datos INSIGHTS

November 2024

CISO 2025 Concerns and Priorities: A Challenging Year Ahead

John Horn

This report provided compliments of:

Arkose Labs

November 2024

CISO 2025 Concerns and Priorities: A Challenging Year Ahead

John Horn

Table of Contents

List of Figures

List of Tables

Summary and Key Findings

With continued data breaches, new attack vectors, and challenging economic conditions, 2024 presented many difficulties for CISOs at financial institutions (FIs), insurers, and other financial services (FS) firms. Artificial intelligence (AI) concerns and hype continued to dominate the market in 2024, with generative AI (GenAI) tools available for attackers for two full years. As criminal teams evolved their use of AI-enabled attack tools (aka adversarial AI), cyberattacks continued to become more sophisticated and delivered at greater scale than ever before. CISOs and other risk leaders at FS firms continued to advance their understanding of AI concerns and defense opportunities. Customer identity and access management (CIAM) solutions have grown in importance to the business. Datos Insights research indicates CISOs have risen to the second most frequent budget holder for CIAM solutions. Cyber governance, risk, and compliance (GRC) tools to enable board-level cyber risk oversight have also risen in priority for FS firms.

As 2024 projects and tasks head to their conclusion, CISOs and business leaders are increasingly focused on the new year. Final adjustments to 2025 cyber budgets are becoming complete. With a growing attack surface, a charge to defend the enterprise, and a call to support business growth, CISOs and other cyber risk leaders have a daunting task for the new year. Driven to reduce assessed risk, support business growth, achieve operational efficiencies, and comply with regulations, CISOs have decided where to place their bets for 2025. While every firm is unique and internal perspectives are invaluable, CISOs and risk leaders need external FS peer perspectives for cyber priorities and investments. How are other CISOs looking at 2025? How do firms' top cyber concerns compare to the concerns of other FS CISOs in the market? The purpose of this research report is to answer these and other critical questions for CISOs, chief risk officers (CROs), and other cyber risk leaders at FIs, insurers, or other FS firms. Key findings for this report follow:

- **Entering 2025, CISOs and cyber risk leaders are more concerned about AI-enabled cyberattacks than they were one year ago:** Increased awareness of deepfakes and other AI-enabled attacks is driving this concern.
- **Customer account takeover (ATO) via phishing and the resilient performance of business applications are the top cyber concerns for the FS customer channel:** Criminal teams have moved to attacking consumers as the weakest link. The financial

impacts of downtime for consumer digital services on the business have become severe.

- **CIAM investments to increase fraud detection rate and elevate resilience of consumer digital services are the top cyber investments tied to business growth:** Business leadership for consumer services urgently needs cyber assistance to shore up fraud prevention and downtime of business applications. While API security improvements remain important, key CIAM improvements have leapfrogged over API security for business growth in 2025.
- **Data breaches via phishing of workforce members and the resilience of the digital enterprise are the top concerns for the FS corporate environment:** Phishing, spear phishing, and social engineering of the workforce became widespread in 2024, becoming the top attack vector for enterprise data risks, including ransomware.
- **Improvements to cloud security, data security, and board-level cyber GRC tools are the largest budgeted cyber investments for 2025:** Most FS firms operate as multicloud enterprises, which have become the key fulcrum to boost operational cloud maturity and security assurance. At the top of the house, most FS firms need to improve tooling for board-level cyber risk oversight.

Introduction

Cybersecurity for FIs, insurers, and other FS firms owes its historical roots to information technology, focused on technically oriented information security (InfoSec) concerns and solutions within the IT estate. For the past two decades, CISOs and their teams have been forced to defend their digital businesses in the context of a rapidly expanding IT estate (aka expanding attack surface) and an increasingly effective worldwide community of cybercriminals. The difficult remit for FS CISOs is to defend the business as their (horizontal) attack surface expands and has become more vulnerable to technically expert cyber attackers. These challenges are becoming greater in the modern age. Attack surfaces continue to broaden in multicloud hybrid deployments. Criminal teams are better financed and equipped—no longer requiring technical expertise to be effective. In just two years, the availability of GenAI-based tools has practically lowered the entry bar for more criminal teams to succeed without strong technical talent.

The modern age has also brought new "vertical" challenges to FS CISOs—namely, the evolution of how their firm financially manages cyber risk at the executive and board levels of the organization. A more robust set of cyber functions at the FS firm looks like this:

- **Cybersecurity** represents traditional, technical information security defending the firm's IT estate. Most CISOs lead this function.
- **Cyber risk management** represents business-focused executive management of risks material to the firm's existence, service quality, and financial responsibilities. This function is often led by the CRO, leveraging tools in the domains of GRC and enterprise risk management. Some CISOs play important roles within this function.
- **Cyber risk oversight** represents board-level oversight and steering of the firm's cyber risk management function, ensuring fiscal and risk management for ongoing business viability and well-being to stockholders and to the market at large. Many CISOs provide board-level risk readouts on a quarterly basis.

As FS CISOs and risk leaders enter 2025, they must organize the defense of their businesses with significant horizontal risk challenges and evolving vertical risk management at their firm. This research report is intended to inform CISOs of these formidable cyber risk tensions, opportunities, and priorities.

Methodology

This report leverages research from a Datos Insights survey of CISOs and cyber risk leaders from 60 North American FIs conducted in August 2024. Given the size and structure of the research sample, the data in this report are considered a directional indication of conditions in the market. The report is also informed by FS CISO discussions throughout 2024, including quarterly sessions with Datos Insights' FI and Insurer CISO executive councils. Finally, this report compares the concerns and priorities of 2025 to those of 2024, spotlighting key trends.

Market Trends

Cyber risk management and cybersecurity concerns for FS firms are evolving rapidly in the market. Topics of intense market hype over the past five years (e.g., zero trust, identity, AI) can also become points of confusion when CISOs believe these strategic capabilities can be purchased through a single vendor rather than functioning as multiyear programmatic strategies. Datos Insights believes the trends in Table A prompt FS CISO strategic planning and practical action for their business.

Table A: Trends for FS CISO Concerns and Priorities

Trend	Description
FS now operate in a sea of breached consumer data. Passkeys are well-positioned to provide value to workforce and customer channels of the business.	2024 research indicates that 61% of U.S. adults have had their personally identifiable information (PII) exposed in a data breach, while 44% of U.S. adults have had their PII exposed in multiple breaches.[1] Passwords and other knowledge-based authentication and identity verification solutions have limited value and create significant risk for FS.
Beyond IT-based cybersecurity, cyber risk oversight (board level) and cyber risk management (C-suite) practices are rising in importance for FS firms.	The business-centric practices of managing cyber risk require different skill sets and tools than many CISOs have expertise. Personal liability for CISOs, CEOs, and board members is the long-term trend and appears closer at hand some days. Process strategy, role definition, and built-for-purpose tooling for board use are needed. Operational maturity for board-level oversight becomes the pursuit.
Hybrid, multicloud enterprise FS deployments have become the standard context for assessing the robustness of cyber defenses and data protection solutions.	Datos Insights' 2024 research indicates most FS firms have five or more cloud deployments. Single cloud security solutions are not well-positioned to adequately defend modern FS enterprises operating across multiple cloud providers. Security, data protection, and identity solutions powered by AI, designed to operate across multiple cloud deployments, are best positioned to protect modern FS enterprises.

[1] Claudia Dimuro, "61% of Americans Have Had Their Personal Data Breached," pennlive.com, February 8, 2024, accessed October 31, 2024, https://www.governing.com/management-and-administration/61-of-americans-have-had-their-personal-data-breached.

Trend	Description
CISOs are increasingly responsible for strengthening operational resilience for the customer side of the business.	CISOs and their cybersecurity teams are well-suited to elevate operational aspects of customer services, including improving system uptime and mitigating performance risks associated with third parties. Datos Insights' 2024 research also indicates that CISOs have surged to become second only to CIOs as the budget owner of CIAM, working with many internal partners.
CISOs are beginning to serve financial crime prevention teams to improve risk detection and operational aspects.	In the age of complex cyberattacks and AI-enabled scale, cyber teams are well-skilled to serve fraud and anti-money laundering teams to share threat intelligence data, lift fraud detection rates through robust CIAM solutions, and help the business gain operational efficiencies.
Based on growing concerns regarding AI cyber risk, CISOs need more institutional structure for AI risk management.	AI hype continues in the market. CISOs have a unique remit for AI to include risk management. Lack of a programmatic structure for AI risk management appears to be a common problem.

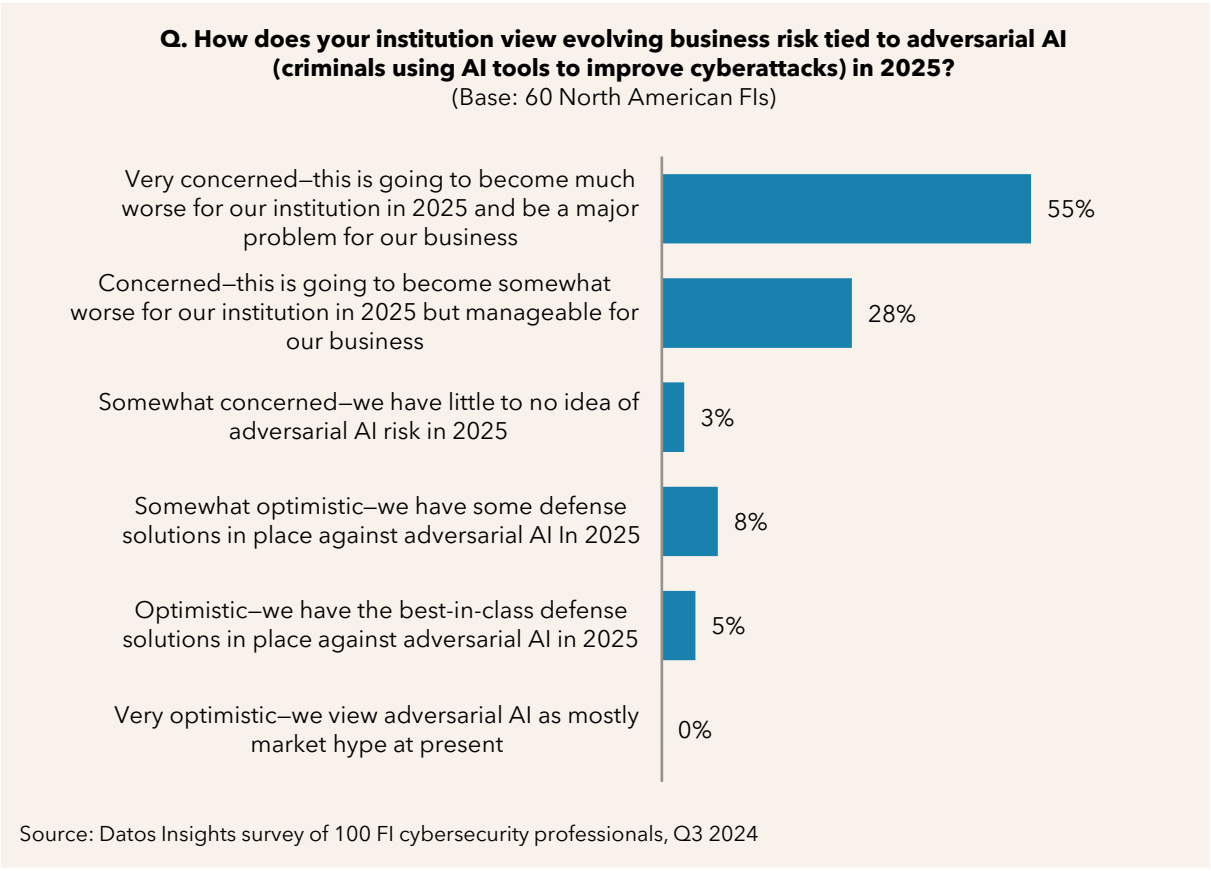
Source: Datos Insights

FS firms are adding to CISOs' scope and business criticality every year. The number of concerns and the variety of strategic trends faced by FS CISOs can be overwhelming. But with peer perspectives, a well-grounded view of concerns, and an increased understanding of the business, CISOs can lead successfully and function as invaluable risk executives for the organization.

AI Cyber Concerns Are Increasing

AI risks and opportunities continued as the most hyped topic within the market in 2024. With almost two years operating in the season of GenAI tool capabilities, CISOs in the Datos Insights 2024 FI survey were asked to describe their risk expectations and concerns for AI-enabled cyberattacks (aka adversarial AI) against their institution in 2025 (Figure 1).

Figure 1: FI Business Risk Concerns Related to AI-enabled Attacks



Source: Datos Insights survey of 100 FI cybersecurity professionals, Q3 2024

Significantly, CISOs and cyber risk leaders appear more concerned about AI-enabled cyberattacks than they were one year ago.

In August 2023, a Datos Insights survey of 27 FS CISOs highlighted only 26% believed adversarial AI represented major concerns and problems for their firm over the next years. Modest adversarial AI concern was shared by 56% of these CISOs.

In the more pointed August 2024 survey, the research indicated that 55% hold major concerns about adversarial AI attacks against their firm in 2025. Common sense might

suggest CISOs would become less concerned with a new technology after 12 months, so what is driving these greater concerns? While each FS firm is unique and on a distinct digital journey, this analyst believes some common aspects in combination are driving greater CISO concerns entering 2025:

- **AI-enabled attacks remain new phenomena for which most CISOs still have no operational basis:** Many CISOs operate from a rich set of previous experiences with new or disruptive technology. This is a strong approach with many practical benefits. But especially for GenAI risk, lack of operational experience fuels risk concerns.
- **Specific AI-enabled attacks such as deepfakes are becoming more known in the market:** Criminal teams are increasingly adept at deepfakes—they can permutate them with GenAI and incorporate created outputs into payloads. CISOs have legitimate concerns about biometric-based controls currently in use.
- **Many FS firms have not made significant progress in deploying needed solutions:** CISOs have many competing priorities and limited budgets. It is straightforward to predict adversarial AI will increase criminal reconnaissance against the IT estate or to assert "you need AI to defeat AI" (which is true strategically). However, market solutions to detect possible AI-based reconnaissance are just emerging in the market. CISOs in these situations have greater concerns, as they know attackers are not waiting for their firm to improve defenses before attacking.
- **Many FS firms appear to lack the AI-centric program structure to organize the major tracks of AI work and solidify C-suite and board-level support:** Many firms have "AI committees" or similar structures, and these are helpful. But AI risk management is a difficult domain requiring strong institutional structure. Lacking this structure, FS firms can become lost in market hype, hearing about the latest AI developments. Lacking AI skill competencies in the organization, FS firms can be very active in learning more but make little progress in deploying improved defenses. CISOs in this situation have greater concerns.
- **Cyberattacks appear to be scaling significantly:** Q3 2024 research from non-Datos Insights source indicates worldwide cyberattacks have increased 75% from the previous year (Q3 2023) and increased 15% from the previous quarter (Q2 2024).[2]

[2] "A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide," Check Point Software Technologies Ltd., October 18, 2024, accessed October 31, 2024, https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/.

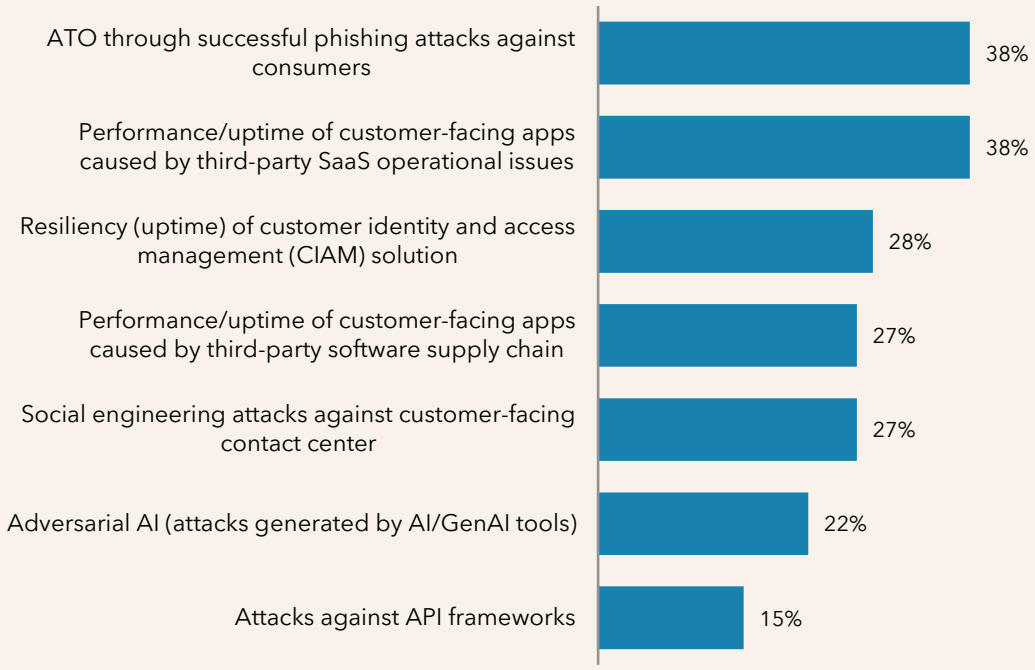
This same research highlights cyberattacks against FS firms worldwide have increased 40% from the previous year (Q3 2023), with FS firms experiencing 242 attacks per day on average. More attacks, plus other factors, contribute to greater concerns that adversarial AI may be involved in the scaling of attacks.

Customer Channel Top Concerns

CISOs are increasingly tasked to strengthen operational resilience for the customer (consumer) side of the business. Cyber teams are well-suited to fortify operational aspects of customer services, including improving system uptime and mitigating performance risks associated with third parties. The financial impacts of a downtime event for consumer digital services to the business have become severe. Datos Insights' 2024 research also highlights that CISOs have surged to become second only to CIOs as the budget owner of CIAM, working with many internal partners. Figure 2 presents the top cyber risks for the FS customer channel.

Figure 2: Top Cyber Risks for FS Customer Channel

Q. Please identify the cyber risks most concerning for your customer-facing businesses in 2025; Select the top two
(Base: 60 cybersecurity professionals at North American FIs)



Source: Datos Insights survey of 100 cybersecurity professionals, Q3 2024

Two cyber risks tied as top identified threats to the customer-facing business:

- **ATO of consumers:** ATO has been a constant risk throughout the last decade. In the modern age, phishing of consumers has become a major business concern. Often operating with low-quality, phish-able user credentials (user IDs and passwords),

and aided by recent AI improvements, criminals have moved to attacking consumers, the weakest link in the FS ecosystem. Mitigating phishing risks for consumers is the top cyber risk CISOs and cyber risk leaders have prioritized for the customer channel.

- **Performance of consumer digital services tied to third-party Software-as-a-Service (SaaS):** SaaS vendor risk is the other top cyber risk for the customer channel. The dependence of FS firms on third-party SaaS-based services (of which the CISO is responsible) is not a new problem. The concern has simply risen in business impact given the financial impacts of consumer services not performing well, increased vulnerability of third-party SaaS services to cyberattacks and operational outages, and other dimensions, such as geopolitical risks.

Other strong cyber risks include base uptime performance improvements associated with the CIAM solution (which the CISO owns). In an earlier 2024 Datos Insights' study, CIAM leaders identified uptime resilience improvements as one of the top needs of the business. Many FS firms (especially larger FIs) need CIAM uptime performance to extend beyond business resumption/disaster recovery (BR/DR) operational models, which are well-known to the business, to increase availability.

Performance aspects related to the third-party supply chain were also emphasized. This was particularly evident on July 19, 2024, with the CrowdStrike/Microsoft operation event, which impacted customers worldwide. Supply chain risk is not new to risk professionals, but the July event elevated these risks in society at large. FI CISOs and cyber risk leaders were surveyed within a few weeks of the worldwide CrowdStrike/Microsoft event.

Several other cyber risks held noteworthy attention, indicating how important CISOs and their teams have become in shoring up the operational aspects of the FS customer-facing business. This analyst believes this trend continues to grow stronger in time, to the point at which CISOs completely own the operational performance and resilience of their firm's digital services for customers.

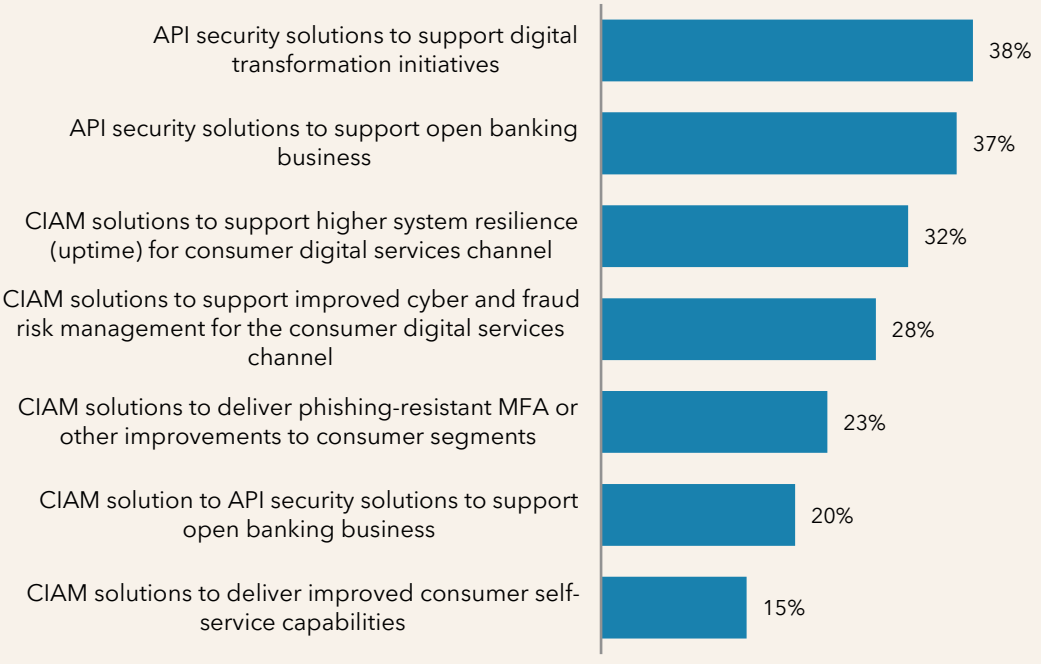
Top Cyber Investments Tied to Business Growth

FS firms have a fundamental charge to grow the business. For more than a decade, FS business leaders have become aware of how important security is to achieving and sustaining business growth. Datos Insights asked FS leaders how they invested in cyber to grow their business in research conducted in Q3 2023 (for 2024 growth) and Q3 2024 (for 2025 growth).

Cyber Investments Supporting 2024 Business Growth

In Q3 2023, a Datos Insights survey asked CISOs and cyber risk leaders to identify their top security investments supporting 2024 business growth (Figure 3).

Figure 3: Cyber Investments Most Connected to 2024 Business Growth



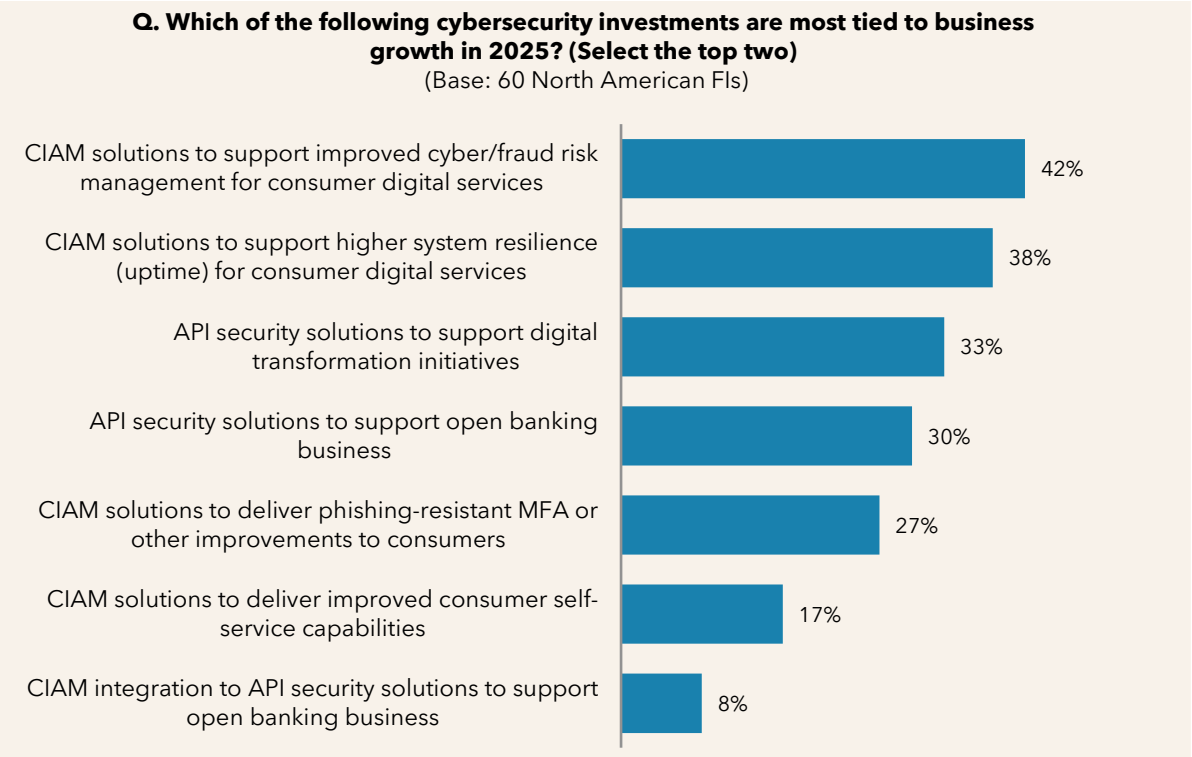
Source: Datos Insights survey of 100 cybersecurity professionals, Q3 2024

To promote business growth in 2024, CISOs and cyber risk leaders were primarily asked to prioritize API security (APISec) investments to support secure digital transformation activities at the FI (top priority) and secure open banking business (close second priority). When asked more specifically what was driving APISec improvements for 2024, CISOs responded that gaps in regulation (such as the Federal Financial Institutions Examination Council Examination Handbook) were the strongest force driving APISec investments and that business growth support was the second-strongest driver for 2024 APISec investments.

Cyber Investments Supporting 2025 Business Growth

This same question was asked of FS CISOs and cyber risk professionals regarding their top cyber investments to support 2025 business growth initiatives (Figure 4).

Figure 4: Cyber Investments Most Connected to 2025 Business Growth



Source: Datos Insights survey of 100 cybersecurity professionals, Q3 2024

CIAM solutions to increase fraud detection rates for consumer business were the top cyber investments tied to supporting business growth in 2025. This came as a surprise to some, with APISec such a critical investment for secure open banking growth—even more so with the final ruling by the Consumer Financial Protection Bureau (CFPB) on Dodd-Frank 1033, occurring on October 22, 2024. But through inquiries and other research projects over the past 18 months, this analyst has observed that CIAM has steadily elevated in FS business criticality. This confirms earlier research and discussions with CISOs and market leaders on how important CIAM has become to their business strategy and growth, how important operational efficiencies have become to the business, and how CISOs have been charged to modernize CIAM for the sake of fraud detection rate improvements (top priority) and for the sake of greater uptime resilience of consumer digital services (second-highest priority).

This leapfrog of CIAM as a growth priority over APISec over the past year is ripe for one possible misinterpretation—namely, that APISec has become less important to FS business. This analyst refutes any interpretation along these lines. API-based business growth remains critical to FIs, insurers, and other FS firms. Security improvements are fundamental for businesses to achieve API-based digital transformation growth (third-highest priority), especially for insurers. In some ways, robust APISec solutions are the lynchpin for open banking growth at FIs (fourth-highest priority). As indicated by the research, APISec remains tied to top business growth for more than 30% of the FI leaders surveyed. This proves the business growth FS firms hold for API-based ecosystems and the need to secure API-based ecosystems from sophisticated attackers who have found API ecosystems and, in some cases, soft targets to exploit.

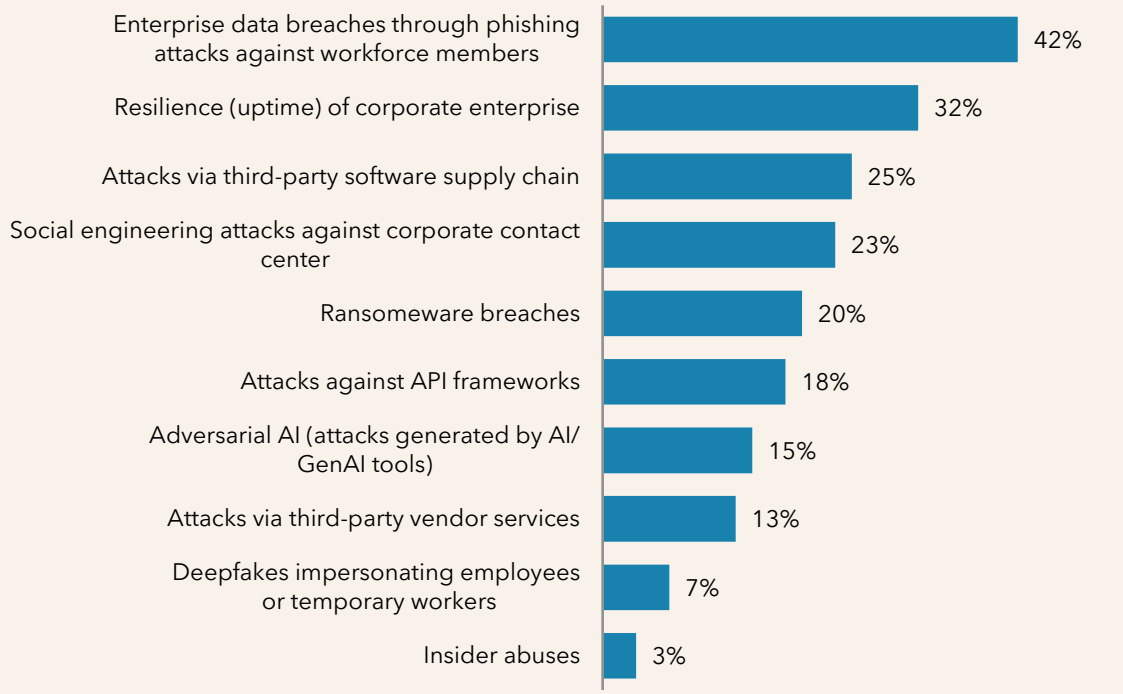
Rather, this analyst believes the rise of CIAM to the top cyber investment tied to growth represents the business holding long-time needs to improve operational realities faced by financial crime prevention teams in a world where consumers increasing use of real-time payment (RTP) rails is being shadowed by growth in fraud. Often operating with numerous siloed fraud solutions and lower-class CIAM solutions, which tend to hinder rather than help fraud detection, businesses want a more cohesive ecosystem in which CIAM insights function as risk signals, which increase the efficacy of fraud detection, lower false positive rates, and improve operational efficiencies. This analyst holds that modern CIAM solutions, fully integrated into critical "utility" functions, such as bot management and threat intelligence, are instrumental to fraud detection improvements. Investment in CIAM to elevate fraud detection rates is an important 2025 trend and is the focus of an active Datos Insights research project expected to publish in Q1 2025.

Corporate Enterprise Top Concerns

CISOs must also defend their corporate enterprises against cyber risks. The stakes are high. A nonfunctioning digital enterprise has a severe negative impact on the business. Criminal teams have become increasingly successful in circumventing enterprise security controls to conduct ransomware attacks on the enterprise and socially engineering workforce employees to conduct insider attacks leveraging enterprise connections. These challenges are made even more difficult due to the complicated deployment nature of most FS enterprises, with multiple cloud service provider (CSP) deployments to host business services and connections to third-party business partners.

As a result, CISOs and cyber risk professionals have many concerns related to cyberattacks against their corporate enterprise environment (Figure 5).

Figure 5: Top Cyber Risk Concerns for the FS Corporate Enterprise



Source: Datos Insights survey of 100 cybersecurity professionals,Q3 2024

Enterprise Data Breaches via Phishing of Workforce Users

Enterprise data breaches are the top concern entering 2025. In January 2024, the Identity Theft Resource Center issued its annual report, which highlighted 3,205 data breaches (compromises) and more than 353 million victims in 2023—a 71% increase from previous highs experienced in 2021.[3] Non-Datos Insights research from Q3 2024 suggests cyberattacks against FS firms worldwide have increased 40% from Q3 of last year.[4] As 2024 comes to a close, this analyst suggests enterprise data breaches for this year will exceed 2023 incidents by a sizeable percentage. While the market has become almost numb to the steady stream of data breaches, FS firms are highly motivated to keep their business out of the "data breach news" and avoid the resulting business penalties. Note that ransomware breaches (20%) and the more recent attack style "extortionware" are specific instances of data breaches that FS firms are strongly driven to prevent.

Phishing of workforce employees (and contractors) is the attack vector leading to enterprise data breaches, which is of highest concern to CISOs and cyber risk leaders. Criminals have moved to attacking individual users—the weakest element of the FS ecosystem. For the customer side of the business, these individuals are consumers. For the corporate enterprise, these individuals are workforce employees, contractors, temporary gig workers, and interns. This corporate enterprise concern was raised in 2022 and 2023, but it was 2024 when all FS came to grips (in various degrees) with the reality that attackers were less prone to attack fortified enterprise security defenses and more likely to circumvent these defenses by phishing and socially engineering workforce individuals.

A July 2024 Datos Insights study examined FS corporate enterprise cyber risks. Phishing success against workforce individuals was the CISO's top cyber risk concern (consistent with the results of this study). Furthermore, the July 2024 study identified system administrators as the category of workforce users that posed the greatest risk to the business when they were phished. System administrators hold premium access to sensitive user data and key infrastructure. Even as most FS firms mitigated system administrator risk somewhat through the use of privileged access management (PAM) solutions, the majority of CISOs found their current PAM solutions inadequate to defend the business and were

[3] "2023 Data Breach Report," Identity Theft Resource Center, January 2024, accessed November 6, 2024, https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf.

[4] "A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide," accessed October 31, 2024.

considering passkey solutions, aka phishing-resistant multifactor authentication (MFA), to further reduce this high threat.

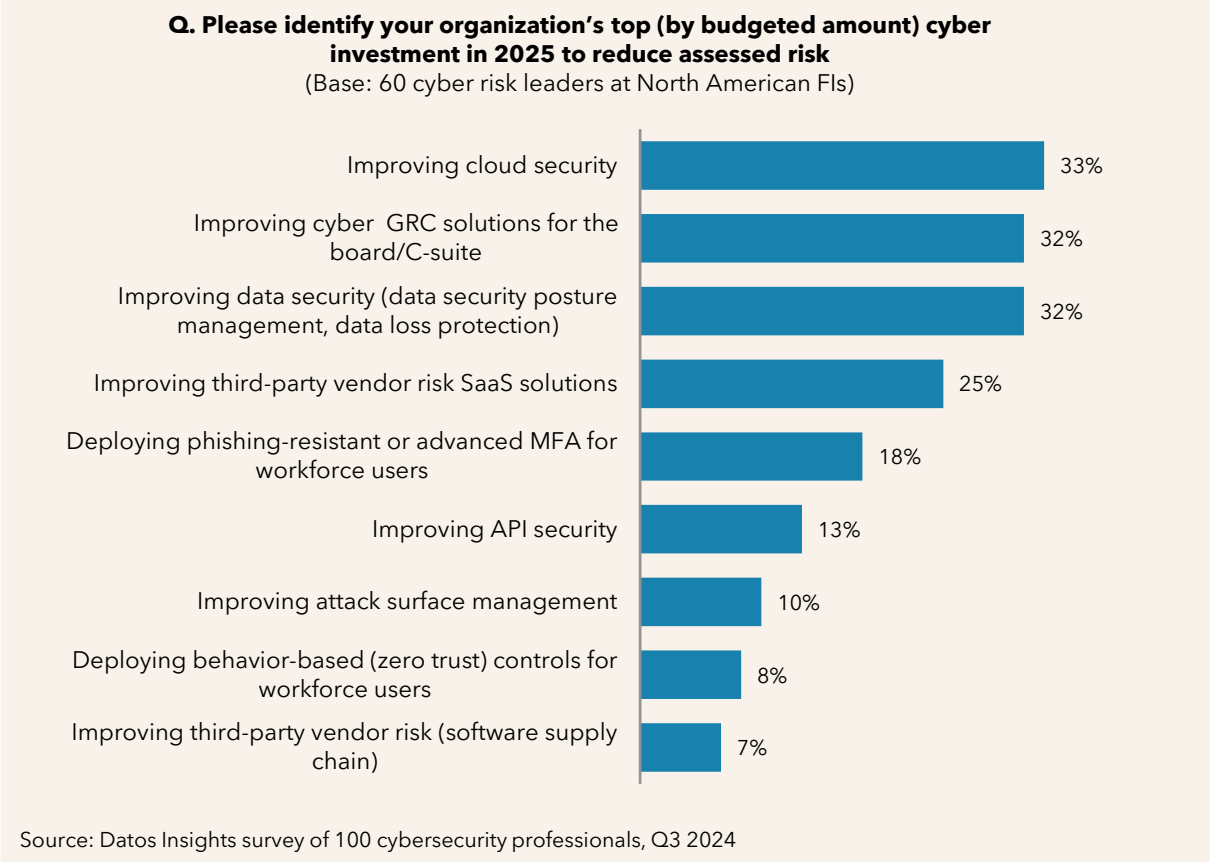
Resilience of the Corporate Enterprise

The resilience of the digital enterprise was the second-highest enterprise cyber risk highlighted by CISOs and cyber risk professionals. Similar to resilience improvements needed on the customer side of the business, FS executives are demanding greater resilience for the corporate enterprise due to the severe business impact of corporate outages. Resilience improvements have become more challenging as FS enterprises have become much more complicated. In the modern age, FS enterprises are composed of multiple cloud deployments, large numbers of third-party partner connections with varying degrees of business criticality, support for remote workers stemming from the recent pandemic, and technical debt. Through the lens of the business, cyber resilience can be practically defined as "improved operational uptime for the business while under the pressure of increasingly effective cyberattacks, and in the context of a complex digital enterprise deployment." This critical business objective will require CISOs to partner across the organization and consider technical architectures and tools that help simplify enterprise management and support, requiring programmatic (multiproject) approaches to achieve elevated resilience outcomes.

Top 2025 Cyber Investments for Enterprise by Budgeted Amount

FS CISOs operate year after year with funding prioritized through the long-range planning process and earned through the annual budget process. Stating the obvious, CISOs do not win all the funding they request and must optimize the impact of the funding they receive from the business. The year ahead is no different. A prioritized view into 2025 is uniquely informed by understanding the kinds of solutions that will receive the greatest amount of funding per budget in the new year (Figure 6).

Figure 6: Top 2025 Cyber Investments for Enterprise by Budgeted Amount



Source: Datos Insights survey of 100 cybersecurity professionals, Q3 2024

Improvements to cloud security, data security, and board-level cyber GRC tools are the largest budgeted cyber investments for 2025. These three solution types have not achieved this degree of FS emphasis in any previous years.

Cloud Security Improvements

Securing the cloud has become more critical and more complicated for FS firms, reaching a kind of tipping point, as indicated by the study's results.

Technical complexity is the enemy of effective operational support and robust cyber resilience. Cloud complexity is common for many FS firms due to multiple factors:

- **Multicloud deployments have become the operational norm:** A recent survey of Datos Insights FI and insurer cyber executive councils in Q3 2024 indicate that 65% of firms operate with five or more CSPs. These results are consistent with other discussions with FS firms. Businesses have "intentionally chosen" a primary CSP to host their applications and services, and often choose a second CSP driven by concentration risks of a single provider. Other CSPs come from the necessity to connect with a vast number of third-party SaaS providers critical to the firm's customer-facing and corporate enterprise services. Multiple CSPs create complexity.
- **Business applications hosted at CSPs are not always upgraded to cloud-native technologies:** Project timelines in moving services to the cloud often require compromises to updating services to cloud-native technology stacks. Teams often commit to "getting that fixed later," but in practice, the follow-up actions fail to materialize. In some cases, so-called "lift and shift" strategies are intentional. In other cases, the lack of cloud technology talent may influence tactical decisions. In all cases, the support and cyber resilience of resulting cloud-hosted business applications suffers due to this tech stack complexity.
- **On-premises services often remain essential as back-end proprietary services can be difficult to move to cloud:** Some business services moved to cloud depend upon key back-end services, which are extremely difficult to operate in a cloud-hosted model. Often, these back-end services are proprietary, legacy services that require expensive refactoring or specialized talent to transition to the cloud. For these reasons and more, firms often require some part of business applications to be deployed on their data center premises, which complicates operational support and cyber resiliency.
- **Shared responsibility models are necessary, but they also tend to be part of the operational maturity problem:** By the nature of their business, CSPs must operate in some kind of "shared responsibility" operational model, in which the CSP is responsible for a clear set of tasks while the customer (FS firm) is responsible for other tasks. However, in practice, many FS firms have struggled to advance operational

maturity across their multiple CSPs due to significant unplanned costs, multiple CSPs, and cloud technology talent challenges. In this context, cyber resilience suffers significantly. Opportunities exist for CSPs to close this gap.

From this advisor's view, CISOs, CTOs, CIOs and other executive leaders within the business should view "cloud security" as challenge. Bringing greater operational maturity and cyber resilience to hybrid, multicloud enterprise deployments is difficult. In this reality, it is no wonder that CISOs and other cyber risk leaders have planned large spends on a variety of tools for 2025 to improve operational maturity and cyber resilience for their hybrid, multicloud digital enterprises.

Multicloud security has become a kind of ground zero in 2025 for many FS firms. In high partnership with executive peers, this advisor recommends FS CISOs pursue the following kinds of multicloud investments:

- Robust security tools natively designed to optimize value for hybrid, multicloud deployments
- Management and operational tools that enhance visibility, simplify management, and help mature operational support of hybrid, multicloud deployments—improving operational maturity also improves cyber visibility and resilience

Enterprise Data Security Improvements

As the top cyber risk concern for the corporate enterprise entering 2025, data breaches–and their close cousins, ransomware attacks and extortionware attacks–are top of mind for leaders. FS firms are strongly motivated to defend against these attacks and provide higher degrees protection for sensitive data.

In the reality of hybrid, multicloud digital enterprises, strong data security should be considered the essential jewel within the FS cloud security strategy. Robust data protection is fundamental to the trust FS firms offer to their customers. FS firms are charged to steward the sensitive data of their customers and hold regulatory obligations toward these ends.

Data security is challenged by some of the same practical realities faced by FS cloud security. Complexity and lack of operational maturity for multicloud deployments are the

same basic difficulties faced by leaders charged with improving data security and de-risking the business from data breaches, ransomware, and extortionware.

Data security has unique aspects, including establishing a robust data model that presumes multicloud as a native aspect. Data security posture management (DSPM) solutions in the market hold multicloud in this manner. Many traditional database security and data loss prevention (DLP) vendors are expected to evolve toward multicloud realities.

At this time in history, data security can be quickly improved through appropriate MFA. For many of the data breaches occurring in the market, the lack of some kind of MFA for a cloud support interface is a common theme in post-mortem analysis. While this advisor strongly recommends the deployment of passkeys (aka phishing-resistant MFA) due to their many benefits to the business, a default practice of requiring at least legacy MFA (e.g., one-time passcodes) for all cloud support interfaces would help FS firms improve their risk posture considerably. Major CSPs began moving toward this "default MFA" model in 2024.

This advisor recommends that FS firms pursue more robust data protection strategies as a key component in a program to improve multicloud security strategies. Some FS firms may seek to drive multicloud security improvements by first establishing a more robust data security strategy. In any case, these two top cyber investments in 2025 have much to do with one another and should be managed accordingly.

Cyber GRC Improvements for the Board and C-Suite of the Business

Improving cyber GRC capabilities at the board and C-suite level of the business is tied for the second-largest 2025 cyber budget spend for 2025, narrowly missing the number one spot for the coming year. The "vertical" challenges to FS CISOs in how their firm manages the business of cyber risk at the top of the house, including financial considerations, have reached a tipping point based on this research.

Enabling a more effective, efficient, and formal three-role function of cyber risk oversight involving the board, cyber risk management (CRO, C-suite), and cybersecurity (CISO) is no easy task. Many firms have multiple GRC products across the enterprise. At the board level, various GRC tooling exist. However, for the cyber tenant of GRC, legacy board solutions are often self-built processes supported by Excel spreadsheets and PowerPoint slides. These legacy solutions are highly manual and resource-heavy, and they tend to emphasize

technical cybersecurity and numbers of defects rather than the cyber risk management aspects board members and C-suite leaders most need to be effective.

All FS firms absolutely need an evolution in tactics to effectively manage the business and financial impacts resulting from cyber risk. Board members and top executives have fiduciary responsibilities with respect to the business—even for aspects such as cyber risk, which historically have been more difficult to rate and quantify, and even if board members and other executives are not formally trained cyber experts. In the market, the CISOs, CEOs, board members, and top executives are being considered to hold "legal liability" in data breach cases—situations in which the firm did not perform sufficient due diligence, did not invest effectively in cyber defenses, or was perceived to mislead investors regarding how cyber risk was managed at the firm. Earlier this year, legal outcomes for the 2019 Solar Winds breach provided some relief for CISO and executive liability aspects in the near term.[5] However, the U.S. Securities and Exchange Commission (SEC) recently charged four security vendors with making materially misleading disclosures regarding cybersecurity risks and intrusions, with the highest penalty US$4 million.[6] Trends for increased corporate penalties are clear.

Fortunately, the market has cyber GRC products for FS firms to evaluate, purchase, and deploy in 2025. Some products originate in IT or cyber while others have traditional GRC roots. Some products are more capable than others.

Cyber GRC maturity for the board and C-suite is an important 2025 trend. It is the focus of an active Datos Insights research project expected to be published in Q1 2025.

[5] "SEC v. SolarWinds Update: U.S. Federal District Court Dismisses Most of the SEC's Case, but Some Fraud Claims and CISO Liability Remain," Greenberg Traurig, July 26, 2024, accessed October 31, 2024, https://www.gtlaw.com/en/insights/2024/7/sec-v-solarwinds-update-us-federal-district-court-dismisses-most-of-the-secs-case-but-some-fraud-claims-and-ciso-liability-remain.

[6] "SEC Charges Four Companies With Misleading Cyber Disclosures," U.S. Securities and Exchange Commission, October 22, 2024, accessed November 6, 2024, https://www.sec.gov/newsroom/press-releases/2024-174.

Conclusion

As FIs, insurers, and other FS firms prepare for 2025, CISOs and cyber risk leaders will use available budget to mitigate top cyber risks and enable secure business growth. FS peer priorities represent an important perspective. Security vendors in the market have attractive opportunities in the new year if they can solve critical challenges for FS firms. Datos Insights makes these recommendations:

CISOs serving FIs, insurers, and other FS firms:

- **Learn the business:** CISOs are increasingly called to help the customer-facing side of the business. Invest in business partners, learn the business acumen, and work to convey traditional cyber strengths into terms that business leaders can understand. Your efforts will be worth it.
- **Seek cloud security and data security solutions designed for multicloud deployments and improved operational maturity:** Tools that simplify operational complexity for multicloud environments also help enable greater cyber resilience. Focus on robust data security as the centerpiece for improved multicloud security.
- **Invest in the selection and deployment of cyber GRC tools for the board:** Find your role in the vertical journey in how the board and C-suite better manage the business of cyber risk at the top of the organization. Products exist to automate traditionally manual GRC tasks and deliver the most needed risk insights to executives and board members.
- **Partner to fund passkeys for the workforce and opt-in capability for consumers:** Criminals continue to attack the weakest link—the user. Phishing is pervasive and effective against consumers and workforce users. It is the attack vector enabling your top cyber risks. Adversarial AI is worsening the problem. Standards-based passkey solutions are widely available in the market. Find a way to fund them.
- **Elevate CIAM business value in partnership with authentication and financial crime leadership:** Modern customer identity solutions are well-positioned to serve teams responsible for customer authentication and fraud prevention. Designed correctly, robust CIAM solutions can strengthen identity proofing, enable 360-degree risk views of consumers, and improve fraud detection rates. Upgrade your CIAM platform to integrate real-time threat intelligence and bot management risk signals.

- **Continue to invest in robust API Security:** The CFPB's final ruling on Dodd-Frank 1033 on October 22, 2024, will usher open banking into its next season for FIs. Expect renewed urgency from the business.
- **Find seasoned cyber-domain talent:** Solutions for some of the top risks require senior talent, which may not be held by the organization. Find seasoned cyber and identity talent outside your firm as needed.

Market security vendors and CSPs:

- **Focus on delivering improved security assurance and cyber resilience for multicloud enterprise cases:** For many security domains, solutions that effectively defend enterprises operating in hybrid multicloud deployments are highly valued by FS firms.
- **Show the practical value of AI within your products or service:** Conceptual AI platitudes mean little at this point. AI should enable your product to deliver operational efficiencies, enhance customer visibility, automate manual customer tasks, and improve cyber resilience. Demonstrate the practical operational value AI provides your customer.

About Datos Insights

Datos Insights is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

Contact

Research, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779
Boston, MA 02109

www.datos-insights.com

Author information

John Horn

jhorn@datos-insights.com