expel | UserEvidence

THE CISO-CFO DISCONNECT

Why security and finance struggle to align on cyber investment

Contents

Letter from the CSO

In an industry where security and finance teams often struggle to find common ground, I want to thank you for taking time from your packed schedule to review our research on CISO and CFO alignment. We know your days are filled with competing priorities and complex decision-making, and it’s our intention for this study to provide insights that make your strategic planning a little more effective.

While the data presented here is based on survey responses, it's informed by the real challenges and successes we've witnessed working with hundreds of organizations. These findings reflect the experiences of security and finance leaders who are genuinely trying to collaborate but often find themselves speaking different languages. In this report, you'll see where alignment breaks down and, more importantly, how high-performing teams bridge these gaps.

Cybersecurity is a team sport, and it's a game of inches—not yards. The most successful security programs aren't built by CISOs working in isolation or CFOs approving budgets without context. Our goal is to translate this research into practical frameworks you can use to improve collaboration between security and finance, ultimately creating more strategic, sustainable cybersecurity investments that protect your business and contribute to better industry practices overall.

Greg Notch
Chief Security Officer, Expel

Executive summary

Enterprise cybersecurity investments continue to grow, with most organizations anticipating at least slight budget increases in the next 12 months. To make the strategic decisions that allow them to remediate threats and strengthen their organization's cyber resilience, CISOs must collaborate and communicate with their finance counterparts.

However, this growing demand for partnership goes both ways. As cybersecurity risk management increasingly becomes a board-level discussion, CFOs often take responsibility for enterprise risk management and obtaining cybersecurity insurance coverage—which requires collaboration and communication with security counterparts.

This report seeks to explore how CISOs and CFOs perceive cybersecurity investment decisions. It analyzes their views on risk tolerance, business impact, and reporting. It also evaluates where the two teams are aligned and reveals where disconnects and knowledge gaps compromise cross-functional collaboration.

Key takeaways

Aligned goals, uneven confidence

Finance and security teams report high strategic alignment, with 88% of security leaders saying their priorities match business goals and 55% of finance decision-makers considering cybersecurity a core strategic driver. Yet finance expresses notably lower confidence in security's core business capabilities.

Measurement maturity varies

71% of security leaders and 56% of finance leaders rate their organization's ability to measure cybersecurity business impact as fully or very mature. Yet they're misaligned on reporting and decision-making. While the two teams believe they're successfully communicating, they're operating completely differently.

Frustrations stem from expertise gaps

Security and finance report excellent collaboration, with 74% and 68% (respectively) saying they work together early and often. Yet security remains frustrated with finance's limited understanding of cybersecurity risk, and finance is concerned with sizing the risk and security's inability to quantify return or risk.

Alignment demands intentional effort

Finance decision-makers believe the solution lies in better communication and deeper education around cybersecurity. The path forward for CISOs and CFOs requires addressing structural issues, measurement approaches, communication gaps, and organization-wide perceptions.

SECTION 1

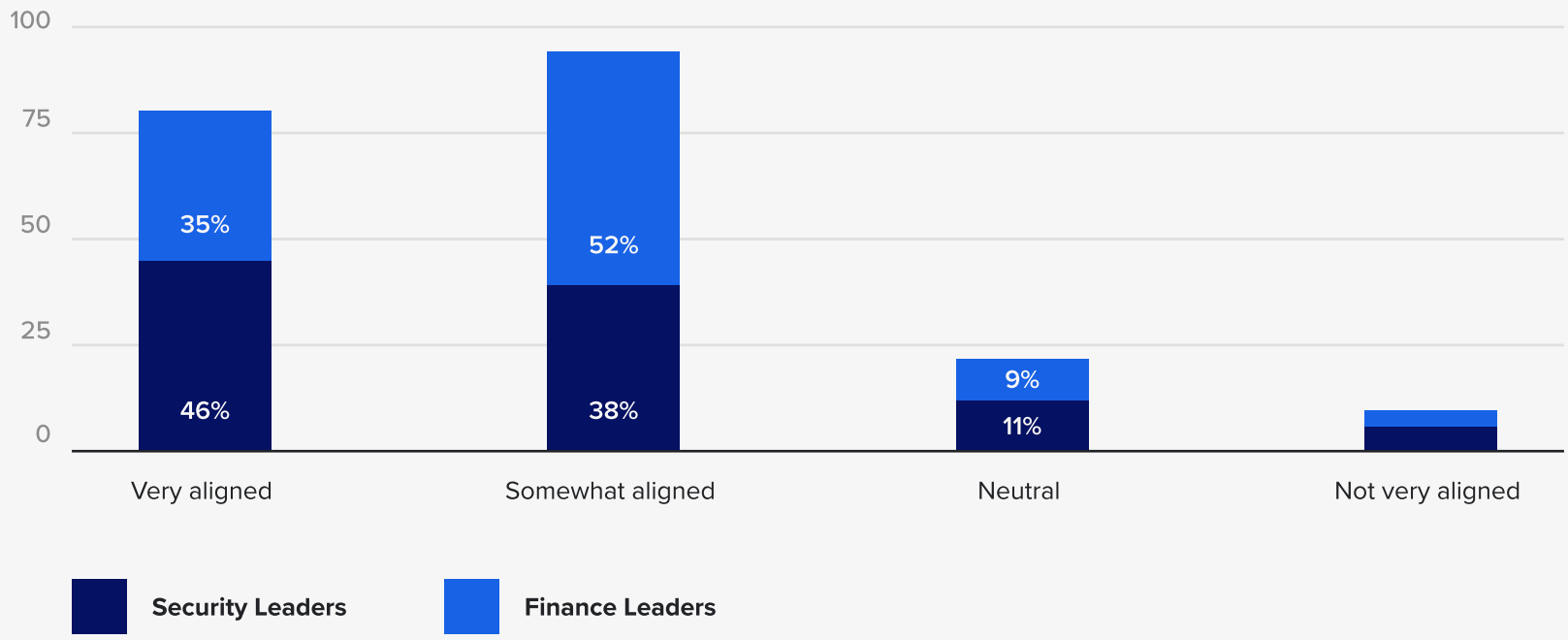
Surface agreement and strategic misalignment

Finance and security decision-makers both report relatively high levels of strategic alignment and mutual understanding. Dig deeper, however, and the cracks begin to emerge within this seemingly optimistic outlook.

84% of surveyed security leaders believe their finance counterparts are aligned with the security team's priorities. But the degree varies: 46% say their finance counterparts are very aligned, while 38% say they're only somewhat aligned.

Finance leaders show a lower level of conviction. While 87% of surveyed finance leaders say their security counterparts are aligned with the finance team's priorities, only 35% say they're very aligned. Instead, more than half (52%) say they're somewhat aligned.

How security and finance leaders perceive their counterparts' alignment with their own team's priorities



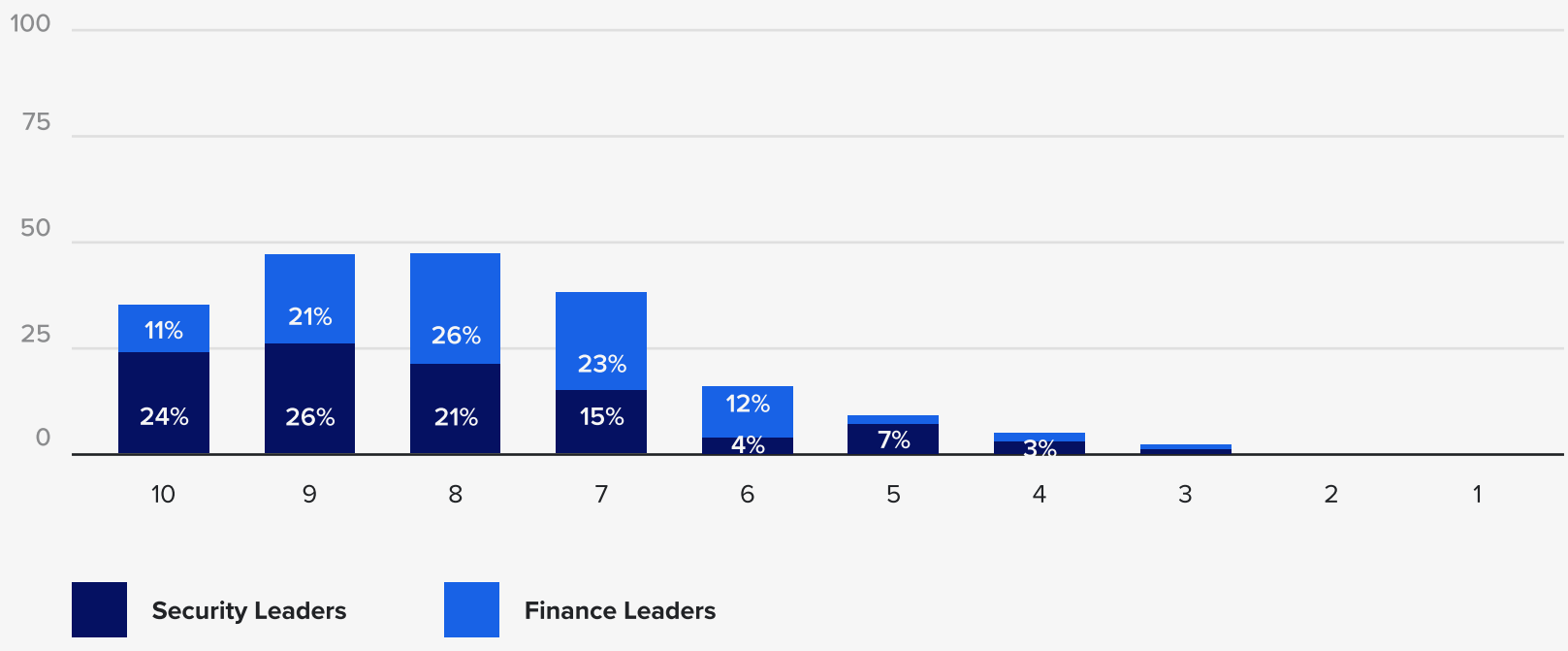
SECTION 1

Surface agreement and strategic misalignment

When it comes to risk tolerance and budget expectations, a similar pattern emerges. 71% of surveyed security leaders say that security and finance teams are fully (10 on a 10-point scale) or very (8 or 9 on a 10-point scale) aligned on these elements.

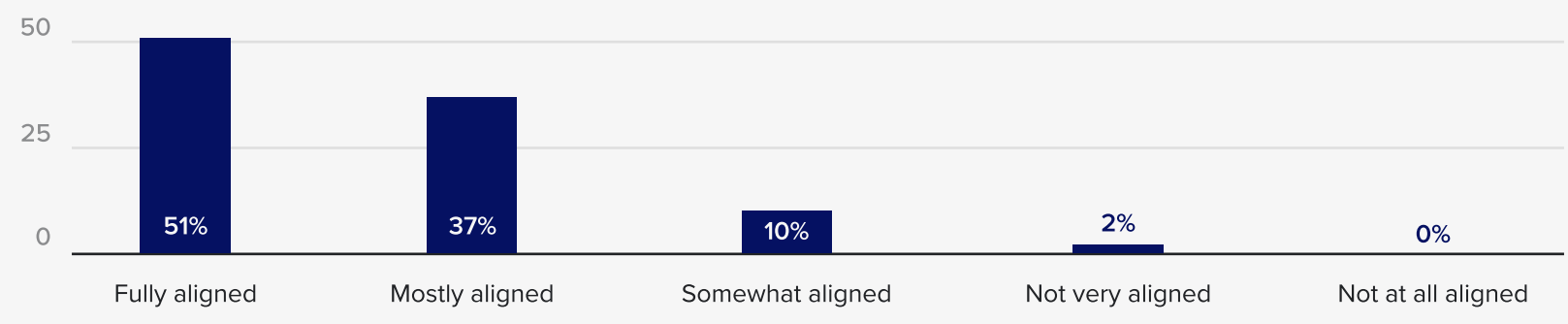
Finance decision-makers generally agree, but they're less optimistic overall. 58% of surveyed finance leaders say they're fully or very aligned with security on risk tolerance and budget expectations.

How security and finance leaders view their counterparts' alignment on risk tolerance and budget expectations on a scale of 1–10



When asked if their priorities align with company objectives, security leaders report an overwhelmingly positive outlook. 98% of surveyed security leaders say their priorities are consistent with the organization's overall business goals. More than half (51%) say they're fully aligned with these goals.

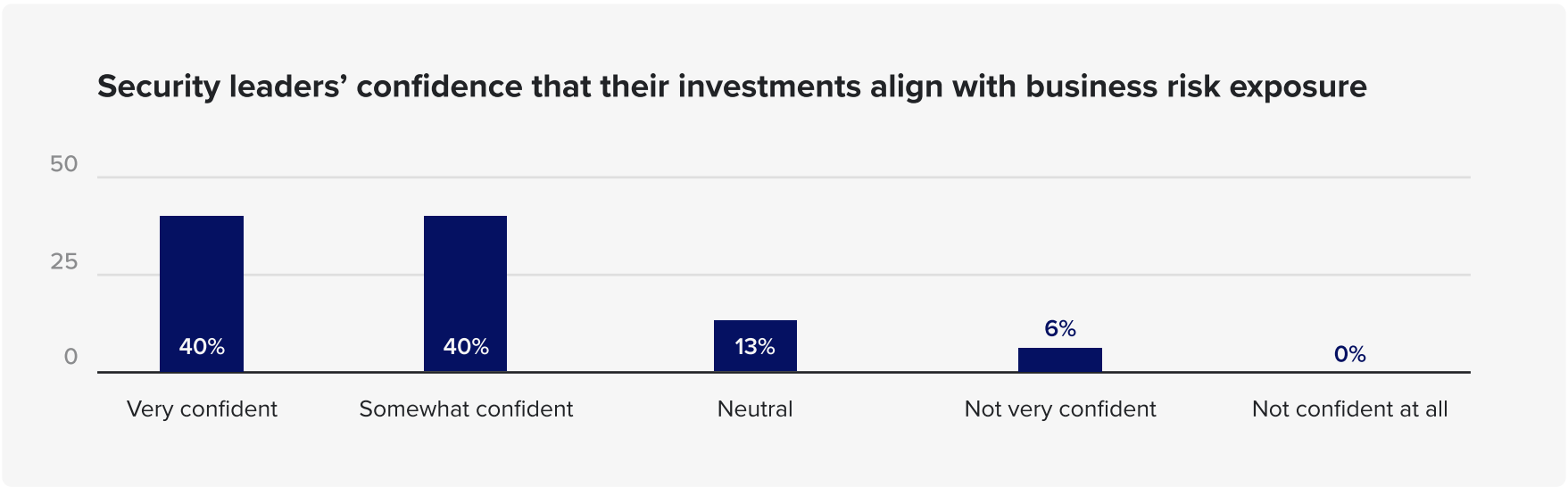
How security leaders view their alignment with the company's business goals



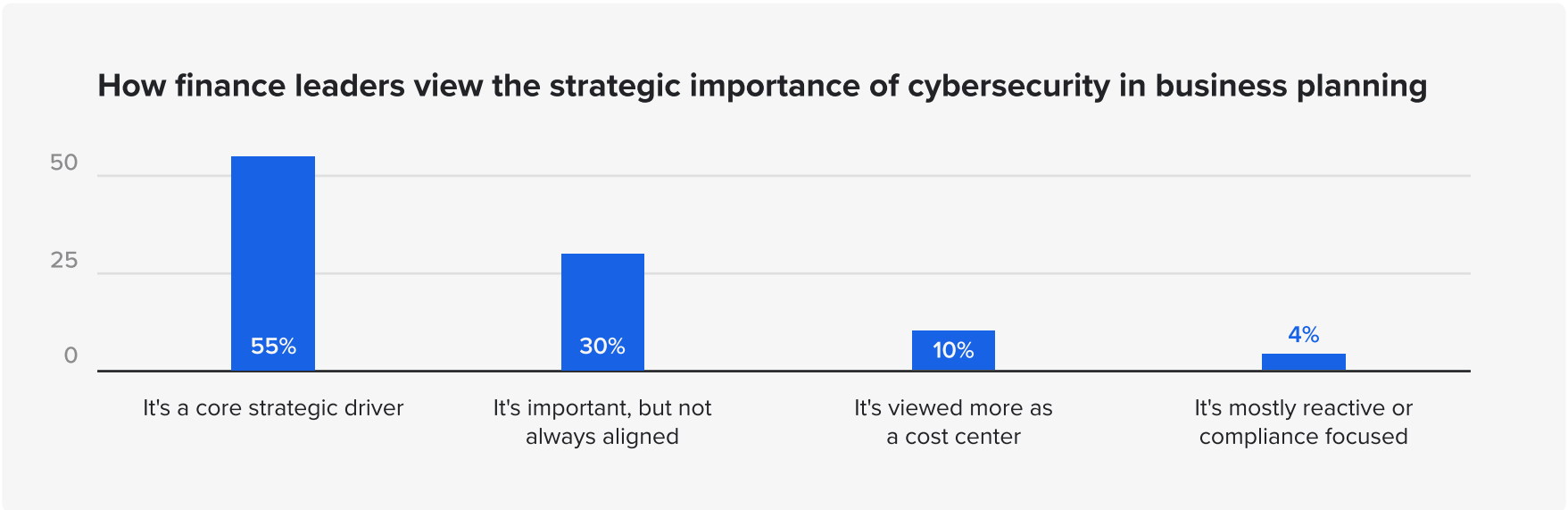
SECTION 1

Surface agreement and strategic misalignment

Yet when it comes to cybersecurity investments and business risk, uncertainty emerges. 60% of surveyed security leaders say they aren't fully confident that their organization's cybersecurity investments are aligned with actual business risk exposure.



However, finance decision-makers generally view cybersecurity as strategically important to their organization's business planning. Overall, 85% of surveyed finance leaders say cybersecurity is a key component of business planning, with 55% describing it as a core strategic driver.



SECTION 1

Surface agreement and strategic misalignment

While most finance decision-makers see security as business-critical, they demonstrate a lower level of assurance in some of their security teams' abilities. Only half of surveyed finance leaders say they're very confident that their security team can communicate business impact clearly (52%) and protect the organization from major cyber events (48%).

Further, only 40% express full confidence in security's ability to align with business strategy. In addition, only 43% are very confident that security can prioritize investments based on risk. Just 46% are very confident that security can deliver cost-efficient solutions.

Finance leaders "very confident" in security team's ability to deliver key outcomes

Communicate business impact clearly	52%	Prioritize investments based on risk	43%
Protect the organization from major cyber events	48%	Align with business strategy	40%
Deliver cost-efficient solutions	46%		

> *Be extremely crisp on the metrics that matter to the business. It's about identifying the three to five business outcomes that actually matter to the organization—revenue protection, operational continuity, customer trust, etc.—and relentlessly connecting every security initiative back to those outcomes. If you can't draw a clear line from a security investment to a business metric that matters, you probably shouldn't be making that investment.*
>
> **Greg Notch**
> Chief Security Officer, Expel

SECTION 1

Surface agreement and strategic misalignment

Security decision-makers recognize these mixed views in their finance counterparts, as well as throughout the organization. In general, those who think leadership has a more negative view of cybersecurity tend to be less confident in their alignment with business objectives.

Almost half (49%) of surveyed security leaders think CEOs perceive cybersecurity in a positive light as a strategic enabler. However, these security leaders tend to think business unit (BU) leaders view them in either a neutral or negative light. 36% say these BU leaders perceive cybersecurity as a cost center, while 35% say they see the function as nothing more than an operational necessity.

Their understanding of CFOs is divided: 38% think CFOs perceive cybersecurity as a cost center, and another 38% think they see the function as a strategic enabler. More than half (54%) of those who say "strategic enabler" report being very confident that their priorities are aligned with their finance counterparts. Just 38% of those who say "cost center" are very confident in their alignment with finance.

The same trend surfaces in security leaders' views of their organization's board of directors. 39% say their board perceives cybersecurity as a cost center, and 31% say the board sees their initiatives as a strategic enabler. Just 36% of those who say "cost center" are very confident in their alignment with finance, while 64% of those who say "strategic enabler" are very confident in that alignment.

Inititative	CEO	Business Unit Leaders	CFO	Board of Directors
Strategic Enabler	49%	27%	38%	31%
Cost Center	26%	36%	38%	39%
Operational Necessity	24%	35%	23%	25%
Not Sure	1%	1%	1%	5%

SECTION 1

Surface agreement and strategic misalignment

In reality, cybersecurity is a cost center, which doesn't necessarily carry a negative connotation. However, a perception shift from neutral "cost center" to positive "strategic enabler" could carry with it more of an openness to providing necessary resources to maintain that positive role within the organization. As you will see, in order to do that, security has to communicate the value it creates in the context of larger business value.

> *The real issue isn't that finance sees security as a cost center—it's that too many security leaders haven't learned to articulate value in terms finance understands. Security leaders should spend their time showing how that cost translates to business protection. Finance teams make cost-benefit decisions all day long. They're not afraid of costs; they're afraid of costs they can't quantify or understand.*
>
> **Greg Notch**
> Chief Security Officer, Expel

SECTION 2

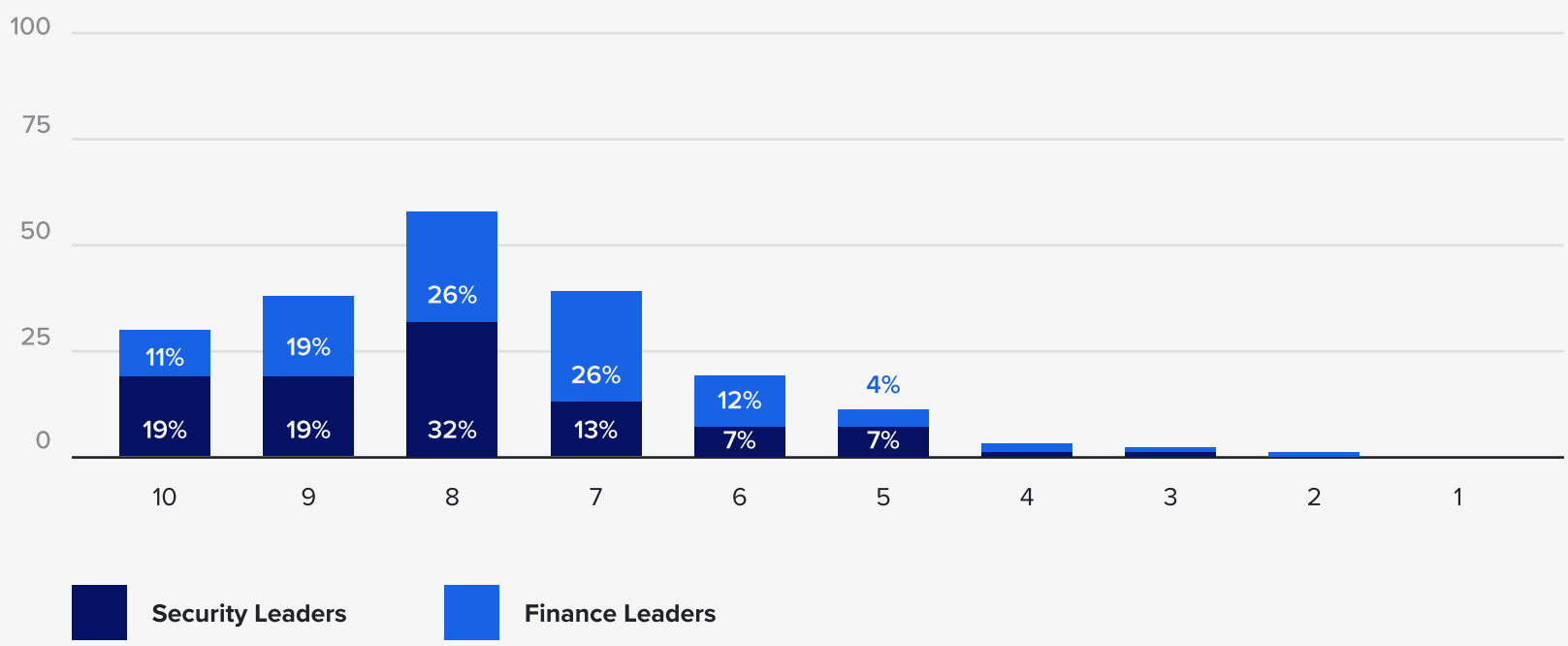
What security reports vs. what finance needs

Although both security and finance leaders consider their business impact measurement capabilities to be relatively mature, their responses show serious discrepancies in how they evaluate and communicate cybersecurity value. The two groups differ significantly in how they define risk, prioritize decision-making factors, and report on metrics.

70% of surveyed security leaders say their organization's ability to measure the business impact of cybersecurity initiatives is fully or very mature (8, 9, or 10 on a 10-point scale).

While finance decision-makers have a similar view, their perspective is decidedly less optimistic. Just over half (56%) of surveyed finance leaders say this ability to measure the business impact of cybersecurity initiatives is fully or very mature.

How security and finance leaders view their organization's cybersecurity business impact measurement capabilities on a scale of 1 to 10



SECTION 2

What security reports vs. what finance needs

> *Some data provided by the security team is difficult for the finance department to understand, which slows down the entire approval process.*
>
> **Director of Cybersecurity, Healthcare**

When reporting results to finance, surveyed security leaders typically prioritize metrics like business impact of actual security incidents (18%), cost of control versus potential losses (17%), security program maturity level (16%), and risk reduction score (15%).

Metrics that security leaders are most likely to report to finance or executive leadership

Business impact of actual security incidents	18%	Compliance / audit readiness	13%
Cost of control vs. potential losses	17%	Number of detected threats blocked	11%
Security program maturity level	16%	Incident response time	11%
Risk reduction score / trend	15%		

However, these metrics don’t align with what finance actually requires for making strategic decisions. In fact, program maturity level versus industry benchmarks is the second least popular metric among surveyed finance leaders.

SECTION 2

What security reports vs. what finance needs

> *Instead of falling back on maturity metrics, leaders need to communicate in the language of risk, especially when justifying security spend. The calculation requires taking the percentage (or percentage range) likelihood you'll have a breach and the cost of said breach. From there, you can determine that an investment that costs $x will likely lower your percentage likelihood of breach by x%. With that information, you can decide if that's something you're willing to take on.*
>
> **Greg Notch**
> Chief Security Officer, Expel

Instead, finance prefers security to report on strategic alignment with enterprise goals (54%) and investment efficiency (50%). Finance decision-makers also say that potential financial loss avoided (46%), audit readiness (45%), and time savings from less manual alert review (45%) are useful for understanding cybersecurity performance and value.

What finance leaders most want their security teams to report

Strategic alignment with enterprise goals	**54%**
Investment efficiency (cost vs. coverage)	**50%**
Potential financial loss avoided	**46%**
Audit readiness	**45%**
Time savings from less manual alert review	**45%**
Maturity vs. industry benchmarks	**44%**
Downtime prevention	**43%**

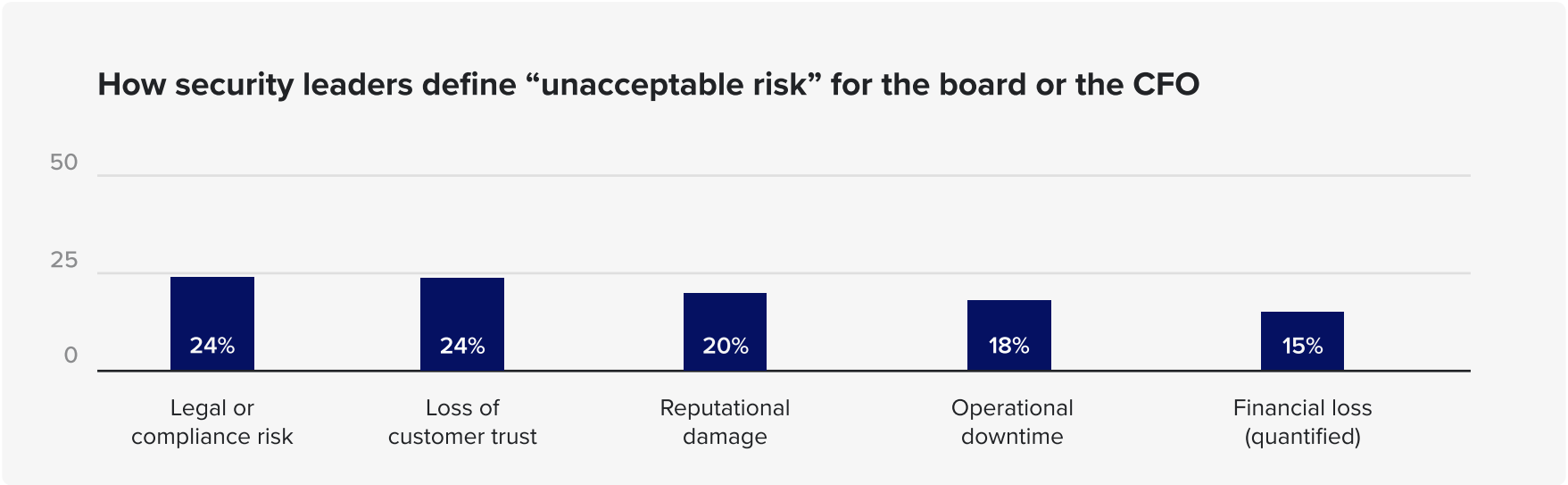
SECTION 2

What security reports vs. what finance needs

> *The biggest challenge is communicating cybersecurity risks in a way that resonates with business leaders. Bridging the gap between technical threats and their financial or operational impact is essential for securing buy-in and budget. But it remains difficult due to differing priorities and language between IT/security and executive teams.*
>
> **Director of Cybersecurity, Technology**

When sharing their perspectives with their CFO or board, surveyed security leaders are most likely to define “unacceptable risk” as legal or compliance risk (24%) or loss of customer trust (24%). Just 15% consider financial loss to be unacceptable risk.

Because security leaders are least likely to view financial loss as unacceptable risk, it’s no surprise that they think the CFO and the board are more likely to view their team as a cost center versus a strategic enabler.



SECTION 2

What security reports vs. what finance needs

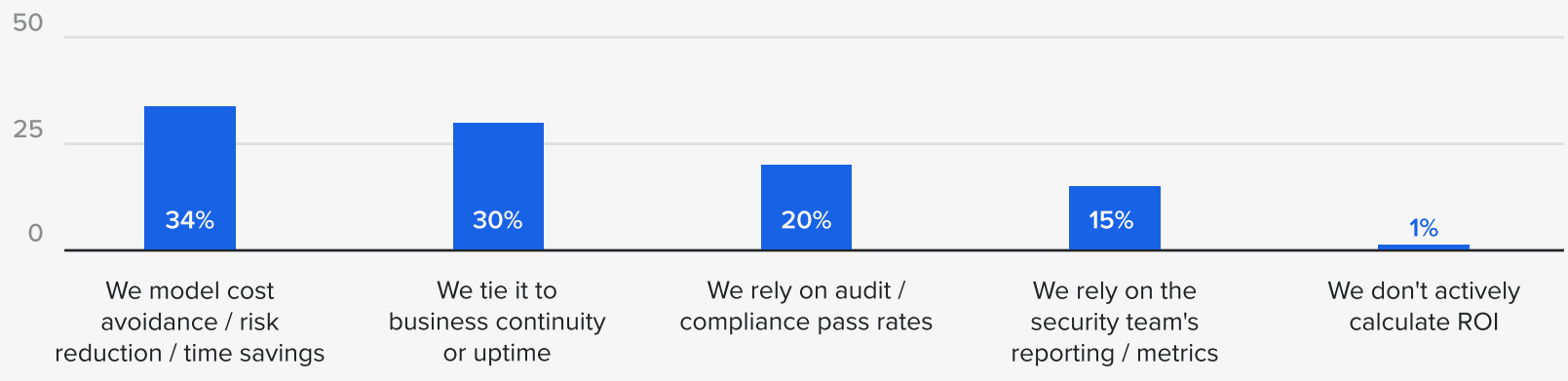
Security decision-makers may have a better chance of getting aligned with their finance counterparts if they reconsider how they define and report on risk. This often comes down to measuring risk by multiplying the likelihood of a security incident by the incident's financial, compliance, and reputational impact.

In fact, finance decision-makers rarely prioritize security reports or compliance metrics. When evaluating the ROI of security investments, just 15% of surveyed finance leaders say they rely on the security team's metrics, while 20% rely on audit or compliance pass rates.

Instead, when measuring security investment ROI, finance teams are more likely to model cost avoidance, risk reduction, or time savings (34%) or tie the investment to business continuity or uptime (30%).

> *These days, security needs to think of risk in terms of business resilience. For a while, breach prevention was the goal. Now, everyone accepts that breaches are inevitable. The trick is determining how to keep the business going post-breach while the breach is being remediated. This shift changes the conversation with finance entirely. Instead of asking for budget to prevent all attacks—which is impossible—security has to ask for investments in resilience that have a clear ROI. That's a conversation finance understands.*
>
> **Greg Notch**
> Chief Security Officer, Expel

How finance leaders evaluate the ROI of security investments



Yet enterprise security leaders are responsible for managing regulatory pressures. This means compliance and best practices tend to drive their investments.

SECTION 2

What security reports vs. what finance needs

In fact, surveyed security leaders say industry best practices (46%) are the biggest influence on security investment decisions. Compliance requirements (41%), ease of integration (41%), and ROI and cost efficiency (41%) are also important factors in these decisions.

Factors most influencing security investment decisions

Industry best practices	46%	Vendor reputation	38%
Compliance requirements	41%	Potential business disruption	35%
Ease of integration	41%	Executive / board pressure	31%
ROI / cost efficiency	41%	Threat landscape shifts	27%

To get on the same page, the two teams have to speak the same language. This may require security leaders to translate metrics into measurements that resonate with finance leaders. For example, “ease of integration” might turn into a time- or cost-based metric while “meeting compliance requirements” might translate into avoiding fines.

> *“Cybersecurity needs to learn to speak in the language of the business.* ***And finance is the lingua franca of the boardroom.*** *Everyone needs to learn to speak in the terms that finance uses—which is impact to bottom line, risk of business disruption, etc.”*
>
> **Greg Notch**
> Chief Security Officer, Expel

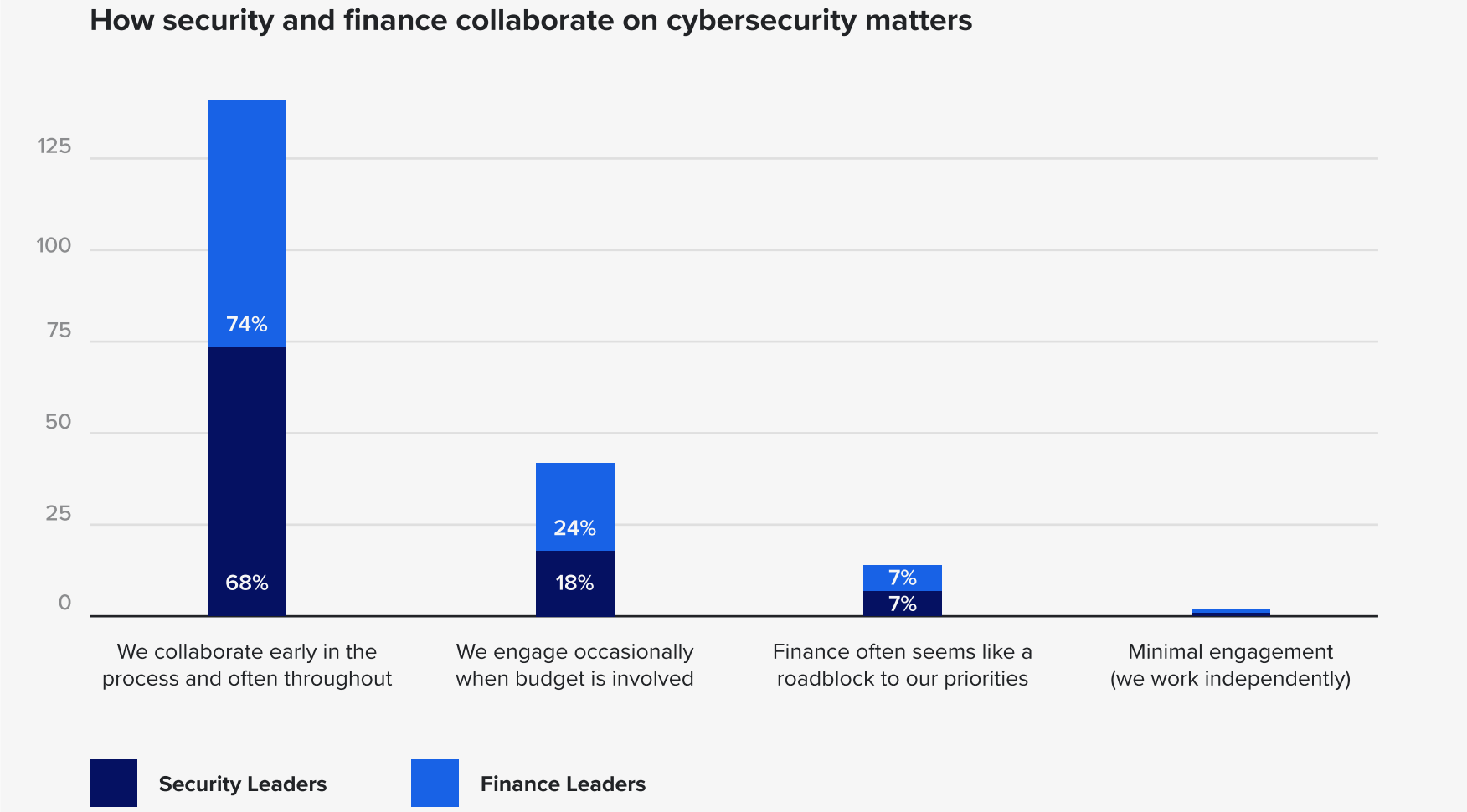
SECTION 3

When collaboration and alignment fall short

Finance and security leaders say they meet regularly for strategic planning, and both groups describe their working relationship positively. Yet their collaborative efforts aren't entirely successful. As a result, security leaders continue to struggle with familiar funding challenges while finance teams contend with persistent cost and ROI concerns.

Both groups of decision-makers agree that they frequently work together on cybersecurity concerns. 74% of surveyed security leaders say they collaborate with finance on cybersecurity matters early in the process and often throughout. 68% of surveyed finance leaders say the same about their collaboration with security.

While only 7% from each group say that their counterparts are roadblocks to their priorities, some still don't collaborate regularly. 18% of surveyed security leaders and 24% of surveyed finance leaders report engaging occasionally, only when budget is involved.



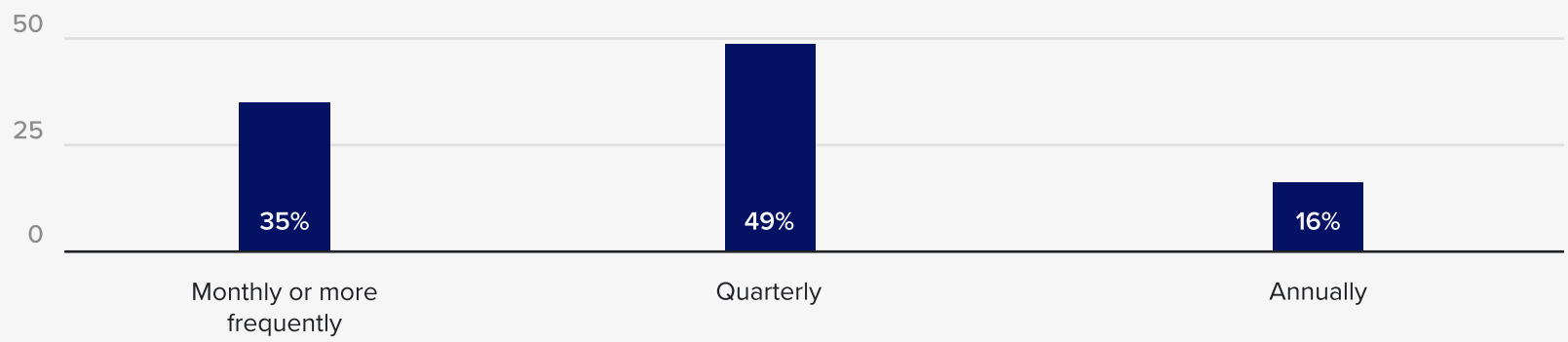
SECTION 3

When collaboration and alignment fall short

> *The biggest challenge is getting everyone to see that cybersecurity isn't just an IT issue, it's a business issue. It's tough to align when the risks we're flagging don't always translate clearly into dollars, delays, or lost opportunities. Bridging that gap between technical threats and business impact is where the real work happens.*
>
> **Director of Cybersecurity, Technology**

While this frequency may seem sufficient, it may not be enough to collaborate effectively. Nearly half (49%) of surveyed finance leaders say they meet with their organization's security leadership quarterly to discuss cybersecurity strategy or investment. While 35% say they meet monthly, 16% only meet annually.

How frequently finance and security discuss cybersecurity strategy or investment



Compared to all surveyed finance leaders, the segment that meets annually is less likely to report alignment with security. In fact, only 38% say they're fully or very aligned with security on risk tolerance and budget expectations, just 38% are very confident that security can align with business strategy, and a mere 27% say their security counterparts are aligned with the finance team's priorities.

SECTION 3

When collaboration and alignment fall short

> *Improving collaboration between security and finance requires better alignment on risk tolerance and clearer metrics that tie security investments to business value. While the relationship is improving, there's still a need for more structured communication and shared KPIs to ensure both teams are working toward common goals.*
>
> **Director of Cybersecurity, Technology**

Stakeholder interaction level may be another factor that limits how successfully finance and security decision-makers can collaborate. Most report interacting with director-level counterparts rather than with the C-suite.

Nearly half (49%) of surveyed finance leaders say they engage with directors of cybersecurity. Much smaller segments report engaging with CISOs (22%) or VPs of security (21%). Surveyed security leaders report similar interactions. The largest segment (41%) engages with directors of finance, while just 24% regularly collaborate with CFOs.

The security team members finance engages with on cybersecurity matters

Chief Information Security Officer (CISO)	22%
VP of Security	21%
Director of Cybersecurity	49%
Chief Risk Officer	7%

The finance team members security engages with on cybersecurity matters

CFO	24%
VP of Finance	14%
Director of FP&A	18%
Controller	3%

SECTION 3

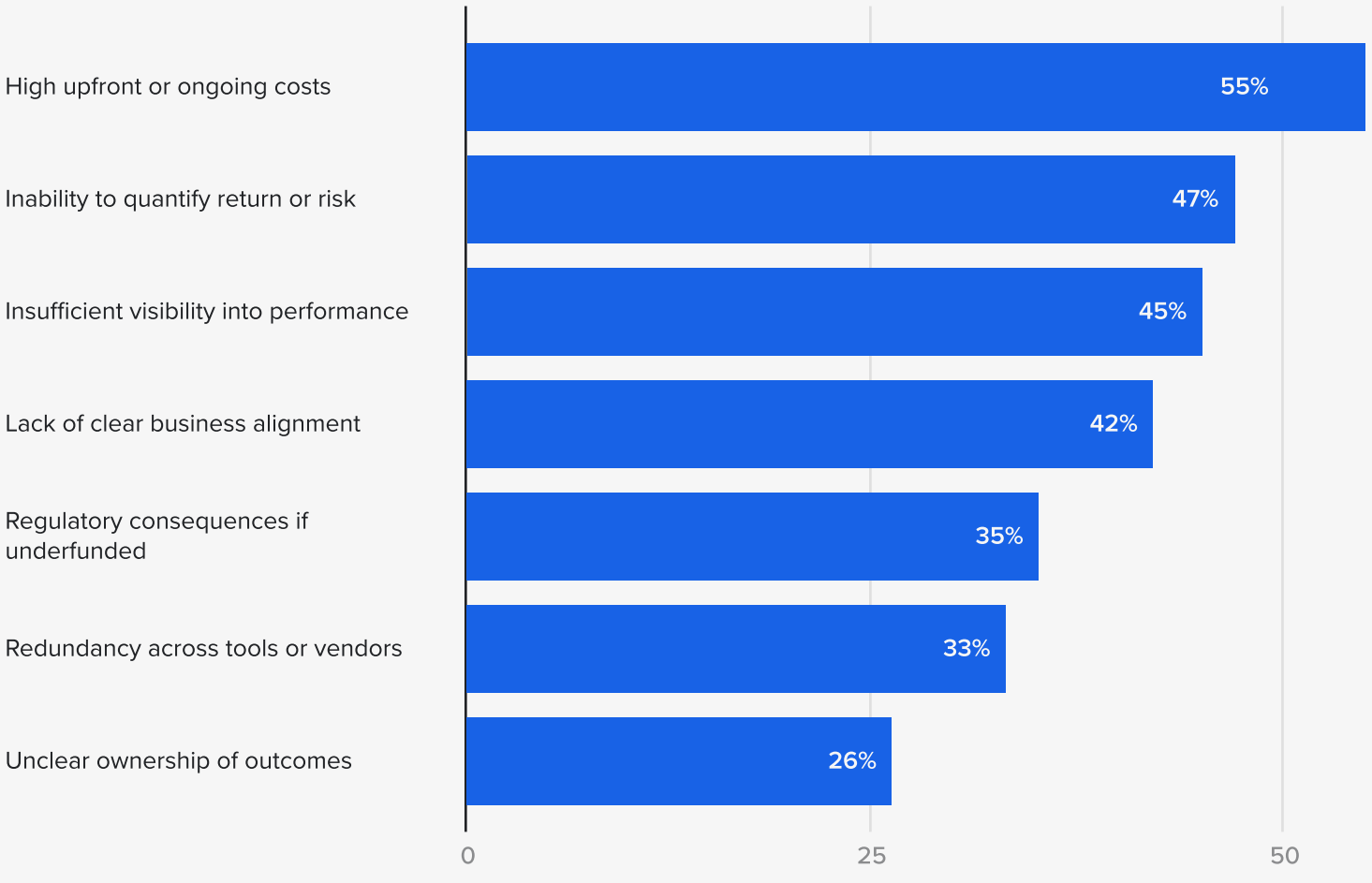
When collaboration and alignment fall short

How much does stakeholder interaction level matter for collaboration? Those who typically engage with C-suite counterparts report markedly higher levels of strategic alignment:

- 63% of security leaders who interact primarily with CFOs say finance is very aligned with security's priorities (versus 46% overall).
- 72% of finance leaders who interact primarily with CISOs say cybersecurity is a core strategic driver for the organization's business planning (versus 55% overall).

If security and finance can't collaborate effectively, cybersecurity investments may stall as security budgets are allocated elsewhere. When reviewing cybersecurity budget requests, surveyed finance leaders say their top concerns are high upfront or ongoing costs (55%), inability to quantify return or risk (47%), insufficient visibility into performance (45%), and lack of clear business alignment (42%).

Finance leaders' top concerns when reviewing cybersecurity budget requests

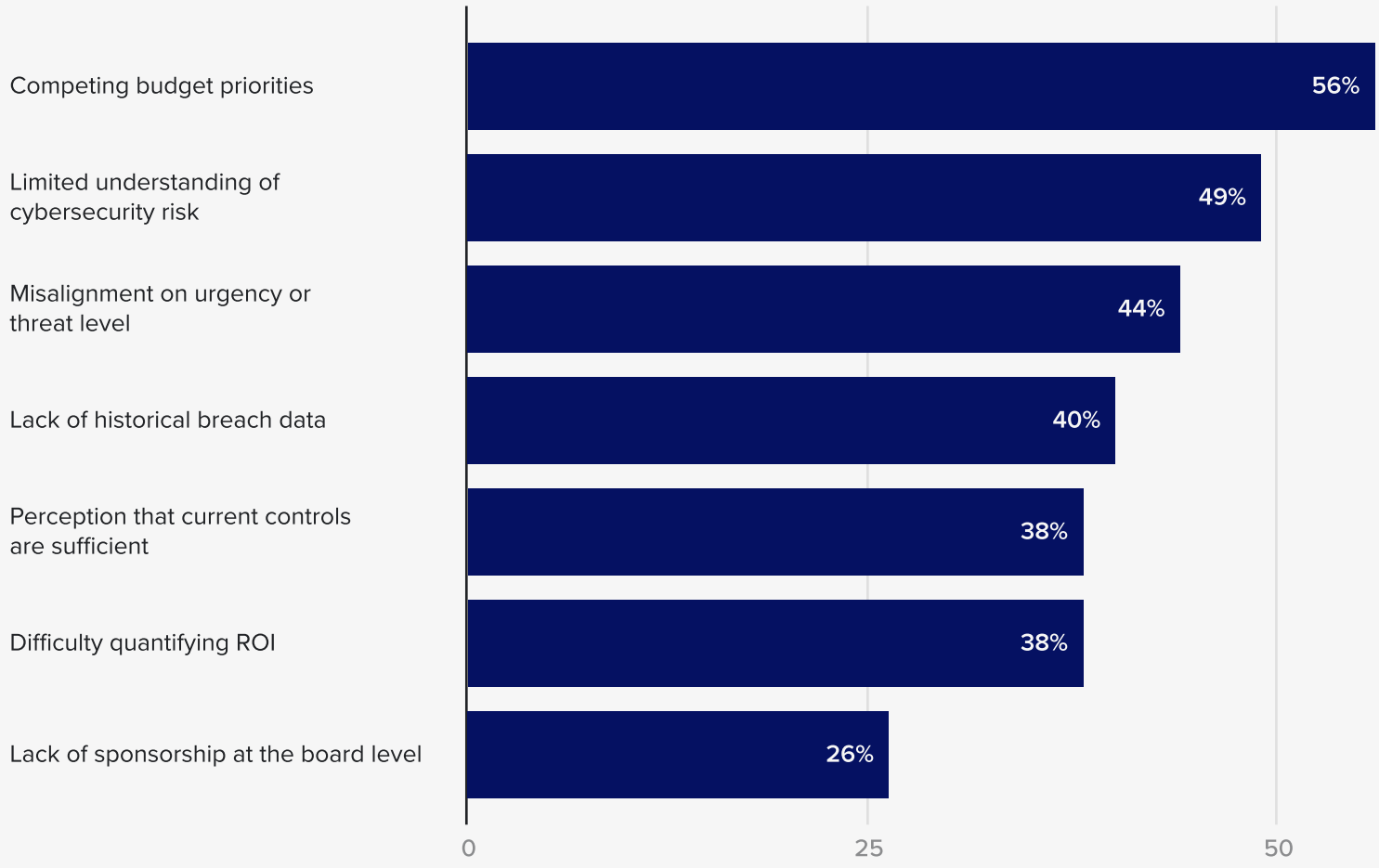


SECTION 3

When collaboration and alignment fall short

However, security teams don't always convey risk and urgency in a way that makes sense to finance. In fact, surveyed security leaders struggle most with competing budget priorities (56%), limited understanding of cybersecurity risk (49%), and misalignment on urgency or threat level (44%) when trying to obtain cybersecurity funding from finance.

Security leaders' main challenges when obtaining cybersecurity funding from finance



These responses reveal a shared problem. When considering cybersecurity budget requests, finance doesn't get the ROI, risk, or business alignment data they need to make a decision. At the same time, security doesn't get the budget they need because finance has a limited understanding of cybersecurity risk. Again, there's a clear language barrier that finance and security have to work together to overcome.

SECTION 4

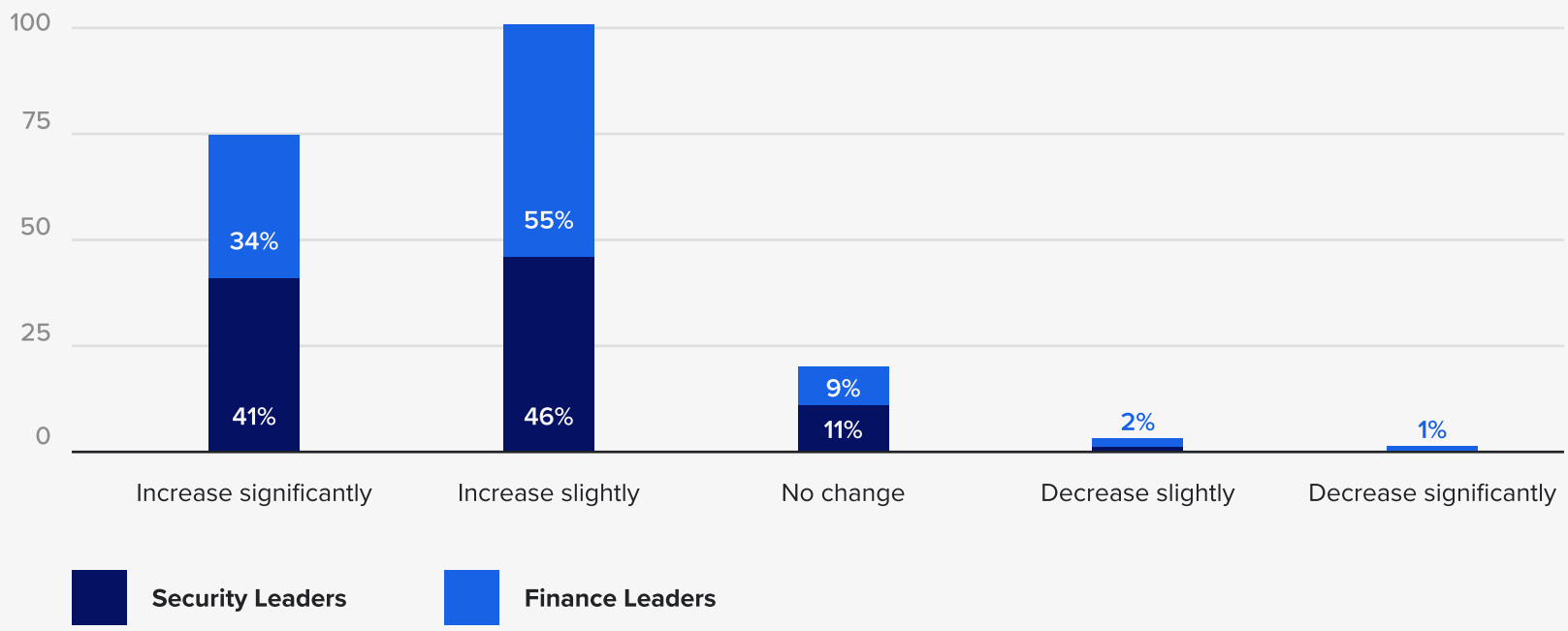
Bridging the gap between CISOs and CFOs

Despite struggles to secure funding, finance and security decision-makers remain optimistic about cybersecurity budget increases. To achieve true alignment and manage cybersecurity more effectively, however, finance and security teams must address communication and knowledge gaps.

Both security and finance teams expect cybersecurity budgets to increase in the coming year. Over the next 12 months, 87% of surveyed security leaders expect their cybersecurity budgets to increase, with 41% expecting a significant increase.

Finance isn't as bullish on budgets increasing by a significant amount. Over the next 12 months, 89% of surveyed finance leaders expect their cybersecurity budgets to increase. However, just 34% expect a significant increase.

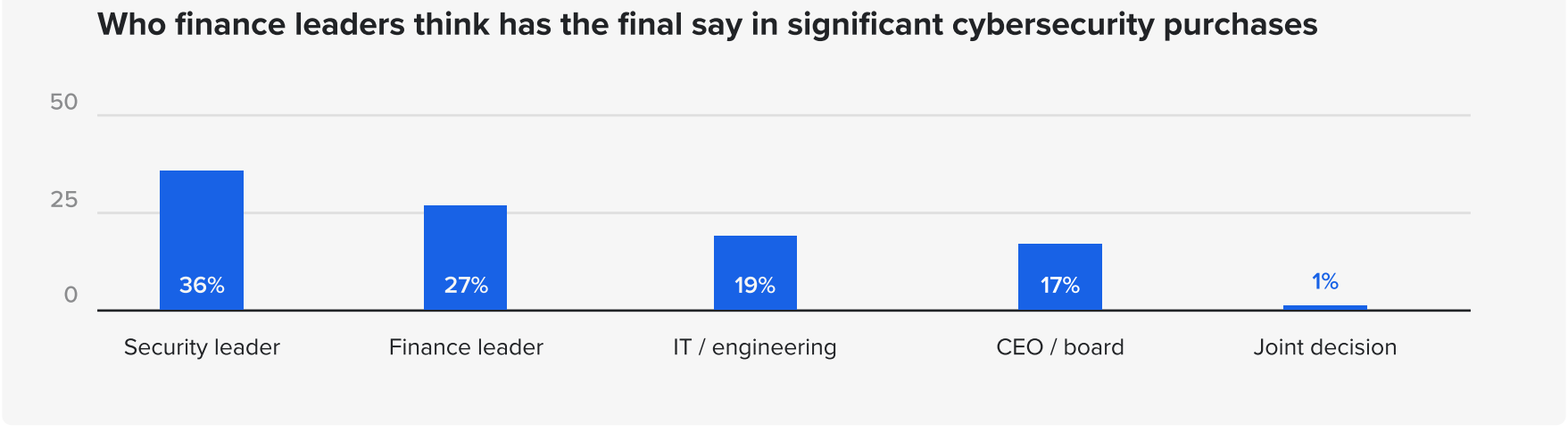
How security and finance leaders expect cybersecurity budgets to change in the next 12 months



SECTION 4

Bridging the gap between CISOs and CFOs

There's no clear consensus among finance leaders on who's ultimately responsible for making cybersecurity investment decisions. 36% of surveyed finance decision-makers think security leaders have the final say, while 27% believe finance leaders do. An additional 19% say IT or engineering does, and 17% report that the CEO or the board has the final say.



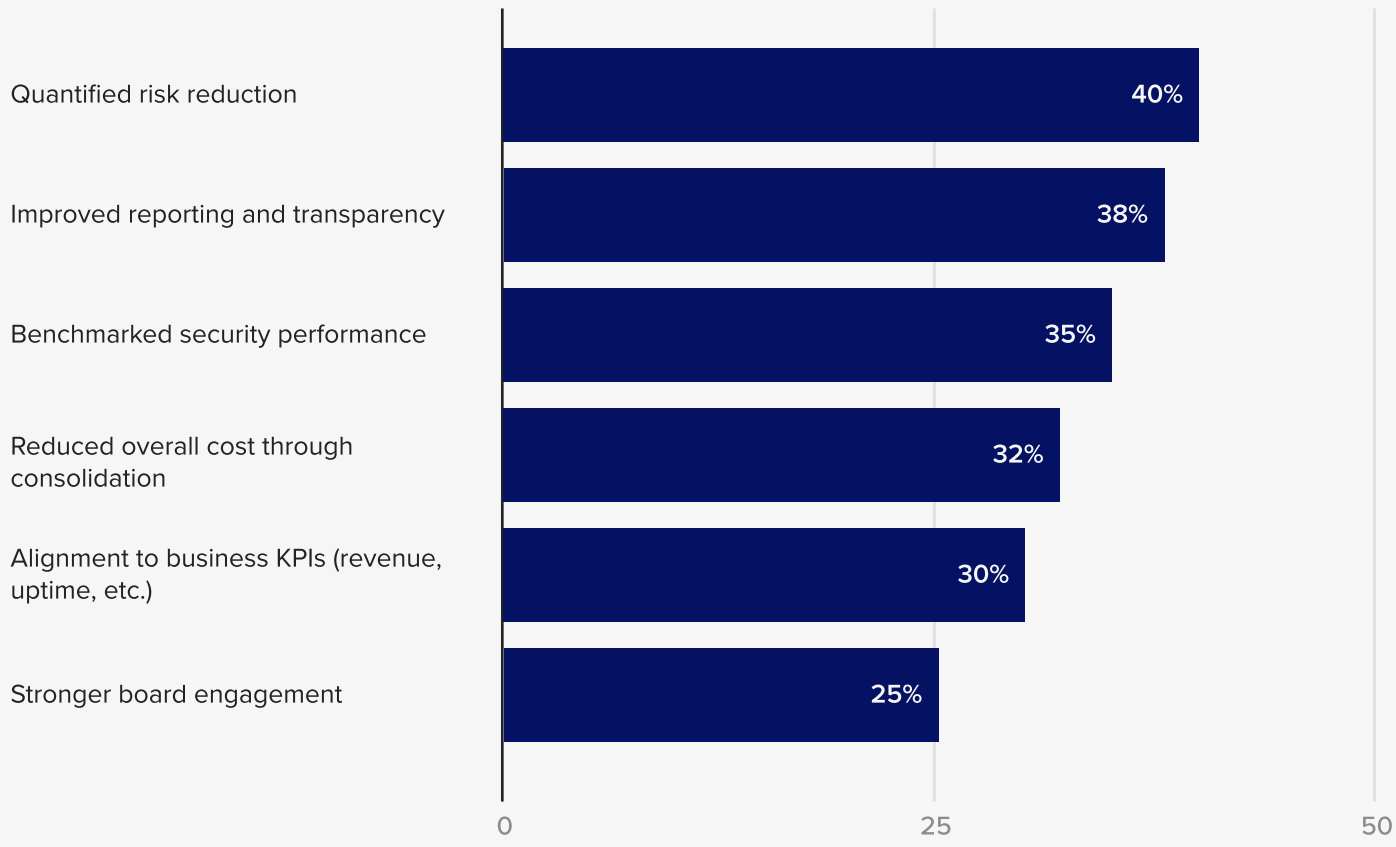
> *[Cybersecurity] is the company's safety barrier, and everyone should work together. The budget should be arranged based on actual needs; it's not a game between two departments.*
>
> **Director of Finance, Financial Services**

SECTION 4

Bridging the gap between CISOs and CFOs

The problem? Finance wants specific, measurable data before approving cybersecurity spending. Surveyed finance leaders say that quantified risk reduction (40%), improved reporting and transparency (38%), and benchmarked security performance (35%) would make it easier to justify an increased security budget.

Factors that would make it easier for finance to justify an increased security budget



> *The challenge is that precisely measuring risk is often impossible. I'd rather present a well-reasoned range than a false precision that falls apart under scrutiny. Finance teams work with uncertainty all the time; they understand models and ranges. What they don't tolerate is hand-waving or security teams who can't explain their assumptions.*

Greg Notch
Chief Security Officer, Expel

SECTION 4

Bridging the gap between CISOs and CFOs

The way that finance and security teams currently collaborate fails to address core structural and communication concerns. This creates a systems issue that prevents the two teams from successfully working together and efficiently making cybersecurity decisions.

When asked what would help improve collaboration between finance and security leadership, 51% of finance decision-makers cite clearer business cases for security investments, and 46% say training or education to bridge knowledge gaps.

> *The biggest challenge is the cross-departmental communication barrier, which makes it difficult to unify the awareness among different departments.*
>
> **Director of FP&A, Manufacturing**

Building on the push for more education, 43% of finance leaders say better translation of technical risk into financial terms would help. An additional 43% think shared accountability for cybersecurity outcomes would help the two teams work together.

Changes that finance says would improve collaboration between finance and security

Clearer business cases for security investments	51%	Joint planning sessions during budget cycles	41%
Training or education to bridge knowledge gaps	46%	Executive-level sponsorship or mandate	41%
Shared accountability for cybersecurity outcomes	43%	Use of common KPIs tied to business goals	40%
Better translation of technical risk into financial terms	43%	More frequent and structured communication	37%

SECTION 4

Bridging the gap between CISOs and CFOs

> *Improving regular communication and understanding of each other's priorities would enhance collaboration between security and finance teams.*
>
> **Chief Financial Officer, Technology**

On the surface, any disagreements between finance and security seem to revolve around metrics and decision-making mismatches:

- Finance wants reports on alignment with enterprise goals, investment efficiency, and financial loss avoided rather than metrics like maturity level or audit readiness. But security reports on security program maturity and business impact.
- Security makes decisions based on industry best practices, compliance requirements, and ease of integration. Yet finance focuses on modeling cost avoidance and risk reduction rather than compliance or security reports.

However, the real misalignment results from the language barrier between finance and security. Because the two teams use completely different frameworks and systems, their resources may be better spent on educating their counterparts and aligning on metrics that matter most to the business—ultimately, dollars and cents.

> *Cybersecurity teams have to understand the KPIs that matter to the business and how their operations ladder up into those. It's all about cybersecurity teams being able to communicate how their impact is contributing to those KPIs in the language of the business—which is all about dollars and cents.*
>
> **Greg Notch**
> Chief Security Officer, Expel

Conclusion

As the number of cyber attacks increases and the cost of these incidents grows year over year, making strategic cybersecurity investments has become mission critical for large enterprises. Yet misalignment on risk tolerance, business impact, and metrics prevents many security and finance teams from working together to mitigate these concerns.

The solution is clear. Rather than doubling down on metrics that their counterparts don't value or can't understand, CISOs and CFOs can both benefit from educating their counterparts. By bridging the knowledge gap, finance and security leaders work toward better alignment, clearer communication, and more strategic cybersecurity investments.

Practical tips for aligning with finance

Speak finance's language

Understand which metrics your finance team finds essential for making key decisions. Then, translate your metrics into terms they understand and educate them on how the disparate metrics actually align.

Prioritize executive dialogue

Prioritize C-suite engagement over director-level interactions. CISOs who regularly engage with CFOs report 63% very aligned relationships versus 46% overall. Push for regular strategic conversations at the executive level, not just tactical budget discussions.

Engage beyond budget cycles

Meet with your finance team at a regular cadence, not just at budget time. Educate them on the challenges you're facing and how those will translate into future investment needs.

Tie security to business resilience

Reframe security investments in terms of business resilience and cost avoidance. Show how security investments protect revenue, maintain operations, and reduce potential losses. Finance teams work with cost-benefit models—speak their language by quantifying risk reduction in dollars.

Establish shared accountability

Build shared accountability for cybersecurity outcomes between security and finance teams. Establish joint KPIs that matter to both functions—such as business continuity metrics, time-to-recovery benchmarks, or compliance cost avoidance—so both teams work toward common goals.

Practical tips for aligning with finance

From this → To that: The evolution of CISO–CFO collaboration

Current state	Target state
Conversations focus on spend and risk avoidance	Conversations focus on resilience, ROI, and measurable outcomes
Security reports technical metrics	Security reports business-aligned metrics (cost avoidance, uptime, continuity)
CFO sees security as a cost center	CFO sees security as a value protector
Meetings are quarterly or reactive	Meetings are monthly, proactive, and data-driven
Alignment depends on individuals	Alignment is built into shared KPIs and governance

From activity metrics to investment decision metrics

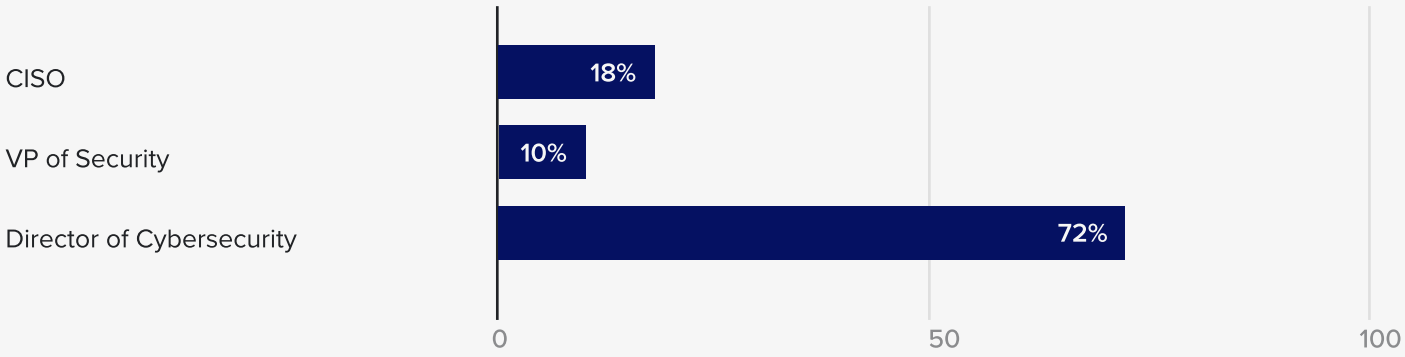
What security often reports	What finance needs for investment decisions
Number of alerts handled	Estimated cost savings from automation or reduced analyst hours
% of systems patched	Risk reduction value of protecting top business-critical systems
Tool coverage / control adoption	ROI of each control (cost vs. risk reduction)
Mean time to detect / respond	Potential financial impact avoided from faster containment
Security training participation rate	Reduction in incident likelihood or loss due to user behavior
Audit pass rate	Regulatory or insurance cost savings linked to compliance
Program maturity score	Projected improvement in risk-adjusted return on security spend

Methodology and demographics

Expel commissioned an independent market survey from UserEvidence that included 300 executive leaders across two audience segments: 136 cybersecurity leaders and 164 finance leaders.

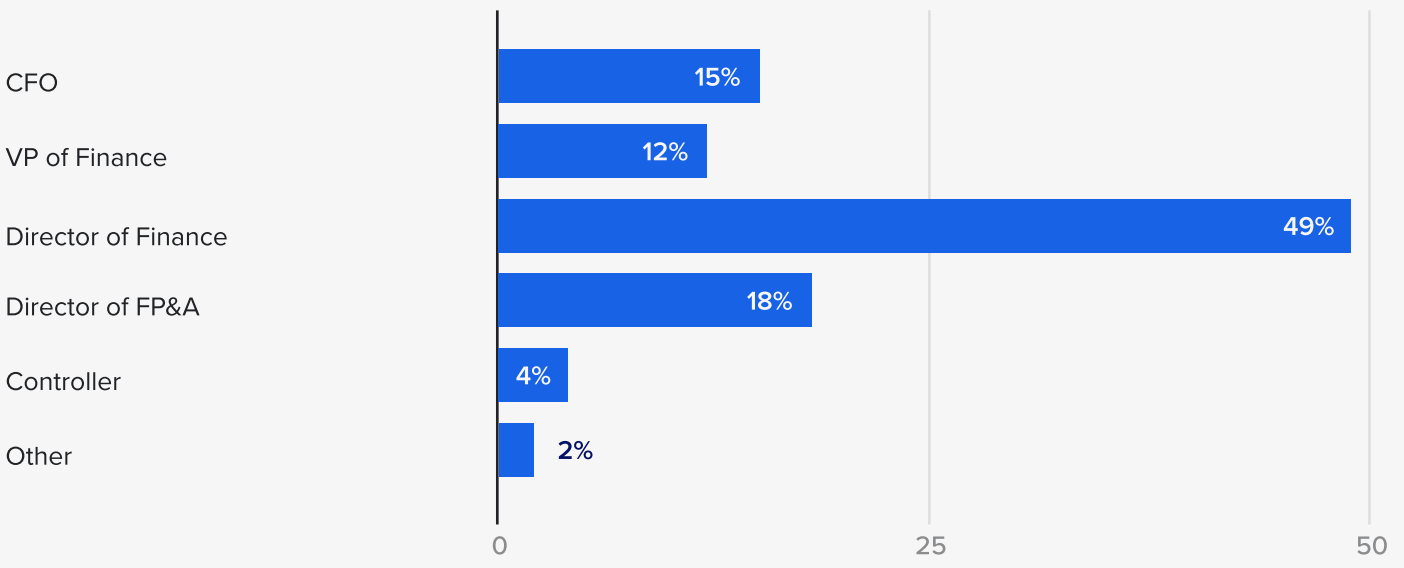
Respondents in the security leader segment primarily held Director of Cybersecurity (72%) and CISO (18%) titles.

Roles in the cybersecurity leader audience segment



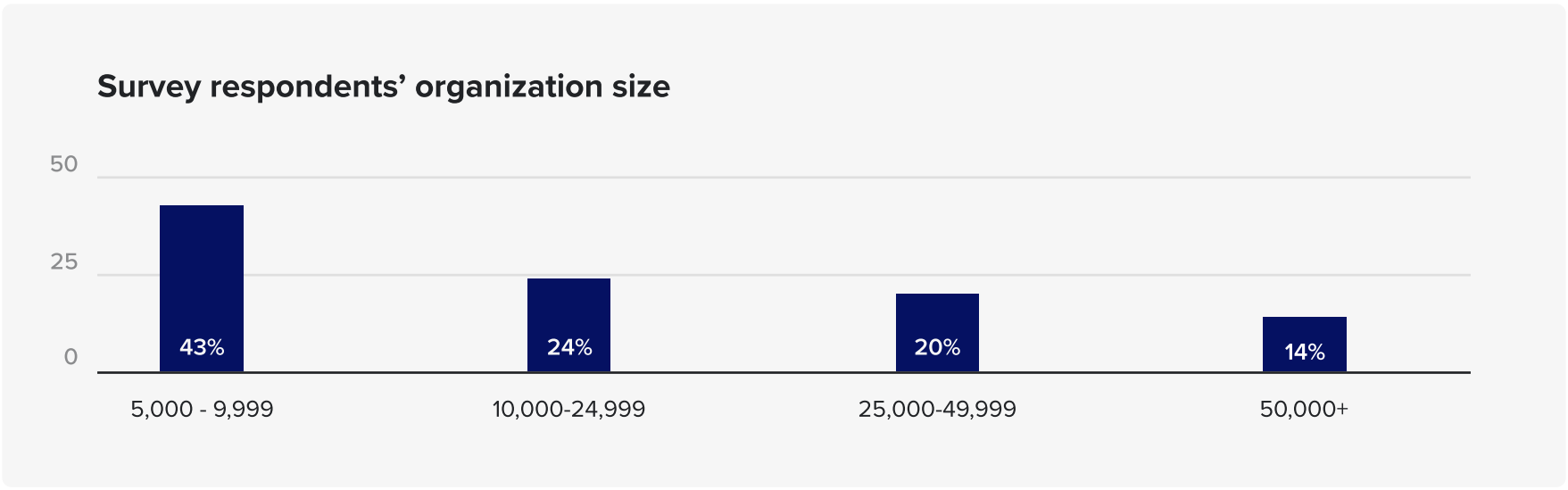
Those in the finance leader segment primarily held Director of Finance (49%), Director of FP&A (18%), and CFO (15%) titles.

Roles in the finance leader audience segment

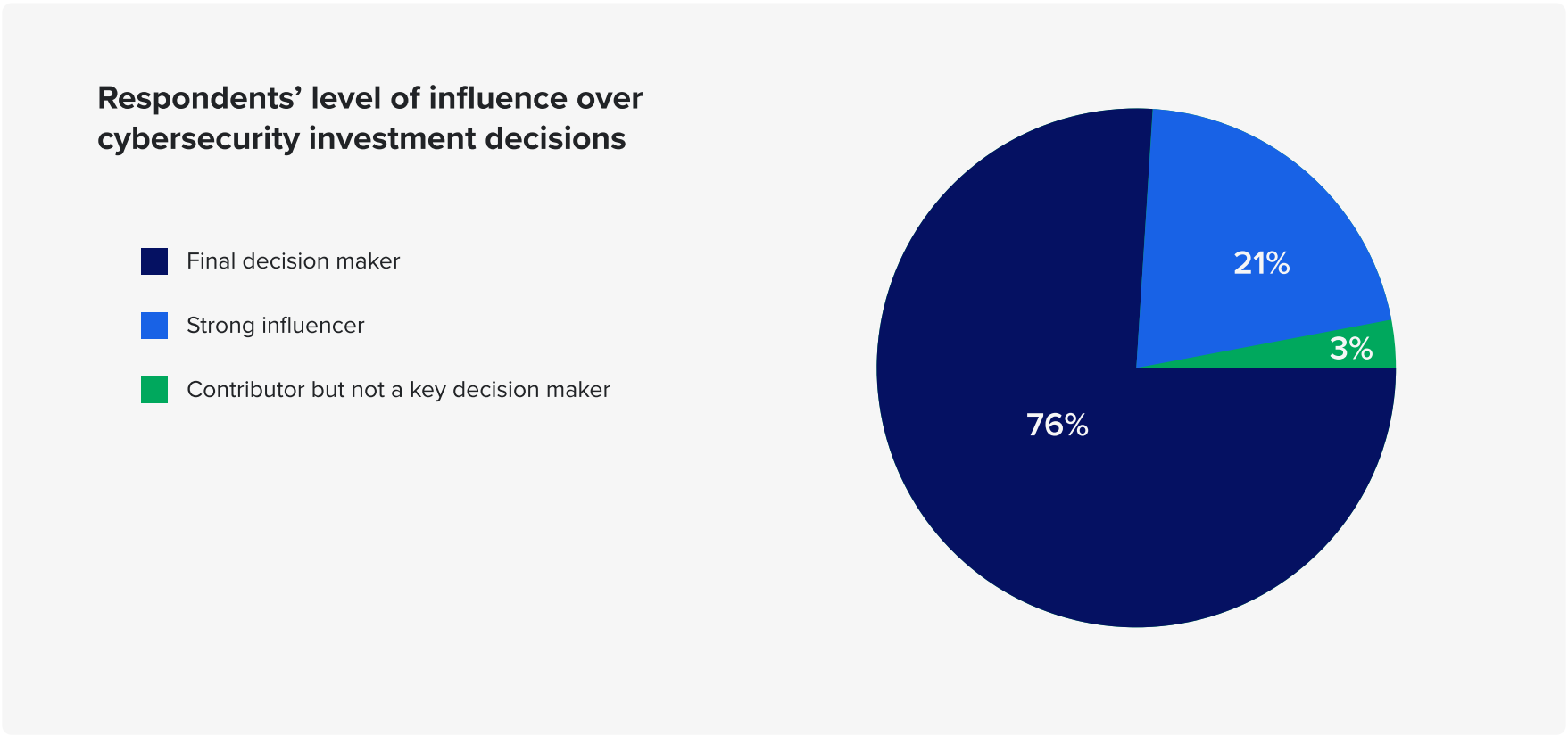


Methodology and demographics

All respondents represented organizations with at least 5,000 employees. More than half (58%) worked for organizations with 10,000 or more employees, and 14% worked for organizations with 50,000 or more employees.

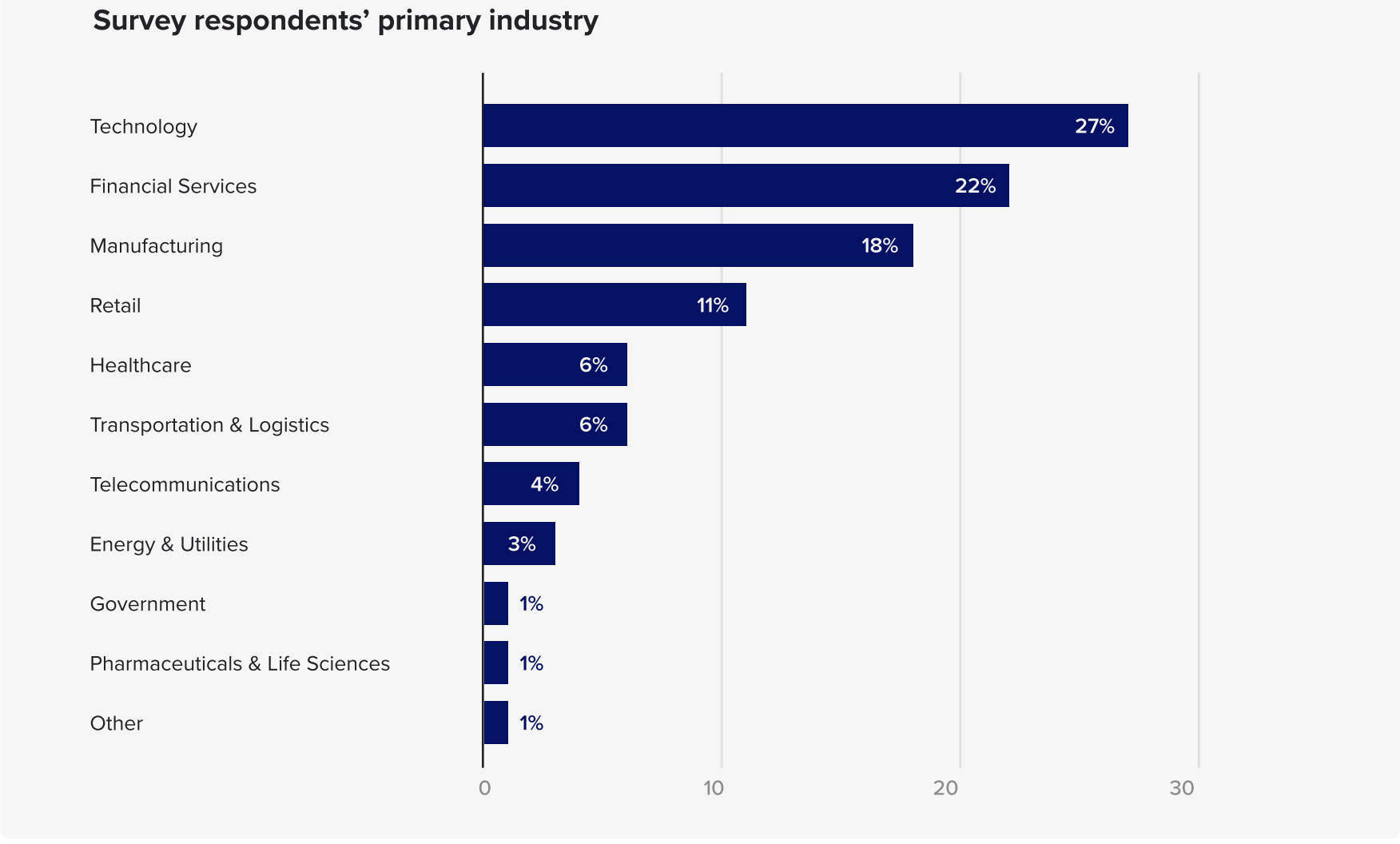


Respondents had a range of authority levels over cybersecurity decisions. More than three-quarters (76%) identified as final decision-makers for cybersecurity investments. 21% identified as strong influencers, while 3% were contributors to these decisions.



Methodology and demographics

Respondents represented 10 industries, including technology (27%), financial services (22%), manufacturing (18%), and retail (11%).



Survey data collection took place in July 2025. The research sample was vendor-neutral and did not target Expel or UserEvidence customers, although they were not excluded from participating in the survey.

About UserEvidence

UserEvidence is a software company and independent research partner that helps B2B technology companies produce original research content from practitioners in their industry. All research completed by UserEvidence is verified and authentic according to their research principles: Identity verification, significance and representation, quality and independence, and transparency. All UserEvidence research is based on real user feedback without interference, bias, or spin from our clients.

UserEvidence research principles

These principles guide all research efforts at UserEvidence—whether working with a vendor's users for our Customer Evidence offering, or industry practitioners in a specific field for our Research Content offering. The goal of these principles is to give buyers trust and confidence that you are viewing authentic and verified research based on real user feedback, without interference, bias, and spin from the vendor.

1. Identity verification

In every study we conduct, UserEvidence independently verifies that a participant in our research study is a real user of a vendor (in the case of Customer Evidence) or an industry practitioner (in the case of Research Content). We use a variety of human and algorithmic verification mechanisms, including corporate email domain verification (i.e., so a vendor can't just create 17 Gmail addresses that all give positive reviews), and pattern-based bot and AI deflection.

2. Significance and representation

UserEvidence believes trust is built by showing an honest and complete representation of the success (or lack thereof) of users. We pursue statistical significance in our research, and substantiate our findings with a large and representative set of user responses to create more confidence in our analysis. We aim to canvas a diverse swatch of users across industries, seniorities, personas—to provide the whole picture of usage, and allow buyers to find relevant data from other users in their segment, not just a handful of vendor-curated happy customers.

3. Quality and independence

UserEvidence is committed to producing quality and independent research at all times. This starts at the beginning of the research process with survey and questionnaire design to drive accurate and substantive responses. We aim to reduce bias in our study design, and use large sample sizes of respondents where possible. While UserEvidence is compensated by the vendor for conducting the research, trust is our business and our priority, and we do not allow vendors to change, influence, or misrepresent the results (even if they are unfavorable) at any time.

4. Transparency

We believe research should not be done in a black box. For transparency, all UserEvidence research includes the statistical N (number of respondents), and buyers can explore the underlying blinded (de-identified) raw data and responses associated with any statistic, chart, or study. UserEvidence provides clear citation guidelines for clients when leveraging research that includes guidelines on sharing research methodology and sample size.

About Expel

Expel is a managed detection and response (MDR) provider that helps security teams detect and stop threats fast. With Expel, customers get 24x7 coverage across cloud, identity, email, endpoint, and network—with complete transparency into every alert, investigation, and action through Expel Workbench™. Our security operations team combines deep practitioner expertise with AI-driven automation to analyze billions of events each month and achieve a sub-20-minute mean time to remediate for critical alerts. We integrate with customers' existing security tools, so organizations can maximize their current investments while building more resilient security programs. Expel serves hundreds of customers globally, from high-growth companies to established enterprises. For more information, visit expel.com or follow us on LinkedIn.

Learn more

expel®