September 4, 2026

How CFOs can turn cybersecurity spend into measurable risk reduction

As cybersecurity mergers and acquisitions reshape the market, CFOs may need to reassess their security portfolios.

A cybersecurity budget can grow every year without producing a corresponding reduction in risk. Each new tool or capability may be individually justified, but collectively they can create complexity that slows decisions and weakens visibility.

This dynamic is playing out against the backdrop of one of the largest consolidation waves the cybersecurity industry has seen. In 2025, there were 426 cybersecurity acquisitions announced, a 5% increase over the prior year, and disclosed deal value jumped to $92.5 billion.[i] A handful of large transactions drove much of that increase, increasing the total disclosed deal value by approximately 82% year-over-year.[ii] So far in 2026, disclosed cybersecurity mergers and acquisitions (M&A) deal value had already crossed $65 billion by June.[iii] That concentration may make the deal-value spike an important market signal, rather than indicating that every enterprise should follow suit and consolidate its own portfolio.

The growing prominence of cyber and AI-related risk on finance leaders' agendas reinforces the case for stronger CFO engagement in cybersecurity decisions. In Deloitte's Finance Trends 2027 report, 31% of finance leaders surveyed identified cyber and AI-related risks as their top external risk, up from 24% in the prior year. For CFOs, the imperative is not simply to contain cybersecurity spending or pursue the newest integrated platform. It is to ensure that current and planned investments are strengthening resilience against the organization's most material and evolving risks, with sufficient speed, visibility, and investment discipline.

The hidden cost of a growing security budget

Redundant tools, fragmented data, and manual workarounds can quietly erode a cybersecurity program's effectiveness even as its line item grows. The average enterprise now manages 83 separate security tools sourced from about 29 vendors, according to a study from the IBM Institute for Business Value conducted with Palo Alto Networks.[iv]

This sprawl typically accumulates as reasonable, one-off purchases driven by emerging threats, acquisitions, compliance requirements, vendor bundling, and decentralized purchasing. Organizations can easily end up with a separate tool for every need over time—creating overlapping capabilities and a portfolio of underused licenses.

The quiet financial and operational costs of that fragmentation can extend well beyond visible licensing fees:

- Integration and implementation costs
- Employee training

- Manual workarounds
- Duplicated administrative overhead can accumulate quietly
- Lower analyst productivity
- Eroded quality and consistency of data relied on by executives and the board
- Slower responses to cyberattacks

When it comes to cyberattacks, the average cost of a data breach at a US company reached $10.22 million in 2025, an all-time high.[v] Organizations that have unified their security tools onto integrated platforms are able to detect incidents 72 days faster, on average, and contain them 84 days faster than organizations still managing fragmented environments.[vi]

CFOs and their finance teams can encounter misleading signals when judging whether a security investment is working. Total spend, year-over-year budget growth, and industry benchmarks can suggest an organization is keeping pace—without indicating whether the underlying risk is going down. CFOs should instead be evaluating security tool investments for meaningful reduction of material business risks.

Three forces raising the stakes for CFOs

Several converging developments are now making tool sprawl a more important financial and governance issue:

Faster-moving threats.
AI models can now find and exploit software vulnerabilities in hours rather than months.[vii] AI-enabled adversaries increased their operations by 89% year over year,[viii] and enterprise response times haven't kept pace—widening the window of exposure. Response speed is an important measure of whether cybersecurity investments are reducing risk.

More identities to protect.
As organizations connect more systems, AI agents, and applications, the number of non-human identities (service accounts, API tokens and the AI agents themselves) is growing far faster than the number of human ones—at a ratio of 109 to 1 and climbing.[ix] This proliferation of identities increases the value of integrated visibility and control across a cyber portfolio.

Sharper regulatory scrutiny.
Fragmented systems can undermine an organization's ability to assess financial materiality and meet disclosure obligations, making it harder to answer a regulator's most basic question after a cyber incident: What did the organization know—and when? Investing strategically in a cyber portfolio that unifies data can make it easier to assess materiality and support accurate disclosures after incidents.

What the wave of cybersecurity M&A is telling CFOs

The scale of recent cybersecurity M&A activity seems to suggest the market broadly expects organizations to move toward fewer vendors (consolidation) and more connected tools (platformization). These trends may overlap, but vendor consolidation does not necessarily result in deeper product integration or a true platform experience.

Platformization vs. vendor consolidation

Vendor Consolidation:

Reducing third-party software providers to minimize costs and contract complexity.

Platformization:

Unifying integrated capabilities and workflows in a single cyber ecosystem.

Key distinction:

The goal of platformization is not merely to reduce vendors, but to create demonstrably integrated capabilities that enable faster, clearer, and more accountable risk decisions.

Reducing the number of vendors, integrating capabilities and workflows, and improving security outcomes are three different things—one doesn't automatically produce the next. Ultimately, a successful consolidation or platformization will shorten the time it takes to make and execute a security decision. It's important to consider that for most large, complex enterprises, going all-in on consolidation isn't likely to produce the best outcomes.

Even organizations that aren't actively shopping for new tools should keep in mind that when a vendor is acquired, the product roadmap, pricing, support model, and integration priorities they budgeted around can change.

Strategies to consider for CFOs evaluating their cybersecurity portfolios

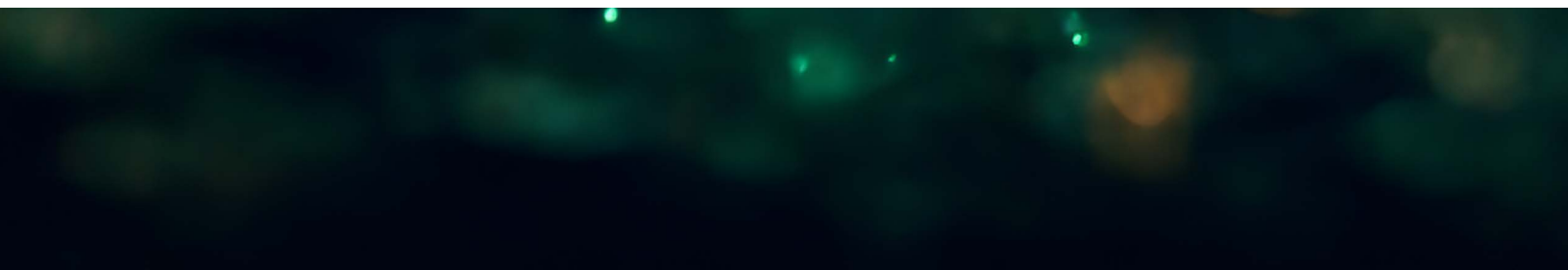
In everyday practice, CFOs can set risk appetite and investment priorities, connecting cybersecurity spending to the business scenarios that matter most. They can weigh the economic, execution, and concentration-risk trade-offs of any option and help fund the capabilities the business needs to adopt cloud, AI, and other technologies safely. This means more than functioning as a cost controller or approval gate, but as a co-governor of the organization's risk appetite alongside the CISO, CIO or CTO, and business leaders.

Here are some actionable steps that CFOs can consider to help drive measurable risk reduction, resilience, and business value for every dollar spent—and a clear way to track whether that value is delivered.

1. **Start with a focused portfolio review.** At regular intervals, map each tool to the material risk scenario it is designed to address, its functional overlap with the rest of the portfolio, and the technical and operational dependencies that make some tools hard to retire once redundant—the kind of license audit and rationalization that CFOs are increasingly pushing for.[x] The goal is to understand what is being used, what is redundant, what is missing, and what can realistically be retired or consolidated. Few organizations have a single owner with full visibility into the security portfolio, which is often the biggest obstacle.
2. **Seek financial quantification of cyber risk.** Rather than relying solely on qualitative risk ratings or heat maps, work with the CISO and CIO or CTO to build a concise set of measurements across the portfolio. Explore these topics:

- Priority cyber scenarios and their plausible financial impact, such as business interruption, lost revenue, response costs, regulatory exposure, reputational harm.
- Coverage of the organization's most critical assets, data, identities, and business services.
- Detection, containment, and recovery performance.
- Three-to-five-year total cost of ownership.
- Whether licensing and integration costs are trending down.
- Tool utilization, integration costs, dual-running periods, and decommissioning dates.
- Critical vendor dependencies and exit options.

Organizations should consider purchasing a small number of strategic platforms for core capabilities, paired with best-of-breed tools for the specific areas where their risk profile or operating environment requires more specialized coverage.



- Whether the investment is helping the business innovate—adopting cloud, AI, and other technology more safely and efficiently.

3. **Build CFO-CISO co-governance.** As cybersecurity becomes an increasingly material business and financial risk, organizations could bring finance and security leadership into closer partnership. In practice, the CISO owns cyber strategy and control effectiveness in this scenario, and the CIO or CTO owns the broader technology architecture and integration decisions, working alongside the CISO. The CFO works alongside those tech leaders while also working with the business leaders whose risk the spending is meant to reduce. The CFO's role is to make sure the investment thesis behind a major security decision holds up, the risk trade-offs are understood, and the expected value gets tracked during implementation. CFOs can anchor the conversation around four questions:

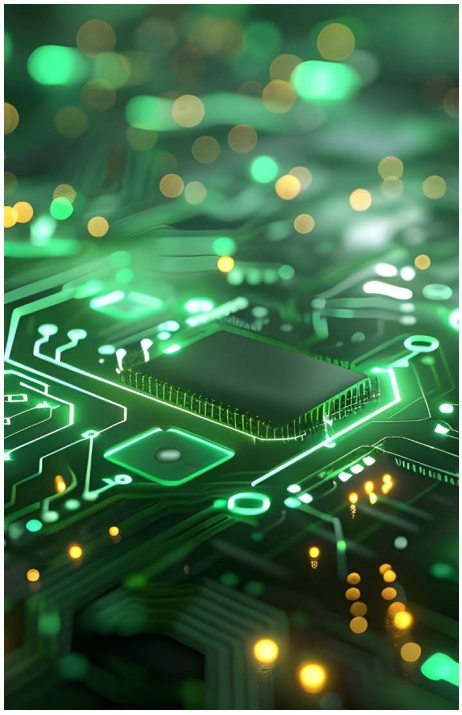
- Are we covering the risks that matter most to us?
- Can we clearly show the board how this spend connects to lower risk?
- Who owns the outcome, and how will we track whether the expected value is delivered?
- Will the operating model help the business become more agile and secure over time?

For emerging risks such as frontier AI models, the most significant investments may involve infrastructure, remediation, resilience, and operating-model changes beyond the CISO's direct control. Effective governance therefore depends on shared accountability for outcomes, not simply on reporting lines or budget ownership.

The CFO's role here can go beyond pressure-testing the business case. A CFO who asks for a scenario-based view of risk, tied explicitly to dollars, can help translate a technical program into financial terms that the board can more easily act on.

4. **Scrutinize the full economics of consolidation—whether you build it or inherit it.** Consolidation is often sold on savings, but the savings are rarely automatic. Before endorsing a proposed platform deal, CFOs should establish a clear baseline of what the organization spends today across the tools the platform would replace—and which of those tools are actually getting used. The proposal should then be tested against two key questions:

- **Are the savings real?** A lower headline price means little if the old tools are never retired. Savings typically materialize when redundant licenses are cancelled, contracts are exited, and the operational overhead of running parallel systems is removed. CFOs should consider insisting on a three-to-five-year TCO view that accounts for migration cost, retraining, dual-running costs (paying for the new platform and the legacy tools at the same time), and the timeline for decommissioning what the platform replaces—not just the first-year license comparison.



CFOs do not need to become cybersecurity architects. They can apply the same financial discipline, risk governance, and outcome measurement to security investments that they apply elsewhere in the business.

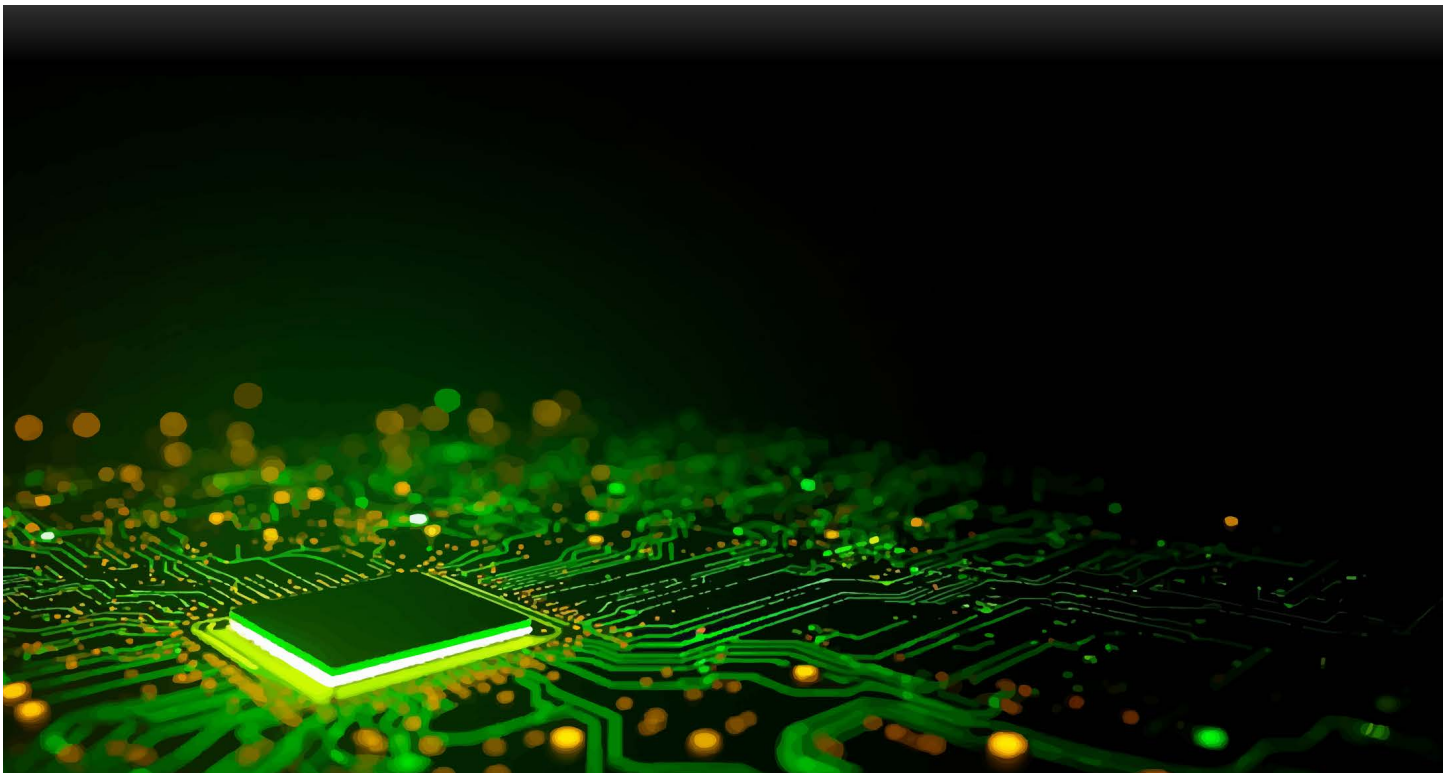
- **Are we creating concentration risk?** Consolidating onto a single vendor can reduce complexity while simultaneously increasing dependence—potentially resulting in fewer alternatives and less leverage, as well as weaker exit options if that vendor suffers an outage, breach, or pricing change. The same discipline applies when a security stack arrives through M&A. Acquirers inherit the target's tools, contracts, and technical debt. Rationalizing tool overlap within Day 1 deal economics can help ensure that uncalculated retirement and dual-running costs don't erode the consolidation thesis.[xi]

5. **Embed regulatory obligations as portfolio guardrails.** CFOs should draw a clear line between security spending calibrated to the organization's own risk appetite and compliance spending required to meet legal obligations, such as SEC disclosure rules, NIS2, DORA, or GDPR. Requirements vary by jurisdiction and industry. Meeting them is necessary, but it isn't the same as having acceptable cyber risk; a fully compliant organization can still be badly exposed. The cost of treating compliance spending as optional could have financial and regulatory consequences. Current SEC rules allow for organizations to be fined for misleading or inaccurate disclosures related to cybersecurity, a reminder that these obligations carry real financial consequences for the organization.

From spend scrutiny to resilience and business enablement

The scale of the current cybersecurity M&A wave may signal that fragmented security environments are becoming a potential business weakness, but also a reminder that cybersecurity governance could no longer be optional for finance leaders—it's foundational.

CFOs who bring discipline to how cybersecurity capital is allocated can give their organizations something more than a bigger budget alone can: confidence that each dollar is either reducing exposure or building resilience. The CFOs who recognize this may not only be able to help protect the business but could also turn a historically defensive function into a source of measurable value.



End notes

i. SecurityWeek, "SecurityWeek Report: 426 Cybersecurity M&A Deals Announced in 2025," February 2026.

ii. SecurityWeek, "SecurityWeek Report: 426 Cybersecurity M&A Deals Announced in 2025," February 2026.

iii. SaaS Mag, "Cybersecurity SaaS Premium: Highest Multiples in 2026," June 2026.

iv. IBM Institute for Business Value and Palo Alto Networks, "IBM and Palo Alto Networks Find Platformization Is Key to Reduce Cybersecurity Complexity," January 2025.

v. Matt Kapko, "Research shows data breach costs have reached an all-time high" Cyberscoop, July 2025

vi. IBM Institute for Business Value and Palo Alto Networks, "IBM and Palo Alto Networks Find Platformization Is Key to Reduce Cybersecurity Complexity," January 2025.

vii. Beatrice Nolan, "AI is supercharging cyberattacks—and most companies aren't ready | Fortune" Fortune, June 2026.

viii. Press release,"2026 CrowdStrike Global Threat Report: AI Accelerated Adversaries," CrowdStrike February 2026.

ix. Palo Alto Networks and IDIRA, "2026 Identity Security Landscape Report," 2026.

x. Bill Tanner, "Cyber Budget Wars: Why CFOs are now steering security strategy," Intelligent CISO, October 2025

xi. SecurityWeek, "SecurityWeek Report: 426 Cybersecurity M&A Deals Announced in 2025," February 2026 & SaaS Mag, "Cybersecurity SaaS Premium: Highest Multiples in 2026," June 2026.

Contacts

Mehdi Houdaigui
Principal, Cyber AI leader
Deloitte & Touche LLP
mhoudaigui@deloitte.com

Cora Chiu
Associate Vice President, Cyber Enterprise Security
Deloitte & Touche LLP
cochiu@deloitte.com

Timothy Murphy
Senior manager, Enterprise Growth and Innovation
Deloitte Services LP
timurphy@deloitte.com

Aditya Narayan
Research specialist, Center for Integrated Research
Deloitte Services LP
adinarayan@deloitte.com

About Deloitte's CFO Program

The CFO Program brings together a multidisciplinary team of Deloitte leaders and subject-matter specialists to help CFOs stay ahead in the face of growing challenges and demands. The program harnesses our organization's broad capabilities to deliver forward thinking and fresh insights for every stage of a CFO's career—helping CFOs manage the complexities of their roles, tackle their company's most compelling challenges, and adapt to strategic shifts in the market.

LEARN MORE