WHITE PAPER

The Future of Secure, Mission-Driven Collaboration

Mattermost
MISSION IN MOTION

Executive Summary

Secure collaboration is no longer optional; it is operational. Across sectors like defense, healthcare, energy, and finance, the ability to connect people, tools, and data across boundaries has become central to mission success. Yet as collaboration increases, so does the risk. Every connection point becomes both a conduit for progress and a target for adversaries. This leaves security leaders with the unprecedented task of moving faster *and* enforcing trust at scale.

This white paper explores how system security, when designed into collaboration from the start, becomes a strategic enabler rather than a constraint. From real-world case studies to emerging technologies, the paper outlines both the threats and the opportunities facing CISOs today when leading the introduction of new collaboration systems.

The key insight? The most resilient organizations are not those with the strictest policies; they are the ones that architect collaboration systems *purpose-built* to be secure. That means context-aware controls, adaptive governance, data protection without friction, and platforms that scale with Zero Trust access requirements. As cyber threats evolve and the demand for cross-boundary work intensifies, CISOs must stop defending the perimeter and start owning the mission. Secure collaboration has evolved from a feature to a foundational capability. The future belongs to those who treat it that way.

Key Findings

- **Modern CISOs are strategic enablers.** Today's security leaders must go beyond just managing controls. They must influence platform architecture, drive cross-functional coordination, and shape digital transformation.
- **Mission-first collaboration is security-sensitive by nature.** Whether in emergency response, public health, or classified intelligence, collaboration across systems and sectors introduces risk that cannot be ignored.
- **Secure-by-design collaboration frameworks help organizations move faster.** When users trust the tools, and when controls are embedded rather than imposed, collaboration becomes safer, smarter, and more scalable.
- **Security and usability are not in conflict…if designed correctly.** Context-aware access, Zero Trust principles, and secure-by-design platforms allow for operational agility without compromising data integrity.
- **Restrictive policies often backfire.** Poorly designed security measures push users toward shadow IT, breaking trust and introducing greater risk. Effective governance requires enablement, not just enforcement.

- **New technologies are only valuable if they reduce friction.** New technologies are only valuable if they reduce friction. Tools like AI and techniques like confidential computing can transform secure collaboration, but only when they are deployed with usability and mission alignment in mind.
- **Organizations need a living framework, not a one-time fix.** Secure collaboration is a dynamic capability that requires phased implementation, measurable KPIs, and continuous adaptation to threats and business needs.
- **The window to lead is now.** As the digital and geopolitical landscape continues to evolve, security leaders have a rare opportunity to shape safe, seamless, and scalable collaboration.

Introduction: The Collaboration Imperative

Just as people cannot function without oxygen, mission-critical programs in defense, healthcare, finance, energy, and public safety cannot function without collaboration. Unfortunately, every byte of data shared across teams, departments, or agencies that creates a new opportunity for efficiency or innovation ***also*** represents a new opportunity for compromise. Security leaders are stuck between the proverbial rock and a hard place. On one side, they are asked to meet the demand to connect people, tools, and organizations faster than ever before. On the other, they are expected to unfailingly defend against a rising tide of adversaries, regulations, and data risk. These challenges are further increased by the explosive growth in fully remote and hybrid working environments. From 2019 to 2024, remote work more than tripled,[1] and recent survey data shows that both domestic and global workers strongly prefer working remotely (fully remote or hybrid).[2] While some teams may shut down collaborative initiatives entirely or go ahead without the appropriate guardrails, neither of those choices is a winning strategy.

Consider a basic example: An interagency task force working on an emergency response requires real-time situational data, shared access to classified resources, and the ability to include non-federal partners across disparate systems. Without secure, interoperable platforms, this kind of collaboration either fails to materialize or moves to shadow IT. In both cases, the mission suffers.[3] The same tension shows up in industry. The National Counterintelligence and Security Center (NCSC) has warned about increased threats targeting U.S. supply chains, particularly in sectors that rely on cross-border data flows and joint research and development (R&D).[4] Meanwhile, cybersecurity mandates like Executive Order 14028 are pushing federal agencies to adopt Zero Trust models, shifting from static perimeters to identity- and context-based access across environments.[5] This transition is overdue and not optional.

In the middle of it all stands the CISO. No longer just the chief of “no,” today’s security leader is pulled into product strategy, cross-sector partnerships, vendor ecosystems, and even geopolitics. The modern CISO must do more than secure assets; they have to ***enable trust at scale.***[6] The takeaway is that security cannot be a bolt-on. It must be engineered into collaboration from the start, so mission outcomes are not delayed, degraded, or derailed by preventable risks. Getting there is both a technical problem and a leadership challenge.

Understanding Mission-Driven Collaboration

Imagine a U.S. defense contractor is coordinating across internal IT, external vendors, a federal liaison, and a regional energy provider as part of an hours-long — or even days-long — live cyber response exercise. The mission objective is to prove the ability to secure operational continuity in the face of a simulated breach. The challenges in this situation are both technical and collaborative; tools do not talk to each other effectively, security postures, processes and standards vary, and nobody is confident that the third-party endpoint logging is even compliant. That is everyday life in the modern world, and it is not confined to exercises and training.

Mission-driven collaboration is a high-stakes convergence of roles, sectors, and technologies, all pointed toward a shared goal but fractured by inconsistent frameworks, cultural friction, and security gaps. It is not simply about working together, but rather aligning people, systems, and partners across organizational and jurisdictional boundaries in service of a shared strategic objective. This kind of collaboration is essential in national security, critical infrastructure, disaster response, and multi-agency governance, but it only works when the connective tissue is secure by design.[7]

Traditional internal collaboration between operations, compliance, and IT within a single agency carries its own set of risks. Most security professionals have dealt with at least one “open access” system that was never properly partitioned. Cross-functional collaboration tends to balloon access permissions in the name of productivity. Without Zero Trust enforcement or role-based access controls (RBAC), even minor misconfigurations can lead to data exposure.[8] When we start adding layers of private sector partners, international liaisons, or vendors embedded under other prime contractors, the risks multiply exponentially. The Government Accountability Office (GAO) has repeatedly flagged federal agencies for inconsistent supply chain risk management protocols, particularly when integrating with commercial partners across IT and OT environments.[9] While many agencies reference NIST SP 800-161 as guidance,[10] implementation often lags behind operations.

In industry consortiums – such as critical infrastructure coalitions or joint regulatory bodies – the security challenge is twofold: standardizing compliance expectations and then trusting each participant to maintain them. One weak link, such as a misconfigured API gateway or unpatched instance, can compromise shared intelligence. As a 2023 RAND study emphasized, “the weakest security posture in a federated data-sharing environment becomes the attack surface for all.”[11]

Even customer-facing platforms, such as those used in veteran services or benefits claims, introduce risk. These platforms often interface with legacy systems that carry personally identifiable information (PII), yet they require high accessibility to be valuable…and accessibility and security are strange bedfellows with competing objectives. In 2022, CISA reported that nearly 70% of data exfiltration attacks in the public sector leveraged user account compromise through poorly secured collaborative tools.[12]

All of the above demonstrates how mission-driven collaboration is not just inherently risky, it is also contextually risky because the risk profile can shift depending on who is involved, what is being shared, and how identity, access, and auditability are enforced. Internal teams need adaptive policy enforcement. Multi-agency efforts need standardized controls and shared trust anchors. And public-private coalitions need contractual security obligations baked into the service-level agreements (SLAs).

While collaboration is no longer optional for mission outcomes, ungoverned collaboration is a liability. Security leaders must implement standards and controls that recognize these distinctions if they intend to protect assets and ensure that missions do not fail because partners can not safely and securely work together.

The Security Leader’s Dilemma

For decades, the default mode of security was containment: Build the perimeter, monitor the traffic, and block what does not belong. In the age of internal networks and predictable workflows, that model made sense. But collaboration does not live inside those walls anymore…and neither does risk. Modern mission environments demand speed, flexibility, and external reach. Yet many security frameworks still treat connectivity as the exception instead of the norm. Tools are locked behind VPNs, access requests get routed through multi-week approval chains, and even basic file sharing across agencies can become a bureaucratic minefield. What was once considered “secure” is now simply restrictive, often not taking actual risks and mitigations into consideration.

This tension is evident in the all-too-common friction between security teams and operational leaders. When program managers push for faster onboarding, real-time communications, or joint workspaces with non-traditional partners, CISOs are forced into an impossible position of either saying “yes” and risking exposure or saying “no” and stalling the mission. Too often, they are punished for choosing either. Collaboration is either slowed to a crawl or it goes rogue.

That divergence creates measurable business impact. A 2025 report highlighted how unauthorized applications — known as "shadow IT" — often do not adhere to an organization's access control policies, potentially leading to security vulnerabilities.[13] In some sectors, high-friction access policies have prompted teams to migrate sensitive conversations to unapproved tools, creating the exact shadow IT risks security teams are trying to prevent.[14] And, to understand how well-meaning security measures can inadvertently fragment mission-critical collaboration, we need only review two recent examples from opposite ends of the federal mission spectrum.

- At the **National Oceanic and Atmospheric Administration (NOAA)**, policies introduced in early 2025 aimed to strengthen information security by tightening oversight of scientists' communications with foreign nationals. But the added administrative burden inadvertently disrupted NOAA's ability to collaborate on climate forecasting models with global research partners. The result: delayed integration of international data and diminished forecast reliability, all in the name of "safeguarding" information.[15]
- At the **Cybersecurity and Infrastructure Security Agency (CISA)**, leadership turnover triggered a clampdown on interagency communication. High-level approvals became mandatory for routine outreach, even to long-standing federal partners. These controls, though intended to reinforce trust boundaries, stalled joint initiatives around AI and open-source software security — domains that thrive on speed and shared context.[16]

The security leader's dilemma is not theoretical; it is operational. And if it is not addressed, it becomes existential. While security cannot afford to be a blocker, it ***also*** cannot afford to be bypassed. This means that the only path forward is one that reframes security not as a gate, but as a built-in enabler of trust across every layer of collaboration.

Emerging Technologies Enabling Secure Collaboration

There is no shortage of tools promising secure collaboration, but the reality is more complicated. For most security leaders, the issue is not whether new technology exists, but whether that technology can reduce risk without introducing more complexity and operational burden. Teams want to move faster while CISOs want (and need) control. Bridging the gap between those two priorities takes more than access controls. It needs scalable and secure architecture.

Zero Trust Architectures for Dynamic Collaboration Environments

Modern collaboration does not stay still. Users jump between devices, networks, roles, and even organizations, often in the same project. That is where Zero Trust earns its place. Instead of assuming anything inside a perimeter can be trusted, Zero Trust treats every access request like it is coming from a stranger. It validates not just who you are, but where you are, what you are using, and whether that behavior makes sense in context. This shift from wall-building to dynamic verification gives security teams real leverage without slowing down the mission.[17]

Confidential Computing and Secure Multi-Party Computation

Data sharing used to be a binary choice: Expose it or do not. But confidential computing changed that by allowing teams to collaborate on sensitive data sets without ever seeing each other's raw input. That means an intelligence agency, a contractor, and a healthcare provider could all contribute to a joint model without breaching internal policies or regulatory boundaries. Secure multi-party computation takes it even further, letting groups compute shared results without revealing their individual data at all. These technical and philosophical shifts mean that privacy and partnership no longer must be in conflict.[18,19]

AI-Powered Security Monitoring and Anomaly Detection

What makes collaboration secure is not just who gets in; it is what happens once they are inside… and that is where AI shines. While traditional monitoring tools drown in data, AI systems learn what "normal" looks like across users, systems, and behaviors, then flag the things that break that pattern. The anomaly might be as subtle as an unusual login time, a slightly different data flow, or a permission change that does not quite fit the profile. But catching it early is the difference between a minor incident and a serious data breach. In fast-moving environments, AI does not just make security better…it can be the only thing that makes security possible.[20]

The Risk of Overreliance on Artificial Intelligence (AI)

AI brings speed, pattern-matching, and scale, but it does not bring judgment...and that is the problem. When applied without constraint, AI systems have a known tendency to "hallucinate;" producing outputs that are syntactically convincing yet factually incorrect. This is not just a bug in chatbots. In security contexts, hallucinations can mislabel risks, flag false positives, or fail to identify real threats under the illusion of confidence.[21]

SecurityWeek recently reported on slopsquatting, a technique where adversaries exploit AI-generated package recommendations by inserting malicious lookalikes into software supply chains.[22] Meanwhile, the UK's National Cyber Security Centre has cautioned that hallucinations can render AI-generated outputs "unverifiable or unsafe without extensive oversight."[23] In short: If the algorithm is wrong, the system still acts unless a human stops it.

This is why the most responsible security leaders adopt AI as a force multiplier; not a decision-maker. They require auditability, cross-checks, and human-in-the-loop governance to verify what AI suggests. Anything less is delegation without accountability. AI can reduce workloads, but overreliance on it creates new blind spots that adversaries will eagerly exploit.

Secure-by-Design Collaboration Platforms and Tools

None of the above capabilities matter if the tools themselves are not built to withstand scrutiny. Secure-by-design is not just a tagline; it is a mandate. From initial code commits to post-deployment

updates, systems must be developed with a mature secure software design lifecycle, that incorporates threat modeling, secure defaults, and effective patching strategies. That reduces exploitable surfaces while also building confidence. When teams know their platforms were designed to resist compromise, they're more willing to use them the way they were meant to be used.[24]

Although these technologies will not eliminate the tension between access and assurance, strategies that use some (if not all) of these components in concert can start to resolve that tension by building systems that are flexible enough to be safe without needing to be so locked down that they are an impediment to mission success.

Building a Secure Collaboration Framework

Most security leaders have come to accept that you do not bolt collaboration onto a security stack; you design for both from the beginning. That starts with a framework flexible enough to adapt to real-world constraints, yet hardened enough to enforce trust boundaries across teams, systems, and organizations.

Risk-Based Classification of Collaboration

Not all collaboration carries the same weight. A real-time chat between two project leads is not the same as a cross-agency exchange of sensitive case data. That is why any functional framework starts with classifying collaboration by risk based on who is involved, what is being shared, and what the likelihood and potential impact if something went wrong. Systems should be able to classify scenarios as low, moderate, or high risk and trigger different policies accordingly.[25] Without that tiering, every control becomes a blunt instrument, and security overkill can cause nearly as much harm to mission success as underestimating security requirements.

Adaptive, Context-Based Security Controls

The rules cannot be static anymore. A user on a government laptop behind a firewall might be fine accessing shared files, but if that same account logs in at 2 a.m. from an unregistered device overseas, the system should raise flags, block access, or escalate to MFA without waiting on a human. Context-aware security is not just about geolocation or device posture; it is about combining signals to make smarter access decisions, dynamically.[26] You cannot scale Zero Trust without it.

Governance Models that Scale

Governance is already challenging when it's internal. But collaboration does not stay in-house. Projects now stretch across contractors, coalition partners, NGOs, and sometimes even adversarial jurisdictions. This demands a governance model that travels – defining ownership, auditability, and lifecycle management across org charts instead of just within them.[27] That means shared standards, portable controls, and enough transparency to earn trust without handing over your playbook.

Authentication and Authorization for Dynamic Environments

In dynamic environments where roles shift, teams are often forming and dissolving, and people wear multiple hats, meaning static role-based access can break down fast. That is why authentication and authorization need to be elastic, driven by real-time identity verification combined with traditional permission systems. Systems must support temporary access scopes, per-object policies, and fast revocation. If your access controls cannot keep up with your org chart, they are a liability.[28]

Data Protection Strategies for Utility *and* Security

It is not enough to simply lock the data down because that data must still be safely used. That means fine-grained encryption, dynamic watermarking, and content-aware data loss prevention (DLP) that does not break workflows…and enforcing policies without blocking progress. The best systems do not ask users to pick between security and utility. They engineer solutions so no one must choose.[29]

The real shape of a secure collaboration framework is flexible, contextual, and built to scale across domains without giving up control. The question is not whether that architecture is possible. It is whether you are running on a platform that supports it.

Case Studies: Security as a Collaboration Enabler

Security, when integrated effectively, serves as a catalyst for collaboration rather than a barrier. The following case studies illustrate how well-implemented security frameworks have enabled real-time collaboration across high-risk sectors.

Financial Services: Secure Data Sharing for Fraud Detection

In early 2025, a coalition of major UK financial institutions - including Barclays, HSBC, and Nationwide – launched a cross-sector data-sharing initiative alongside Google and Amazon to combat fraud in real time. The approach focused on exchanging fraud indicators such as malicious URLs and behavioral red flags within secure channels. By prioritizing encrypted, policy-governed data sharing, these organizations were able to identify threats faster than any single institution could alone. The pilot's success has already influenced broader regulatory conversations about proactive collaboration models.[30]

Healthcare: Protected Information Exchange for Improved Patient Outcomes

A federally supported study on Health Information Exchange (HIE) use in emergency departments revealed a measurable drop in redundant testing and medical errors when clinicians had real-time access to a patient's secure medical history. Hospitals that integrated HIEs into frontline care – while complying with HIPAA and regional privacy mandates – saw faster diagnostics, shorter stays, and fewer adverse events.[31] The security controls were not just safeguards. They were the reason such critical sharing was even possible.

Defense/Government: Classified Collaboration Across Agencies

Within the U.S. Intelligence Community, secure interagency collaboration was formalized through the launch of A-Space, a classified platform designed to allow analysts from multiple agencies to pool findings and challenge assumptions.[32] Instead of relying on email chains or stovepiped reports, users could post, refine, and vet sensitive intelligence inside a hardened digital workspace. The architecture prioritized compartmentalization and cross-clearance controls, demonstrating how the right security posture can unlock faster, more collective insight in the most sensitive environments.

Manufacturing: Secure Supply Chain Collaboration for Innovation

Ford Motor Company's partnership with Redwood Materials illustrates how comprehensive data protection can drive sustainable innovation.[33] As part of a closed-loop supply chain for EV battery recycling, the companies designed encrypted collaboration workflows to exchange proprietary design data and material traceability records without risking exposure. Secure integration allowed them to align logistics, inventory, and compliance systems while preserving trade secrets that resulted in forward-leaning environmental gains without sacrificing IP or competitive advantage.

These examples are not edge cases. They are proof that when security is integrated into the foundation of collaboration — rather than added as an obstacle after the fact — it becomes the reason missions move faster instead of the friction that slows down operations.

The CISO's Roadmap to Secure Mission-Driven Collaboration

Security leaders cannot afford to be reactive when it comes to collaboration. The complexity of modern missions — and the diversity of tools used to support them — requires a framework that is strategic, iterative, and grounded in measurable outcomes. Here is what that roadmap looks like.

Assessment: Evaluating Current Collaboration Capabilities and Security Gaps

Before building anything new, CISOs need visibility into what already exists. That means assessing current collaboration systems, data flow dependencies, and integration points between internal teams and external partners. The Department of Homeland Security (DHS) recommends starting with a maturity model analysis to pinpoint where shadow IT, insecure APIs, or ad hoc permissions are undermining existing posture.[34] The goal is not just to identify risks, but to also surface where collaboration breaks down specifically because security hasn't been built in.

Strategy: Aligning Security Investments with Mission-Critical Collaboration Needs

Security budgets do not expand without justification. Tying investment decisions to specific mission outcomes, including faster response times, reduced duplication, and improved data trustworthiness, helps CISOs move from a defensive stance to a strategic one. NIST emphasizes prioritizing controls based on operational impact and data classification.[35] The goal is alignment, so secure collaboration serves mission needs while simultaneously protecting mission integrity.

Implementation: Phased Approach to Building Secure Collaboration Capabilities

Trying to retrofit secure collaboration across an entire enterprise at once is a recipe for failure. Start with high-risk, high-value environments where collaboration is most essential and current tools are underperforming. Pilot deployments allow CISOs to pressure-test controls, refine governance models, and build stakeholder buy-in incrementally. CISA recommends phased integration of Zero Trust principles across identity, device, and data layers precisely because rushing it guarantees failure.[36]

Measurement: KPIs for Successful Secure Collaboration Initiatives

Every CISO knows that you cannot prove success without metrics, which is why it is imperative to track key performance indicators (KPIs) that reflect both security and usability, including number of collaboration-related incidents, time to detect anomalies in shared environments, and user-reported friction with security protocols. Metrics like mean time to resolution (MTTR) and policy exception requests also help spotlight where tools are helping (or hindering) collaboration.[37]

Continuous Improvement: Adapting to Evolving Threats and Business Needs

The roadmap does not end with deployment. Teams, missions, technologies, and threats all evolve. That is why secure collaboration frameworks must include mechanisms for regular red-teaming, policy review, and feedback loops from users. The Office of Management and Budget (OMB) guidance under Executive Order 14028 calls for agencies to adopt a posture of “continuous diagnostics and mitigation,” not static checklists.[38] The objective is to build for change, not just control. Secure, mission-aligned collaboration does not require more tools. It demands better orchestration and a roadmap that makes trust both intentional and actionable.

Outlook

Over the next three to five years, secure collaboration will evolve from a defensive posture to a proactive business enabler. The shift will be driven by converging forces: the explosion of distributed work, growing regulatory complexity, and adversaries that increasingly operate more like tech companies than criminal enterprises. What is coming is not just a new generation of tools…it is a new definition of trust.

Integrated collaboration platforms will begin to consolidate. Rather than stitching together messaging, file-sharing, project management, and compliance tools across multiple vendors, security leaders will increasingly favor unified environments where access, context, and auditability are managed centrally. This trend reflects predictions from cybersecurity analysts forecasting the "platformization" of secure workspaces where modular controls sit on top of extensible, self-hostable cores.[39]

Simultaneously, threat actors will continue to adapt faster. The Cloud Security Alliance anticipates a rise in AI-assisted attacks that target behavioral patterns in collaborative systems, including spoofing identities, crafting context-aware phishing campaigns, and exploiting inter-system trust paths.[40] These attacks will not just steal data, they will erode confidence in shared environments. And once trust is lost, collaboration stalls.

Meanwhile, the expectations placed on CISOs will continue to change as they are increasingly pulled into strategy, transformation, and board-level planning. Deloitte's 2025 cyber executive survey found that 71% of organizations already expect CISOs to act as "change agents," influencing product design, vendor ecosystems, and even organizational culture.[41] In other words, the CISO is not just securing collaboration; they are expected to facilitate it.

Evolution never comes easily. Secure collaboration demands both architecture and governance, including clear rules, active monitoring, and the political capital to drive behavioral changes across departments. The organizations that thrive in this next phase will be those that stop asking how to ***control*** collaboration and start asking how to ***earn trust at scale*** as the foundation for adopting better collaboration.

Conclusion and Recommendations

Collaboration has never been more essential or more complex. As the pace of digital transformation accelerates, security leaders are being asked to simultaneously protect data and enable trust across distributed teams, interdependent systems, and adversarial threat environments. That shift demands more than updated policies. It demands a mindset change.

Security does not have to constrain collaboration…it can power it. But only if it is built-in from the beginning. When security controls are designed to be context-aware, risk-aligned, and user-informed, they stop feeling like guardrails and start operating like infrastructure. For CISOs and security strategists, there are three imperatives to meet that new standard:

1. **Act immediately on visibility.** You cannot secure what you cannot see. Mapping collaboration systems, users, and data flows – across both sanctioned and shadow platforms – must be the first move.

2. **Operationalize secure-by-design principles.** The fastest path to trust is embedding security at the architecture level, not trying to enforce it after the fact. Invest in platforms that prioritize transparency, modularity, and control.

3. **Measure what matters**. Security performance is no longer only about how many attacks were blocked; it is also about how effectively teams can collaborate while staying compliant and secure. Track friction, exceptions, and trust.

Organizations that will lead the way are those that treat secure collaboration not as a tech feature, but as a **mission function** they resource like a core capability. It means elevating the CISO into product and policy conversations and shifting from a culture of restriction to one of **resilient enablement** where users do not just work securely, **they work better *because* they are secure**.

The threat landscape is not going to calm down. Regulatory complexity is not going to ease up. So, the demand for faster, broader, smarter collaboration is not going anywhere. For security leaders willing to rethink the playbook, this moment represents an opportunity to not just secure the enterprise, but to strengthen the mission.

About Mattermost

Mattermost is a secure collaboration platform purpose-built for organizations that need to maintain control over sensitive and confidential data in complex, high-stakes environments. Mattermost ensures focused, adaptable, secure and resilient collaboration, keeping your teams connected when the mission is on the line. Learn more about Mattermost at https://mattermost.com/

Endnotes

[1] National Cyber Security Centre. AI and cyber security: what you need to know. Accessed May 7, 2025. Socioeconomic Inequalities Between Remote Workers and Commuters

[2] Federal Reserve Bank of Atlanta. Survey of Business Uncertainty. Accessed May 7, 2025. https://www.atlantafed.org/-/media/documents/datafiles/research/surveys/business-uncertainty/monthly-report/2025/2025-04.pdf

[3] VCU Wilder School of Government and Public Affairs. The Importance of Interagency Collaboration in National Security. Published April 27, 2023. Accessed April 3, 2025. https://onlinewilder.vcu.edu/blog/importance-of-interagency-collaboration-in-national-security/

[4] National Counterintelligence and Security Center. Supply Chain Risk Management - The Recipe for Resilience. Published April 2023. Accessed April 3, 2025. https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats

[5] Executive Office of the President. Executive Order 14028 on Improving the Nation's Cybersecurity. Published May 12, 2021. Accessed April 3, 2025. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[6] IBM. The evolution of a CISO: How the role has changed. Published 2024. Accessed April 3, 2025. https://www.ibm.com/think/insights/ciso-role-evolution

[7] National Institute of Standards and Technology. NIST's Collaborative Approach to Cybersecurity and Cultivating Trust. Available at: https://www.nist.gov/speech-testimony/nists-collaborative-approach-cybersecurity-and-cultivating-trust

[8] National Institute of Standards and Technology. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. NIST SP 800-37 Rev. 2. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

[9] Government Accountability Office. Federal Agencies Need to Strengthen Supply Chain Risk Management Practices. GAO-23-105534. Available at: https://www.gao.gov/products/gao-23-105534

[10] National Institute of Standards and Technology. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST SP 800-161 Rev. 1. Available at: https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

[11] RAND Corporation. Insuring Catastrophic Cyber Risk: Challenges and Opportunities. Available at: https://www.rand.org/pubs/working_papers/WRA3817-1.html

[12] Cybersecurity and Infrastructure Security Agency. Collaboration Security: Managing the Risks of Modern Platforms. Available at: https://www.cisa.gov/news-events/news/collaboration-tools-security-guide

[13] CIO Influence. What is Shadow IT and why does it matter for enterprise security? Published March 2025. Accessed April 3, 2025. https://cioinfluence.com/security/what-is-shadow-it-and-why-does-it-matter-for-enterprise-security/

[14] Omega Systems. Shadow IT: Risks & Examples. Published June 2024. Accessed April 3, 2025. https://omegasystemscorp.com/insights/blog/what-is-shadow-it-examples-risks-explained/

[15] The Guardian. NOAA imposes limits on scientists, sparking concerns over global forecasts. Published February 12, 2025. Accessed April 3, 2025. https://www.theguardian.com/us-news/2025/feb/12/noaa-restrictions-climate-science-forecasts

[16] Wired. 'People Are Scared': Inside CISA as It Reels From Trump's Purge. Published March 13, 2025. Accessed April 3, 2025. https://www.wired.com/story/inside-cisa-under-trump/

[17] NIST. Zero Trust Architecture. NIST Special Publication 800-207. Published August 2020. Accessed April 3, 2025. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[18] Microsoft. Confidential computing: Scenarios and use cases. Updated January 2025. Accessed April 3, 2025. https://learn.microsoft.com/en-us/azure/confidential-computing/use-cases-scenarios

[19] Confidential Computing Consortium. Industry adoption report 2024. Accessed April 3, 2025. https://confidentialcomputing.io/resources/industry-adoption-report-2024

[20] CrowdStrike. AI-powered threat detection and anomaly response. Accessed April 3, 2025. https://www.crowdstrike.com/cybersecurity-101/next-gen-siem/anomaly-detection

[21] National Cyber Security Centre. AI and cyber security: what you need to know. https://www.ncsc.gov.uk/guidance/ai-and-cyber-security-what-you-need-to-know.

[22] Arghire I. AI hallucinations create a new software supply chain threat. SecurityWeek. https://www.securityweek.com/ai-hallucinations-create-a-new-software-supply-chain-threat/.

[23] National Cyber Security Centre. AI and cyber security: what you need to know. https://www.ncsc.gov.uk/guidance/ai-and-cyber-security-what-you-need-to-know.

[24] Cybersecurity and Infrastructure Security Agency (CISA). Secure by Design. Published April 2023. Accessed April 3, 2025. https://www.cisa.gov/resources-tools/resources/secure-by-design

[25] Stanford University. Risk Classifications. Accessed April 3, 2025. https://uit.stanford.edu/guide/riskclassifications

[26] StrongDM. Context-Based Access Controls: Challenges, Importance & More. Published August 2024. Accessed April 3, 2025. https://www.strongdm.com/blog/context-based-access-controls

[27] Portland State University. Building a Collaborative Governance Framework. Published June 2020. Accessed April 3, 2025. https://www.pdx.edu/policy-consensus-center/policy-consensus-center/sites/g/files/znldhr3416/files/2020-06/1-Building-a-Collaborative-Governance-Framework.pdf

[28] Portnox. What is a Dynamic Access Control List? Accessed April 3, 2025. https://www.portnox.com/cybersecurity-101/what-is-a-dynamic-access-control-list/

[29] SealPath. 5 Data Protection Use Cases Using Automation and Integration Between Security Technologies. Published January 2022. Accessed April 3, 2025. https://www.sealpath.com/blog/data-security-technologies-integration-automation/

[30] Parker G. Big tech firms and UK banks to share data to fight fraud. Financial Times. Published March 5, 2025. Accessed April 3, 2025. https://www.ft.com/content/12bbd99e-ed46-418d-bc15-04433e13db30

[31] Dixon BE, Grannis SJ, Revere D, Vest JR. Exploring utilization and outcomes of health information exchange in emergency departments. Agency for Healthcare Research and Quality. Final Report; 2020. Accessed April 3, 2025. https://digital.ahrq.gov/sites/default/files/docs/citation/r21hs025502-dixon-final-report-2020.pdf

[32] Office of the Director of National Intelligence. A-Space fact sheet. Published February 2011. Accessed April 3, 2025. https://www.dni.gov/files/documents/ODNI%20Fact%20Sheet_2011.pdf

[33] Ford Media Center. Ford and Redwood Materials create closed-loop battery recycling supply chain. Published September 22, 2021. Accessed April 3, 2025. https://media.ford.com/content/fordmedia/fna/us/en/news/2021/09/22/ford-redwood-materials-battery-recycling.html

[34] U.S. Department of Homeland Security. Cybersecurity Evaluation Tool (CSET) Maturity Model. Published 2023. Accessed April 3, 2025. https://www.us-cert.gov/resources/cset

[35] National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Published April 2018. Accessed April 3, 2025. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[36] Cybersecurity and Infrastructure Security Agency (CISA). Zero Trust Maturity Model, Version 2.0. Published April 2023. Accessed April 3, 2025. https://www.cisa.gov/sites/default/files/2023-04/cisa-zero-trust-maturity-model-2.0.pdf

[37] Government Accountability Office (GAO). Cybersecurity Metrics: Agencies Need to Improve Implementation of Performance Measures. GAO-22-105259. Published July 2022. Accessed April 3, 2025. https://www.gao.gov/assets/gao-22-105259.pdf

[38] Executive Office of the President. Executive Order 14028: Improving the Nation's Cybersecurity. Published May 12, 2021. Accessed April 3, 2025. https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[39] Palo Alto Networks. Cyber Predictions 2025. Published January 2025. Accessed April 3, 2025. https://www.paloaltonetworks.com/resources/research/cyber-predictions-2025

[40] Cloud Security Alliance. Emerging Cybersecurity Threats in 2025: What You Can Do to Stay Ahead. Published January 14, 2025. Accessed April 3, 2025. https://cloudsecurityalliance.org/blog/2025/01/14/the-emerging-cybersecurity-threats-in-2025

[41] Deloitte Insights. The CISO's Evolving Role in Strategic Business Leadership. Published February 2025. Accessed April 3, 2025. https://www2.deloitte.com/us/en/insights/topics/cybersecurity/ciso-evolving-strategic-leadership-2025.html