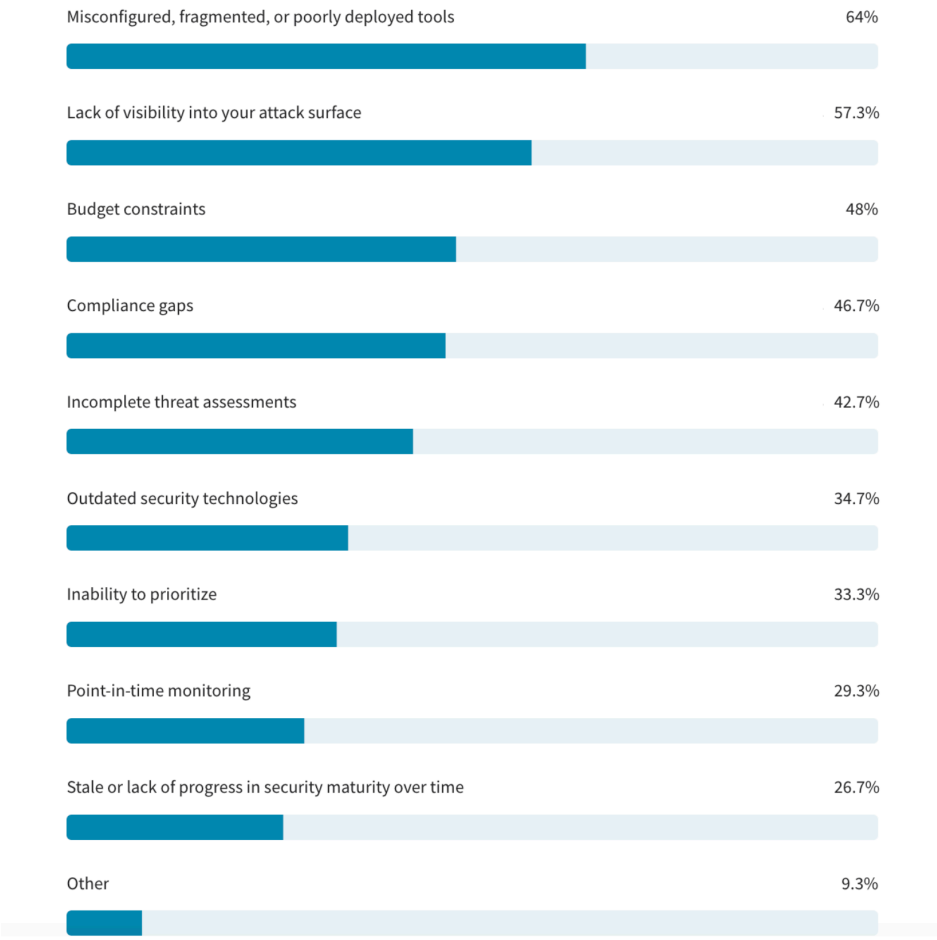
Security Debt Survey

Question 1. What specific challenges or incidents have you faced due to accumulated security debt? (Check all that apply)



Challenges and Incidents Faced Due to Accumulated Security Debt

Organizations have reported several challenges and incidents stemming from accumulated security debt, impacting their operations in various ways:

Vendor / Third-Party Incidents: Some organizations highlighted incidents involving vendors or third parties, leading to operational ineffectiveness and business continuity/disaster recovery (BC/DR) issues. These incidents underscore the risk external partners can pose when security debt is not adequately managed.

Delayed Fixes for Simple Issues: A common theme was that organizations face simple issues that require simple fixes but remain unresolved due to resource constraints or prioritization challenges, leading to delays and backlogs in resolving security debt.

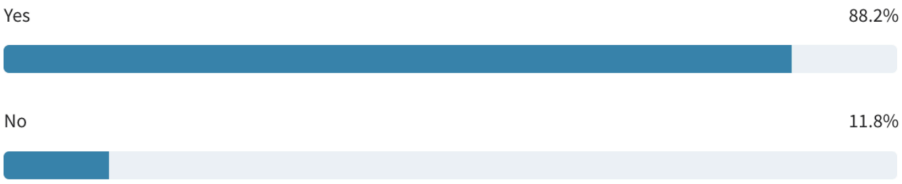
These insights reveal that accumulated security debt can significantly hinder operational efficiency, business continuity, and overall security posture if not managed proactively.

Comments:

1) “Increasing the attack surface”
2) “Staff burnout”
3) “Culture of security”
4) “Hacked”
5) “Velocity”
6) “I think all of these topics are very relevant. My response is focused on the reality that we need to keep the most important thing, the most important thing. Ergo, you accept risk on certain fronts. And that's why you build a defense-in-depth architecture. So my response is really focused on what stops us MOVING FORWARD, not what has held us up in the past/current state.”
7) “Business priorities”

Question 2. Do you currently have a strategy in place to assess and eliminate security debt within your organization?

Technology Debt (i.e. misconfigurations, unpatched vulnerabilities, poor asset management, etc.)



Strategy for Assessing and Eliminating Technology Debt

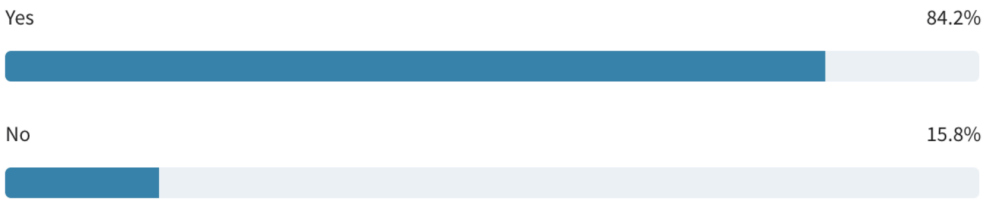
Organizations are increasingly prioritizing strategies to tackle technology debt, which includes misconfigurations, unpatched vulnerabilities, and poor asset management. The responses reveal the following:

- Yes: A significant 88.2% of organizations have a strategy in place to assess and eliminate technology debt, showing a strong commitment to proactively managing and mitigating security risks.
- No: Only 11.8% do not currently have such a strategy, highlighting a small segment still needing to implement proactive measures.

This data underscores the importance placed on having a clear, structured approach to manage technology debt, with the vast majority of organizations recognizing the critical need to address these vulnerabilities systematically.

Question 3. Do you currently have a strategy in place to assess and eliminate security debt within your organization?

Process Debt (i.e. lack of automation, reactive approach, limited metrics and reporting, etc.)



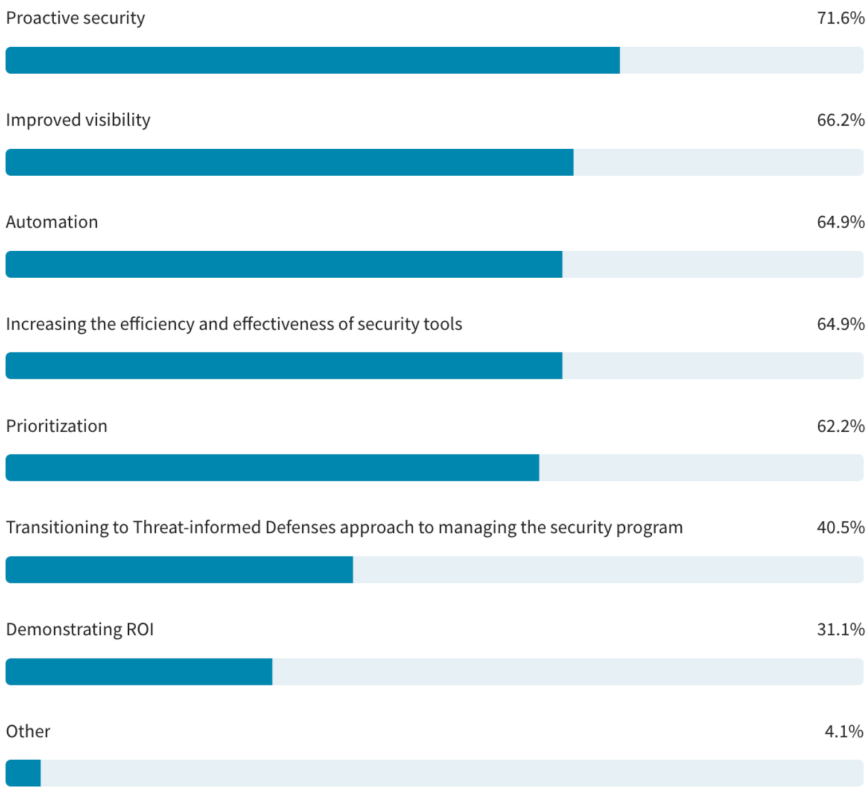
Strategy for Assessing and Eliminating Process Debt

Organizations are actively implementing strategies to address process debt, which includes challenges like lack of automation, reactive approaches, and limited metrics and reporting. The responses show:

- Yes: An overwhelming 84.2% of organizations have a strategy in place to assess and eliminate process debt, indicating a widespread focus on improving operational efficiency and proactive management.
- No: Only 15.8% of organizations lack a strategy, reflecting a minimal portion still working towards adopting measures for process optimization.

This data demonstrates that most organizations are committed to systematically improving their processes, emphasizing automation, proactive planning, and comprehensive reporting.

Question 4. Which of the below do you have a strategy to address in regards to debt in your organization? (Check all that apply)



Strategic Approaches to Address Debt Within Organizations

Organizations employ multiple strategies to manage and reduce debt effectively. The most common strategies include:

- Automation: 64.9% of organizations focus on automation to streamline processes and reduce manual intervention, highlighting its critical role in debt management.
- Increasing the Efficiency and Effectiveness of Security Tools: 64.9% prioritize optimizing their security tools to ensure they are effective and efficient.
- Prioritization: 62.2% of organizations emphasize prioritizing tasks and resources to address debt systematically.
- Improved Visibility: 66.2% aim to enhance their visibility, ensuring they have a comprehensive understanding of their security posture.
- Proactive Security: 71.6% implement proactive measures to anticipate and mitigate risks before they escalate.
- Transitioning to Threat-informed Defenses: 40.5% of organizations are adopting a threat-informed defense approach to manage their security programs more effectively.

- Demonstrating ROI: 31.1% focus on showing the return on investment from their strategies and tools to justify and optimize security spending.
- Other Methods: A small segment, 4.1%, reported using additional, organization-specific strategies.

Overall, organizations emphasize a holistic approach, integrating various elements like automation, tool efficiency, and proactive measures, to create a comprehensive strategy that addresses multiple facets of security debt.

Comments:

1) “Recruitment”
2) “It's all of these things. They are not siloed. The things called out in the last 3 questions ARE THE STRATEGY.”
3) “In depth Risk assessment designed to clearly call out Risk”

Question 5. What specific challenges or incidents have you faced due to accumulated security debt, and how have they affected your operations?

Comments:

1) Vendors not keeping pace with new security attack methods thus event being classified as low risk when it should have been medium or high.
2) Alert Fatigue
3) It was a long time ago and mostly with IT
4) Translation of huge data to actionable items
5) Outdated systems. Is some difficult to protector legal systems
6) None at the moment, however staying on top of security that are industry specific can be challenging.
7) Lack of visibility
8) Increased risk
9) Unknown. I am new to the organization.
10) Mean Time to Remediate
11) Lack of availability of the resources to remediate the vulnerabilities. Lack of internal knowledge to fine-tune and leverage the existing tools

12) The challenge is getting the resources outside of security (Infrastructure team) to work alongside to obtain the access and configurations needed in security tools.
13) Due to understaffing, we've seen burnt out staff impacting productivity and retention.
14) data loss, increased labour needed to resolve the issue thus costing the company time and money
15) challenge of trained resources, up-to-date technology, can't update the legacy
16) complicated incident response
17) Assisting the threat to prioritize it
18) In a past org every security incident involved assets the security team was unaware existed.
19) Technical debt is a regular source of systemic failures. Something that should have easily been maintained, it ends up costing a lot of labour and finances
20) We have had high profile exploits
21) Getting hacked, cost a lot of money
22) Exposure happened and the patch didnt go quickly enough
23) Getting Certifications - took long
24) Lack traceability, if you don't know what you are using, you dont know the vulnerabilities
25) length of the project and level of investment required
26) Aligning Senior management to understand the cyber risk is now a business risk.
27) Budget cuts and CICD de prioritization.
28) Lack of understanding companywide about why this is important to address.
29) Lack of visibility to threats on the perimeter, inability to understand application based data leakage, and inability to patch for zero day vulnerabilities. This creates and environment where we are fire chasing and overly reliant on individuals knowledge of legacy systems and traffic patterns, forcing me to hire more specialized resources.
30) Visibility and automation
31) Tools designed to monitor non-cloud environment that is now being replaced by cloud. Running duel tools (one for cloud and one for dying on prem)
32) Vendor / Third Party Incidence - Operational ineffectiveness and BC/DR issues
33) Simple issues, with simple fixes, that are just waiting in line.
34) No real incidents, but greater inefficiencies

35) Agile methods have resulted in multiple overlapping teams providing services/apps to a single customer product that each individually are secure but have no corelated security with the overall product. For example, it is impossible to see which internet host attempted a credit fraud because there are 15 API layers between the product edge and the internal fraud prevention control.
36) It really pushes to IAM Governance. Legacy stuff always ends with 'some person/function still needs access to some old thing, cuz that's how they work'. That applies to business units, and it applies to our own cyber teams who want to work the way they want to work. This is a change management issue, and how you organizationally address forcing change for the laggards who don't want change to occur.
37) Compliance gaps
38) Lack of attack surface
39) Lack of sdlc program due to budget constraints leading to risky processes and no standards.
40) Inability to provide clear and defendable metrics to executives and board.
41) Because of the scope of our security landscape and a legacy of decentralized IT, it is a challenge to get a holistic picture of our security posture and to get past the "playing whack-a-mole" stage of information security.
42) The impact of accumulated security debt is a pressing and persistent challenge, particularly in large, established environments like ours. This debt, which results from years of postponed updates, deferred replacements, and the prioritization of immediate business needs over long-term security health, demands our immediate attention. Some of the specific incidents I've faced include: Delayed Patching & Vulnerability Exposure: We have had instances where legacy systems, due to age and lack of updates, created unpatched vulnerabilities. An incident from last year comes to mind—an outdated database running a crucial application had missed several patches. Despite compensatory controls, a minor exploit slipped through. Although we were able to contain it before escalation, it was a wake-up call for the business to prioritize security debt. Compliance Gaps: Security debt often manifests as regulatory compliance challenges, particularly in industries like energy, where OT security is critical. We once faced an audit that uncovered gaps in compliance with newer regulations—mostly related to legacy

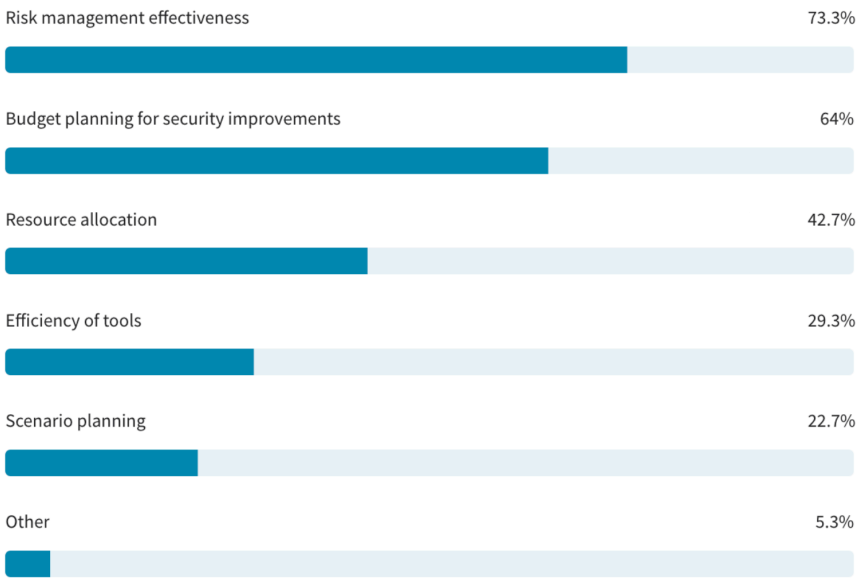
systems that were difficult to secure by modern standards. These gaps created urgency for remediation and showcased the operational delays that debt can cause, especially as teams scramble to retroactively patch. Incident Response Lag: Security debt can slow incident response, especially when legacy components don't communicate well with modern monitoring systems. In one case, our response time was hindered by poor integration between old and new systems, which complicated data aggregation and extended analysis time. Impact on Operations Operationally, this debt strains resources increases costs and adds complexity to already challenging projects. Integrating older systems with newer security platforms, for instance, demands additional attention from both security and IT teams. It also affects project timelines, especially when bringing new services to production, as we need to factor in extra cycles for securing legacy dependencies. Strategies I've Implemented To manage and reduce security debt, I've pushed for a tiered remediation strategy that classifies debt by risk impact, allowing us to prioritize high-risk areas first. We've also emphasized better visibility into our debt by adding dashboards that track outstanding issues, making the impact visible to the executive team. Additionally, I'm working to embed security risk assessments into the business case for all new technology projects, ensuring that we address debt from the outset rather than retroactively.

43) Budget restrictions
44) Achieving transparency and consistent risk output
45) Growth through aggressive acquisition for many years have created a large backlog of medium-low risks to address
46) Speed in remediation or mitigation
47) High number of exploitable vulnerabilities.
48) Prioritization
49) Cloud security gaps
50) Inability to innovate
51) Lack of visibility and in ability to connect out dated tech to new advance security tech that limits and hampers ability to drive true zero trust approach
52) Limited visibility into legacy technologies limits ability to proactively detect and respond to issues

53) limited skillsets, resourcing, and training across IT operations owners leads to increased burden and oversight of IT Security across all areas, tools, and domains
54) Increased cs teams to keep up with patch/vulnerability demands.
55) Gaps in security compliance
56) Under resourced security staffing
57) staff burnout, firedrills
58) Never-ending firefighting, tons of extra time to investigate issues and implement improvements, unclear impacts of changes
59) Lack of available resources on the IT Infrastructure side
60) Delay in security response due to incomplete CMDB
61) no incidents but a handful of legacy systems present a compliance and insurance challenge

---

Question 6. How do you measure the financial and operational impact of security debt on your organization? (Check all that apply)



Measuring the Financial and Operational Impact of Security Debt

Organizations employ several methods to assess the financial and operational impact of security debt. The most common approaches include:

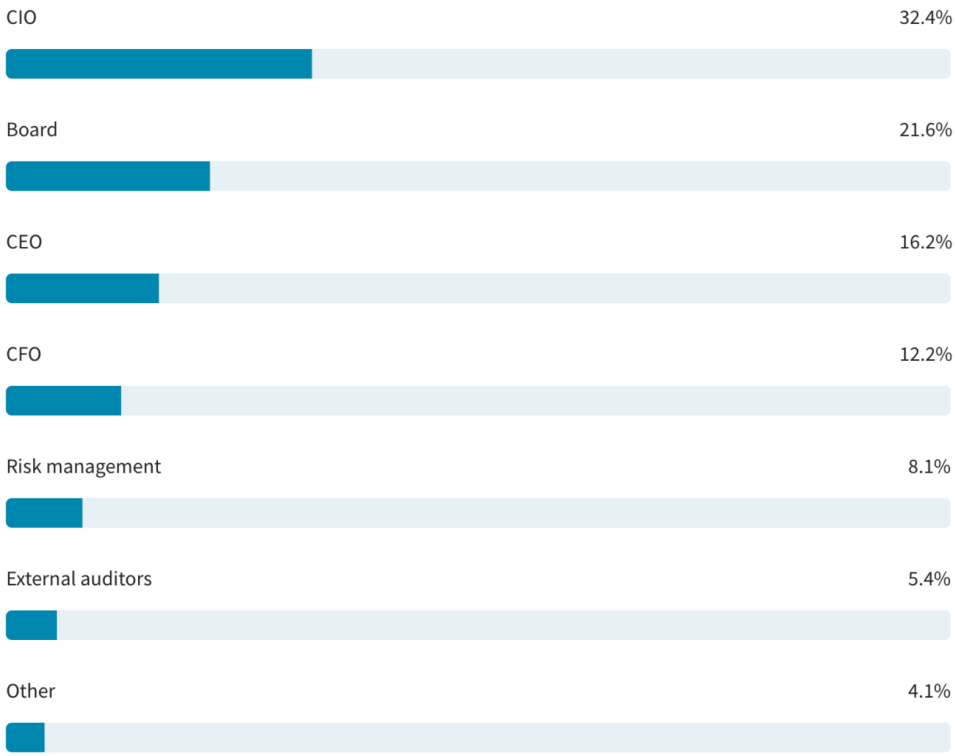
- Risk Management Effectiveness: Used by 73.3% of organizations, this method is the most prevalent, emphasizing the need to evaluate security risks continuously.
- Budget Planning for Security Improvements: Adopted by 64% of organizations, this approach aligns financial resources with security needs, ensuring that investment decisions address security debt effectively.
- Resource Allocation: Utilized by 42.7% of organizations, focusing on optimizing manpower and other resources to mitigate the impact of security debt.
- Efficiency of Tools: 29.3% of organizations assess the performance of their tools and technologies to ensure they are effectively managing security debt.
- Scenario Planning: Practiced by 22.7%, this approach anticipates potential challenges and develops strategies to address them proactively.
- Other Methods: A smaller segment, 5.3%, reported using alternative methods specific to their organizational needs.

This data illustrates that organizations prioritize aligning risk management and budget planning as primary strategies to manage and mitigate the impact of security debt.

Comments:

1) Incident Response and Operational Recovery delay
2) we don't
3) we do not measure it
4) Compliance gaps / challenges

Question 6. Aside from you as the CISO, who in your organization cares the most about the impact of your security debt?



Key Stakeholders Concerned About the Impact of Security Debt

Organizations identify several stakeholders, aside from the CISO, who are most concerned about the impact of security debt:

- CIO: 32.4% of organizations indicate that the CIO is the most invested in understanding and managing the impact of security debt, given their role in overseeing technology and information systems.
- Board: 21.6% report that the board of directors is highly concerned, emphasizing the strategic importance and potential business implications of security debt at the highest organizational level.
- CEO: 16.2% highlight the CEO's interest, demonstrating the executive-level attention given to the issue due to its impact on organizational performance and reputation.
- CFO: 12.2% note that the CFO cares about security debt, likely due to its financial implications and potential impact on budgeting and resource allocation.
- Risk Management: 8.1% of organizations identify the risk management team as a key stakeholder, reflecting their role in assessing and mitigating organizational risks.

- External Auditors: 5.4% mention external auditors, underscoring their interest in ensuring compliance and evaluating the security posture from an independent perspective.

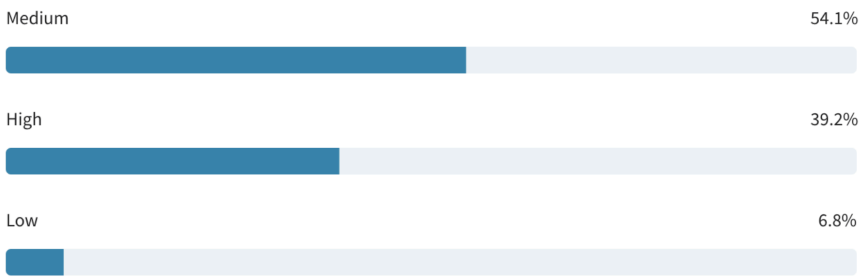
This distribution shows that while the CIO is the primary stakeholder concerned with security debt, various executive and governance roles are also significantly invested in understanding and managing its impact.

Comments:

1) COO
2) CTO
3) Legal

Question 7. What are the potential long-term consequences if you fail to address your security debt, and how might these affect your organization's reputation and stakeholder trust? Rank the severity of the following.

Increased cost (i.e. operational disruptions, resource allocation, budget constraints, etc.)



Potential Long-term Consequences of Failing to Address Security Debt: Increased Cost

Organizations assess the impact of increased costs due to unaddressed security debt, which can include operational disruptions, resource allocation challenges, and budget constraints. The severity rankings are as follows:

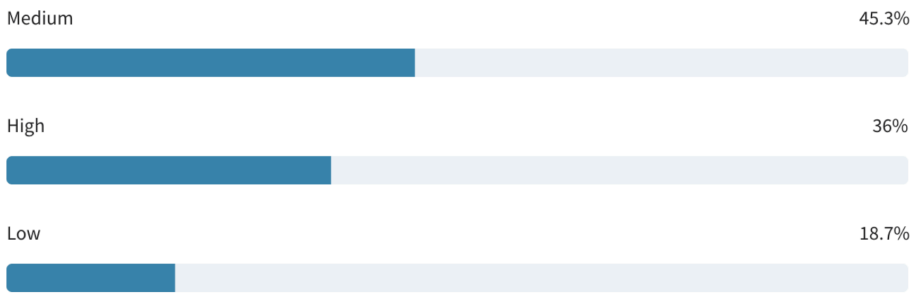
- Medium Severity: 54.1% of organizations view increased costs as a medium-level concern, indicating that while it is impactful, it is seen as a manageable risk.

- High Severity: 39.2% consider it a high-severity issue, recognizing that the financial strain from unaddressed security debt could significantly disrupt operations and resource planning.
- Low Severity: 6.8% rate it as a low-level concern, showing confidence that their organization can manage the financial implications without substantial impact.

These insights highlight that while most organizations recognize the financial consequences of security debt, the majority view it as an issue that, with proper management, can be controlled to minimize disruptions and constraints.

Question 8. What are the potential long-term consequences if you fail to address your security debt, and how might these affect your organization's reputation and stakeholder trust? Rank the severity of the following.

Increased labor (i.e. increased workloads, training and development, etc.)



Potential Long-term Consequences of Failing to Address Security Debt: Increased Labor

Organizations recognize the impact that unaddressed security debt can have on labor demands, such as increased workloads and the need for additional training and development. The severity rankings are as follows:

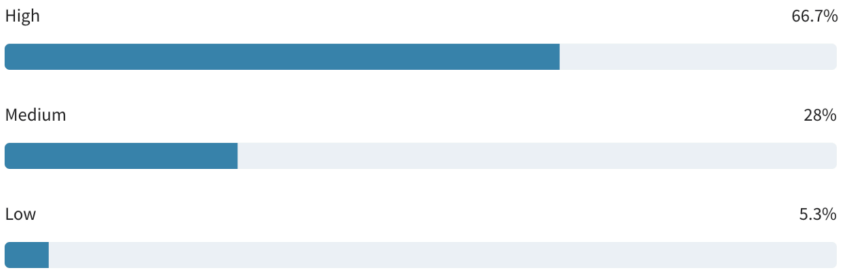
- High Severity: 36% of organizations view increased labor demands as a high-severity consequence, indicating that they anticipate significant operational strain if security debt remains unresolved.
- Medium Severity: 45.3% rate it as a medium-level concern, suggesting that while impactful, they may be able to manage the effects through mitigation efforts.

- Low Severity: 18.7% consider it a low-severity issue, reflecting a belief that the organization can absorb the additional labor demands with minimal disruption.

These insights reveal that a substantial portion of organizations regard the increase in labor requirements due to unaddressed security debt as a critical issue that could heavily affect their operations, reputation, and stakeholder trust if not proactively managed.

Question 9. What are the potential long-term consequences if you fail to address your security debt, and how might these affect your organization's reputation and stakeholder trust? Rank the severity of the following.

Increased risk (i.e. increased risk of breaches, compliance violations, legal consequences, etc.)



Potential Long-term Consequences of Failing to Address Security Debt: Increased Risk

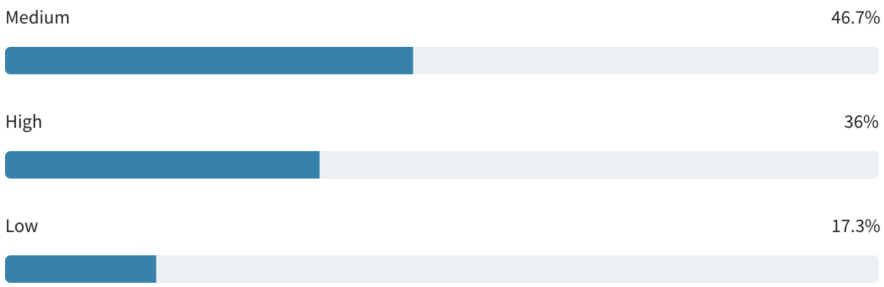
Organizations identify the risks associated with unaddressed security debt, such as breaches, compliance violations, and legal consequences, and rank their severity as follows:

- High Severity: 66.7% of organizations consider the risk of breaches and other consequences as highly severe, indicating that failure to manage security debt could have critical, potentially damaging impacts on their reputation and stakeholder trust.
- Medium Severity: 28% view it as a medium-level concern, acknowledging the risks but suggesting they may have some controls in place to mitigate the impact.
- Low Severity: Only 5.3% perceive the risk as low, indicating confidence in their ability to manage security debt effectively without significant repercussions.

These findings show that most organizations regard the increased risk from unaddressed security debt as a serious threat to their operational integrity and trustworthiness, emphasizing the importance of proactive risk management.

Question 10. What are the potential long-term consequences if you fail to address your security debt, and how might these affect your organization's reputation and stakeholder trust? Rank the severity of the following.

Decreased efficiency (outdated tools and processes, reduced innovation, decreased investor confidence, etc.)



Potential Long-term Consequences of Failing to Address Security Debt: Decreased Efficiency

Organizations assess the impact of decreased efficiency due to unaddressed security debt, which includes outdated tools and processes, reduced innovation, and decreased investor confidence. The severity rankings are as follows:

- Medium Severity: 46.7% of organizations rate decreased efficiency as a medium-level concern, indicating that while it is impactful, they believe it is manageable with some adjustments.
- High Severity: 36% view it as highly severe, suggesting that the inability to innovate and maintain efficient processes could have significant long-term repercussions on reputation and stakeholder trust.
- Low Severity: 17.3% consider it a low-level risk, indicating confidence in their ability to maintain efficiency despite potential security debt.

These insights demonstrate that while many organizations see decreased efficiency as a manageable issue, a significant portion still recognizes its potential to severely affect operations, innovation, and investor relations if security debt remains unaddressed.