TISS
CYBERSECURITY
INSIGHTS

TISS

CYBERSECURITY MARKET INSIGHTS REPORT 2025

TRILLIUM
INFORMATION SECURITY SYSTEMS

TABLE OF CONTENTS

ABOUT THIS REPORT

Cybersecurity Market Insights Report 2025 is a cybersecurity intelligence resource developed by Trillium Information Security Systems to help senior cybersecurity leaders, CISOs, and executive decision-makers to make informed decisions on investment planning, risk prioritization, and strategic direction for 2026.

HOW TO READ THIS REPORT

Each section in this report follows a consistent structure: a contextual introduction that establishes what the data covers and why it matters, followed by the data findings themselves, and concludes with analytical interpretation and leadership implications.

DISCLAIMER

This report is based on survey responses collected from 131 organizations across industries and reflects the perspectives, experiences, and self-reported data of participating respondents. While the findings provide meaningful insights into current cybersecurity trends and challenges, they should not be interpreted as a definitive or exhaustive representation of the broader market.

Variations may exist due to differences in organizational context, geography, industry, and maturity levels. The analysis and conclusions presented in this report are intended to offer directional guidance and informed perspectives to support decision-making, rather than precise measurements of industry-wide performance.

Where relevant, the report distinguishes between reported data and analytical interpretation to ensure clarity between observed findings and derived insights.

EXECUTIVE SUMMARY

Cybersecurity has entered a new phase where whether to invest in cybersecurity is no longer the fundamental question, according to 131 organisations surveyed in this study.

The pressing challenge now is to ensure that the increasing investments are translated into measurable risk reduction, improved security outcomes, and stronger operational efficiency.

Today, organizations operate in an environment shaped by:

- Increasing reliance on digital infrastructure and cloud ecosystems
- Expanding attack surfaces due to remote work and third-party dependencies
- A threat landscape that increasingly targets human behavior, identity, and access

This report highlights a set of critical challenges that senior leaders must address as they plan for 2026. While these challenges are not new, the data indicates that they have intensified and, in some areas, become more pronounced compared to prior years of insights.

WHAT LEADERS MUST ADDRESS IN 2026

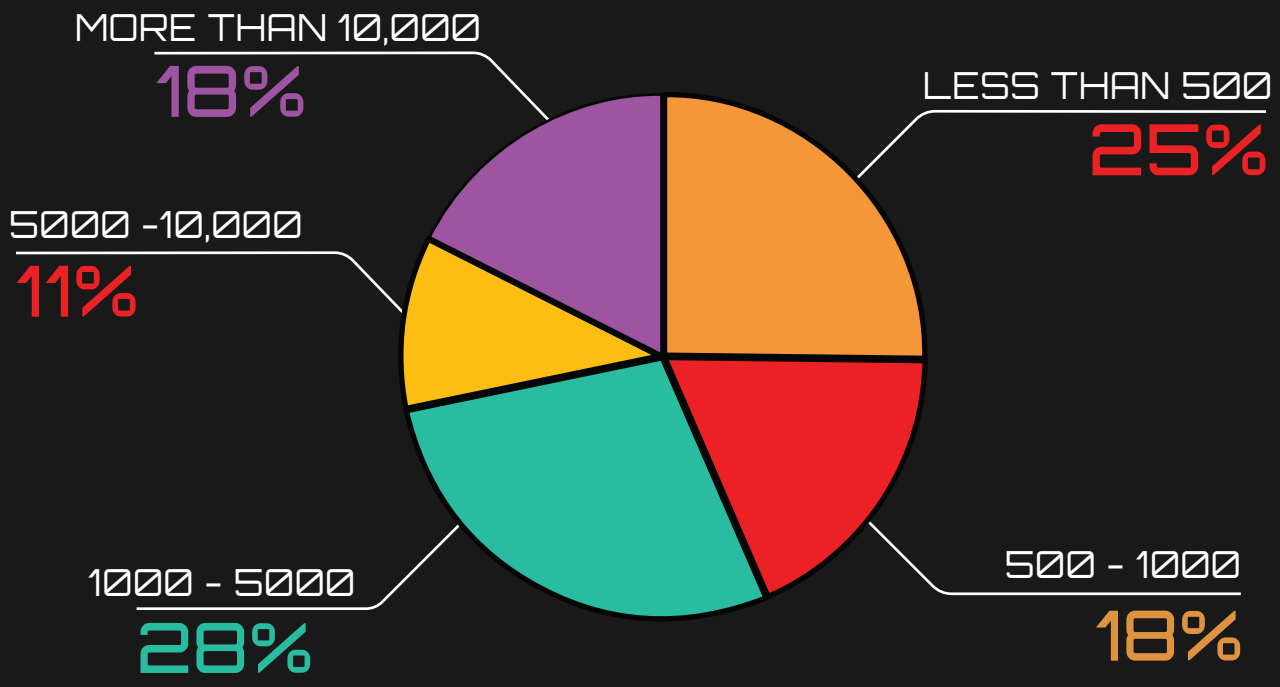
CHALLENGE	LEADERSHIP ACTION
Security budgets are rising without proportional risk reduction	Position security investments to deliver quantified risk reduction and demonstrable business impact
Security teams lack the scale to manage growing complexity manually	Establish operating models centered on automation, integration, and scalability
Human-centric threats and attacks continue to dominate	Place identity, access, and behavioral risk at the center of the security strategy
Organizational silos are driving gaps in defense execution	Position cybersecurity as an enterprise-wide operational risk, not a functional issue
Fragmentation across security tools and platforms is limiting visibility and control	Rationalize and consolidate toward integrated, platform-based security architectures
Security effectiveness is assumed rather than proven	Embed continuous validation, testing, and performance measurement across controls

SURVEY OVERVIEW & RESPONDENT PROFILE

CONTEXT

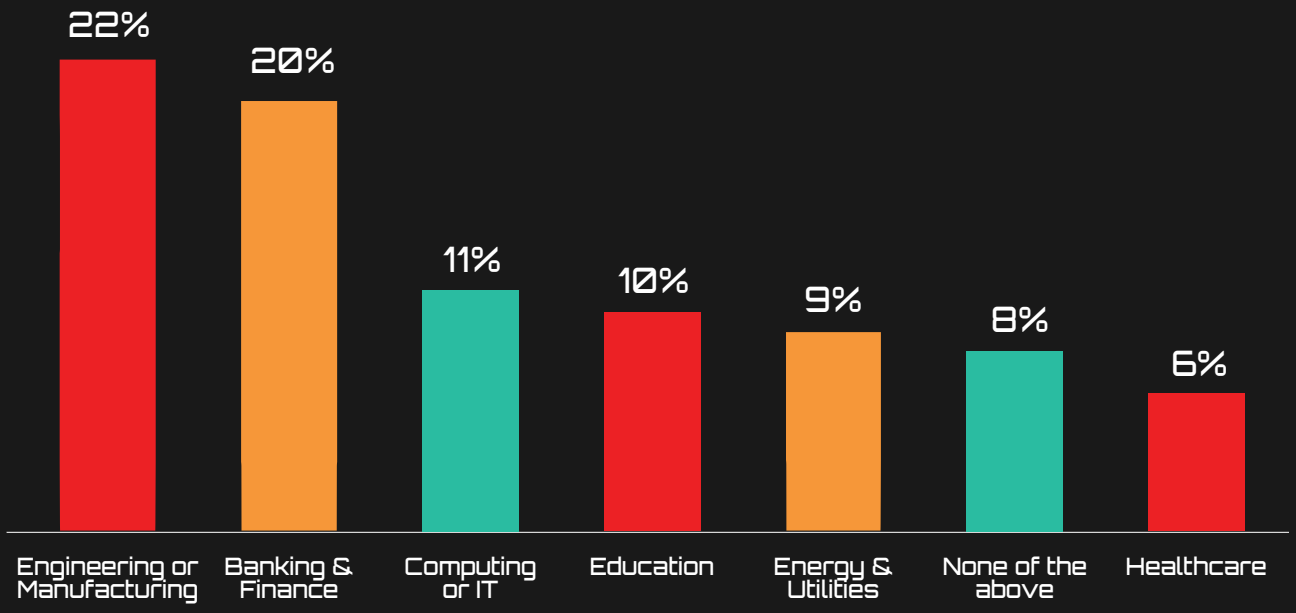
This report is based on responses from 131 organizations across a range of industries and organizational sizes, providing a cross-sectional view of how cybersecurity is being managed across different operating environments.

ORGANIZATION SIZE DISTRIBUTION



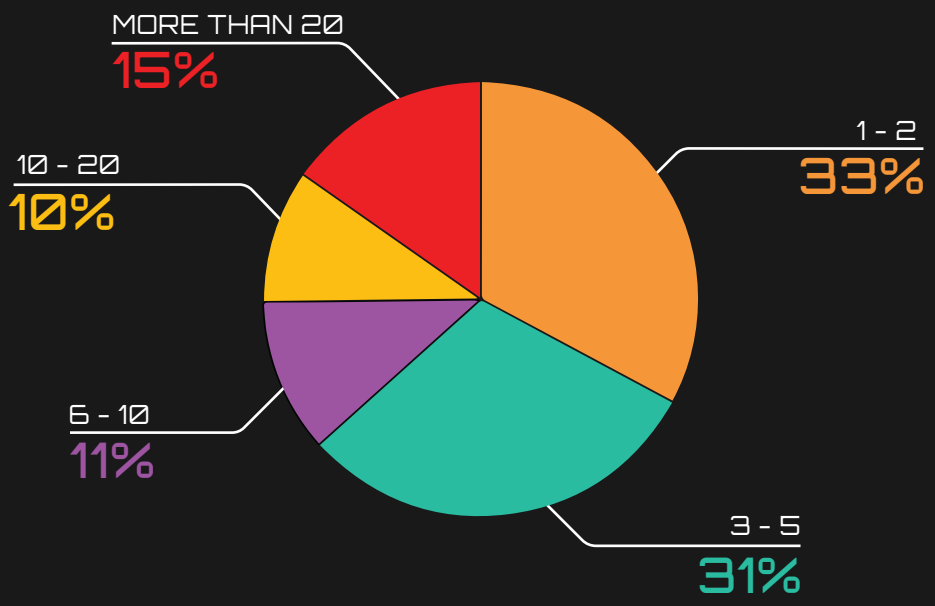
The respondent base is distributed across small, mid-sized, and large organizations, with the largest concentration in the 1,000–5,000 employee segment.

INDUSTRY REPRESENTATION



Participation spans multiple industries, with the highest representation from Engineering & Manufacturing and Accountancy, Banking & Finance.

SECURITY TEAM SIZE



Most organizations operate with small security teams, with 63% having five or fewer dedicated cybersecurity professionals.

NOTE ON INTERPRETATION

The findings presented in this report reflect the composition and responses of participating organizations and should be interpreted as directional insights rather than a statistically representative view of the broader cybersecurity market.

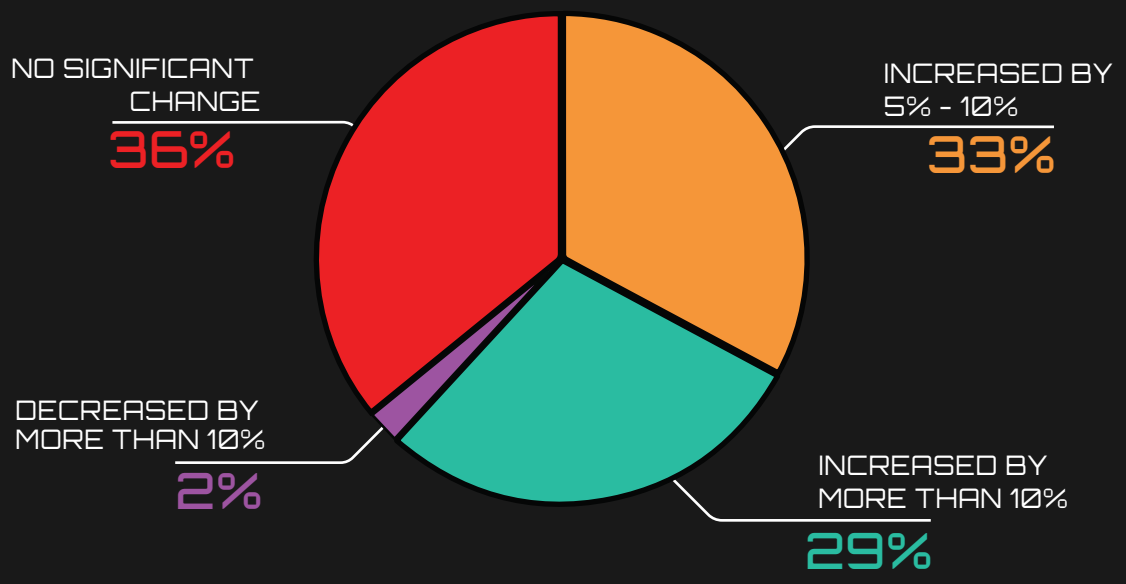
KEY MARKET OBSERVATIONS

Our 2025 survey reveals a set of consistent patterns across investment, threat exposure, operational capacity, and organizational readiness. These observations are derived directly from respondent data and are explored in greater detail in subsequent sections of the report.

1. CYBERSECURITY INVESTMENT IS SUSTAINED, NOT REACTIVE

Respondents were asked to report how their organization's cybersecurity budget changed in 2025.

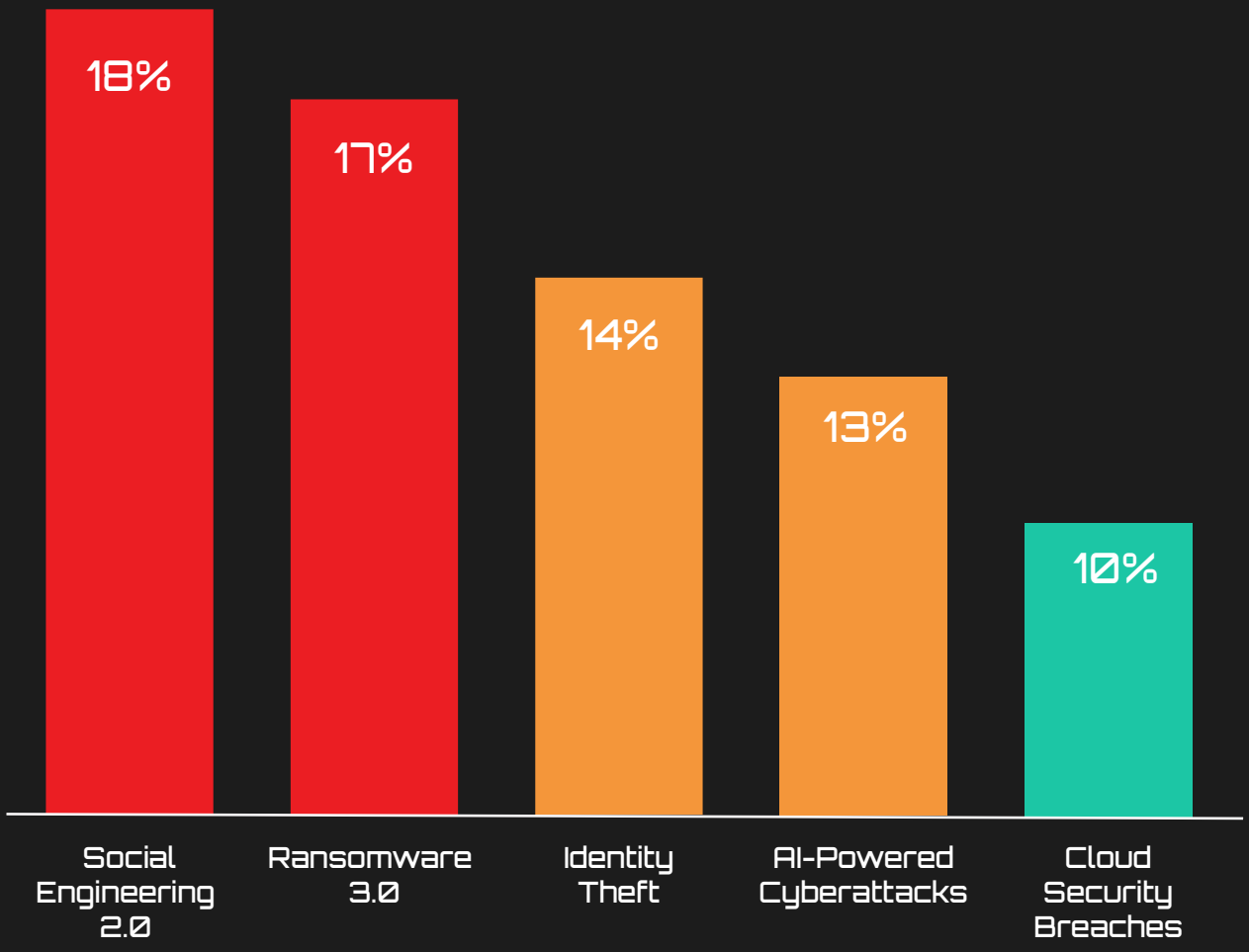
CHANGE IN CYBERSECUEITY BUDGET 2025



WHAT THIS INDICATES

Cybersecurity investment has stabilized as a core operational commitment, with ~98% organizations either maintaining or increasing spend.

2. THREAT ACTIVITY IS CONCENTRATED AROUND IDENTITY AND HUMAN EXPLOITATION

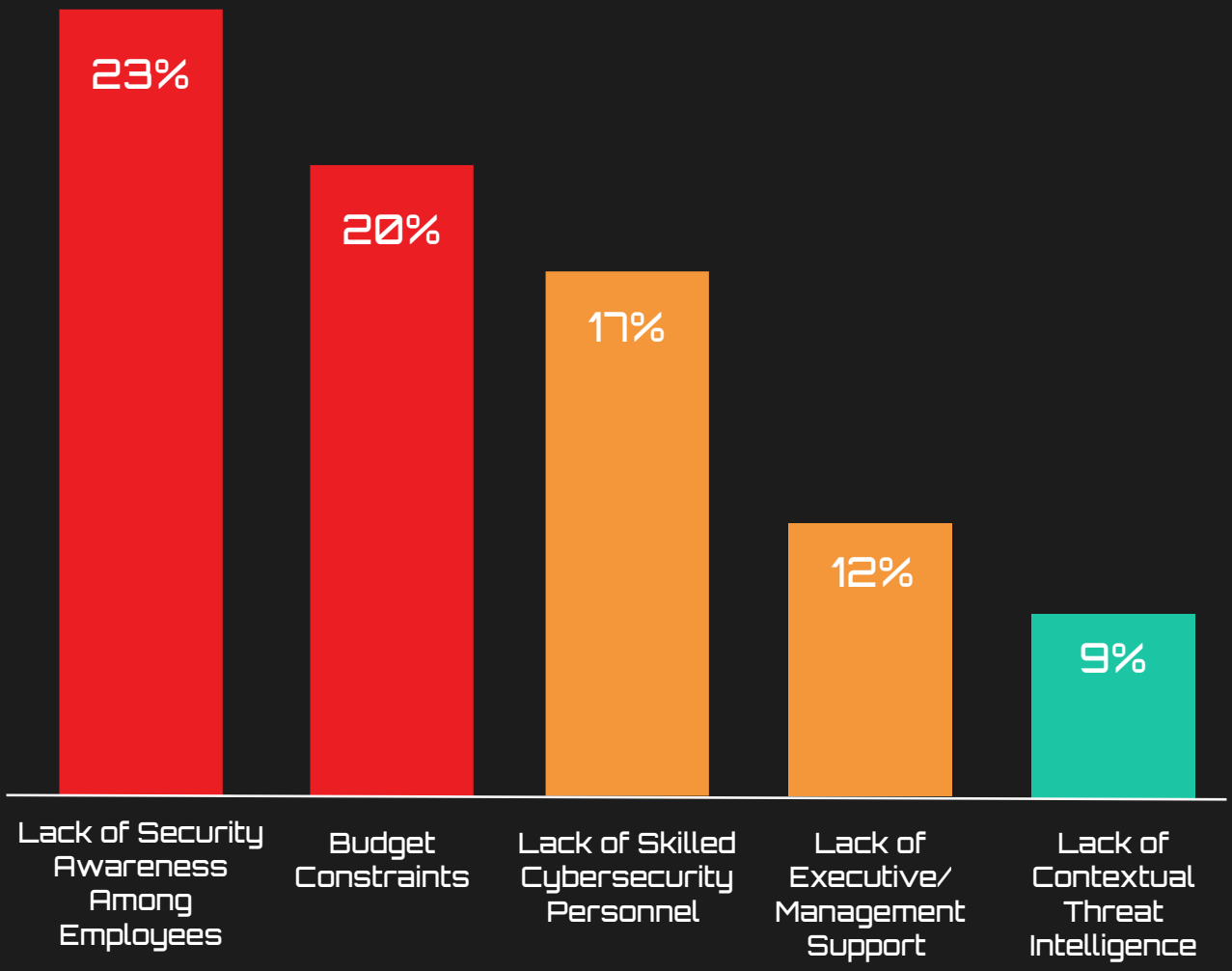


WHAT THIS INDICATES

The most prominent threats are those that exploit identity, credentials, and human behavior, rather than relying primarily on technical vulnerabilities.

3. INTERNAL BARRIERS ARE DOMINATED BY ORGANIZATIONAL, NOT TECHNICAL FACTORS

Respondents were asked to identify the key barriers preventing their organization from effectively defending against cyber threats. As multiple selections were allowed, the results reflect the frequency with which each barrier was cited.



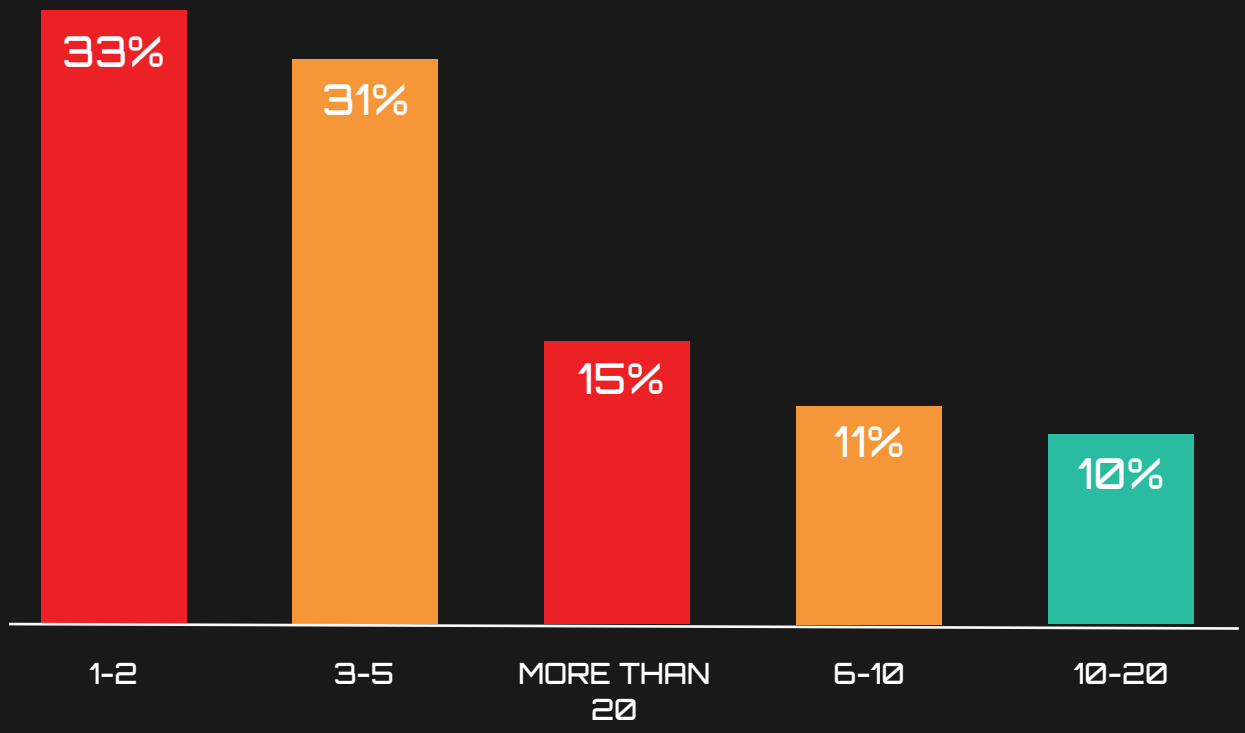
Respondents were asked to identify the key barriers preventing effective defense against cyber threats. As multiple selections were allowed, the results reflect the frequency with which each barrier was cited.

WHAT THIS INDICATES

The primary constraints on cybersecurity effectiveness are organizational and capability-driven, rather than purely technical limitations.

4. SECURITY TEAMS OPERATE WITH LIMITED CAPACITY

SECURITY TEAM SIZE DISTRIBUTION 2025

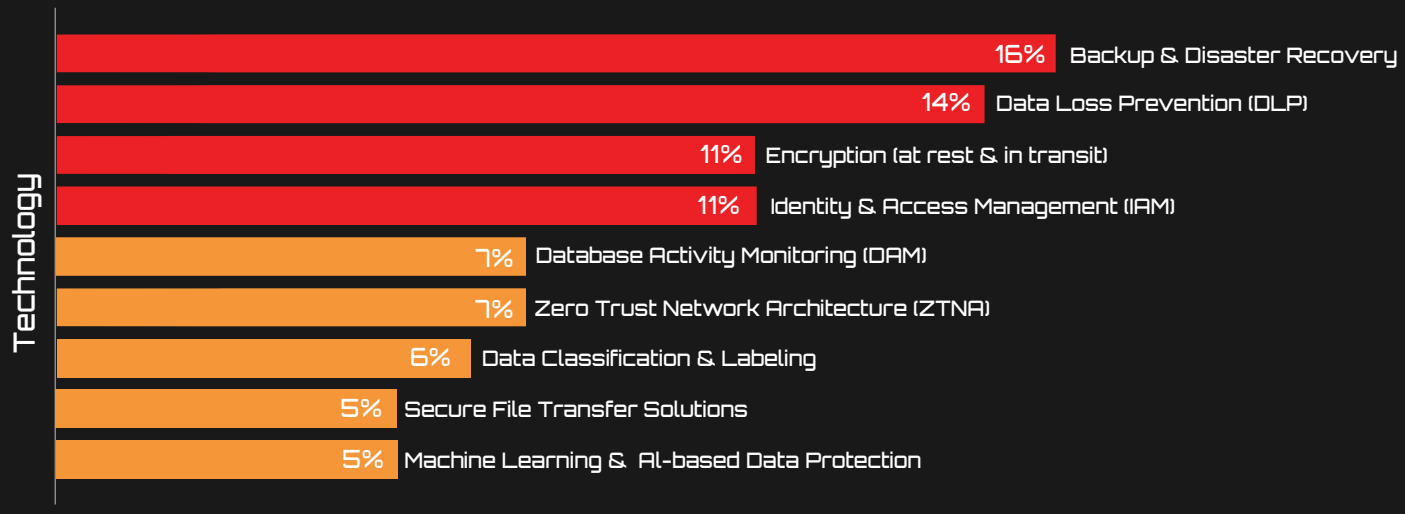


Security teams are heavily concentrated at the lower end of the scale, with the majority of organizations operating with five or fewer dedicated professionals, and only a small proportion having teams larger than 20.

WHAT THIS INDICATES

Security operations are being managed within limited human capacity, requiring organizations to balance increasing threat complexity with constrained resources.

TECHNOLOGY ADOPTION IS BROAD BUT DISTRIBUTED ACROSS MULTIPLE DOMAIN



Investment is concentrated around foundational controls such as backup & recovery, data loss prevention (DLP), encryption, and identity & access management (IAM), while more advanced or emerging technologies show comparatively lower adoption.

WHAT THIS INDICATES

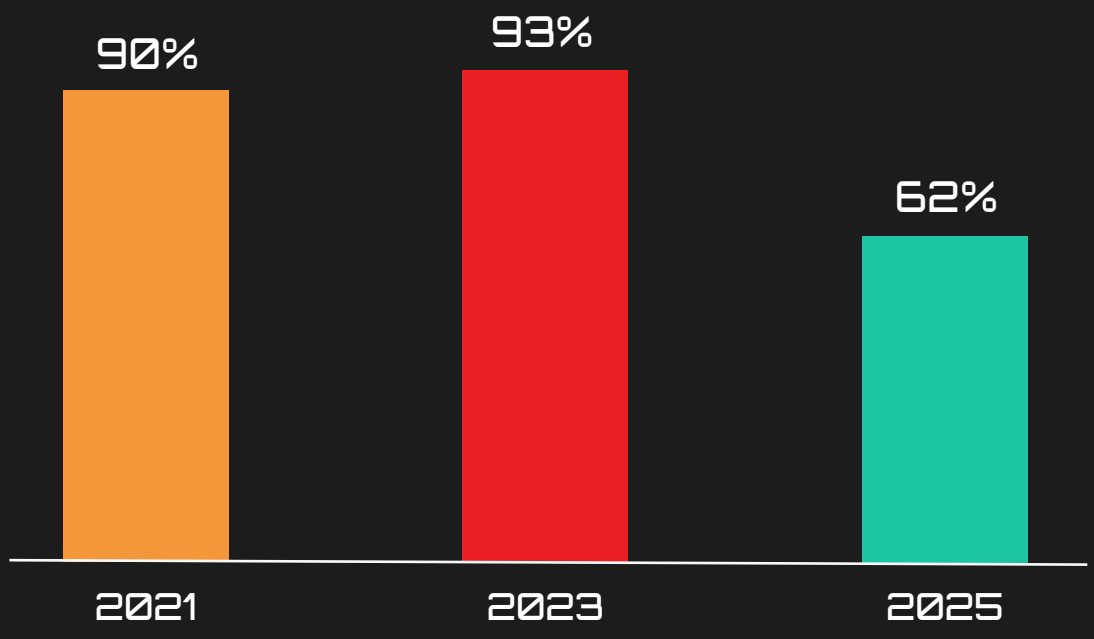
Organizations are prioritizing core data protection capabilities that address immediate operational and risk requirements, with more advanced architectures and emerging technologies being adopted more selectively.

EVOLUTION OF CYBERSECURITY TRENDS (2019-2025)

Cybersecurity trends have evolved over multiple survey cycles conducted by Trillium Information Security Systems.

While survey structures have varied across years, consistent patterns emerge that indicate how organizational priorities, threat exposure, and operational challenges have changed over time.

CYBERSECURITY INVESTMENT ALONG THE YEARS



INSIGHT

Cybersecurity investment has remained consistently strong over time, but the rate of increase has moderated in 2025, indicating a transition from rapid expansion to a more stable investment baseline.

PERSISTENT HUMAN RISK

YEAR	TOP BARRIER
2019	Employee Awareness
2021	Employee Awareness
2023	Employee Awareness
2025	Employee Awareness

INSIGHT

Human-related risks have consistently remained the most significant barrier to cybersecurity effectiveness, despite ongoing investments in awareness and training programs.

SHIFT IN THREAT LANDSCAPE

YEAR	TOP BARRIER
2019	Technical (e.g., unpatched systems, SQL injection)
2021	Phishing / Social Engineering
2023	Phishing / Ransomware
2025	Social Engineering / Identity / AI-driven attacks

INSIGHT

The threat landscape has progressively shifted from technical vulnerabilities toward attacks targeting identity, access, and human behavior.

RECURRING ORGANIZATIONAL BARRIERS

YEAR	KEY BARRIERS
2019	Awareness, Budget, Skills
2021	Awareness, Skills
2023	Awareness, Budget, Skills
2025	Awareness, Budget, Skills

INSIGHT

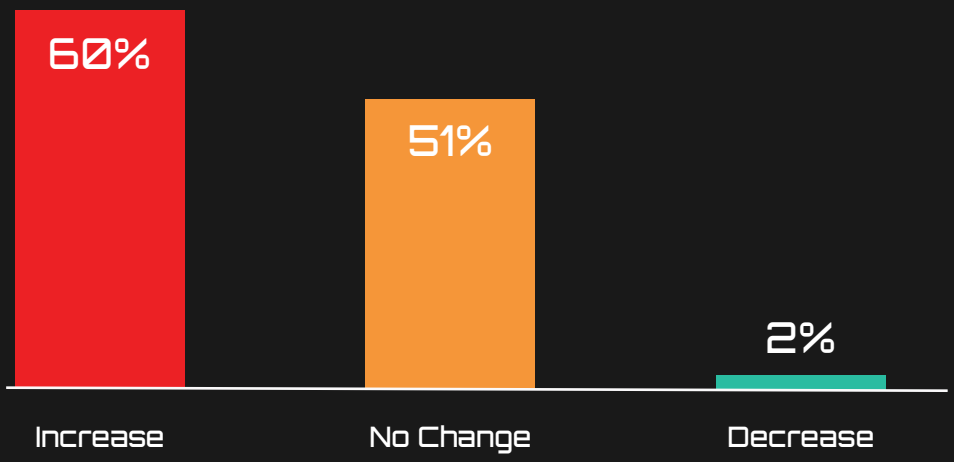
Core organizational challenges, including awareness gaps, budget constraints, and skill shortages have remained consistent across survey cycles, indicating limited structural progress in addressing these issues.

The following sections examine these patterns in detail, providing a deeper view of the underlying data and their implications for cybersecurity strategy and execution.

CYBERSECURITY INVESTMENT TRENDS

Cybersecurity budget allocation provides a direct view into how organizations are structuring security as an operational priority.

MARKET REALITY



Cybersecurity budgets are largely stable or increasing, with minimal contraction across organizations.

STRATEGIC INSIGHT

There are primarily two distinct investment states.

1. Most organizations continue to increase budgets, indicating ongoing capability build-out.
2. At the same time, a considerable segment has reached a steady state, where budgets are maintained rather than expanded.

This split highlights a transition in the market:

- Some organizations are still building security capability
- Others are focused on operationalizing and extracting value from existing investments

The absence of meaningful budget reductions reinforces that cybersecurity is now embedded within core financial planning.

LEADERSHIP IMPLICATION

Cybersecurity leaders must recognize that increased spending and sustained spending require different strategies.

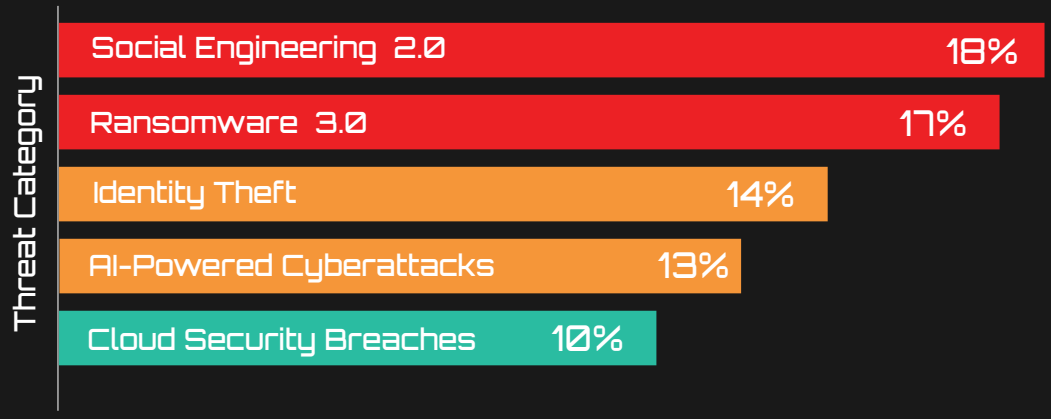
- Organizations still increasing budgets must ensure investments are prioritized and structured, not reactive
- Organizations with stable budgets must focus on maximizing effectiveness of existing capabilities

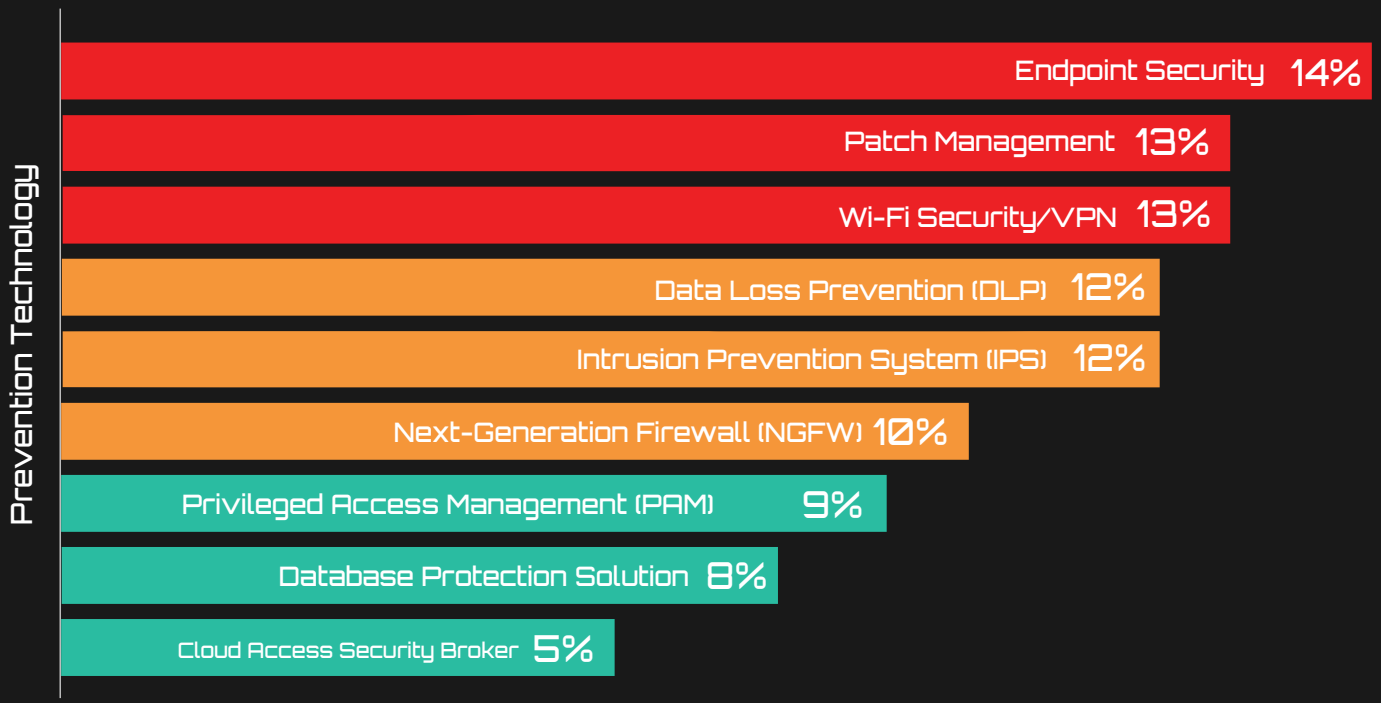
The challenge is no longer how much to spend, but how effectively that spend translates into measurable risk reduction.

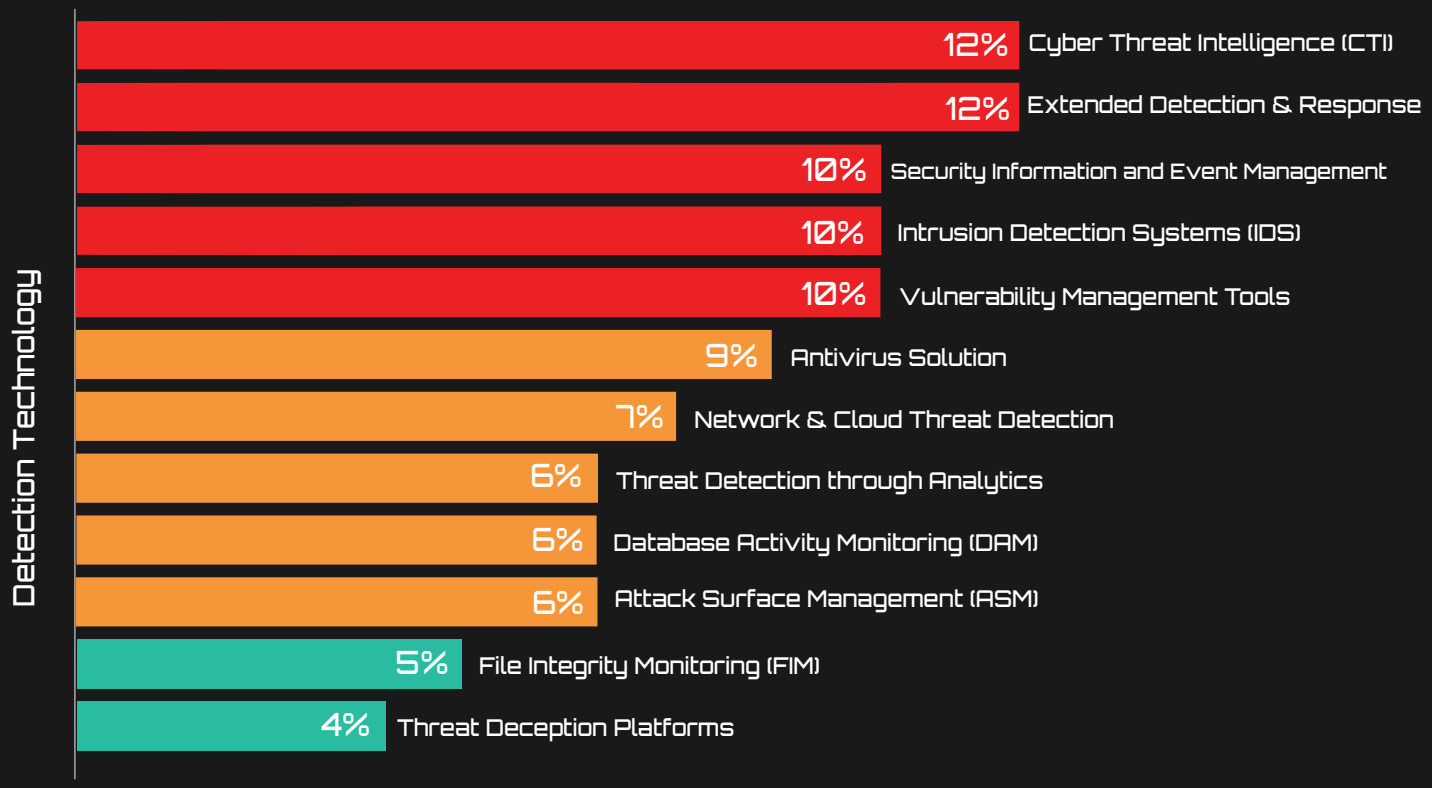
THREAT LANDSCAPE & SECURITY TECHNOLOGY PRIORITIES

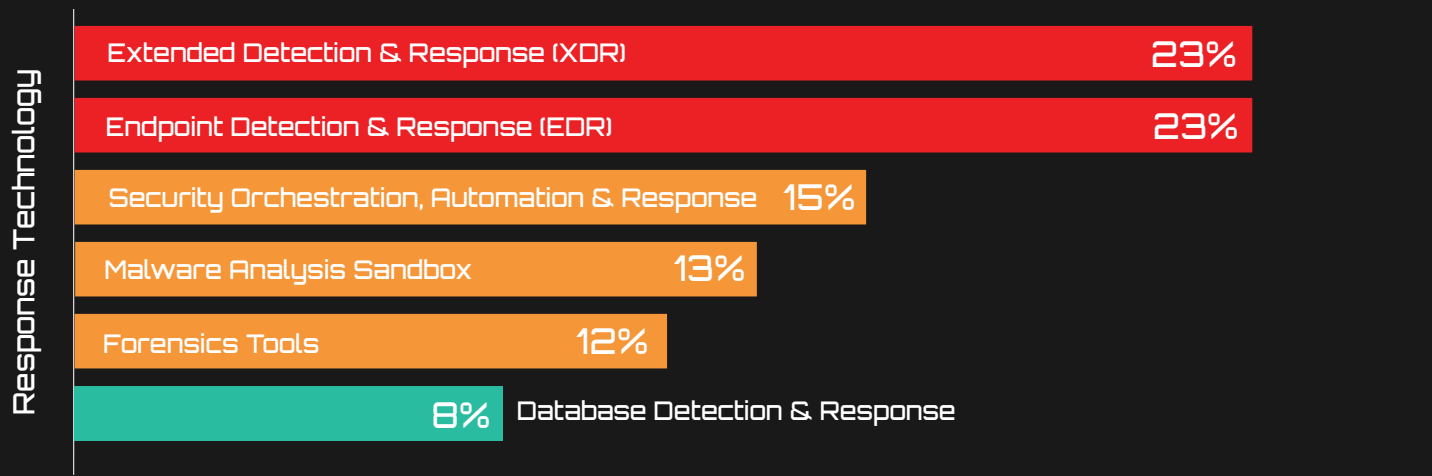
The threat landscape reflects the types of risks organizations are prioritizing based on their exposure and experience. In parallel, planned investments in prevention, detection, and response technologies indicate how organizations are aligning their defenses to address these risks.

MARKET REALITY






Detection Technology
12% Cyber Threat Intelligence (CTI)
12% Extended Detection & Response
10% Security Information and Event Management
10% Intrusion Detection Systems (IDS)
10% Vulnerability Management Tools
9% Antivirus Solution
7% Network & Cloud Threat Detection
6% Threat Detection through Analytics
6% Database Activity Monitoring (DAM)
6% Attack Surface Management (ASM)
5% File Integrity Monitoring (FIM)
4% Threat Deception Platforms


Response Technology
Extended Detection & Response (XDR) 23%
Endpoint Detection & Response (EDR) 23%
Security Orchestration, Automation & Response 15%
Malware Analysis Sandbox 13%
Forensics Tools 12%
8% Database Detection & Response

STRATEGIC INSIGHT

The data shows a broad expansion of cybersecurity capabilities across prevention, detection, and response, with a clear concentration in detection and response technologies.

High adoption of endpoint security, Endpoint Detection & Response (EDR), Extended Detection & Response (XDR), and Cyber Threat Intelligence (CTI) indicates that organizations are prioritizing the ability to detect and respond to threats once they occur.

However, when compared with the most frequently reported threats particularly Social Engineering 2.0, Ransomware 3.0, and Identity Theft there is relatively lower emphasis on identity and access focused preventive controls such as Privileged Access Management (PAM) and Cloud Access Security Broker (CASB).

This indicates a structural imbalance:

- Threats are primarily identity and human-driven
- Investments are more heavily focused on post compromise detection and response

As a result, organizations are strengthening response capabilities but are not proportionally reducing the likelihood of successful attacks.

LEADERSHIP IMPLICATION

Cybersecurity leaders must rebalance their security approach toward preventive controls aligned with identity and human-centric threats.

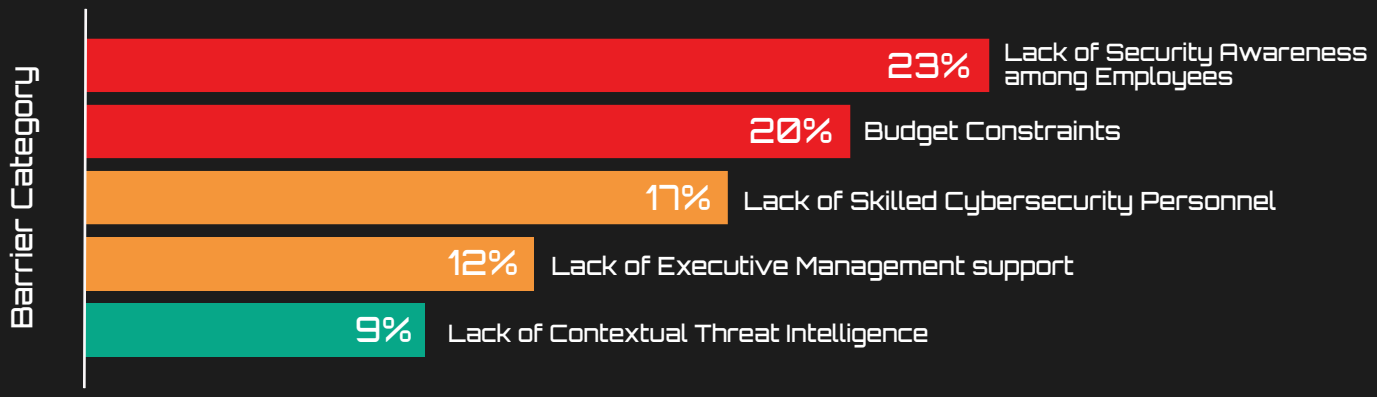
- Strengthen identity and access controls, including Privileged Access Management (PAM) and cloud security
- Reduce over-reliance on detection and response as the primary defense layer
- Ensure prevention, detection, and response capabilities are aligned to address the same threat vectors

Improving detection and response alone will not reduce risk unless the underlying drivers of identity- and human-centric attacks are addressed.

INTERNAL BARRIERS ANALYSIS

Understanding internal barriers provides insight into why organizations struggle to translate cybersecurity investments and capabilities into effective defense outcomes.

MARKET REALITY



STRATEGIC INSIGHT

The primary barriers to effective cybersecurity are internal and organizational rather than purely technical.

Employee awareness emerges as the most significant constraint, highlighting the continued challenge of managing human risk. At the same time, budget limitations and skill shortages remain persistent issues, reinforcing that organizations are operating under both financial and resource constraints.

The presence of executive support as a reported barrier further suggests that cybersecurity is not always fully aligned with broader business priorities, impacting decision-making and execution.

Collectively, these factors indicate that improving cybersecurity effectiveness is not solely dependent on technology adoption, but on addressing structural and organizational gaps.

LEADERSHIP IMPLICATION

Cybersecurity leaders must focus on addressing internal execution barriers alongside external threats.

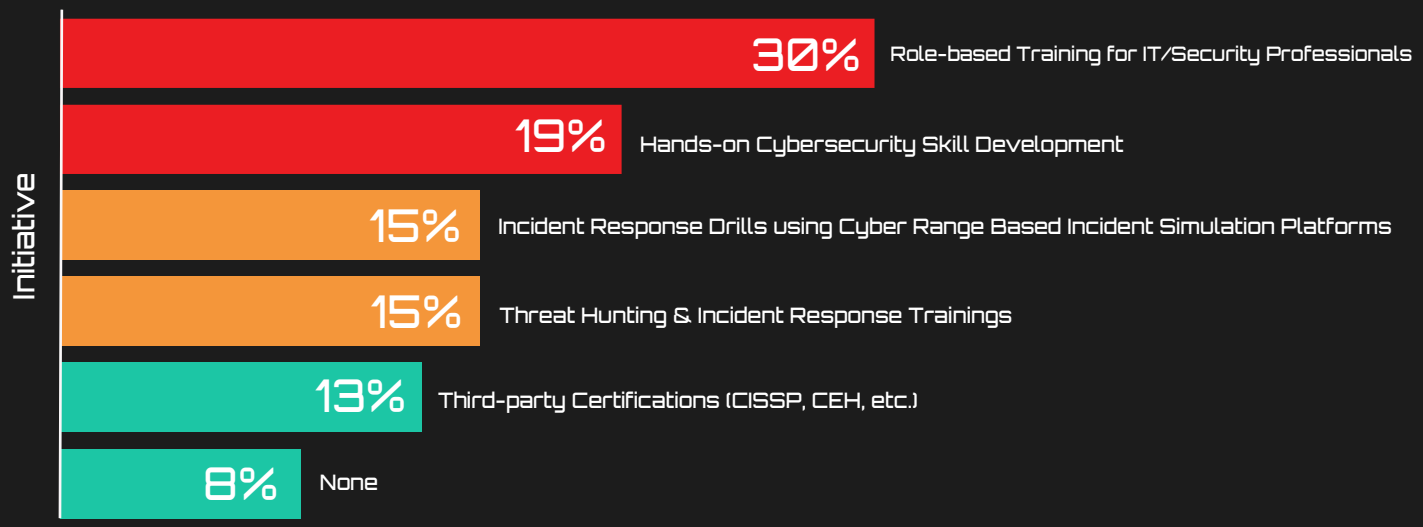
- Strengthen organization-wide security awareness and behavior
- Address skill gaps through targeted hiring, training, or external support
- Improve alignment between cybersecurity and executive leadership

Without resolving internal constraints, increased investment and technology adoption will not translate into improved security outcomes.

AWARENESS & TRAINING

Security awareness and training programs reflect how organizations address human risk, which remains a key factor in cybersecurity effectiveness.

MARKET REALITY



STRATEGIC INSIGHT

While awareness programs are widely implemented, their frequency remains limited. Annual training is the dominant approach, suggesting that awareness is often treated as a compliance-driven activity rather than a continuous capability. More frequent training models, which are better aligned with evolving threat patterns, are adopted by a relatively small proportion of organizations.

Given the prominence of human-targeted threats, this gap between threat dynamics and training frequency creates a misalignment between risk exposure and preparedness.

LEADERSHIP IMPLICATION

Cybersecurity leaders must move beyond periodic training toward continuous awareness programs.

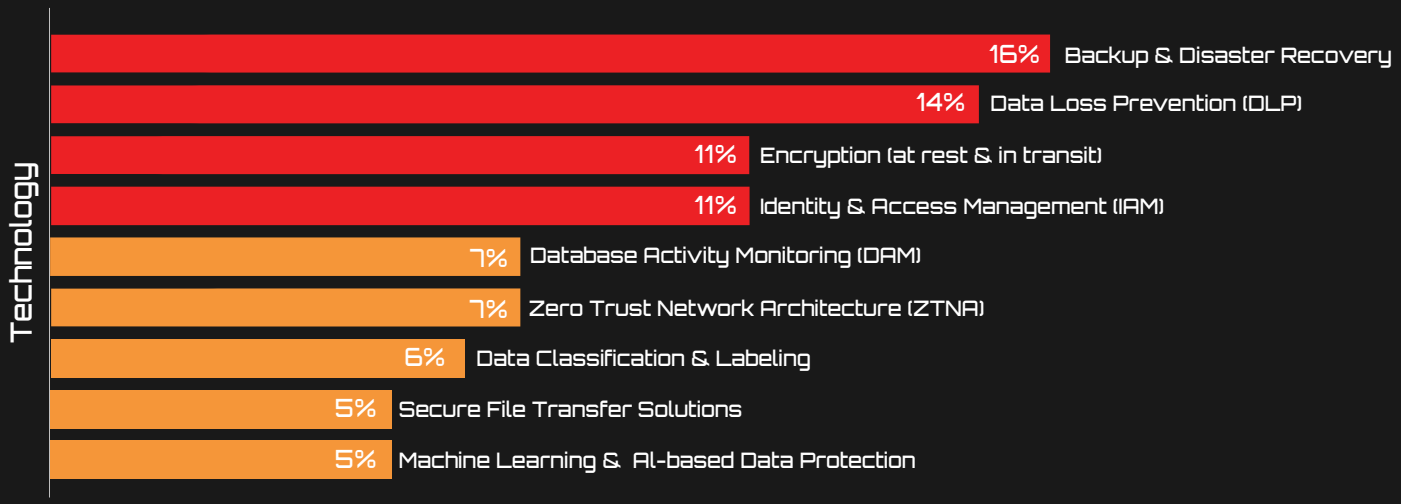
- Shift from annual compliance exercises to ongoing engagement
- Reinforce training with real-world simulations and behavioral interventions
- Align awareness initiatives with evolving threat patterns

Managing human risk effectively requires sustained behavioral change, not periodic training events.

TECHNOLOGY ADOPTION

Technology adoption reflects how organizations are building and evolving their cybersecurity capabilities across prevention, detection, and response.

MARKET REALITY



Respondents were asked to identify the cybersecurity technologies they plan to adopt in 2025. As multiple selections were allowed, the results reflect the frequency with which each technology was selected.

STRATEGIC INSIGHT

Organizations show broad adoption across multiple layers of cybersecurity, spanning data protection, endpoint security, and detection and response capabilities.

Organizations are not focusing on a single domain but are instead investing across the security stack, indicating a multi-layered approach to defence. However, the spread of adoption across numerous technologies also suggests increasing complexity in managing and integrating these capabilities.

This pattern reflects a shift toward comprehensive security coverage but also highlights the growing challenge of ensuring that these technologies operate cohesively.

LEADERSHIP IMPLICATION

Cybersecurity leaders must focus on integration and operational effectiveness, not just technology adoption.

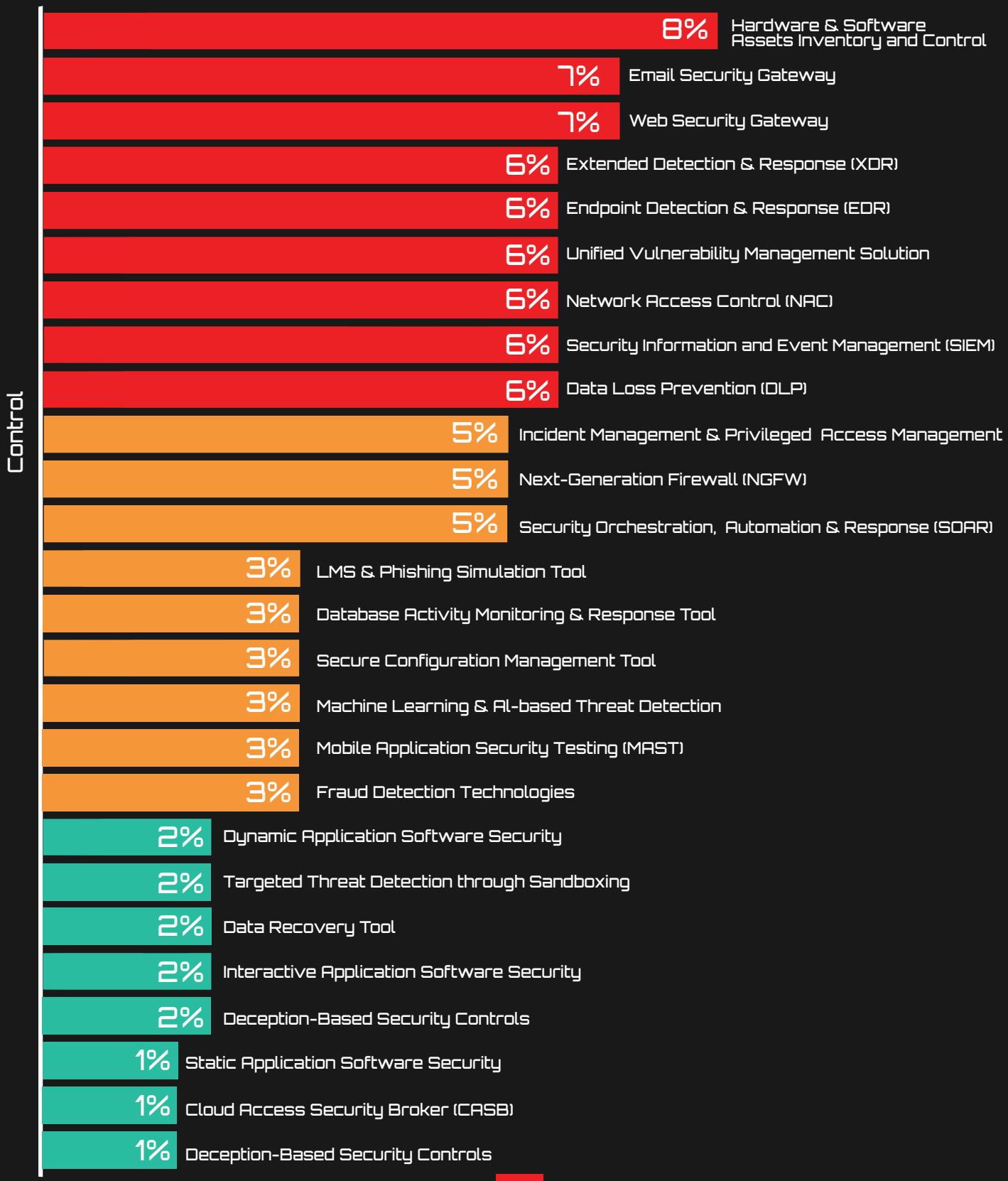
- Prioritize interoperability across security tools
- Avoid fragmented implementations that increase operational burden
- Focus on outcomes rather than tool deployment

The value of cybersecurity investments will depend on how effectively technologies are integrated and operationalized, not on the number of tools deployed.

SECURITY CONTROL PRIORITIES

Security control priorities indicate where organizations are focusing their efforts to strengthen core defensive capabilities and reduce exposure to cyber risks.

MARKET REALITY



STRATEGIC INSIGHT

There seems to be a strong emphasis on foundational and perimeter-focused security controls, including asset inventory, email and web security gateways, and endpoint protection.

Core operational controls such as SIEM, XDR, EDR, and NAC also show significant adoption, indicating that organizations are strengthening monitoring, detection, and access control capabilities.

However, more advanced and specialized controls, including application security, deception technologies, and cloud-specific controls such as CASB show comparatively lower prioritization.

This suggests that organizations are focusing on strengthening baseline security hygiene and widely applicable controls, while adoption of advanced and emerging security capabilities remains selective.

LEADERSHIP IMPLICATION

Cybersecurity leaders must ensure that foundational controls are complemented with capabilities that address evolving risks.

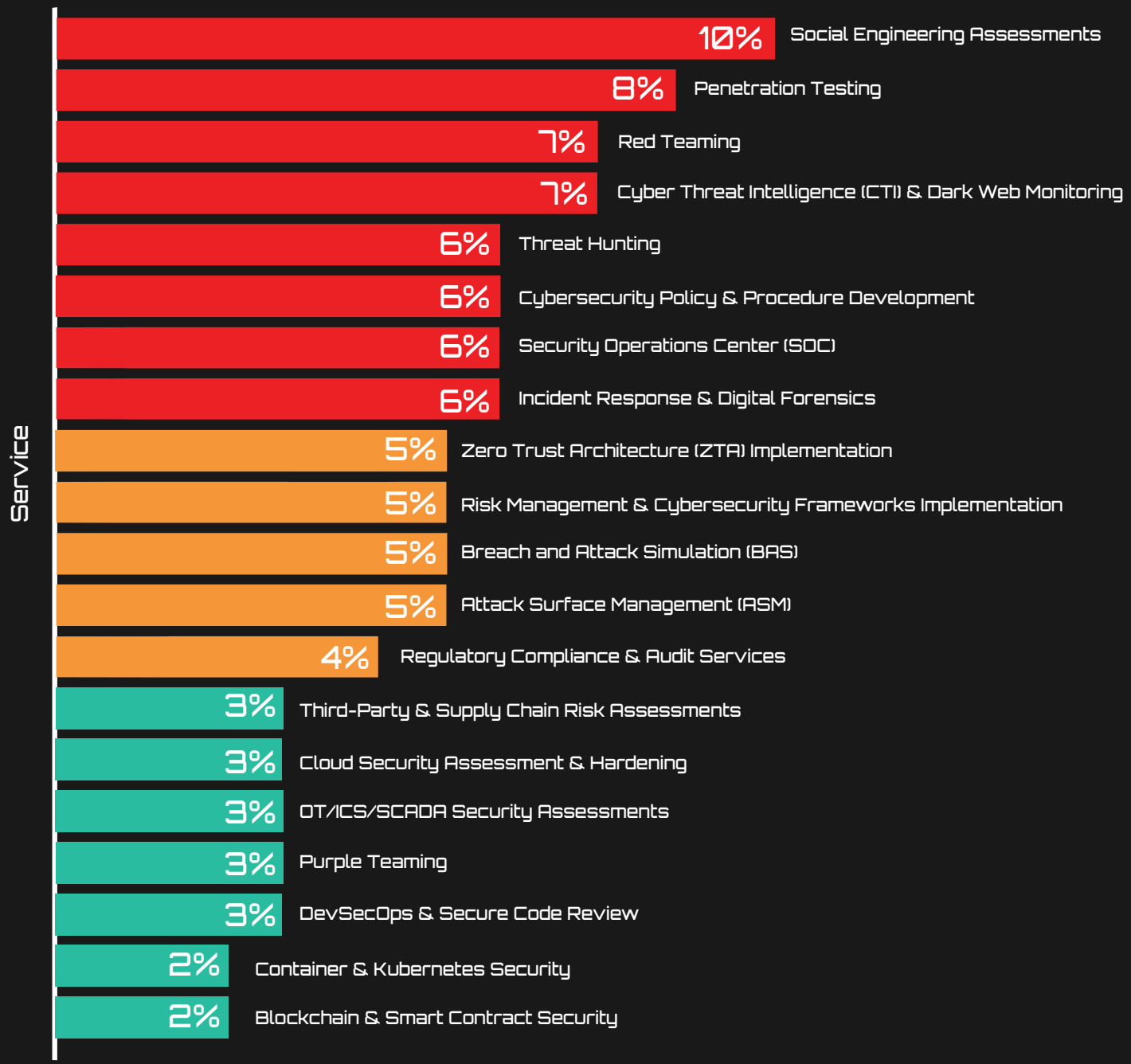
- Maintain strong baseline controls such as asset management, endpoint security, and gateway protections
- Expand focus toward application security, cloud security, and advanced threat detection capabilities
- Ensure that control investments are aligned with modern threat vectors, not just traditional perimeter defenses

A strong baseline alone is not sufficient as organizations must evolve their control strategy to address increasingly sophisticated and targeted threats.

CYBERSECURITY SERVICES PRIORITIES

Cybersecurity service priorities reflect how organizations are leveraging specialized expertise and external capabilities to enhance their security posture and operational effectiveness.

MARKET REALITY



STRATEGIC INSIGHT

The data highlights a strong focus on testing, validation, and human-centric security services.

Social engineering assessments, penetration testing, and red teaming are among the most prioritized services, indicating that organizations are actively testing their defenses against real-world attack scenarios.

At the same time, services such as threat intelligence, incident response, and SOC capabilities show steady adoption, reflecting a need for continuous monitoring and response readiness.

However, more specialized areas such as cloud security, DevSecOps, container security, and OT/ICS security show lower prioritization, suggesting that these domains are still emerging or not uniformly addressed across organizations.

LEADERSHIP IMPLICATION

Cybersecurity leaders must ensure that service investments extend beyond testing and validation into sustained capability development.

- Continue leveraging offensive testing (red teaming, penetration testing) to identify gaps
- Strengthen continuous capabilities such as threat intelligence, SOC operations, and incident response
- Expand focus toward cloud, application, and emerging technology security domains

Effective cybersecurity requires not only identifying weaknesses, but building continuous capabilities to monitor, respond, and adapt to evolving threats.

STRATEGIC RECOMMENDATIONS

1. ANCHOR INVESTMENTS IN MEASURABLE RISK REDUCTION

Cybersecurity spending is largely sustained or increasing, but effectiveness is not guaranteed.

RECOMMENDATION

- Establish a clear linkage between security investments and quantified risk reduction
- Define metrics to measure control effectiveness and program performance
- Prioritize initiatives that deliver demonstrable outcomes, not just capability expansion

2. ALIGN SECURITY STRATEGY WITH IDENTITY AND HUMAN-CENTRIC THREATS

The most frequently reported threats target identity, credentials, and human behavior.

RECOMMENDATION

- Place identity and access at the center of the security strategy
- Strengthen controls around credential protection and access management
- Integrate human risk management into core security programs

3. ADDRESS ORGANIZATIONAL BARRIERS TO IMPROVE EXECUTION

Internal challenges such as awareness gaps, budget constraints, and limited capabilities continue to impact effectiveness.

RECOMMENDATION

- Strengthen organization-wide security awareness and behavioral practices
- Improve alignment between cybersecurity and executive leadership
- Ensure clear ownership and accountability for security initiatives

4. PRIORITIZE INTEGRATION OVER TOOL EXPANSION

Technology adoption is broad, spanning multiple domains across the security stack.

RECOMMENDATION

- Focus on integration and interoperability across existing tools
- Rationalize overlapping technologies
- Improve operational efficiency rather than expanding toolsets

5. MOVE TOWARD CONTINUOUS VALIDATION OF SECURITY CONTROLS

Validation practices remain largely periodic and assessment-driven.

RECOMMENDATION

- Shift from point-in-time assessments to continuous validation approaches
- Incorporate adversary simulation into regular operations
- Establish ongoing monitoring of control effectiveness

CONCLUSION

Cybersecurity has moved beyond a discretionary function to become a core operational priority for organizations. Investment levels have stabilized, threat patterns have evolved, and organizations are increasingly adopting a broad range of technologies to strengthen their defenses.

However, the findings of this report highlight a consistent gap between investment and effectiveness. While organizations continue to invest in cybersecurity capabilities, challenges related to human behavior, organizational alignment, and control validation continue to limit outcomes.

The data indicates that improving cybersecurity effectiveness will not be achieved through increased spending alone. It requires a shift toward measurable outcomes, operational efficiency, and continuous validation of security controls.

For cybersecurity leaders, the focus for 2026 must be clear:

- Translate investment into demonstrable risk reduction
- Align security strategies with evolving threat patterns
- Address internal barriers that limit execution

Organizations that can effectively operationalize their security capabilities, rather than simply expand them, will be better positioned to manage risk in an increasingly complex threat environment.