

.....
WERNER[®]

Freight Security in a High-Risk Era:

How Shippers Are Investing in Safety Tech

A WHITE PAPER IN PARTNERSHIP WITH  **FREIGHTWAVES**





Table of Contents

- 3** Overview
- 5** The Security Investment Landscape
- 7** Technology Adoption Priorities
- 10** Response Capabilities and Organizational Structure
- 11** Implementation Challenges and External Drivers
- 15** Conclusion



Overview

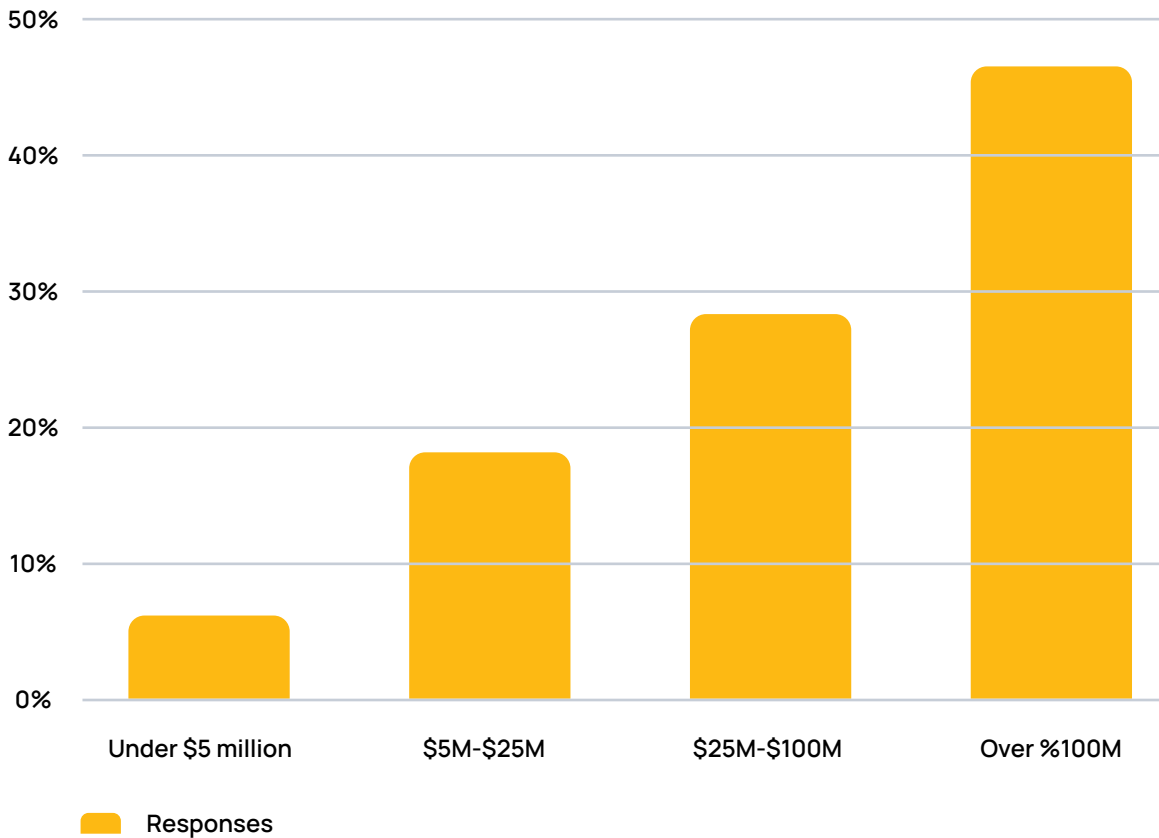
The freight and logistics industry faces an unprecedented convergence of security challenges, from sophisticated cargo theft operations to escalating cyber threats. While technological solutions have emerged to address these risks, the industry's adoption and investment patterns reveal significant gaps between threat awareness and strategic action.

The transportation sector has witnessed dramatic changes in security requirements over the past five years. Traditional approaches to cargo protection – basic locks, insurance policies, and reactive monitoring – are proving insufficient against increasingly sophisticated threats. Modern freight security now demands integrated technology solutions, real-time monitoring capabilities, and proactive risk management strategies.

To better understand how shippers are responding to this evolving threat landscape, FreightWaves and Werner conducted a comprehensive survey of freight industry professionals representing organizations with substantial transportation investments and complex supply chain operations.

The survey gathered responses from logistics leaders across multiple industries, with the majority representing organizations managing annual freight budgets exceeding \$25 million. These respondents oversee complex, multi-modal supply chains with both domestic and global networks, providing valuable insights into enterprise-level security investment patterns.

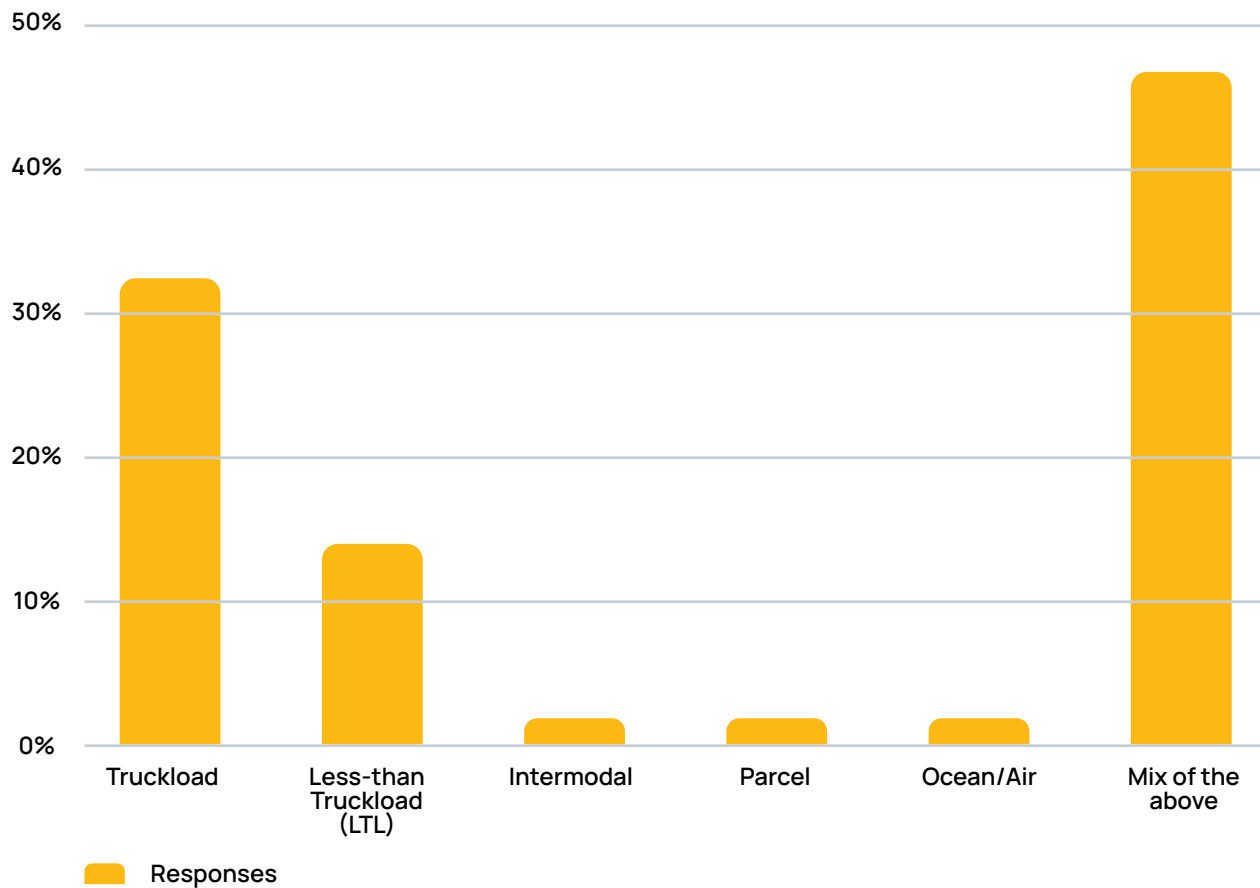
What is your organization's annual freight spend?



No single revenue category dominated responses, illustrating the wide range of perspectives represented in the survey data. This variance is important because it ensures both smaller operations, which make up the bulk of the industry, and enterprise companies, which have outsized impact on industry trends, are well represented.

When examining primary transportation modes, nearly half of respondents (46.94%) indicated they use a mix of transportation modes, reinforcing the complexity and diversity of today's supply chains. Truckload emerged as the top single-mode category, selected by 32.65% of respondents. This aligns with industry norms where over-the-road transportation dominates freight movement.

What is your organization's primary mode of freight transportation?



The predominance of mixed-mode operations creates unique security challenges, as each transportation method introduces distinct vulnerabilities and requires specialized protective measures. This operational complexity underscores why security technology investment decisions have become increasingly strategic rather than tactical.

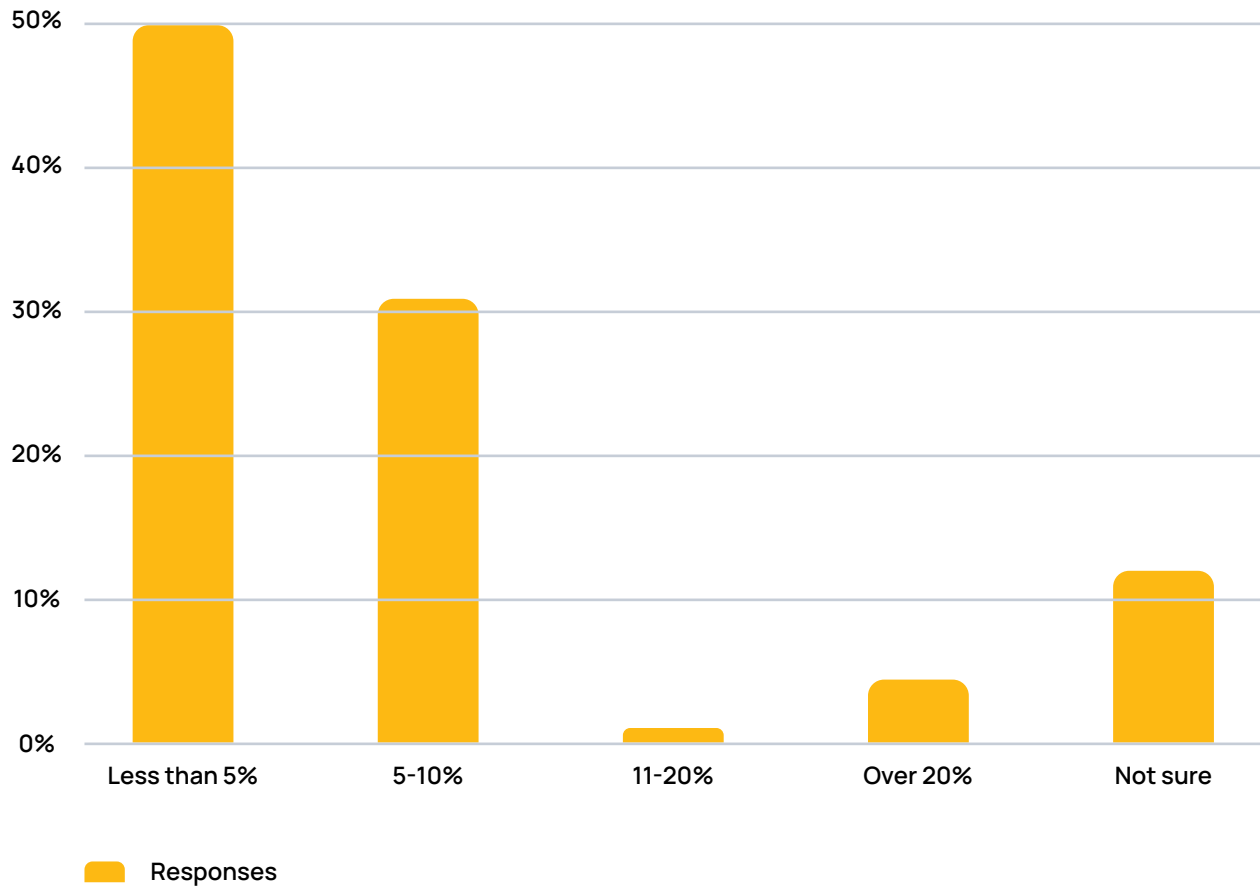
Survey results make it clear that while shippers recognize growing security threats, significant gaps remain in budget allocation, response capabilities, and strategic implementation. Overall, organizations appear somewhat committed to security improvements while recognizing substantial room for enhancement.

THE SECURITY INVESTMENT LANDSCAPE

While awareness of freight security threats has increased dramatically in recent years, actual investment patterns reveal a more cautious approach. Organizations continue to allocate relatively modest portions of their logistics budgets to security and risk management, even as threats become more sophisticated and frequent.

Perhaps the most striking finding concerns budget allocation priorities. When asked what percentage of their overall logistics budget is allocated to security and risk management, responses revealed a concerning pattern of underinvestment relative to the threat landscape.

What percentage of your overall logistics budget is allocated to security and risk management?



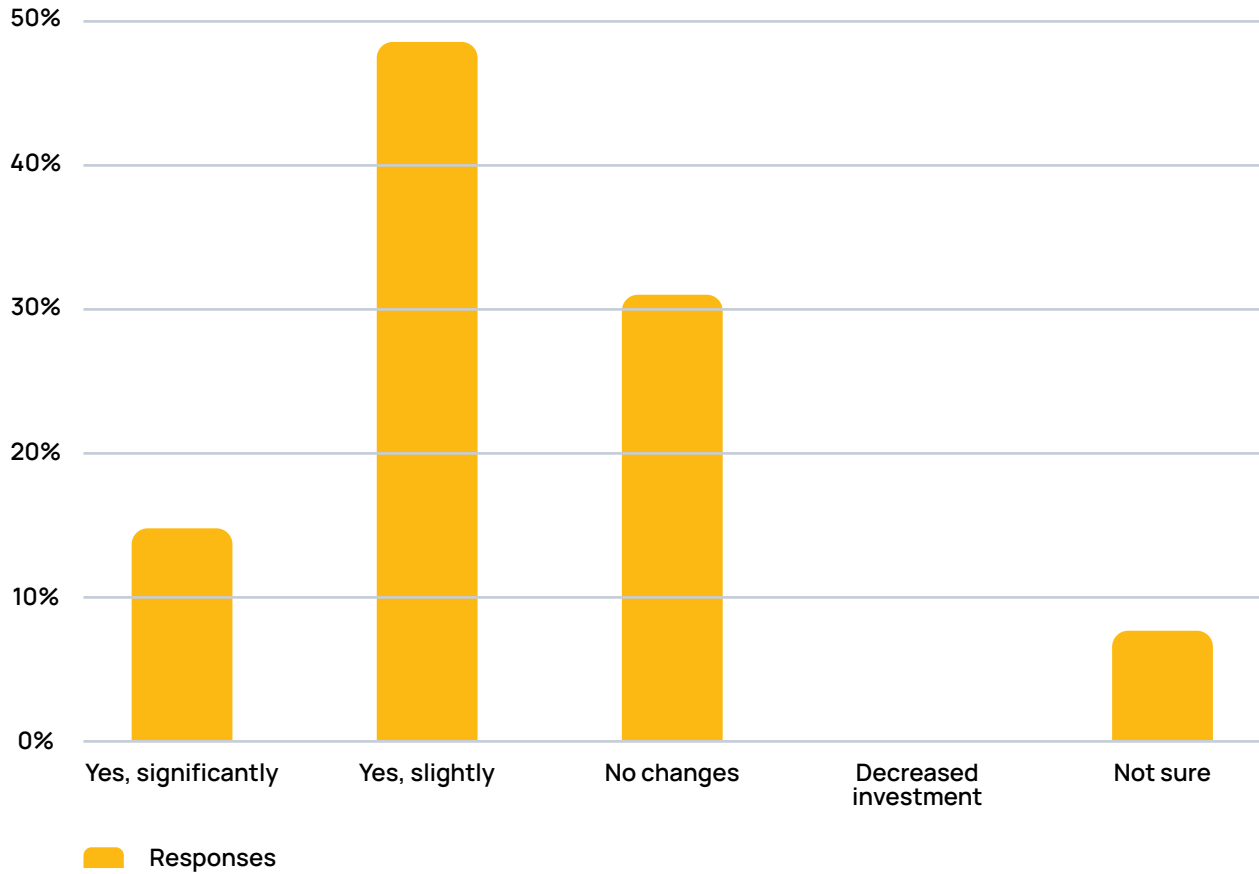
These numbers illustrate that over 80% of respondents dedicate 10% or less of their logistics budget to security and risk management. This conservative allocation stands in stark contrast to the escalating threats facing the industry, including sophisticated cargo theft operations, cyber attacks targeting transportation networks, and geopolitical disruptions impacting global supply chains.

The 12.5% of respondents who are unsure of their security spending allocation suggests potential

gaps in visibility or internal prioritization. This uncertainty may reflect organizational silos where security investments are distributed across departments without centralized tracking or strategic coordination.

Despite modest budget allocations, there are also positive indicators of growing security awareness and investment momentum. When asked about changes in security technology investment over the past 12 months, responses showed encouraging trends.

Has your company increased investment in freight security technology over the past 12 months?



A majority of respondents (62.5%) indicate their companies have increased investment in freight security technology over the past year. While only 14.58% described that increase as "significant," a much larger group (47.92%) reported a slight uptick in spending. This suggests growing awareness of security threats, though most organizations are still taking incremental steps rather than major leaps.

Nearly a third (31.25%) reported no change in their investment, which could point to stable security postures, budgetary constraints, or competing priorities. Encouragingly, no respondents reported a decrease in investment, signaling that security is not being deprioritized even in cost-conscious environments.

The 6.25% who were "not sure" may reflect operational silos where logistics professionals don't have direct visibility into security-specific spending or where technology investments are spread across departments. Taken together, these findings indicate that while security investment is trending in the right direction, many companies are still in a phase of gradual rather than transformational adoption.

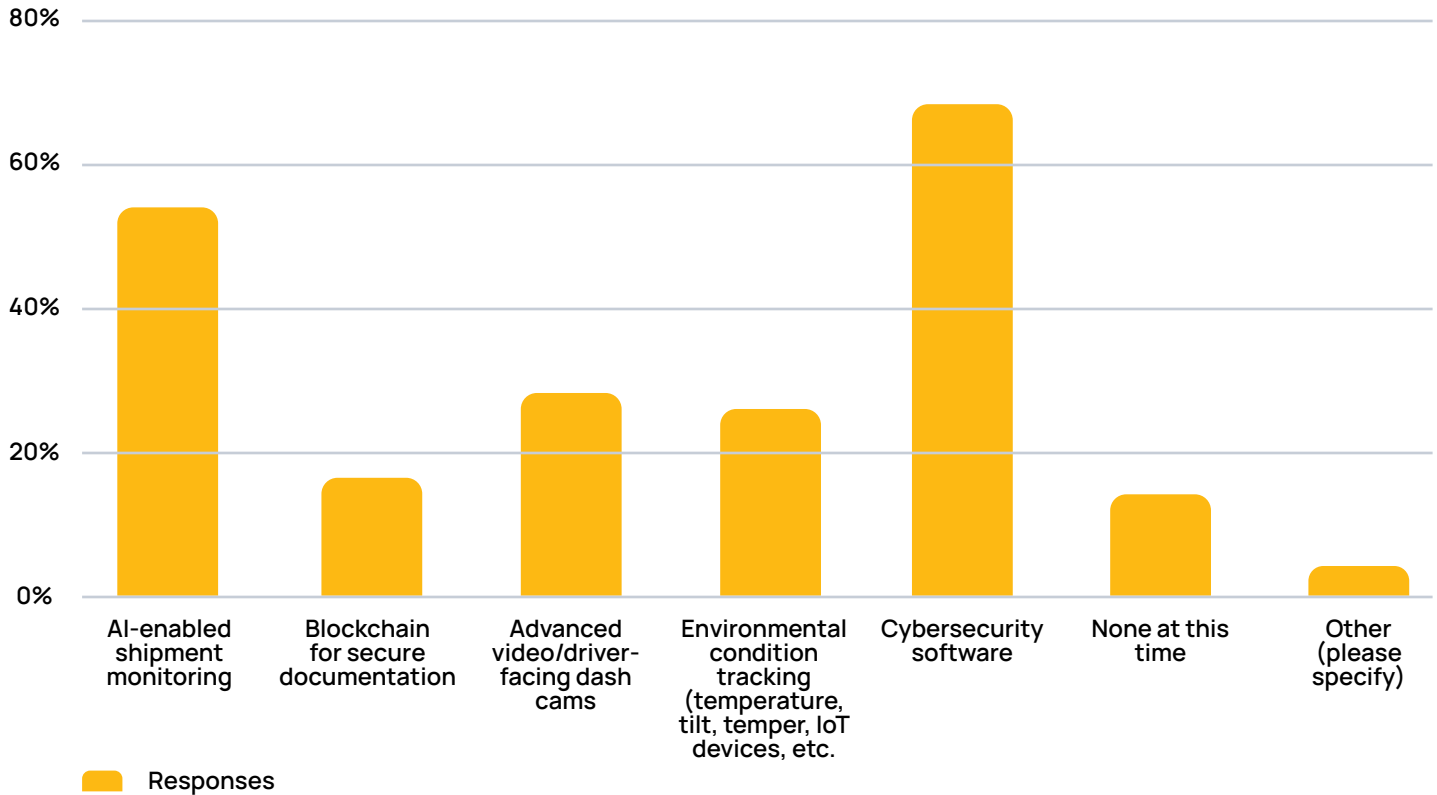
TECHNOLOGY ADOPTION PRIORITIES

When examining specific technology investments, clear priorities emerge that reflect both current threat patterns and organizational capabilities. The survey revealed distinct preferences for certain security technologies, with cybersecurity emerging as the dominant concern across all respondent categories.

Cybersecurity topped the list of safety and security technologies that respondents are actively considering in the coming year, selected by 67.35% of participants. This reflects a broader industry shift

as digital threats ranging from ransomware attacks to data breaches become as concerning as physical cargo theft.

Which safety/security technologies are you actively considering or piloting in the next 12 months?



As freight networks become increasingly digitized, cybersecurity is no longer solely an IT concern; it has become a core pillar of operational resilience. The high prioritization of cybersecurity reflects recognition that modern supply chains depend heavily on digital systems for everything from load booking to real-time tracking, creating multiple potential attack vectors.

AI-enabled shipment monitoring emerged as the second-highest priority, with 53.06% indicating plans to explore or implement this technology. This represents the convergence of security and supply chain optimization, offering real-time insights into cargo movements, potential delays, and suspicious behavior patterns that could indicate theft or tampering.

Other notable areas of investment include advanced dash cams (28.57%) and environmental condition tracking (26.53%). These tools prove especially important for high-value, temperature-sensitive, or liability-prone freight. The interest in advanced dash cams reflects recognition that comprehensive visual monitoring can provide crucial evidence for insurance claims while deterring theft attempts.

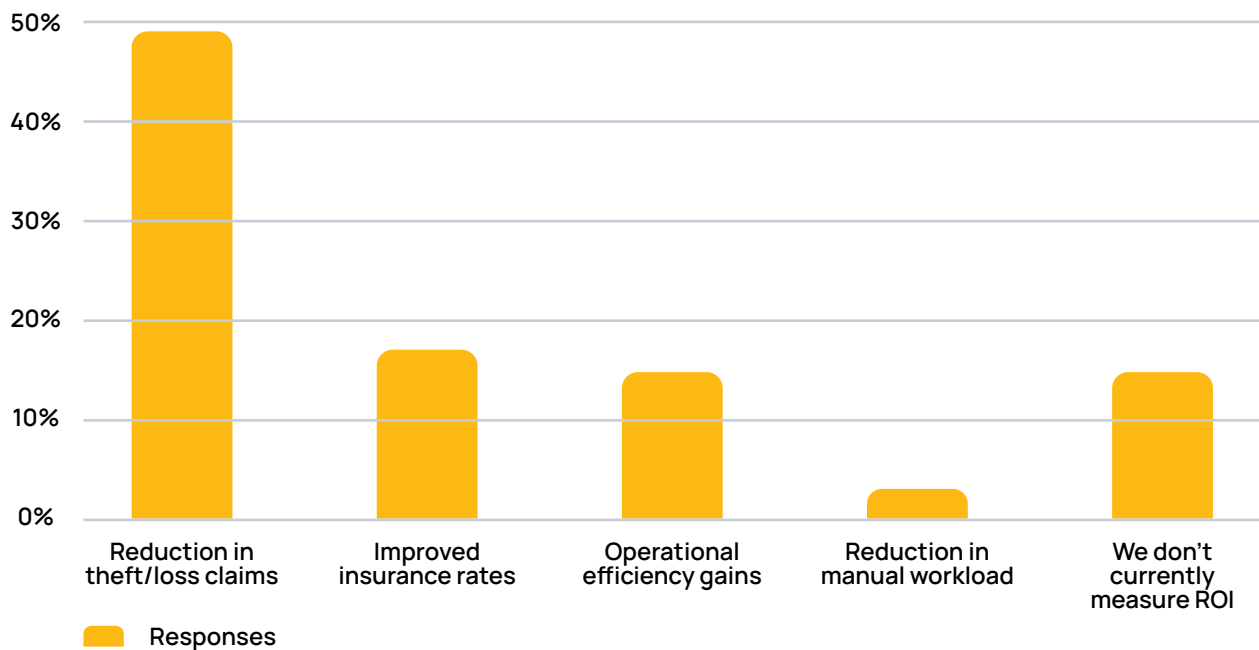
Blockchain technology, while still developing, was selected by 16.33% of respondents, suggesting niche but growing interest in secure documentation and digital chain-of-custody solutions. The relatively modest adoption rate likely reflects both

technological complexity and uncertain return on investment calculations.

Only 14.29% of respondents said they're not planning to explore any new technologies this year, underscoring that the vast majority of shippers and logistics leaders are actively seeking technology-forward approaches to mitigate risk, improve visibility, and secure their operations.

When it comes to evaluating return on investment for security technology, organizations employ varied approaches, with most focusing on direct loss prevention rather than operational benefits.

How do you typically evaluate ROI on security technology investments?



Nearly half of respondents (48.98%) said they measure ROI by reductions in theft or loss claims. This indicates that, for many organizations, the clearest justification for investing in security solutions lies in preventing costly incidents that directly impact the bottom line.

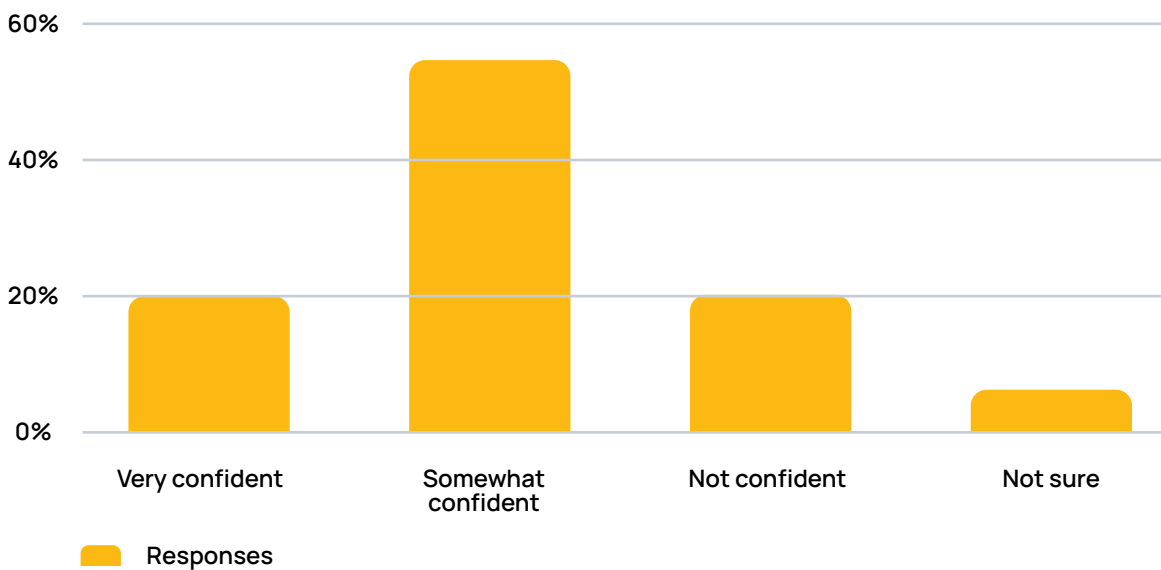
However, 16.33% of respondents said they don't currently measure ROI on security investments at all. This represents a significant gap in strategic security management, as organizations without proper measurement struggle to optimize their investments or justify expanded budgets.

RESPONSE CAPABILITIES AND ORGANIZATIONAL STRUCTURE

One of the most concerning findings relates to organizational confidence in real-time incident response capabilities. When security incidents occur, the ability to respond quickly and effectively often determines the difference between minor disruptions and major losses.

Only 20.41% of respondents said they are very confident in their organization's ability to respond to a freight security incident in real time. This means that fewer than one in five companies feel prepared to handle security crises as they unfold.

How confident are you in your organization's ability to respond to a freight security incident in real-time?



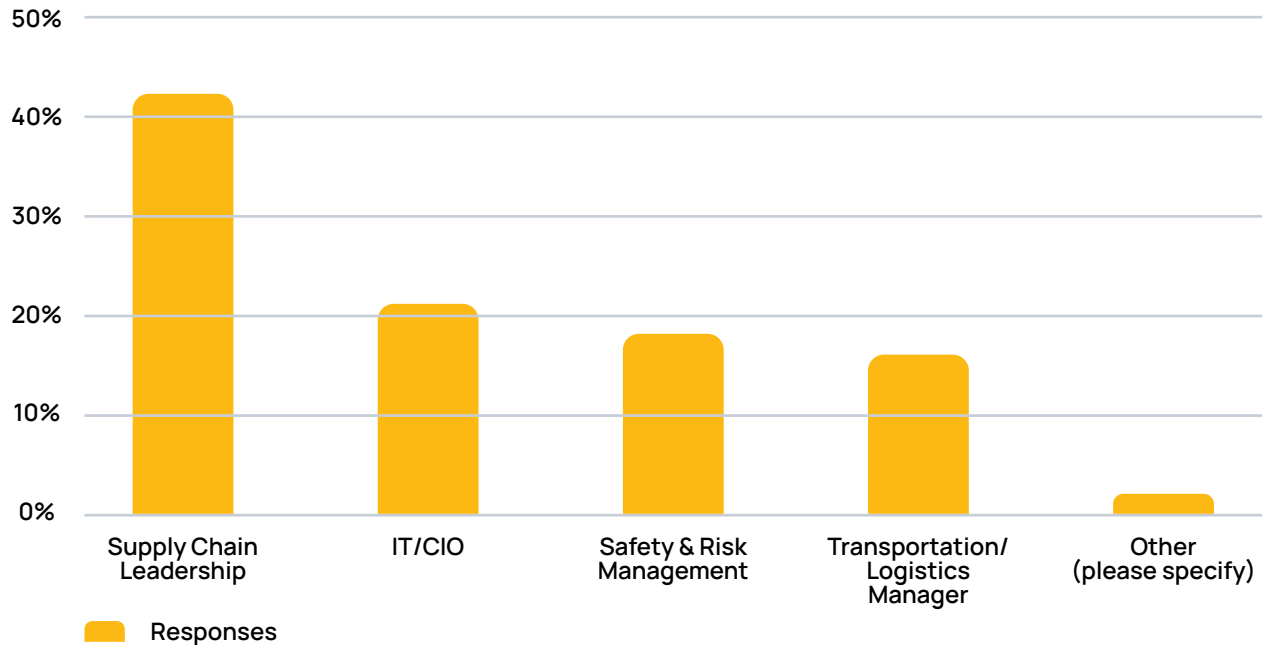
The majority (53.06%) are somewhat confident, suggesting that while many companies have some foundational tools or processes in place, they may lack the end-to-end capabilities or coordination necessary for swift, decisive action during security incidents.

Notably, the same percentage of respondents who reported high confidence (20.41%) also said they are not confident in their organization's real-time response capabilities. This polarization suggests

that organizations have either invested significantly in response infrastructure or recognize serious deficiencies in their current systems.

The organizational structure for security investment decisions reveals interesting patterns about where responsibility lies within companies. Supply chain leadership holds final decision-making authority over safety and security technology investments for 42.86% of organizations.

Who in your organization has the final say over safety and security technology investments?



This concentration of authority with supply chain leadership reflects growing recognition that security is an integral part of overall supply chain strategy rather than just a niche function. Supply chain leaders are uniquely positioned to balance operational efficiency with risk mitigation, making them logical stewards of security technology budgets.

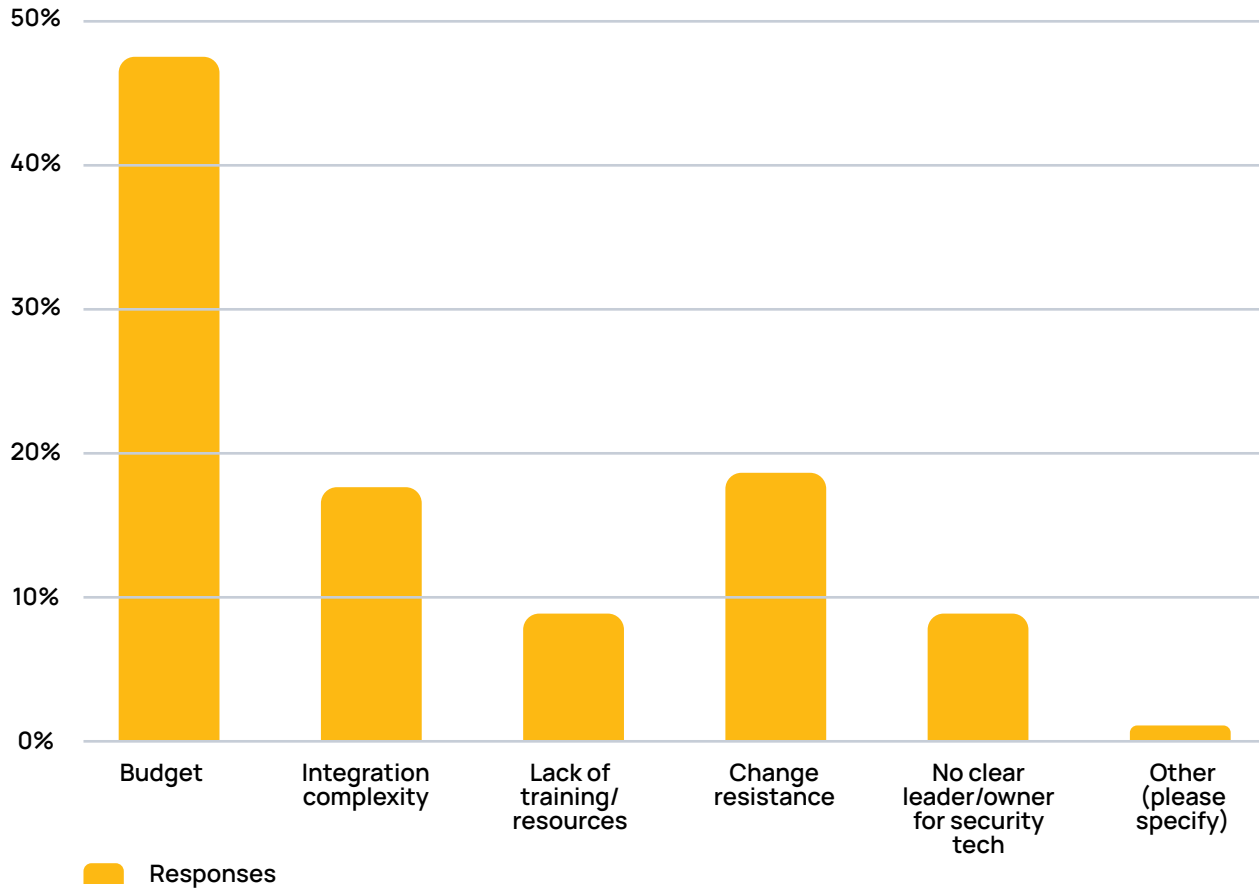
IT or CIO departments come next, responsible for 20.41% of these decisions. This makes sense given the increasing role of cybersecurity, digital tools, and data management in modern freight security solutions. The significant IT involvement underscores how security has evolved from primarily physical measures to sophisticated digital solutions.

IMPLEMENTATION CHALLENGES AND EXTERNAL DRIVERS

Despite growing awareness and some increased investment, organizations face significant barriers when attempting to implement new security solutions. Understanding these challenges is crucial for developing successful security enhancement strategies.

When asked about the biggest internal challenge to adopting new freight security solutions, budget limitations dominated responses at 46.94%. This overwhelming majority underscores that, despite increasing awareness of security risks, financial resources remain the primary hurdle preventing organizations from fully modernizing their security infrastructure.

What's the biggest internal challenge to adopting new freight security solutions?

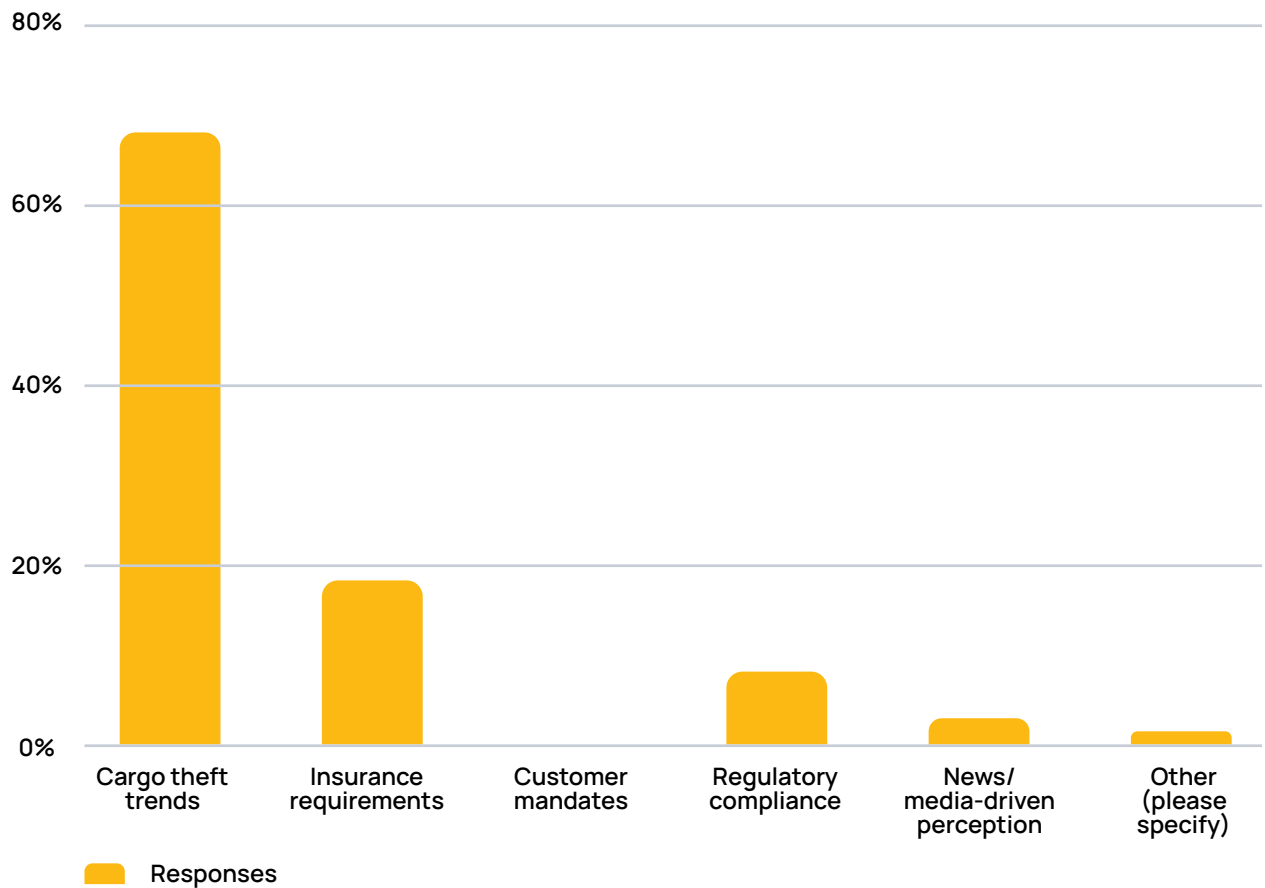


Change resistance (18.37%) and integration complexity (16.33%) represent the next most significant challenges. Resistance to change suggests cultural or organizational inertia that can slow adoption even when leadership supports security initiatives. Integration complexity points to technical difficulties in connecting new security solutions with existing operational systems.

External factors also significantly influence how organizations shape their safety strategies, with cargo theft trends dominating strategic thinking.

An overwhelming 67.35% of respondents identified cargo theft trends as the primary external factor influencing their safety strategy. This highlights how the rising frequency and sophistication of freight theft continues to dominate strategic considerations in logistics security.

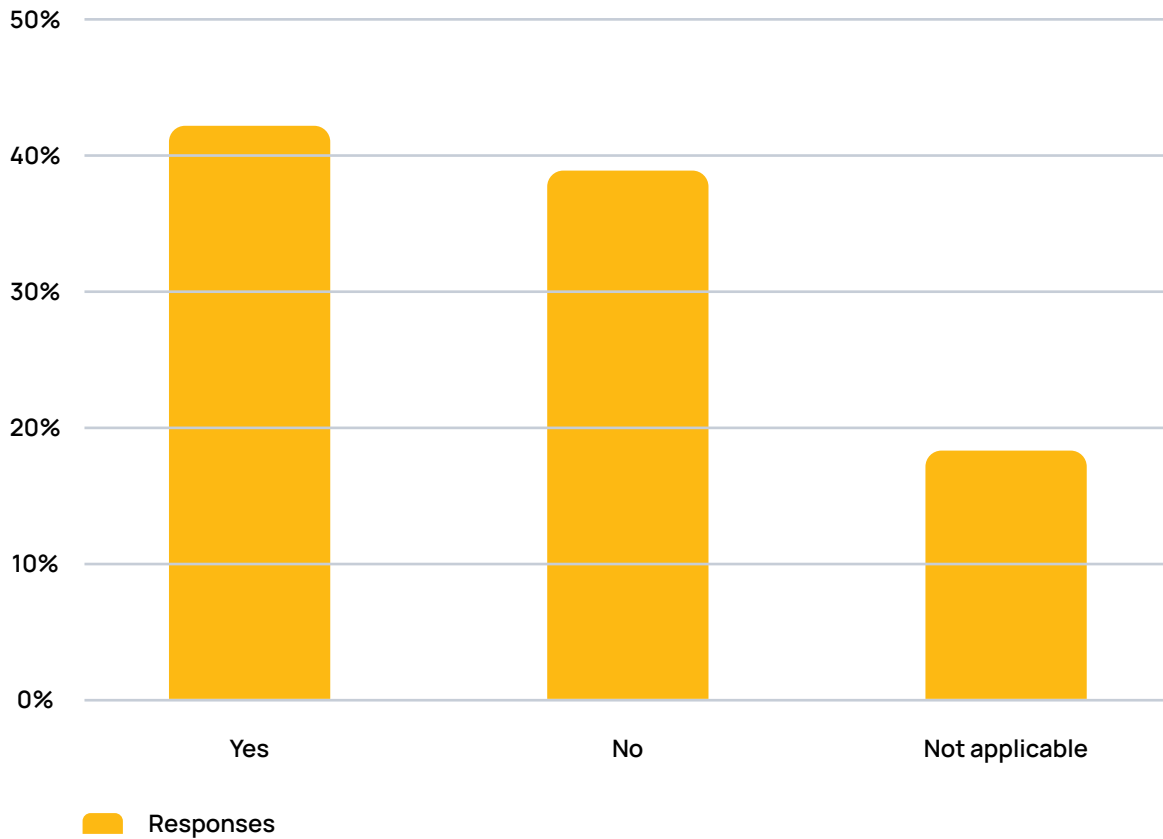
What's the biggest external factor influencing your safety strategy?



Insurance requirements come second at 18.37%, highlighting that carriers and shippers face pressure from insurers to meet certain security standards and demonstrate risk reduction measures. Regulatory compliance influenced 8.16% of participants, reflecting ongoing but relatively limited impact from government rules and standards.

Interestingly, no respondents pointed to customer mandates as a key driver, suggesting that buyer-driven security requirements may not yet be widespread, or that companies are proactively addressing safety independent of client pressures.

Have you had to reevaluate your safety and security approach because of a high-profile incident or near-miss?



The impact of high-profile incidents on strategic thinking proves significant, with 42.86% of respondents saying their company has had to reevaluate its safety and security approach because

of a high-profile incident or near-miss. This indicates that real-world events serve as powerful catalysts for change, pushing organizations to reassess vulnerabilities and strengthen protocols.



Conclusion

The freight security landscape presents both challenges and opportunities for industry leaders. While organizations are beginning to increase security technology investments, significant gaps remain in budget allocation, response capabilities, and strategic implementation.

Shippers have made it clear that they recognize growing security threats, but many continue to approach security investment cautiously rather than strategically. The finding that over 80% of organizations allocate 10% or less of their logistics budget to security suggests a fundamental misalignment between threat awareness and resource commitment.

The survey reveals an industry in transition, moving from reactive security approaches toward more strategic, technology-enabled protection. However, success requires addressing fundamental challenges including budget constraints, organizational resistance to change, and technical integration complexity.

Organizations that proactively invest in comprehensive security strategies, supported by adequate budgets and robust measurement systems, will be better positioned to protect their operations, reduce costs, and maintain competitive advantage in an increasingly complex threat environment.