PART 16

Cybersecurity, Identity, and Fraud Technology

for the Finance Function

Cybersecurity is now a finance function accountability. The CFO who treats it as a CIO problem is unprepared for the regulatory and disclosure environment that has emerged.

The Finance Technology Stack
A CFO's Strategic and Architectural Guide

Why Cybersecurity Is Now a CFO Accountability

Cybersecurity has historically been treated as the responsibility of the chief information officer and the chief information security officer, with the finance function as one stakeholder among many that the security function serves. The treatment was always incomplete. The finance function has always held specific cybersecurity exposures that the broader security function could not address from outside the finance domain. The treatment is now structurally inadequate. The disclosure regime that has emerged over the past several years, the insurance regime that has evolved alongside it, the audit regime that has incorporated cybersecurity into the financial reporting framework, and the broader regulatory environment that increasingly treats cybersecurity as a financial reporting matter have together changed the chief financial officer's accountability for cybersecurity from a peripheral concern to a central one.

The change is visible in several specific developments. The Securities and Exchange Commission rules on cybersecurity disclosure that came into effect in 2023 require public companies to disclose material cybersecurity incidents within four business days of determining materiality, and require annual disclosures about cybersecurity risk management, strategy, and governance. The rules place the cybersecurity disclosure obligation squarely on the chief financial officer's certification responsibilities and on the audit committee's oversight responsibilities. The European regulatory framework including the Digital Operational Resilience Act and the broader cybersecurity directives place similar requirements on companies operating in European jurisdictions. The audit profession has incorporated cybersecurity considerations into the audit of internal controls over financial reporting, with the consequence that cybersecurity weaknesses can produce audit findings that affect the financial statements. The insurance market for cyber coverage has matured to a point where the underwriting requirements impose specific cybersecurity disciplines on insured companies.

These developments mean that the chief financial officer who continues to treat cybersecurity as the chief information officer's concern is operating with an outdated accountability model. The chief financial officer signs the disclosure controls certification that includes cybersecurity. The chief financial officer engages with the audit committee on the cybersecurity oversight that the committee now exercises in most public company boards. The chief financial officer engages with the cyber insurance market that requires substantive cybersecurity capabilities for coverage. The chief financial officer engages with the regulatory framework that increasingly addresses cybersecurity at the financial reporting level. The chief financial officer cannot delegate these engagements to others without delegating accountability that cannot in fact be delegated.

The position taken in this masterclass is that cybersecurity in the finance function is a jointly held accountability between the chief financial officer and the chief information security officer, with specific dimensions that the chief financial officer owns directly. The dimensions include the

access governance over the finance platforms, the fraud control architecture, the disclosure framework for cybersecurity incidents, the cyber insurance and risk transfer posture, the ransomware financial readiness, and the broader integration of cybersecurity with the financial control environment. The chief financial officer who claims these dimensions explicitly will produce a cybersecurity posture that satisfies the regulatory environment and that protects the function. The chief financial officer who continues to defer entirely to the chief information security officer will operate with a posture that may not satisfy the regulatory environment and that exposes the function to risks the security function alone cannot address.

The work of this part is to lay out the cybersecurity landscape from the finance function's perspective rather than from the information technology function's perspective. The part treats identity and access management as a finance discipline, the fraud technology stack with attention to the specific exposures of the finance function, the Securities and Exchange Commission cyber disclosure regime, ransomware financial readiness, and the integration of cybersecurity with the broader control environment. The reader will leave with the framing to engage with the cybersecurity agenda from the chief financial officer's perspective rather than from the information technology perspective that has historically dominated the discussion.

Identity and Access Management as a Finance Discipline

The most foundational dimension of cybersecurity in the finance function is identity and access management. The discipline addresses the question of who can access which systems, with what privileges, under what controls. The discipline operates at the intersection of cybersecurity and the segregation of duties framework that Sarbanes-Oxley compliance depends on. The discipline is treated by most enterprises as a cybersecurity question with limited finance engagement. The position taken in this masterclass is that identity and access management is fundamentally a finance discipline that the cybersecurity function operates rather than the reverse.

The Identity Platform Landscape

The identity and access management category is dominated by several established platforms. Okta has built the leading independent position in the workforce identity category, with broad adoption across the enterprise segment. The platform handles authentication, single sign-on across applications, multi-factor authentication, and increasingly the broader identity governance dimension. Microsoft Entra, formerly Azure Active Directory and now part of the broader Microsoft Entra identity platform, has built the largest installed base given the Microsoft footprint across enterprises. The platform offers identity and access management integrated with the broader Microsoft platform and increasingly with broader external applications.

SailPoint serves the enterprise segment with depth in identity governance, including the periodic access reviews, the provisioning and deprovisioning workflows, and the broader governance dimension that distinguishes identity governance from pure authentication. CyberArk has built a strong position in privileged access management, the specialized category that addresses the elevated access required for system administration and other privileged operations. The category includes additional players in specific segments, but the four named platforms together address the majority of enterprise identity and access management deployments.

The Connection to Segregation of Duties

The connection between identity and access management and the segregation of duties framework is direct but commonly underappreciated. Segregation of duties is the control discipline that prevents any single individual from performing combinations of activities that together would enable fraud or material error. The classic examples include the segregation between the individual who adds vendors and the individual who approves payments to those vendors, between the individual who creates customer credits and the individual who approves customer credit policy, and between the individual who records journal entries and the individual

who approves them. The segregations are well-established in audit and accounting practice and are required by Sarbanes-Oxley compliance for the controls over financial reporting.

The segregations must be enforced architecturally rather than by policy for the controls to be effective. A policy that prohibits the same individual from performing multiple functions is a policy that depends on individual compliance and that fails when individuals violate the policy. An architectural enforcement through the identity and access management infrastructure makes the violations impossible rather than depending on compliance. The architectural enforcement requires that the identity platform integrate with every finance application, that the access rights in every application reflect the segregation requirements, and that the periodic access reviews verify the continued correctness of the access rights as the workforce evolves.

The architectural enforcement is a finance discipline that the cybersecurity function operates rather than a cybersecurity discipline that the finance function consumes. The finance function defines what segregations are required. The finance function specifies which roles must be segregated. The finance function approves the access configurations. The cybersecurity function provides the platform infrastructure that enforces the configurations. The chief financial officer who recognizes this division of responsibility will engage with the identity and access management agenda substantively. The chief financial officer who treats identity as the cybersecurity function's concern will inherit access configurations that may not align with the segregation of duties that the control framework requires.

The Periodic Access Review Discipline

The access configurations drift over time as the workforce evolves. Employees change roles. Employees leave the enterprise. New employees join. Temporary access is granted for specific projects and is not always rescinded when the projects end. The cumulative effect of this drift is access configurations that no longer reflect the segregation requirements and that contain dormant or excessive access rights. The discipline that addresses this drift is the periodic access review.

The periodic access review is a structured exercise in which the access rights across the finance applications are examined against the current workforce and against the segregation requirements. The exercise identifies the access rights that should be modified or revoked, processes the modifications through the identity platform, and produces the documentation that the audit will examine. The discipline must be operated at a defined cadence, typically quarterly for the highest-risk applications and annually for the broader portfolio. The discipline requires the identity platform capability to support the review and the operational discipline to conduct the review rigorously.

The discipline is one of the more underdeveloped areas of identity and access management at most enterprises. The reviews are often performed perfunctorily, with the reviewers approving access without examining it carefully. The audit findings on access management often identify deficiencies in the review process specifically. The chief financial officer who insists on a rigorous access review discipline will produce a control environment that satisfies the audit. The chief financial officer who allows the review discipline to operate perfunctorily will produce a control environment with the access management deficiencies that the audit identifies.

The Fraud Technology Stack

The fraud technology stack addresses the specific cybersecurity exposures that target the finance function for financial gain. The stack is distinct from the broader cybersecurity infrastructure that addresses the protection of the enterprise data and the broader information assets. The fraud technology stack focuses on the patterns of attack that specifically target the finance function and on the defenses that specifically protect against those patterns. The chief financial officer who understands the stack will produce a fraud control environment that addresses the specific exposures. The chief financial officer who treats fraud as a subset of general cybersecurity will produce a control environment that addresses the broader concerns without addressing the finance-specific patterns adequately.

Business Email Compromise

Business email compromise has emerged as the dominant fraud pattern targeting the finance function over the past several years. The pattern involves the use of compromised email accounts or spoofed email addresses to impersonate vendors, executives, or other counterparties and to redirect payments to fraudster-controlled accounts. The pattern is sophisticated, well-resourced, and continuously adapted to defeat the defenses that enterprises put in place. The financial losses from business email compromise have grown substantially each year and now represent one of the larger categories of cyber-enabled financial loss.

The defense against business email compromise requires a combination of technology and process. The technology includes the email security platforms that detect and block spoofed emails, the verification platforms that confirm vendor banking changes through independent channels, and the anomaly detection that flags unusual payment patterns. The process includes the verification protocols that require independent confirmation for payment changes, the structured handling of vendor banking changes, the team training that develops the recognition of business email compromise patterns, and the cultural posture that welcomes the questioning of unusual requests rather than treating it as obstruction.

The chief financial officer who treats business email compromise as a serious and persistent threat will produce a defense that materially reduces the exposure. The chief financial officer who treats it as an occasional incident will operate a finance function that the fraud schemes can exploit at substantial cost. The defense is not a single platform but a combination of platform capabilities, process controls, and cultural posture that together produce the control environment the threat requires.

Vendor Master Integrity

The vendor master is the foundation of payment fraud defense and was treated in Part Eight on the procure-to-pay spine. The treatment from the cybersecurity perspective emphasizes the specific dimensions that the security architecture must address. The vendor onboarding process must include identity verification that confirms the vendor is who they claim to be. The vendor master must be protected from unauthorized modification, with the change controls that prevent fraudsters from inserting fictitious vendors or modifying legitimate vendors to redirect payments. The vendor master must be subject to periodic review that identifies dormant or suspicious records. The integration with the payment systems must enforce that payments can only be processed to vendors in the verified master.

The platforms that support vendor master integrity include the vendor management capabilities of the broader procure-to-pay platforms, the dedicated vendor onboarding platforms that focus specifically on the verification dimension, and the integration platforms that enforce the constraints across the broader architecture. The chief financial officer who treats vendor master integrity as a foundational discipline will produce a payment control environment that satisfies the regulatory requirements and that materially reduces the fraud exposure.

Payment Anomaly Detection

The payment anomaly detection category applies machine learning and structured rules to the payment activity to identify the payments that warrant additional scrutiny. The patterns that the detection identifies include unusual amounts relative to the vendor history, unusual timing relative to the typical payment schedule, unusual destinations relative to the vendor's normal banking, and the broader category of patterns that the machine learning identifies as deviating from the historical norm. The detection is supported by the platforms that operate alongside the payment infrastructure and that flag the anomalies for review before the payments are released.

The category leaders include the anomaly detection capabilities embedded in the major accounts payable and treasury platforms, dedicated payment fraud platforms that specialize in the detection problem, and the broader financial crime platforms that address payment fraud alongside the other financial crime patterns. The category is one of the more mature applications of machine learning in finance, with capabilities that have been refined through years of operational experience and that produce reliable detection in production use.

Account Takeover Defense

Account takeover is the pattern in which fraudsters gain control of legitimate user accounts and use the legitimate access to perform fraudulent activities. The pattern is particularly dangerous in the finance function because the legitimate access bypasses many of the controls that would

otherwise detect the fraud. The defense against account takeover includes the multi-factor authentication that makes unauthorized access more difficult, the behavioral analytics that detect unusual access patterns even from legitimate accounts, the conditional access policies that require additional verification for unusual access situations, and the broader identity protection capabilities that the major identity platforms have invested in over recent years.

The defense is supported by the integration between the identity platform and the finance applications. The chief financial officer who insists on the integration with the strongest authentication and the strongest behavioral analytics will produce a control environment that materially reduces the account takeover exposure. The chief financial officer who accepts weaker authentication and weaker analytics will operate a control environment in which the legitimate access can be exploited by the fraud schemes.

The SEC Cyber Disclosure Regime

The Securities and Exchange Commission rules on cybersecurity disclosure that came into effect in 2023 have changed the chief financial officer's accountability for cybersecurity in ways that the previous regulatory environment did not. The rules require specific disclosures that the chief financial officer's certification covers and that the audit committee's oversight addresses. The chief financial officer who understands the rules and the operational implications will produce a disclosure framework that satisfies the requirements. The chief financial officer who does not will discover during the first material cyber incident that the disclosure framework is not adequate for the requirements.

The Four-Day Reporting Requirement

The most consequential element of the rules is the requirement that public companies disclose material cybersecurity incidents within four business days of determining that the incident is material. The requirement creates a specific operational discipline that the enterprise must operate. The discipline includes the incident response process that identifies cyber incidents promptly, the materiality assessment process that determines whether an incident reaches the disclosure threshold, the disclosure preparation process that produces the Form 8-K filing within the required timeframe, and the broader communication discipline that addresses the various stakeholders affected by the disclosure.

The materiality assessment is the dimension that most directly involves the chief financial officer. The assessment is not simply a technical determination of whether the incident affected systems or data. The assessment is a financial and operational determination of whether the incident's effects rise to the level that a reasonable investor would consider important. The assessment requires the chief financial officer's engagement because the chief financial officer is the executive accountable for the disclosure framework and because the assessment involves judgment that the chief information security officer alone cannot make. The chief financial officer who engages with the materiality framework before the first incident will produce an assessment process that operates effectively under the time pressure that the four-day requirement creates. The chief financial officer who has not engaged with the framework will discover during the first incident that the assessment requires more time than the four-day requirement allows.

The Annual Disclosures

The rules also require annual disclosures about the cybersecurity risk management, strategy, and governance. The annual disclosures appear in the 10-K and require the company to describe the processes for assessing and managing cybersecurity risk, the engagement of third parties in

cybersecurity, the cyber threat profile relevant to the company, and the governance structure including the board's oversight and management's role. The disclosures are made under the chief financial officer's certification and are examined by the external auditor in the broader audit of internal controls.

The annual disclosures require that the cybersecurity program be documented in a form that supports the disclosure. The documentation includes the risk assessment methodology, the governance structure, the third-party engagements, and the broader operational framework. The chief financial officer who maintains the documentation in a form that supports the disclosure will produce annual filings that satisfy the requirement. The chief financial officer who does not will produce disclosures that may not satisfy the requirement or that may be inconsistent with the actual operational reality.

The Audit Committee Oversight

The rules emphasize the board's oversight of cybersecurity and the disclosure of how the oversight operates. The dominant pattern at public companies has been for the audit committee to hold the cybersecurity oversight responsibility, with the chief financial officer as one of the executives engaged with the committee on the cybersecurity agenda. The chief financial officer participates in the audit committee discussions about cybersecurity, supports the disclosures that the company makes about the oversight, and engages with the committee on the broader cybersecurity strategy.

The engagement requires the chief financial officer to develop the capacity to discuss cybersecurity substantively rather than to defer to the chief information security officer. The audit committee will ask questions about cyber risk that the chief financial officer must answer. The committee will examine the disclosure framework that the chief financial officer signs. The committee will engage with the broader cyber agenda that the company pursues. The chief financial officer who develops the substantive engagement capacity will support the audit committee effectively. The chief financial officer who continues to defer entirely to the chief information security officer will produce committee engagements in which the chief financial officer's role is performative rather than substantive.

Ransomware Financial Readiness

Ransomware has emerged as one of the more consequential cybersecurity threats facing enterprises. The pattern involves attackers gaining access to enterprise systems, encrypting the systems and the data, and demanding payment for the decryption keys or for the assurance that exfiltrated data will not be published. The pattern produces both immediate operational disruption and the broader strategic question of whether to pay the ransom. The chief financial officer holds specific accountabilities in the ransomware response that the broader cybersecurity function cannot address.

The Treasury Dimensions

If the enterprise decides to pay a ransom, the payment itself is a treasury operation that involves specific capabilities. The payment is typically requested in cryptocurrency, which most enterprises do not operate in their normal treasury operations. The payment must be made under significant time pressure with the systems unavailable. The payment must be made through channels that the regulatory framework addresses, including the sanctions framework that prohibits payments to certain attackers and the broader anti-money-laundering framework. The treasury function must be prepared to execute the payment if the decision is made to pay, while the broader leadership debates whether the decision should be made.

The treasury preparation includes the relationships with the specialized firms that handle ransomware payment, the legal framework that addresses the sanctions and anti-money-laundering questions, the insurance coverage that may address the ransom payment, and the broader documentation that the decision will require. The chief financial officer who prepares these dimensions before the first incident will be ready to execute the decision if the leadership makes it. The chief financial officer who has not prepared will discover during the incident that the operational capacity does not exist to execute the payment even if the leadership decides it should be made.

The Cyber Insurance Dimension

Cyber insurance has matured substantially over the past several years and is now a standard component of the enterprise risk transfer portfolio. The insurance addresses the costs of incident response, the business interruption losses, the data restoration costs, the legal and regulatory response costs, the third-party liability exposures, and in some cases the ransom payment itself. The insurance market has become more sophisticated and more selective, with the underwriting requirements imposing specific cybersecurity disciplines on insured companies. The chief financial officer who engages with the cyber insurance market will produce both the coverage that

the enterprise needs and the discipline that the underwriting requires. The chief financial officer who treats cyber insurance as a procurement transaction will receive coverage that may not match the actual exposure and that may impose disciplines that the cybersecurity function has not built.

The insurance engagement includes the periodic review of the coverage against the evolving exposure, the negotiation with the underwriters on the terms and the pricing, the compliance with the underwriting requirements that may include specific cybersecurity capabilities, and the broader integration of the insurance with the incident response framework. The chief financial officer who treats cyber insurance as a strategic risk transfer mechanism will produce a coverage portfolio that supports the enterprise. The chief financial officer who treats it as a procurement exercise will produce coverage that may not address the specific exposures the enterprise faces.

The Business Continuity Dimension

A ransomware incident produces business interruption that affects the finance function specifically alongside the broader enterprise. The finance applications may be unavailable. The bank connectivity may be disrupted. The payment execution may be blocked. The close work may be interrupted. The reporting may be delayed. The chief financial officer must hold the business continuity plan for the finance function in a form that addresses these specific disruptions.

The business continuity plan includes the alternative operational procedures that allow critical finance work to continue even when the primary platforms are unavailable. The plan includes the redundancy in the bank connectivity that allows payments to continue. The plan includes the offline capabilities for the critical close and reporting work. The plan includes the communication framework that addresses the various stakeholders during the disruption. The chief financial officer who maintains the plan in a tested and current form will produce a finance function that can continue operating during a ransomware incident. The chief financial officer who has not maintained the plan will discover during the incident that the function's operational capacity does not extend to the disrupted state.

The Architectural Decisions Across the Security Domain

Several architectural decisions span the cybersecurity domain and must be held deliberately by the chief financial officer in partnership with the chief information security officer.

The Zero Trust Posture

The first architectural decision is the posture on zero trust. Zero trust is the security architecture in which no user, device, or network is trusted by default, with access requiring authentication and authorization at every interaction rather than depending on perimeter security. The architecture has become the dominant pattern in modern cybersecurity, though the implementation varies substantially across enterprises. The implications for the finance function include the integration of zero trust with the identity and access management for the finance applications, the conditional access policies that govern finance application access, and the broader architectural commitments that the zero trust posture requires.

The zero trust posture is more defensive than the perimeter security model it replaces but imposes more operational discipline. The chief financial officer should engage with the chief information security officer on the zero trust posture for the finance applications and ensure that the implementation supports the operational reality of the finance work. A zero trust implementation that imposes friction beyond what the threat model justifies will produce operational degradation that the security benefit may not justify. A zero trust implementation that calibrates the friction to the threat level will produce security improvement with acceptable operational impact.

The Data Loss Prevention Posture

The second architectural decision is the posture on data loss prevention. Data loss prevention is the discipline of preventing sensitive data from leaving the enterprise through unauthorized channels including email, file transfer, removable media, and cloud uploads. The discipline is particularly relevant to the finance function given the sensitivity of financial data and the regulatory implications of data breaches affecting financial information.

The data loss prevention capabilities are operated by the cybersecurity function with the configurations developed in partnership with the finance function. The configurations specify which categories of financial data require protection, which channels are monitored, what actions trigger blocking versus alerting, and what exceptions are permitted for legitimate business purposes. The chief financial officer should engage with the configurations because they affect the operational reality of how the finance function shares data with auditors, advisors, customers,

vendors, and other legitimate counterparties. A data loss prevention configuration that blocks legitimate data sharing will produce operational friction. A configuration that permits broad sharing will produce data loss exposure that the prevention should have addressed.

The Third-Party Risk Posture

The third architectural decision is the posture on third-party risk. The finance function depends on substantial third-party relationships including platform vendors, implementation partners, audit firms, advisors, and the broader ecosystem. Each third-party relationship represents a potential cybersecurity exposure if the third party is compromised or if the data shared with the third party is exposed. The third-party risk management discipline addresses these exposures through the assessment of third parties before engagement, the contractual provisions that govern the cybersecurity expectations, the ongoing monitoring of the third parties, and the incident response framework that addresses third-party incidents.

The third-party risk management is operated by the cybersecurity function in partnership with the procurement function and the legal function. The chief financial officer should engage with the framework because the finance function is one of the largest consumers of third-party relationships in the enterprise. The framework's calibration to the actual third-party exposure determines whether the framework produces appropriate protection or whether it produces operational friction that the protection does not justify. The chief financial officer who engages with the framework will produce third-party engagements that are both productive and adequately secured. The chief financial officer who does not will operate third-party relationships that may impose security requirements the framework has not addressed adequately.

The Diligence Questions

The diligence questions for the cybersecurity dimensions of the finance function address both the security capabilities and the integration with the broader finance function operating model.

Questions to Ask of the CISO

How does the cybersecurity architecture protect the finance function specifically, and where are the specific gaps that we should address? How does the identity and access management infrastructure support the segregation of duties that the finance control framework requires? How does the fraud technology stack address the specific exposures of the finance function, and what is our current state on business email compromise defense, vendor master integrity, payment anomaly detection, and account takeover defense? What is our cyber insurance coverage, and how does it align with the actual exposure the finance function faces? What is our ransomware readiness, and what is the operational plan if a ransomware incident affects the finance function? How does our cybersecurity posture address the Securities and Exchange Commission disclosure requirements, and what is our framework for the materiality assessment and the disclosure preparation? What is our third-party risk management for the substantial third-party relationships the finance function operates? How are you partnering with my finance team on the cybersecurity agenda, and what is the operating cadence that maintains the partnership?

Questions to Ask of Platform Vendors

How does your platform integrate with our identity and access management infrastructure, and what controls do you support for segregation of duties enforcement? What is your security architecture, and how does it compare to the broader category of platforms in your category? What is your audit reporting framework, and what audit reports do you provide that support our compliance requirements? How does your platform handle the security incident response, and what is your communication framework with customers during incidents? What is your data protection framework, and how does it address the regulatory requirements that apply to our data? What is your business continuity framework, and what is the recovery time objective and recovery point objective that you support? What is your third-party risk profile, and how do you manage the third-party relationships that affect the security of our data? How is your security posture evolving, and what is your roadmap for the cybersecurity capabilities?

Questions to Ask of One's Own Team

What is the current state of our identity and access management for the finance applications, and where are the segregation of duties gaps? What is our state on business email compromise defense, and how confident are we in the defense against this dominant fraud pattern? What is our vendor master integrity, and what work is required to bring the master to the standard the fraud control architecture requires? What is our cyber insurance coverage, and is it adequate for the exposure we actually face? What is our ransomware readiness, and what is the gap between the current state and the readiness the threat warrants? What is our disclosure framework for cybersecurity incidents, and is it adequate for the four-day reporting requirement? What is our partnership with the cybersecurity function, and is the operating cadence sufficient to maintain the joint accountability that the regulatory environment imposes?

Operating Implications

The cybersecurity accountability is operated continuously through the partnership between the finance function and the cybersecurity function. The operating implications include the partnership architecture, the audit committee engagement, and the incident response readiness.

The Partnership Architecture

The partnership between the chief financial officer and the chief information security officer is one of the more strategic partnerships in the executive suite for the current regulatory environment. The partnership operates through several specific mechanisms. The monthly working sessions between the two executives address the operational dimensions of the joint accountability. The quarterly portfolio reviews examine the cybersecurity investments against the strategic agenda. The annual planning cycle integrates the cybersecurity agenda with the broader finance and information technology agenda. The incident response framework addresses the specific events that arise. The audit committee engagement coordinates the executive presentations to the committee.

The partnership requires explicit investment in the form of the meeting cadences, the documentation, the joint accountabilities, and the operating principles. The chief financial officer who treats the partnership as a strategic priority will produce a cybersecurity posture that satisfies the regulatory environment. The chief financial officer who treats the partnership as a peripheral concern will produce a posture that operates at the minimum required level without producing the strategic protection that the substantive partnership would deliver.

The Audit Committee Engagement

The audit committee engagement on cybersecurity has become one of the more substantive dimensions of the chief financial officer's audit committee relationship. The committee engages with the cybersecurity agenda quarterly at most public companies, with specific discussions of the threat landscape, the cybersecurity investments, the incident history, the regulatory developments, and the disclosure framework. The chief financial officer participates substantively in these discussions alongside the chief information security officer.

The substantive participation requires the chief financial officer to develop ongoing capacity to engage with the cybersecurity agenda rather than to defer to the chief information security officer's prepared materials. The committee will ask questions that the chief financial officer must answer in real time. The committee will probe positions that the management has taken. The committee will examine the disclosure framework that the chief financial officer signs. The chief

financial officer who develops the substantive engagement capacity will support the committee effectively. The chief financial officer who has not will discover during the engagements that the committee's expectations exceed what the prepared materials address.

The Incident Response Readiness

The incident response readiness includes the operational capacity to respond to cybersecurity incidents when they occur. The readiness includes the incident response team that the enterprise operates, the relationships with the external incident response firms that supplement the internal capacity, the legal counsel that supports the response, the communications framework that addresses the various stakeholders, the disclosure preparation capacity, the insurance engagement framework, and the broader operational continuity capacity.

The readiness is tested through tabletop exercises that simulate incidents and that examine the response capacity. The exercises surface the gaps in the readiness before the actual incident demands the capacity. The chief financial officer should participate in the tabletop exercises that involve the finance function specifically and should engage with the broader exercises that may affect the function indirectly. The participation develops the chief financial officer's own readiness alongside the broader organizational readiness. The chief financial officer who engages with the exercises will be prepared for the actual incident when it occurs. The chief financial officer who has not engaged will discover during the actual incident that the readiness exists on paper but not in operational reality.

Synthesis

Cybersecurity in the finance function is now a jointly held accountability between the chief financial officer and the chief information security officer rather than the exclusive concern of the cybersecurity function. The change has been driven by the Securities and Exchange Commission disclosure rules that came into effect in 2023, by the evolving regulatory framework across multiple jurisdictions, by the maturation of the audit profession's engagement with cybersecurity, and by the broader recognition that cybersecurity exposures intersect with the financial reporting framework directly. The chief financial officer who continues to treat cybersecurity as the chief information officer's concern is operating with an outdated accountability model and is accepting personal exposure that the substantive engagement could address.

Identity and access management is the foundational dimension of cybersecurity in the finance function. The category leaders include Okta, Microsoft Entra, SailPoint, and CyberArk. The discipline operates at the intersection of cybersecurity and the segregation of duties framework that Sarbanes-Oxley compliance depends on. The architectural enforcement of segregation of duties through the identity infrastructure is a finance discipline that the cybersecurity function operates rather than the reverse. The periodic access review discipline is one of the more underdeveloped areas at most enterprises and requires the chief financial officer's insistence on rigor to satisfy the audit.

The fraud technology stack addresses the specific cybersecurity exposures that target the finance function for financial gain. The stack includes the business email compromise defense, the vendor master integrity, the payment anomaly detection, and the account takeover defense. Business email compromise has emerged as the dominant fraud pattern and requires a combination of technology, process, and cultural posture to defend against effectively.

The Securities and Exchange Commission cyber disclosure regime imposes the four-day reporting requirement for material incidents and the annual disclosures about cybersecurity governance. The materiality assessment is the dimension that most directly involves the chief financial officer and requires the operational framework to operate effectively under the time pressure that the requirement creates. The audit committee oversight has become substantive at most public companies and requires the chief financial officer's substantive engagement rather than deference to the chief information security officer.

Ransomware financial readiness includes the treasury dimensions of potential ransom payment, the cyber insurance dimension that addresses the broader incident costs, and the business continuity dimension that addresses the operational disruption to the finance function specifically. The chief financial officer who prepares these dimensions before the first incident will be ready to execute the necessary responses. The chief financial officer who has not prepared will discover during the incident that the operational capacity does not exist.

Three architectural decisions span the cybersecurity domain. The zero trust posture determines the architectural pattern for access control. The data loss prevention posture determines the protection against sensitive data leaving the enterprise through unauthorized channels. The third-party risk posture determines the protection against exposures from the substantial third-party relationships the finance function operates.

The operating implications include the partnership architecture between the chief financial officer and the chief information security officer, the audit committee engagement that has become substantive at most public companies, and the incident response readiness that requires testing through tabletop exercises before the actual incident demands the capacity. The chief financial officer who builds the cybersecurity accountability with awareness of these operating dimensions will produce a finance function that satisfies the regulatory environment and that protects the function from the threats the environment addresses. The chief financial officer who treats cybersecurity as the cybersecurity function's concern alone will discover that the regulatory environment, the audit profession, the board, and ultimately the threat landscape all hold the chief financial officer accountable regardless of how the operating model is structured.

The next part treats integration architecture, application programming interfaces, and the integration platform as a service decision. The integration layer is the invisible layer of the finance technology stack that consumes substantial cost and that determines whether the architecture holds together. The architectural reasoning developed across the preceding parts carries forward into the treatment of this critical but underexamined layer.