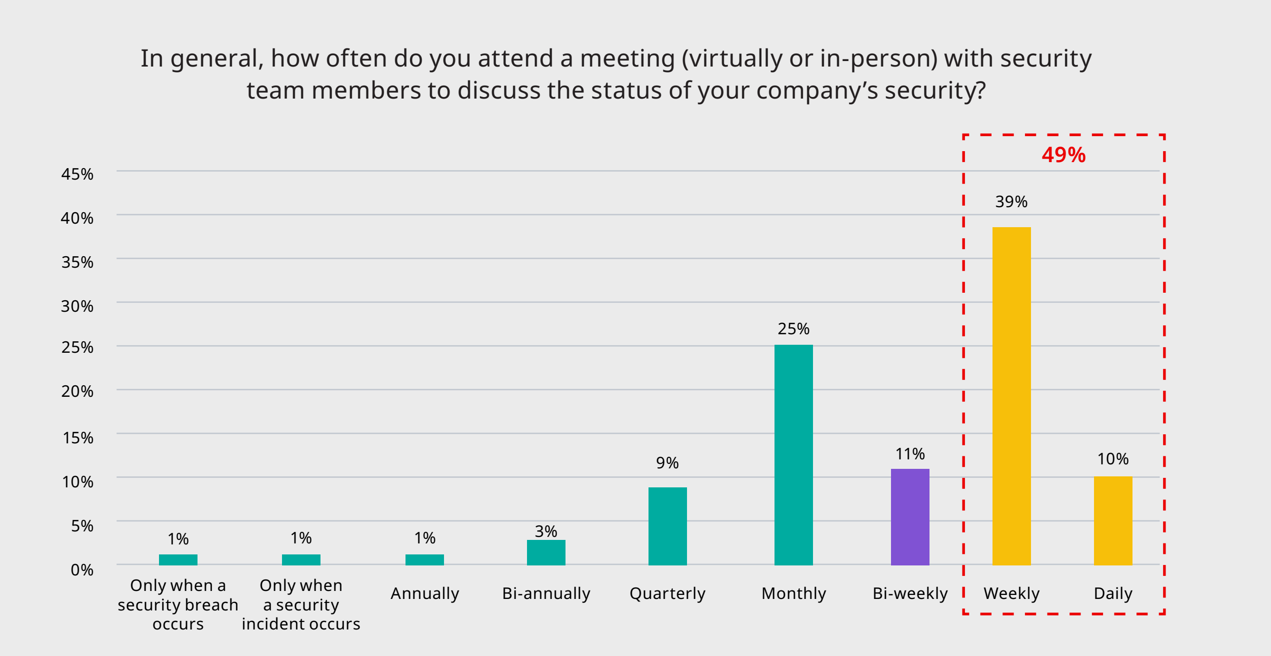


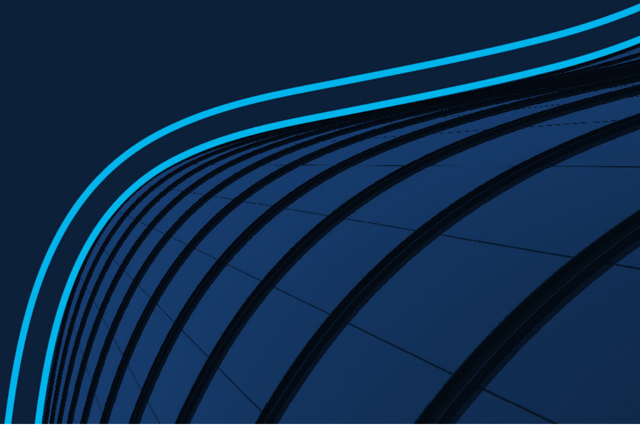
Figure 5

The 2024 cybersecurity landscape is marked by rapid change, driven by external pressures from regulations and customer expectations, and internal shifts in organizational responsibility.

Companies find that staying ahead in this environment requires technological innovation and agility and a top-down commitment to embed cybersecurity into the fabric of business strategy and operations.

03 ___

Security Strategies in Transition



In 2024, security strategies are constantly adapting, a testament to organizations' agile, resilient and responsive nature navigating the intricate web of cyberthreats, regulatory landscapes, and technological innovations.

Reasons Behind Frequent Changes in Security Strategies

The high percentage (95%) of companies altering their cybersecurity strategies within the past year indicates the dynamic nature of the digital threat landscape (Figure 1). This widespread adaptation stems from several factors, each contributing to the evolving security posture of organizations across the globe.

1. Artificial Intelligence

AI has emerged as both a formidable tool in the arsenal of cyber defenders and a sophisticated weapon in the hands of adversaries. With **65% of companies acknowledging AI's role in prompting changes to their cybersecurity strategy**, it's evident that AI-driven threats and solutions are at the forefront of shaping modern security practices (Figure 1). The dual-edged nature of AI necessitates a nuanced approach, integrating advanced AI solutions to augment threat detection and response while staying vigilant against AI-powered attacks.

2. Regulatory Changes

Compliance with evolving regulatory requirements is a major catalyst for change, influencing 98% of organizations (Figure 2). Regulatory frameworks are increasingly stringent, pushing companies to adapt their policies, processes, and product offerings to meet stricter compliance standards. For **25% of businesses**, regulatory pressures have led to the significant step of **removing revenue generating products or services from the market**, highlighting the profound impact of compliance on operational decisions and the bottom line (Figure 2).

3. Budget Adjustments

Cybersecurity budgets are not static; they reflect an organization's strategic priorities and response to the changing threat landscape. The industry is experiencing a clear shift from financial considerations driving security strategies to companies prioritizing proper defense against cyberattacks with **76% of companies experiencing increases to their cybersecurity budget** in response to evolving threats.

76% Reveal Budget Increase Driven by Changing Threat Landscape

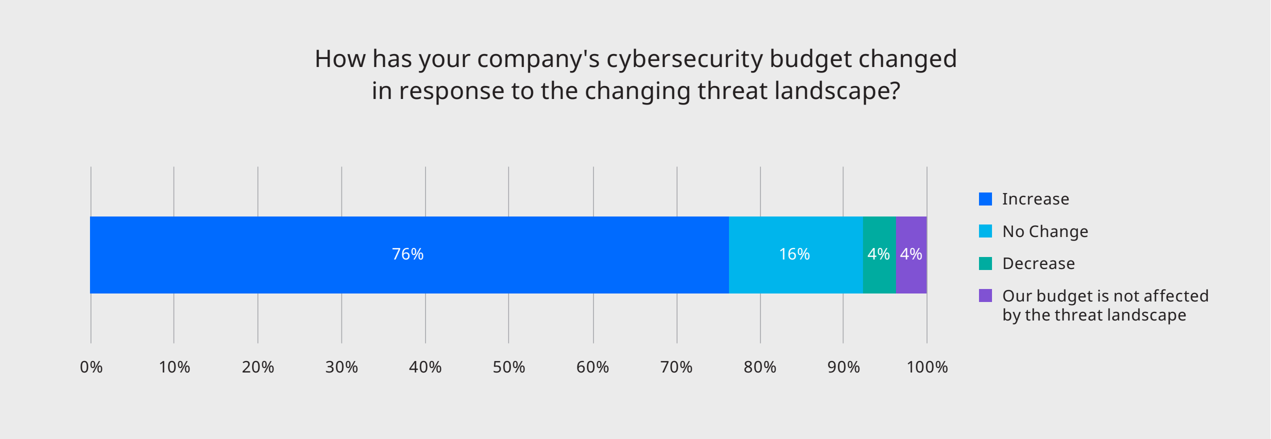


Figure 6

These adjustments enable organizations to invest in new technologies, enhance team capabilities, and bolster their defenses against an array of cyberthreats.

04

Maintaining Compliance While Driving Business Value

Balancing compliance with regulatory requirements and pursuing business value is a perennial challenge for organizations. The stringent demands of compliance can sometimes be at odds with the need for innovation and agility in business operations. Yet, the repercussions of non-compliance — ranging from financial penalties to reputational damage — make it an indispensable aspect of cybersecurity strategy.

The key to navigating this challenge lies in integrating compliance into the broader business strategy, ensuring that security measures match regulatory requirements and support business objectives. This approach requires a continuous dialogue between security teams, executive leadership, and a consistent pulse on regulations, while fostering an environment where compliance is viewed as an enabler of business value rather than a constraint.

The transition in security strategies is a complex interplay of technological advancements, regulatory dynamics, and financial considerations. As organizations strive to remain competitive and secure in the digital era, adapting swiftly to these changing forces is paramount. Integrating AI into security practices, navigating regulatory changes, and strategically allocating budgets are critical components of this adaptive approach, ensuring that companies can maintain compliance while driving forward their business objectives.

05

Success Metrics of Modern Security Teams

In 2024, a significant transformation has occurred in the cybersecurity landscape in terms of strategies, technologies, and measuring success. Modern security teams are evaluated on a broader spectrum of metrics, reflecting a deep integration of cybersecurity into the business fabric.

Nearly 50% Reduction in Deals Lost Due to Security Concerns

A metric of success for modern security teams is the decrease in business opportunities lost due to security concerns. In a year, the **percentage of deals lost** because of perceived inadequacies in a company's cybersecurity posture has **plummeted from 67% to 38%**. This improvement is a testament to more robust security defenses. It also signals a better alignment of security strategies with business objectives.

Deals Lost from Poor Security Strategies Dramatically Reduced From 67% to 38% in Just 12 Months

Has your company ever lost a deal due to a customer's lack of confidence in your company's security strategy?

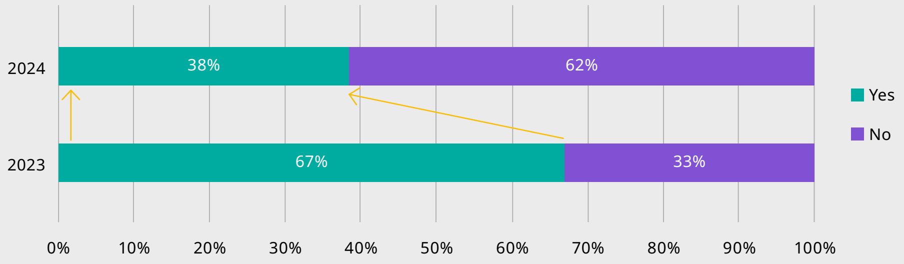


Figure 7

By effectively communicating their security measures and ensuring that they meet the expectations of clients and partners, companies have been able to regain trust and minimize the financial impacts of security vulnerabilities.

Increased Confidence in Security Resources and Budget Allocation

Staying ahead of cybersecurity threats requires vigilance and appropriate resources. In 2024, security professionals have markedly increased confidence regarding the adequacy of resources allocated to them. A significant **96% of companies have adjusted their cybersecurity budgets** in response to the changing threat landscape, with the majority reporting an increase (Figure 5).

This boost in financial resources underlines the growing recognition of cybersecurity as a critical business function that warrants substantial investment. In 2024, 78% of security teams are confident they have the right resources to defend the company from cyberattacks. With these resources, security teams are better equipped to tackle new threats, innovate in their defensive approaches, and enhance the overall security posture of their organizations.

78% Are Confident They Have the Right Resources to Defend The Company from Cyberattacks

In your opinion, does your company have sufficient resources (tools, personnel, expertise, budget, etc.) to properly secure your company from cyberattacks?

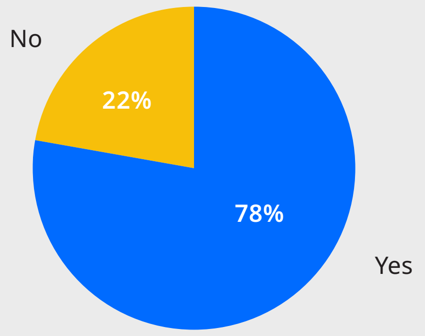


Figure 8

The Perception of Security Effectiveness Among Professionals

The perception of security effectiveness among cybersecurity professionals is a crucial indicator of the health of an organization's security practices. A remarkable 79% of security professionals now rate their security defense as either good or excellent.

79% Rate Their Security Defense as Good or Excellent

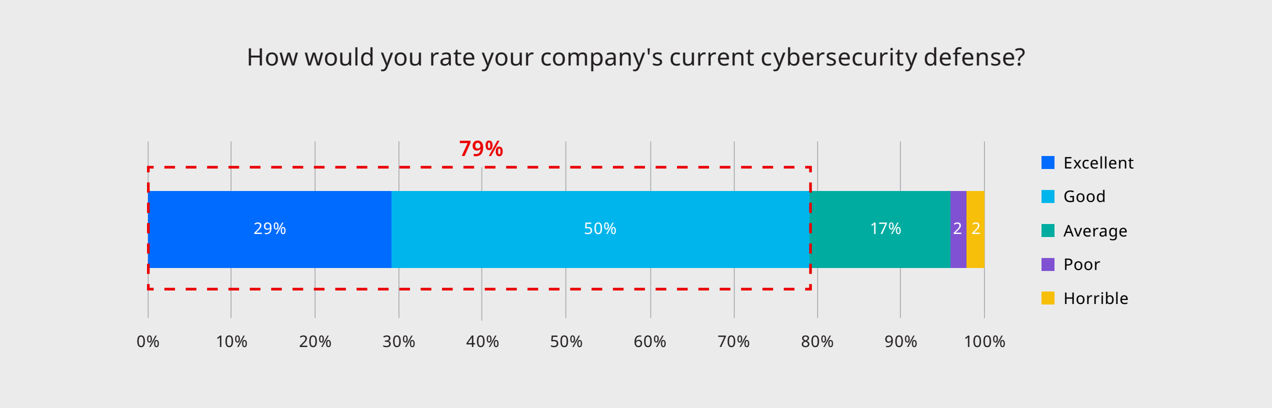


Figure 9

This positive self-assessment reflects the successful implementation of robust security measures and the increasing synergy between security teams and the broader organizational goals. Confidence among security professionals fosters a proactive and resilient security culture within organizations.

The enhanced confidence in security resources and the positive perception of security effectiveness highlight the strides made in equipping teams with the necessary tools and fostering an environment where security is deeply integrated into the organizational ethos. Together, **these metrics paint a picture of a cybersecurity landscape that is more mature, aligned, and effective** in protecting businesses against the myriad of cyberthreats they face today.

06

Bridging the Communication Gap in Cybersecurity

The communication chasm between security teams and non-security executives represents a critical barrier to effective cybersecurity management. This gap can significantly impact an organization's ability to respond effectively to cybersecurity threats and to align security strategies with business objectives. Addressing this gap is essential for enhancing organizational resilience against cyberthreats. It requires a concerted effort to refine how security information is communicated, emphasizing clarity, conciseness, and actionability.

Conveying the Necessity of Specific Security Solutions to Non-Security Executives

One of the main hurdles in cybersecurity communication is the difficulty of explaining the need for specific security solutions to non-security stakeholders. Approximately 59% of cybersecurity professionals report challenges in conveying the importance and necessity of particular security measures to executives who may not have a technical background.

59% Share It Is Difficult to Explain the Need for Specific Security Solutions to Non-security Stakeholders

In your experience, is it difficult to explain the need for a specific security solution to non-security stakeholders (executives, board members, etc.)?

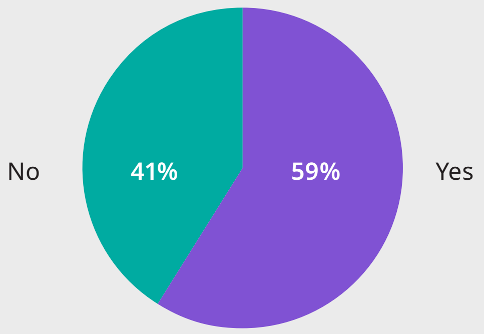


Figure 10

Meanwhile, just 56% of non-security executives understand the regulatory requirements and constraints the company must follow.

Just 56% of Non-security Executives Truly Understand Regulatory Requirements and Constraints the Company Must Adhere To

In your experience, do non-security executives truly understand all the regulatory requirements that the security must comply with?

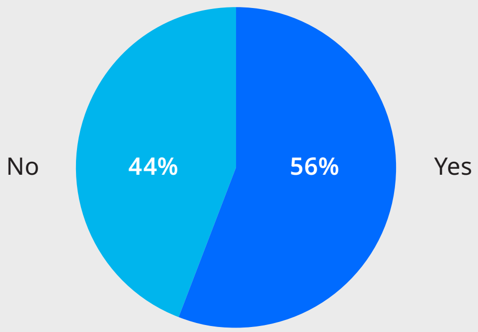


Figure 11

This communication barrier can lead to misunderstandings about the value of investments in cybersecurity, potentially impacting the organization's preparedness and response capabilities.

The Current State of Security Reporting and the Need for Improvement

The effectiveness of security reporting mechanisms plays a pivotal role in bridging the communication gap between security teams and executive leadership. Currently, the primary methods for sharing security information include static reports, meetings, and emails, with 75% of organizations relying on these traditional, time-consuming formats.

75% Are Using Manual and Time Intensive Approaches to Share Security Status Information

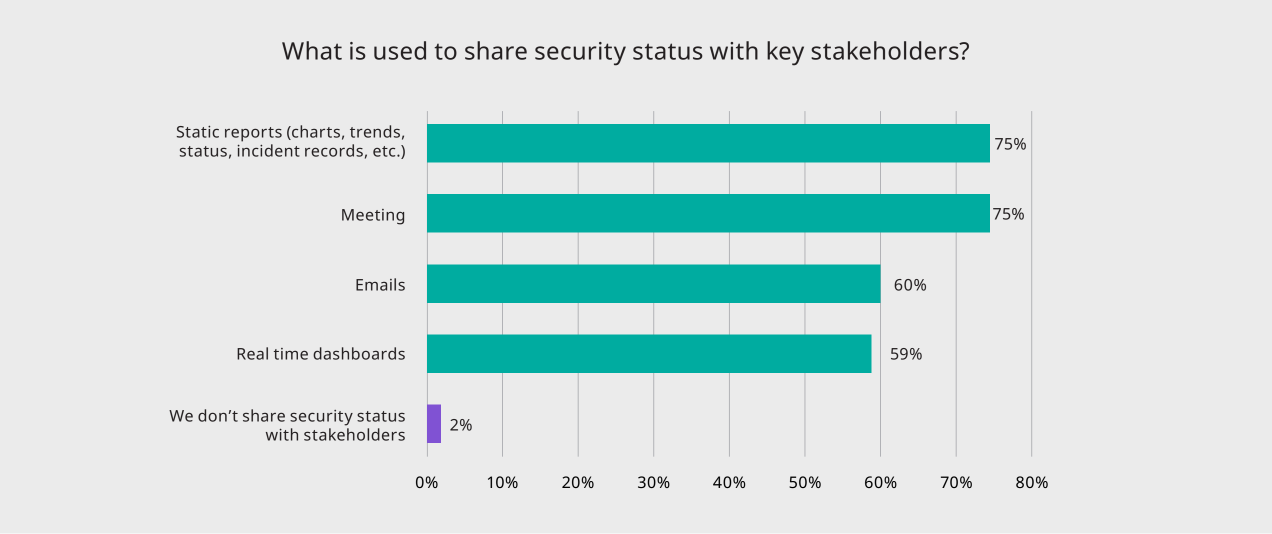


Figure 12

However, only 65% of these reports include critical information such as breaches, incidents, and security risks. Additionally, less than half of respondents are reporting on time to respond (49%), time to detect (48%) and time to recover (45%). All of which are key metrics for evaluating whether the efficacy of an organization's security strategy is declining or improving.

Only 65% Report Critical Information — Breaches, Incidents, and Risk — Less than Half Report Security Operational Metrics

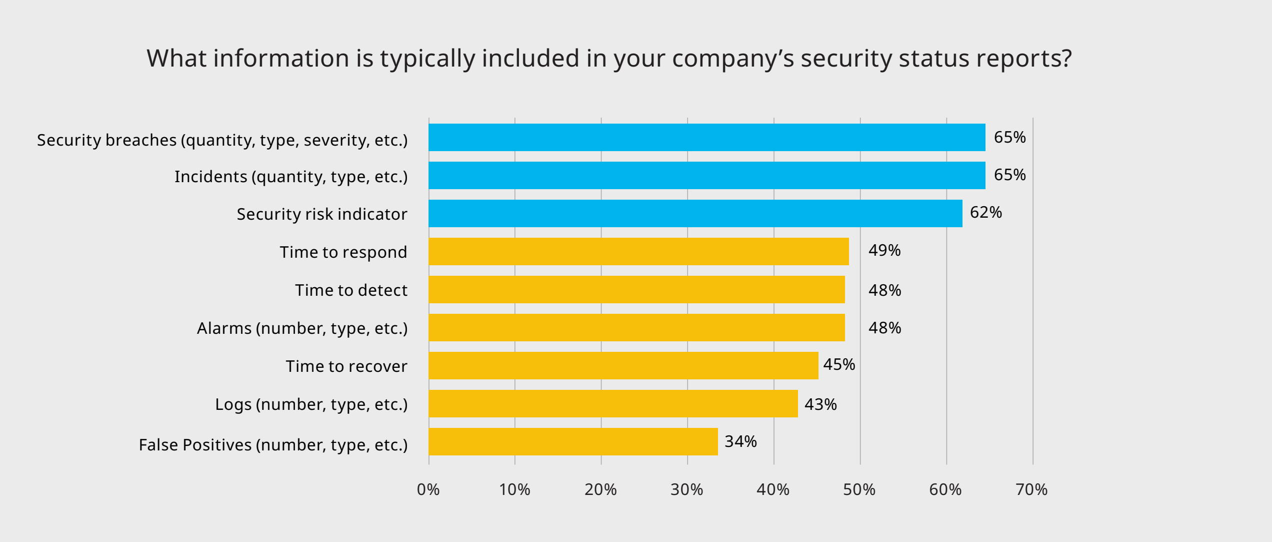


Figure 13

The lack of real-time, actionable data in these reports can hinder timely decision-making and the organization's ability to address security threats proactively. Operational metrics such as time to detect, respond and recover, are key to indicating the efficiency and effectiveness of a security strategy and the tools security teams deploy.

Enhancing Security Communication with Modern Reporting Tools and Practices

Organizations must adopt modern reporting tools and practices that facilitate clear, concise, and actionable communication to bridge the communication gap in cybersecurity effectively. The following recommendations can help enhance the security communication landscape:

1. Implement Real-Time Dashboards

Transitioning from static reports to dynamic, real-time dashboards can provide executives with up-to-the-minute insights into the organization's security posture. These dashboards should highlight key metrics, threat alerts, and compliance status, enabling informed decision-making.

2. Simplify Technical Language

Security reports should translate complex technical jargon into business-centric language that emphasizes the impact of security activities on business objectives. This approach can help non-security executives understand the significance of security investments and initiatives.

3. Enhance Interdepartmental Collaboration

Establishing regular cross-functional meetings that include security teams, IT, compliance, and business units can foster a culture of collaboration and mutual understanding. These meetings can serve as a platform for discussing security challenges, strategies, and business implications.

4. Tailor Communication to Stakeholder Needs

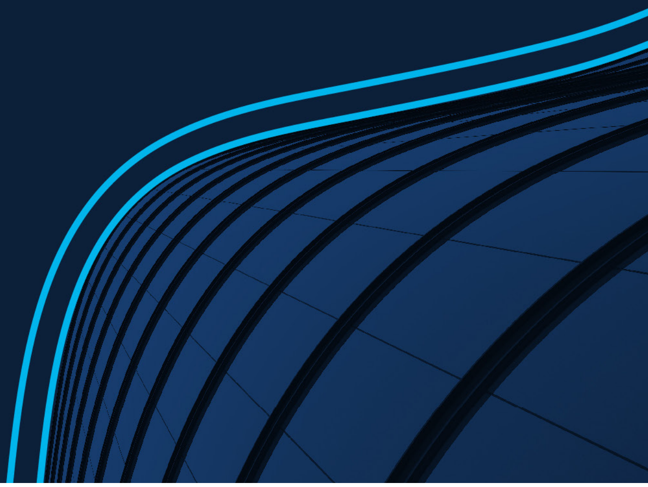
Security communication should be customized to address different executive stakeholders' specific concerns and priorities. By aligning security reporting with business goals, security teams can better demonstrate the value of cybersecurity efforts.

By implementing these recommendations, organizations can significantly improve the effectiveness of cybersecurity communication, ensuring that security strategies are synced with business objectives provides a platform for security leaders to communicate with executive leadership to ensure they are well-informed and engaged in cybersecurity initiatives.

Enhancing communication in cybersecurity is not just about sharing information; it's about fostering a shared understanding and commitment to protecting the organization's sensitive data, infrastructure and reputation.

07 ___

Confronting Resource Constraints with Strategic Choices



Despite a widespread increase in cybersecurity budgets and confidence in security strategies, organizations continue to grapple with resource constraints in 2024. These limitations stem from financial budgets and the availability of skilled cybersecurity professionals. Companies adopt strategic approaches to maximize existing resources and navigate these challenges while ensuring robust security postures. Key strategies for organizations confronting resource constraints include:

Strategies to Manage Limited Resources

One of the most effective strategies to address resource limitations is leveraging cloud infrastructure. In 2024, **51% of organizations report using more secure cloud solutions to manage risk**, given their resource constraints. Cloud providers offer advanced security features that are more cost-effective and easier to manage than on-prem solutions. This shift reduces the burden on internal resources while enhancing security capabilities.

Cybersecurity Resource Shortages Force Companies to Use Cloud Infrastructure and Just Protect High Risk-Items

Given the lack of cybersecurity resources, how does your company manage risk?

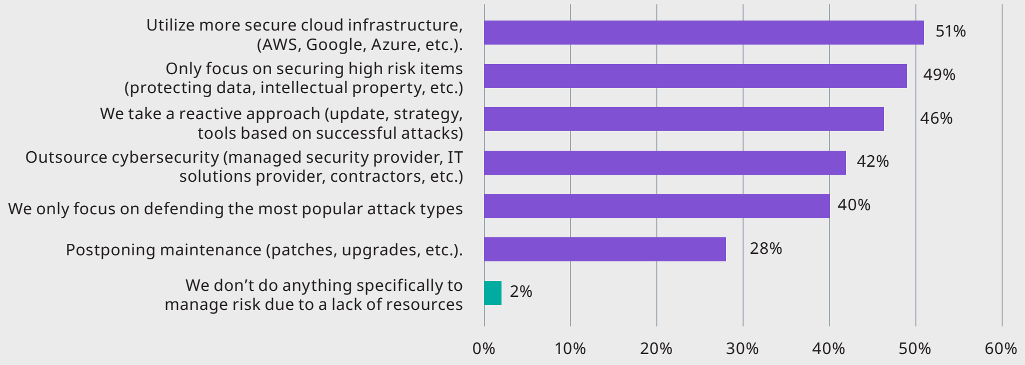


Figure 14

Additionally, focusing on high-risk items has become a priority for 49% of companies. This strategy involves identifying and protecting the most critical assets and data, which, if compromised, could have the most significant impact on the organization. Furthermore, **companies are increasingly channeling investments into advanced technologies and bolstering team capabilities to counter AI-driven threats**.

Reactive vs. Proactive Security Approaches

The decision between adopting a reactive or proactive approach to cybersecurity has significant implications for organizations with resource constraints. A proactive stance involves anticipating and addressing threats and vulnerabilities before they can be exploited. In contrast, a reactive approach focuses on responding to incidents after they occur. While **46% of organizations take a reactive approach due to limited resources** (Figure 13), this strategy can be more costly in the long run, as the impact of cyber incidents can far exceed the initial savings from reduced upfront investments in security.

Outsourcing as a Viable Strategy

Outsourcing cybersecurity functions to managed security service providers (MSSPs) is another strategy gaining traction among organizations facing resource limitations. Approximately 42% of companies now outsource some aspect of their cybersecurity operations (Figure 13). Outsourcing allows organizations to access specialized expertise and advanced security technologies without investing in building these capabilities in-house. This approach alleviates the strain on internal resources and enables organizations to adapt quickly to new threats and technologies.

Taking a Multi-Faceted Approach

Confronting resource constraints in cybersecurity requires a strategic and multi-faceted approach. **By leveraging cloud infrastructure, prioritizing the protection of high-risk assets, and considering outsourcing a viable option, organizations can navigate the challenges posed by limited resources**.

However, these strategies must be part of a broader, proactive security posture that anticipates threats and vulnerabilities rather than merely reacting to them after the fact. As cybersecurity continues to evolve, the ability to make strategic choices in the face of resource constraints will be a defining factor in an organization's resilience against cyberthreats.

08

Moving Toward a Unified Cybersecurity Strategy

Navigating the complexities of cybersecurity in 2024 emphasizes the need for organizations to embrace continuous adaptation and foster enhanced communication. The dynamic nature of the cybersecurity domain demands an agile approach, where strategies evolve with emerging threats, technological advancements, and shifting regulatory requirements.

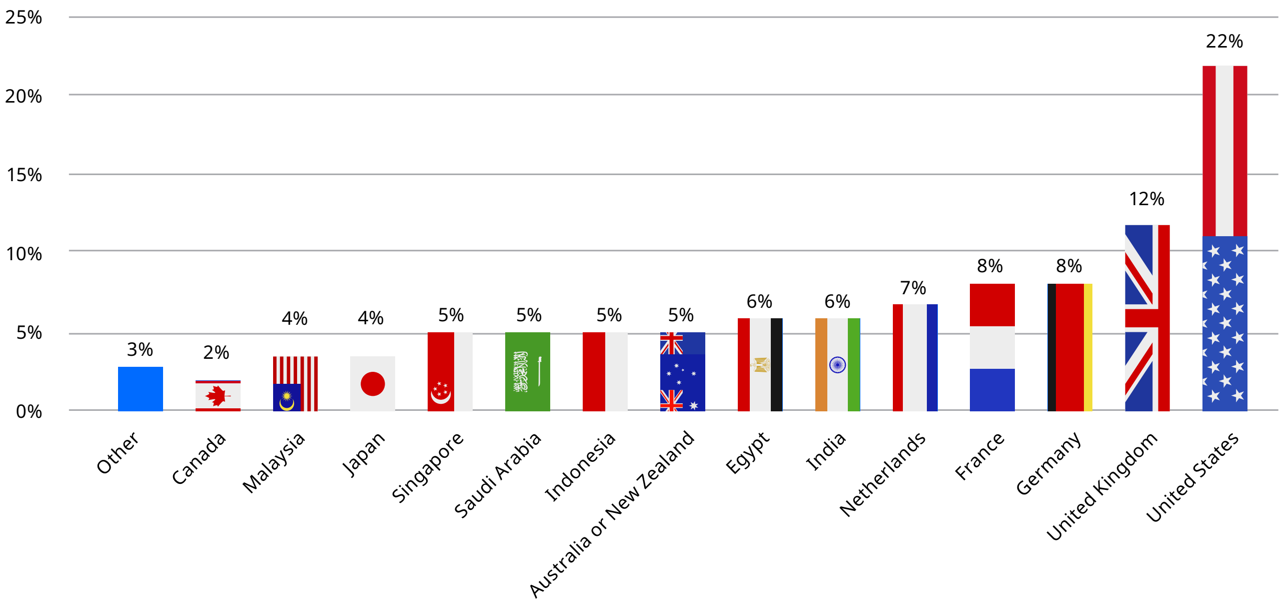
Executive leadership is pivotal in this process, not only for allocating resources and setting strategic priorities, but also for cultivating a culture of security that permeates every level of the organization. This engagement is crucial in bridging the communication gap between technical teams and business stakeholders, ensuring that cybersecurity is integrated into the broader business strategy.

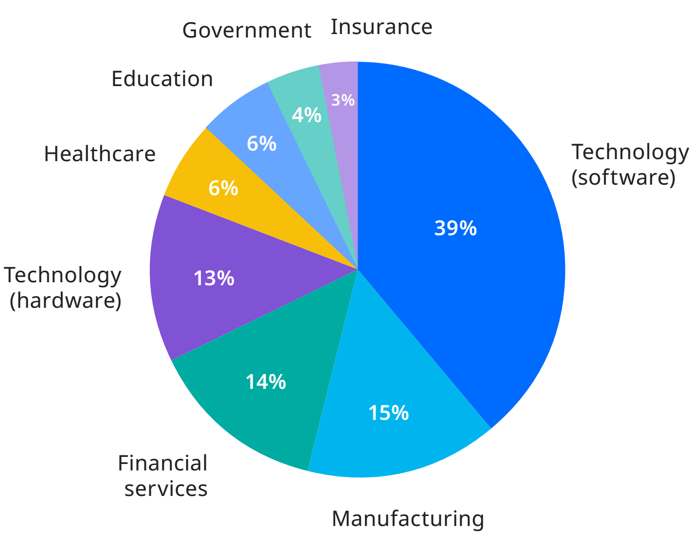
Looking ahead, the ability to anticipate and prepare for future challenges in cybersecurity will set resilient organizations apart. Achieving success will require companies to stay abreast of technological developments while understanding the socio-political factors that shape the cyberthreat environment.

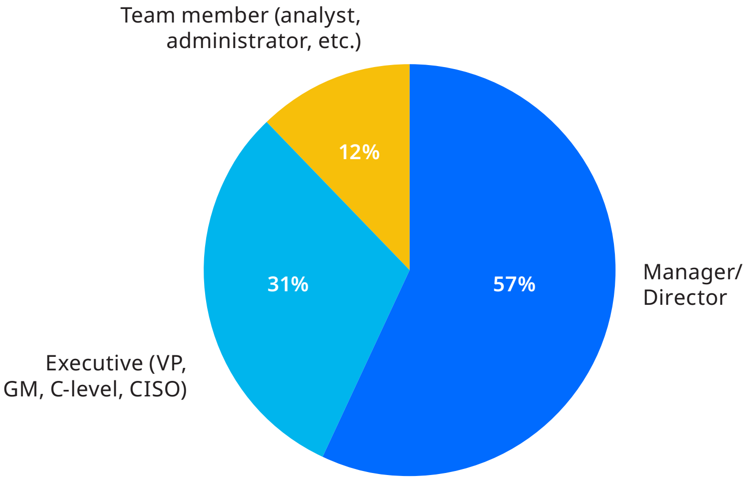
A unified cybersecurity strategy that aligns with organizational goals, promotes proactive risk management, and leverages the collective strength of the entire workforce will be indispensable in navigating the cyber terrain of tomorrow.

Methodology

LogRhythm sought to understand what external factors are affecting companies' security strategies. In partnership with Dimensional Research, LogRhythm surveyed a total of **1176 qualified participants**. Participants were executives and security professionals at medium to enterprise companies from over **20 countries across 5 continents**. The research investigated security team resources, budget, confidence, and breach responsibility.







About LogRhythm

LogRhythm helps security teams stop breaches by turning disconnected data and signals into trustworthy insights. From connecting the dots across diverse log and threat intelligence sources to using sophisticated machine learning that spots suspicious anomalies in network traffic and user behavior, LogRhythm accurately pinpoints cyberthreats and empowers professionals to respond with speed and efficiency.

With cloud-native and self-hosted deployment flexibility, out-of-the-box integrations, and advisory services, LogRhythm makes it easy to realize value quickly and adapt to an ever-evolving threat landscape. Together, LogRhythm and our customers confidently monitor, detect, investigate, and respond to cyberattacks.

Learn more at logrhythm.com.

www.logrhythm.com // info@logrhythm.com

United States: 1.866.384.0713 // United Kingdom: +44 (0)1628 918 300
Singapore: +65 6222 8110 // Australia: +61 2 8019 7185
Middle East: +97155 642 2224