

WHITE PAPER

The Silent Liability: Understanding Security Debt

Table of Contents

The Silent Liability: Understanding Security Debt Before It Collects

Executive Summary. 4

The Debt That Doesn't Show Up on Any Balance Sheet. 5

The Forces Working Against You: How Security Debt Accumulates. 5

The Digital Transformation Multiplier. 5

IT/OT Convergence: The Long-Cycle Risk 6

Third-Party Risk and Open-Source Opacity.. 6

Mergers, Acquisitions, and Inherited Liability. 6

AI: The Newest Accelerator 7

Measuring Your Debt: The CISO's Obligation to Quantify and Communicate. . . . 7

Leading with Business Value, Not Cost Savings 7

The Four Pillars of Security ROI 7

FAIR and Its Limits 8

Identity: The Most Underexamined Debt Environment 8

The Tools for Debt Reduction: Governance, Accountability, and Structural Solutions.. 8

Shared Ownership Is the Foundation. 8

Annual Debt Reviews as Operational Discipline. 9

Regulation as a Forcing Function 9

The CISO Burnout Problem 9

Table of Contents

The AI Inflection Point: Security Debt in the Era of Intelligent Systems. 9

AI as a Debt Creator. 10

AI as a Debt Management Tool. 10

Key Takeaways & Recommendations. 10

The Organizations That Get Ahead of This Will Win.. 11

Executive Summary

Every organization carries security debt. The dangerous ones don't know how much, and won't until a breach forces the reckoning.

Security debt is the accumulated risk created by every deferred patch, skipped security review, inherited legacy system, and under-resourced team. Like financial debt, it compounds in the background. Unlike financial debt, you won't know the interest rate, and the creditor coming to collect is an attacker, a regulator, or a catastrophic failure event.

This white paper makes four arguments:

1. **Security debt is a business liability, not an IT backlog.** It must be evaluated through the lens of financial exposure, regulatory consequence, and reputational damage
2. **The forces accelerating debt accumulation are multiplying.** Digital transformation, IT/OT convergence, mergers and acquisitions, third-party dependencies, and AI adoption are all adding to the balance faster than most security teams can address.
3. **Measurement and communication are the CISO's most underdeveloped capabilities.** The inability to translate technical risk into business language is itself a driver of debt accumulation, which prevents the informed investment decisions that would reduce it.
4. **Reducing debt requires structural solutions, not one-time remediation.** Shared accountability, governance discipline, and a proactive risk posture are the foundations of an organization that manages security debt rather than being managed by it.

Key Takeaways:

- More than 80% of cybersecurity debt scenarios have a budgetary component, but money alone cannot solve the problem.
- Identity infrastructure is one of the highest-density debt environments in any organization, and one of the most underexamined.
- AI is changing the technical debt equation in both directions: creating new liabilities while also providing new tools to manage them faster and at greater scale.
- The CISO who cannot calculate ROI will consistently lose the budget conversations that determine how much debt the organization carries.
- Regulatory pressure and disclosure requirements are moving accountability for security debt to the board level.

The Debt That Doesn't Show Up on Any Balance Sheet

There is a category of organizational risk that never appears on a balance sheet, rarely surfaces in a board report, and rarely shows up in an annual audit... until it shows up everywhere at once.

Security debt is that risk. And most organizations are carrying far more of it than their leadership teams recognize.

The balance grows every time a team deploys a cloud environment without a security review, a patch gets deferred to the next maintenance window that never comes, a merger closes without proper security due diligence, or an AI tool gets adopted by a business unit without IT's knowledge. None of these decisions feel catastrophic in isolation, but they represent an accumulating liability that is typically only revealed by a breach, a regulatory finding, or a failed audit.

What makes security debt distinctly dangerous is its cost structure. With financial debt, you know the interest rate. You can model the exposure. You can make an informed decision about when to pay it down.

Security debt works differently. The liability accumulates invisibly, and the "interest" is only revealed when an attacker, a regulator, or a catastrophic failure triggers repayment – all at once.

This is the condition CISOs and business leaders are managing today.

- The attack surface expands faster than security teams can cover it.
- CVE volumes grow faster than remediation capacity.
- Digital transformation creates new infrastructure faster than governance can follow.

The organizations that navigate this environment successfully are not the ones with the most security tools. They are the ones whose leaders understand security debt as a business risk, and make deliberate, informed decisions about how much to carry, how to reduce it over time, and how to communicate it clearly at every level of the organization.

The Forces Working Against You: How Security Debt Accumulates

Security debt does not accumulate because organizations are careless, but because the forces driving it are systemic, relentless, and often invisible until they have already done damage.

The Digital Transformation Multiplier

Digital transformation delivers competitive advantage and operational efficiency, but it also creates a generation of invisible security liabilities. In many organizations, the liabilities are accumulating faster than the benefits.

The pattern is consistent across industries: security teams are excluded from transformation planning, legacy tools are retrofitted into cloud-native environments, and configuration hygiene falls behind the pace of deployment. SaaS adoption by individual business units creates shadow infrastructure that the security team cannot monitor or govern.

The result is organizations that are perpetually reactive – chasing the debt after transformation instead of building security into each transformation.

IT/OT Convergence: The Long-Cycle Risk

Operational technology (OT) is one of the most underappreciated sources of security debt in the enterprise today. Industrial controls, building management systems, surveillance infrastructure, and manufacturing equipment all have life cycles of 10 to 15 years, compared to five years for traditional IT. They are now connected to IP-based networks at scale, creating a persistent attack surface that is genuinely difficult to remediate, because most weren't built with security or remediation in mind.

The consequences are not theoretical. In one documented case, attackers compromised a European bank's surveillance camera system to observe employee movements and capture typed passwords. This enabled fraudulent fund transfers through a vector that had nothing to do with traditional IT intrusion. The entry point was a connected OT device that no one in the security organization owned.

As Hussein Syed, CISO of RWJBarnabas Health, notes: "OT technologies have a longer life cycle management than IT technologies and were not built with cybersecurity or privacy in mind. These systems are used to manage some of the most critical operations and can even present an existential threat to an organization."

"Existential threat" is not an exaggeration, but an accurate description of what unsecured OT infrastructure can represent in healthcare, energy, finance, and manufacturing.

Third-Party Risk and Open-Source Opacity

Outsourcing creates its own category of persistent debt, as third-party security practices may be less rigorous than represented. Data flows across vendor environments create exposure that is difficult to audit, while SLA gaps reduce responsiveness when incidents occur.

The open-source software dimension compounds this. As Johann Balaguer, VP Global CISO of Hard Rock, puts it plainly: "No one truly knows what lies behind the millions of lines of open-source code." Every application that depends on open-source components inherits those components' vulnerabilities, including the ones that haven't been discovered yet.

Mergers, Acquisitions, and Inherited Liability

M&A activity is a security debt wild card that is consistently underestimated in deal economics.

When organizations merge, they inherit the accumulated security decisions (and non-decisions) of the acquired entity. Legacy systems, outdated software, inconsistent security practices, and unknown third-party dependencies all come with the deal. The pressure to consolidate systems and capture synergies creates shortcuts that can take years to unwind, especially since integration timelines rarely accommodate security remediation.

The CISO's challenge in M&A is often that they are brought in to due diligence too late to influence the evaluation, and too early to have the resources to address what they find. Every acquisition becomes a security debt acquisition as well.

AI: The Newest Accelerator

AI tools are being adopted by business units faster than security governance can follow, and models are consistently deployed without adequate security controls. The attack surface of AI infrastructure (NHIs, local MCPs, APIs, model endpoints, data pipelines) is largely uncharted territory for most security teams.

In many ways, AI creates security debt through the same mechanism as every previous technology wave, with deployment outpacing controls. The notable difference is velocity, as what took years in earlier technology cycles now takes months or weeks.

The question for security leaders is not whether to govern AI adoption. It is whether governance will be in place before the debt becomes unmanageable.

Measuring Your Debt: The CISO's Obligation to Quantify and Communicate

Security debt accumulates partly because we cannot communicate it effectively. The inability to translate technical risk into business language is not just a communication failure, but a driver of security debt, because it prevents organizations from making informed decisions about how much risk they are actually carrying.

Lock Langdon, VP and CISO of Aprio Advisory Group, is direct: "Much of cybersecurity debt accumulates because organizations lack clear risk articulation between technical and business leaders. A CISO's ability to communicate the cost-benefit relationship of cybersecurity decisions is vital."

Leading with Business Value, Not Cost Savings

Brian Miller, CISO of Healthfirst, makes the distinction clearly: "Business value is what decision makers care about." His approach is to establish the business value that debt reduction enables, then use financial data to support the case.

Starting with value is important because a cost-savings argument stays in the IT budget discussion, while a business-value argument reaches the CEO, the CFO, and the board. The CISO who leads with value controls the conversation. The one who leads with cost is always defending a line item.

The Four Pillars of Security ROI

For CISOs who need a framework to structure board-level conversations, the four pillars of cybersecurity ROI provide a durable starting point:

1. **Competitive enablement:** Security posture is increasingly a condition of doing business, particularly in enterprise sales, government contracting, and regulated industries. Strong security opens doors, while weak security closes them.
2. **Compliance enablement:** Investment in security infrastructure reduces the cost and risk of regulatory exposure across GDPR, HIPAA, SEC reporting, and sector-specific requirements.
3. **Risk reduction:** Reducing the probability and potential impact of incidents has calculable expected value, even when the exact timing of an incident is unknowable.
4. **Cost reduction:** Security investment reduces the ongoing cost of incident response, remediation, regulatory penalties, and insurance premiums.

These four pillars give business leaders a framework they can work with and give the CISO a structure for requesting investment that is grounded in business logic.

FAIR and Its Limits

The FAIR™ model (Factor Analysis of Information Risk) offers a methodology for assigning quantified risk numbers that can support board-level conversations. While it is a useful tool, the outside-in view it provides is a limitation. As an industry, we still lack a standard inside-out methodology for measuring security program effectiveness against the organization's actual risk posture. When we rely exclusively on FAIR, we are measuring exposure without properly measuring resilience.

Identity: The Most Underexamined Debt Environment

One area where security debt accumulates with particular density and receives insufficient attention in most risk inventories is identity infrastructure.

Orphaned accounts from departed employees. Over-privileged service accounts that have accumulated access rights through years of incremental grants. Fragmented identity systems inherited through M&A. Unmanaged privileged access that exists outside formal provisioning processes. Each represents a specific, exploitable liability.

Identity is the attack surface through which the majority of breaches now occur and should be treated accordingly. Organizations that have not systematically audited and rationalized their identity infrastructure are carrying debt they cannot quantify, which means they cannot accurately assess their actual risk exposure.

The Tools for Debt Reduction: Governance, Accountability, and Structural Solutions

Identifying security debt and communicating the risk are essential. But neither matters unless the organization is structured to reduce it over time.

This is where many security programs stall. Remediation gets treated as a project (a one-time effort to close known gaps) rather than as an ongoing operational discipline. The debt gets addressed, and then new debt accumulates to replace it. The organization runs in place.

Structural problems require structural solutions.

Shared Ownership Is the Foundation

Security debt persists where no one clearly owns it. In many enterprises, security responsibility is fragmented: the security team owns alerts and incidents; IT owns infrastructure; business units own applications; HR owns identity provisioning; legal owns compliance. Somehow, no one owns the accumulated security debt.

In practice, the CEO's risk tolerance often dictates the CISO's threshold. This means the CISO's focus is not to solve every security problem, but to ensure that the CEO, the board, and the business leaders understand which risks they are accepting, which they are mitigating, and which they are transferring. Risk acceptance without awareness is negligence. Risk acceptance with clear documentation and deliberate choice is governance.

A structured response worth emulating is to embed security goals across each team's annual objectives. While this is a difficult exercise to work through, every leader is already carrying the costs and risks of security in their budget. Shared ownership is a matter of recognizing what is already there.

Annual Debt Reviews as Operational Discipline

One of the most practical structural interventions is a formal, annual assessment. This includes real-world security validation exercises that test whether controls work as implemented, not just as documented. It also includes a review of every security tool in the portfolio:

- Are they being used?
- Do they work together effectively?
- Are they still appropriate for the current threat environment?

Cybersecurity debt can be calculated by reviewing the tool landscape and examining hardware and software that is approaching end of life. This is not a complicated methodology, just asset management applied to security infrastructure. Most organizations that conduct reviews systematically find they are both over-tooled in some areas and critically under-covered in others.

Regulation as a Forcing Function

SEC disclosure requirements, GDPR, HIPAA, and sector-specific frameworks create external accountability that can accelerate debt reduction investments that might otherwise stall in budget discussions. When the CFO asks why identity infrastructure needs to be rationalized, the answer that includes "SEC cybersecurity disclosure rules require us to accurately represent our risk posture" lands differently than "we have too many orphaned accounts."

Regulatory pressure does not create a good security strategy on its own. But it can accelerate organizational change that the security team has been unable to drive through internal arguments alone.

The CISO Burnout Problem

There is a structural risk factor that belongs in board reports, but rarely appears as it should: CISO burnout. This is a tricky situation to address, since the person burned out is likely the one making the board report, and professional norms work against that level of public vulnerability.

Boards and CEOs who want to manage security risk effectively need to treat the CISO role as a strategic leadership position that requires sustainable operating conditions.

The AI Inflection Point: Security Debt in the Era of Intelligent Systems

AI changes the security debt equation in two directions simultaneously. Security leaders who understand both will be positioned to act. Those who focus only on AI as a threat, or only as a solution, will get the strategy wrong.

AI as a Debt Creator

The rapid, often ungoverned adoption of AI tools inside the enterprise is creating a new generation of security debt in real time. Business units are deploying large language models, AI-powered analytics platforms, and automation tools without involving security teams in the evaluation. Training data is being ingested without adequate controls. API connections are being established without governance review.

This is the digital transformation pattern repeating at a higher velocity, with the same governance deficit as prior technology cycles. The key differences from previous cycles are the speed of change and the attack surface. Model infrastructure, data pipelines, inference APIs, identities, distributed MCP servers, and data itself. Every element is a potential threat vector, and most security teams have not yet developed the competency to assess that surface area.

Every AI deployment that happens outside of security governance is security debt. The longer it takes to rationalize, assess, and bring those deployments under control, the larger the balance grows.

AI as a Debt Management Tool

AI-driven tools are now capable of accelerating vulnerability prioritization, automating routine threat detection, improving configuration monitoring, and providing real-time attack surface visibility at a scale that human analysts cannot match. For security teams already operating under resource constraints, AI-assisted operations represent a genuine force multiplier. The ability to identify and prioritize high-risk vulnerabilities faster, detect anomalous identity behavior in real time, and automate responses to known threat patterns reduces the rate at which debt accumulates. Leveraged properly, AI can also accelerate the rate at which security debt can be addressed.

The organizations that manage security debt most effectively over the next five years will be those that treat AI as both a governed risk and a deployed capability.

AI should enable human capability in security, not replace security judgment. When AI handles volume, people can focus on the decisions that require context, accountability, and organizational authority. The CISO's role becomes more strategic, not less.

Key Takeaways & Recommendations

1. **Reframe security debt as a business liability in every budget conversation.** Stop presenting security investment as an IT cost center. Use the four pillars of cybersecurity ROI (competitive enablement, compliance enablement, risk reduction, and cost reduction) to frame every resource request in terms the board can evaluate and act on.
2. **Conduct a formal security debt inventory, and repeat it annually.** Audit your tool landscape for redundancy and effectiveness. Identify hardware and software approaching end of life. Assess every third-party dependency for security posture.
3. **Build shared accountability into organizational structure.** Embed security goals into the annual objectives of every team; security cannot be a siloed function and also be effective.
4. **Put identity infrastructure at the top of your debt reduction agenda.** Orphaned accounts, over-privileged users, fragmented identity systems from M&A, and unmanaged privileged access represent some of the highest-density, most exploitable security debt in any organization.
5. **Develop a board-ready risk communication framework before you need one.** Use models like FAIR to assign quantified risk numbers. Connect technical findings to financial exposure, regulatory consequences, and reputational impact. Practice the conversation before the crisis.
6. **Integrate security into AI governance now, before deployment outruns oversight.** Every AI tool adopted without a security review is a security debt. Establish governance standards for AI deployment before the adoption curve outruns your ability to manage it.
7. **Treat the CISO role as a strategic position that requires sustainable conditions.** CISO burnout is a risk factor, not a personal problem. Boards that want resilient security organizations invest in the leadership structures, resourcing, and organizational support that allow CISOs to operate strategically.

The Organizations That Get Ahead of This Will Win

Security debt is not going away. The forces driving its accumulation are structural features of the modern enterprise. The question is not whether your organization carries security debt. It does. The question is whether your leadership team understands what you owe, makes deliberate decisions about what to address and when, and builds the organizational discipline to keep the balance from growing faster than you can manage it.

Managing and reducing that debt requires more than periodic assessments or reactive incident response. It requires the ability to continuously observe identity activity across Active Directory and Entra ID, identify risky exposures before they become compromise paths, and contain attacks before they spread across the environment. It also requires operational context that helps security teams understand not only that something happened, but who initiated it, what changed, where it occurred, and how to respond quickly.

This is where platforms focused on identity protection, resilience, and operational visibility become increasingly important. Solutions such as Quest Identity Defense and the broader Quest Security Management Platform are designed to help organizations reduce accumulated identity risk through continuous monitoring, proactive protection, deep auditing, and accelerated incident response. By combining identity threat detection, posture management, AI-driven insights, and resilience capabilities into a unified operational model, organizations can move from reacting to security debt after incidents occur to systematically reducing it over time.

Ultimately, security debt is not a technical problem to eliminate. It is a business reality to govern. The organizations that get ahead of it will be the ones that treat cybersecurity as an operational discipline tied directly to resilience, accountability, and long-term business continuity.

About Quest Software

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.

Explore our solutions →

© 2026 Quest Software Inc. I ALL RIGHTS RESERVED.
Quest, and the Quest logo are trademarks of Quest Software Inc.
For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks are properties of their respective owners. Whitepaper-Understanding-Security-Debt-HO-104664