A Value-Driven Framework for OT Security in Corporate Spin-Offs

Rakesh Reddy Panati
IEEE Senior Member, USA

Abstract

Corporate spin-offs involving Operational Technology (OT) assets present complex challenges where cybersecurity must evolve from a supporting function into a foundational element of operational continuity. The Cyber Factory Model provides a structured framework to address the unique vulnerabilities of OT environments during corporate separations, where availability often outweighs confidentiality and integrity priorities. It integrates four strategic principles—prioritized risk reduction, integrated capability deployment, standardization for velocity, and operational independence by Day One—into a phased execution process encompassing site assessment, control prioritization, validation, and handover. Through systematic architectural scaffolding and embedded capabilities such as identity management rationalization, network segmentation redesign, asset visibility enhancement, and threat detection implementation, the model enables separated entities to establish secure, autonomous operations within Transitional Service Agreement (TSA) timelines. By embedding security into asset transfer activities rather than treating it as a parallel workstream, organizations can avoid inherited technical debt, reduce post-separation remediation costs, and build resilient foundations for future modernization. The framework redefines OT security—transforming what was once a separation barrier into a pathway for strategic value—positioning newly independent entities to sustain uninterrupted operations and defend against emerging industrial threats.

Keywords: Operational Technology Security, Corporate Spin-offs, Cyber Factory Model, Identity and Access Management, OT Threat Detection

1. Introduction

Corporate spin-offs involving Operational Technology (OT) assets create challenging scenarios where strategic opportunity often collides with cybersecurity vulnerability. Unlike traditional IT systems, industrial environments operate under fundamentally different priorities. The surge in global OT security investment reflects this growing tension, with market forecasts projecting an expansion to $34.9 billion by 2028—a clear indicator of the mounting pressure on organizations to safeguard critical infrastructure [1]. This growth is driven by converging factors: aging systems facing modern threats, increasingly stringent regulatory mandates, and adversaries employing more sophisticated methods to target industrial operations. What sets OT apart comes down to a simple equation: availability trumps everything else. Production lines can't afford downtime. Safety systems must function without interruption. A compromised controller or misconfigured network segment doesn't just mean lost data—it translates directly into halted operations, endangered personnel, and financial hemorrhaging measured in millions per hour. Recent findings paint a sobering picture, with industrial organizations reporting multiple cybersecurity incidents annually, many resulting in measurable production losses and safety concerns [2]. These are not abstract risks in threat reports; they are actual implications trickling down balance sheets and operational continuity plans.

The architecture of these systems often reflects decades of incremental evolution—proprietary protocols conceived in eras when security was an afterthought, control systems running on operating platforms that require extensive testing before any patch can be applied, and organizational structures that distribute responsibility across operations, engineering, and IT. These environments were designed for reliability and uptime, not for modern threat resilience, and their security foundations have typically been retrofitted over time rather than intentionally architected.

In corporate spin-offs, this legacy challenge intensifies. The newly formed SpinCo frequently inherits the entire OT ecosystem without the institutional knowledge, cybersecurity governance, or mature processes necessary to operate it independently. Unlike IT carve-outs—where security governance and enterprise controls are often well-defined and transferable—OT environments rely heavily on embedded practices and tribal expertise that rarely survive the separation. When compounded by aggressive Transitional Service Agreement (TSA) timelines—typically twelve to twenty-four months—the complexity multiplies. Security cannot be deferred; it demands immediate, coordinated action while production remains active and separation activities accelerate. For executives guiding these transitions, one question dominates: how can a secure and independent operational foundation be established without disrupting the very systems that must remain continuously available?

2. The Cyber Factory Model: Reframing OT Security in Divestitures

Most separation programs treat OT security as a workstream that runs alongside legal structuring, financial carve-outs, and operational transitions. This parallel approach, while administratively tidy, creates dangerous disconnects. Controls get implemented without understanding dependencies. Timelines slip because security requirements weren't factored into cutover planning. Gaps emerge at integration points where nobody took ownership. The cybersecurity M&A landscape has matured considerably, with transaction volumes reflecting an industry-wide recognition that security capabilities represent core business value rather than overhead to be minimized [3]. Yet despite this awareness, divestitures continue to stumble over the same fundamental error: treating security as something that happens to the business rather than something embedded within the business transformation itself.

The Cyber Factory Model challenges this conventional approach by positioning cybersecurity as intrinsic to asset transfer rather than adjacent to it. Rather than theoretical frameworks or best practices, the model

offers a structure built from actual separation programs—places where TSA deadlines collided with technical reality, where legacy architectures resisted clean separation, and where security teams learned what actually works under pressure. Carve-out transactions demand more than standard playbooks; they require establishing completely independent infrastructures while maintaining uninterrupted operations, necessitating comprehensive security architectures and continuous monitoring from the earliest planning stages [4]. The model coordinates three elements that typically operate in isolation: architectural scaffolding that defines "*what good looks like*", execution discipline that delivers changes without disruption, and separation planning that synchronizes security milestones with business transitions.

While factory-style delivery may appear unconventional for industrial environments dispersed across geographies, each with distinct equipment, processes, and constraints, this is precisely where the model demonstrates its effectiveness. Standardization does not negate local differences; rather, it identifies and codifies the patterns that can be consistently repeated amid variability. Every site requires rationalized identity management, segmentation architectures that reflect its unique threat model, and asset visibility extending beyond legacy documentation. By codifying these common elements—assessment frameworks, remediation playbooks, and validation criteria—security teams can achieve scalable delivery across multiple sites, transforming isolated efforts into repeatable, high-quality executions rather than approaching each location as a standalone project.

Traditional maturity models prescribe idealized end states: level five capabilities, comprehensive coverage, defense-in-depth everywhere. Separation timelines make such aspirations unrealistic. The model instead prioritizes practical uplift aligned with TSA constraints and real operational limitations. Controls get sequenced by risk reduction per unit of effort. Deployment focuses on what can be validated and sustained. Documentation captures what SpinCo actually has, not what aspirational frameworks suggest it should have. This pragmatism allows the separated entity to exit with capabilities genuinely fit for its inherited environments—controls that address immediate threats, architectures that support near-term operations, and foundations stable enough to support future modernization when TSA pressures subside and resources become available for optimization rather than survival.

Principle	Focus Area	Primary Objective
Prioritized Risk Reduction	Immediate threat neutralization	Address exploitable vulnerabilities and operational continuity risks before pursuing theoretical security improvements
Integrated Capability Deployment	Coordinated security implementation	Deploy identity, network, endpoint, and application controls as cohesive systems rather than isolated solutions
Standardization for Velocity	Repeatable delivery processes	Apply consistent assessment frameworks, remediation playbooks, and validation criteria across multiple sites
Operational Independence by Day One	Autonomous security operations	Enable separated entities to function securely without reliance on parent company infrastructure or expertise

Table 1: Core Principles of the Cyber Factory Model [3, 4]

3. Core Principles and Architectural Scaffolding

Four principles anchor the Cyber Factory Model, each derived from patterns observed across real-world separation programs rather than theoretical constructs. Prioritized Risk Reduction acknowledges a hard truth: achieving comprehensive security within separation timelines is unrealistic, and difficult choices must be made. Industrial environments remain inherently fragile—recent surveys highlight persistent weaknesses across manufacturing, energy, and critical infrastructure sectors, underscoring the need for ruthless prioritization over aspirational roadmaps [5]. This principle directs teams to focus first on controls that neutralize exploitable vulnerabilities before addressing theoretical improvements; on preventing production stoppages before chasing compliance milestones; and on remediating active attack paths before hardening infrequently used systems.

Integrated Capability Deployment recognizes that OT environments function as interconnected ecosystems, not isolated components. When security capabilities are deployed independently, well-intentioned efforts often conflict or create exploitable gaps:

- Deploying endpoint protection without aligned identity governance can result in authenticated malware.
- Implementing network segmentation while leaving remote access unrestricted gives adversaries an easy bypass route.
- Configuring firewalls without visibility into actual communication patterns leads to either overly permissive rules that nullify protection or restrictive ones that disrupt operations.

Recent industrial cyber campaigns underscore how attackers exploit these very seams—the blurred boundaries between security domains where ownership and accountability diverge [6]. The Cyber Factory Model addresses these interdependencies through coordinated deployment, integrating identity, network, endpoint, and application controls as a cohesive system rather than a set of competing initiatives.

Standardization for Velocity applies manufacturing thinking to security transformation. Sites become production lines. Assessments follow documented workflows. Remediation playbooks capture lessons from early implementations and propagate them forward. Evidence packages maintain consistent structures that simplify validation. This approach doesn't eliminate site-specific variations—unique equipment, legacy systems, operational constraints all demand accommodation—but it does prevent teams from reinventing solutions already proven at similar locations. Knowledge compounds. Velocity increases. Quality remains high because errors caught at one site inform procedures applied at subsequent locations.

Operational Independence by Day One defines the ultimate measure of success: can SpinCo operate securely and confidently without relying on ParentCo support?

Independence extends beyond technical functionality—it encompasses:

- Comprehensive visibility into assets
- Control over access and permissions
- The ability to detect and respond to threats
- The internal capability to sustain these functions over time

This principle drives key planning decisions:

- Which authentication dependencies can be safely decoupled or transitioned?
- What telemetry and monitoring data must be redirected to SpinCo-managed platforms?
- Where must specialized expertise be transferred or developed to maintain continuity?

The goal is not compliance on paper, but resilience in practice—achieving true operational autonomy from the moment separation becomes effective. Architectural scaffolding transforms these principles from aspirations into executable reality. Site-level blueprints establish baseline truth about each location: what

actually exists, how systems interconnect, where security controls currently operate, and what gaps demand attention. Without this foundation, teams work from assumptions that collide painfully with reality during implementation. Future-state architecture defines the target: not an idealized vision divorced from constraints, but a pragmatic design aligned with SpinCo's risk tolerance, operational model, and resource availability. This becomes the reference point that guides tactical decisions—when choosing between competing priorities, when evaluating vendor solutions, when sequencing implementation activities.

Control-to-architecture alignment prevents a common failure pattern in which well-intentioned security improvements, each effective in isolation, combine into an inconsistent whole filled with gaps and overlaps. Mapping proposed controls to the target architecture before implementation exposes misalignments early, when adjustments remain low-cost and minimally disruptive. Gap identification and remediation planning then address inherited risks systematically, rather than uncovering them reactively through incidents. Integration with conveyance activities keeps security initiatives synchronized with business timelines—controls reach production readiness precisely when sites need them. Standardization captures lessons learned into reusable artifacts that accelerate future deployments while maintaining the quality required for separation readiness and SpinCo autonomy.

Component	Purpose	Key Deliverables
Site-Level Blueprints	Baseline understanding establishment	Asset inventories, interdependency maps, security posture assessments, and technical debt catalogs
Future-State Architecture Definition	Target design specification	Risk-aligned designs, operational models, resource allocation plans, modernization roadmaps
Control-to-Architecture Alignment	Implementation validation	Control mapping matrices, gap analyses, overlap identification, and remediation priorities
Gap Identification and Remediation Planning	Inherited risk mitigation	Structured assessments, remediation plans, TSA-integrated timelines, resource requirements
TSA-Aware Migration Integration	Business synchronization	Cutover coordination, production continuity plans, milestone tracking, evidence packages
Standardization for Scale	Knowledge codification	Reusable artifacts, documented workflows, quality assurance procedures, and lessons learned repositories

Table 2: Architectural Scaffolding Components [5, 6]

4. Phased Execution Process and Key Capabilities

The Cyber Factory Model operationalizes OT security uplift through a phased execution process that mirrors how real separation programs unfold—structured enough to provide consistency, yet flexible enough to adjust to production constraints, TSA pressures, and local realities. These phases do not progress in perfect sequence; they overlap, accelerate, or pause based on site readiness, SME availability, and

manufacturing schedules. What distinguishes the model is not the existence of phases themselves, but the disciplined way they anchor decision-making, expose risks early, and synchronize remediation with separation milestones rather than running as parallel or disconnected security workstreams.

4.1 Site Intake and Readiness Mapping

Separation begins with establishing factual clarity about each site—what exists, how it operates, and where critical weaknesses reside. Intake is deliberately exhaustive because OT environments rarely reflect existing documentation. Aging SCADA systems running on Windows XP, vendor-maintained network bridges buried in switch closets, or critical applications maintained solely by a retiring engineer are common discoveries. These findings are not anomalies but predictable patterns inherent to industrial environments shaped by decades of incremental change.

Intake also exposes organizational constraints that materially influence sequencing: the maintenance window that only opens quarterly, the production schedule that forbids network changes for several months, or the line supervisor who becomes temporarily unavailable during peak season. The process benchmarks each site against foundational OT security practices—complete asset inventories, segmented networks, controlled access pathways, and continuous monitoring for actionable visibility [7]. The goal is not to produce a theoretical state diagram but to reveal the practical baseline from which the separation must proceed, and the specific gaps that must be closed before more advanced capabilities can succeed.

4.2 Control Baseline and Prioritization

Once baseline truth is established, the model shifts toward prioritization grounded in risk, TSA timing, and operational feasibility. Sites facing imminent separation deadlines naturally take precedence, but timing alone does not dictate priority. Controls addressing exploitable vulnerabilities—open remote access paths, shared privileged accounts, unmanaged devices bridging security zones—rise above enhancements that merely improve security posture without materially reducing separation risk.

This phase is intentionally pragmatic. OT environments cannot absorb sweeping change at once, and separation programs cannot wait for idealized maturity. Instead, the model sequences remediation in a way that minimizes operational disruption and maximizes uplift within TSA constraints. Activities enabling operational independence—identity boundary redefinition, telemetry redirection, and segmentation realignment—are prioritized ahead of optimizations that can be deferred without exposing SpinCo to immediate risk. This is where separation strategy and security architecture intersect: efforts align not to an abstract maturity model but to the real path SpinCo must travel to operate autonomously.

4.3 Integrated Control Validation

Unlike IT separation programs where controls can often be validated in domain-specific silos, OT environments demand cross-domain validation to prevent architectural seams from exposing new attack surfaces. The model validates identity separation, segmentation redesign, endpoint deployment, remote access restructuring, and threat detection capability as a coordinated whole.

This integrated validation prevents a common failure pattern: each domain doing the "right thing" individually, yet collectively producing a system with exploitable gaps. For example:

- identity separation without segmentation restructuring creates authenticated traversal paths
- segmentation without remote access redesign allows external actors to bypass boundaries
- endpoint protection without visibility into OT protocols produces blind detection zones

Integrated validation identifies these interactions early, when they can still be corrected without derailing TSA timelines or impacting production. It ensures that uplift is not merely implemented but *operationalized* in a way that supports the future-state architecture SpinCo will rely on post-separation.

4.4 Closure and Evidence for Day One

As separation nears, the emphasis shifts to proving effectiveness rather than continuing expansion. This phase compiles validated configurations, test results, exception logs, compensating controls, and remediation plans for deferred gaps.

The objective is to provide SpinCo with:

- A known and defensible security posture
- Transparency into residual risk
- Clarity on what must be addressed post-Day One

The rigor here protects both entities: ParentCo minimizes post-separation exposure, and SpinCo gains a documented foundation from which to continue its security journey. Security becomes part of the separation deliverable—not an afterthought addressed only when an audit or incident forces reconsideration.

4.5 SpinCo Handover

Handover formalizes the transition from uplift to ownership. It includes procedural documentation, knowledge transfer, operational readiness checks, and alignment with SpinCo's governance model. Crucially, this phase confirms that SpinCo can operate without dependency on ParentCo identities, networks, monitoring systems, or subject matter expertise. The goal is not functional completeness but sustainable autonomy—security capabilities that can be maintained without relying on assumptions embedded in the legacy environment.

4.6 Embedded Capabilities Across All Phases

The phases above are supported by core capabilities that enable consistency and scalability across diverse industrial sites.

1. **Active Directory Management** establishes identity autonomy—clean OU structures, validated group policy, and carefully designed trust relationships where temporary coexistence is unavoidable.
2. **Identity and Access Management Rationalization** modernizes legacy access practices. Shared accounts are removed, service accounts are governed, and privileges align to least privilege rather than historical accumulation—a critical safeguard given the expanding role of IAM failures in M&A-related cyber events [8].
3. **OT Security Architecture Assessment** provides structured baselines across assets, protocols, access paths, and controls, then maps findings to architectural patterns to expose deviations such as dual-homed systems, unmanaged assets, insecure remote access, and undocumented external connectivity.
4. **Control Framework Realization** emphasizes foundational, sustainable controls rather than exhaustive coverage. Gaps are assessed against industry benchmarks; POAMs guide deployment focused on what can be operationally sustained.
5. **Accelerated Application Security Review** inventories bespoke, undocumented OT applications, identifies critical dependencies, and prioritizes reviews for high-risk systems that could disrupt operations if compromised.
6. **PKI and Certificate Management** addresses overlooked certificate dependencies—renewing expiring certificates, replacing self-signed implementations, and establishing lifecycle processes to prevent authentication failures and communication outages.
7. **Asset Visibility and Continuous Monitoring** deploys OT-native tools that reveal unknown devices, undocumented communication patterns, and deviations from expected Bill of Materials.

8. **Firewall Policy Management and Segmentation** redesigns rulesets based on validated requirements, not accumulated legacy configurations, isolating critical zones and restructuring remote access.
9. **Threat Detection and Response** focuses on OT-specific detection logic, actionable visibility, and documented triage procedures rather than noise-heavy log forwarding that overwhelms operations without improving response capability.

4.7 Phase Summary

Phase	Activities	Outcomes
Site Intake & Readiness Mapping	Architecture assessment, risk posture evaluation, TSA context analysis, constraint documentation	Comprehensive baseline understanding, realistic planning parameters, and resource allocation frameworks
Control Baseline & Prioritization	Risk-based sequencing, separation dependency identification, and timeline alignment	Prioritized capability roadmaps, resource optimization, and milestone definitions
Integrated Control Validation	Identity separation, network segmentation, endpoint protection, remote access restructuring, application hardening, threat detection, and asset visibility	Coordinated security capabilities, validated implementations, and operational integration
Closure and Evidence for Day One	Control validation, documentation completion, exception logging, and audit preparation	Plans of Action and Milestones, evidence packages, and known residual risk profiles
SpinCo Handover	Site transition, capability transfer, knowledge documentation, operational readiness confirmation	Secure autonomous operations, validated security postures, independence enablement

Table 3: Phased Execution Process [7, 8]

5. Strategic Value and Implementation Considerations

Cybersecurity in spin-offs goes beyond a defensive function—it becomes part of the foundational infrastructure that enables operational autonomy. Organizations that integrate security into separation planning avoid inheriting technical debt that would cost several times more to remediate post-transaction, while setting a clear trajectory toward sustainable resilience. Effective cybersecurity during transactions extends beyond technical controls to include due diligence, integration planning, and post-transaction governance—all of which determine whether the new entity can operate securely and compliantly after the transition [9]. By front-loading critical capabilities into the separation timeline—before TSA constraints expire and coordination with ParentCo becomes difficult—organizations can leverage existing expertise

and implement architectural decisions collaboratively, rather than resorting to reactive fixes after independence.

Identity boundaries, network zoning, and control validation don't represent optional enhancements addressable after separation; they constitute prerequisites for secure autonomous operations maintaining production continuity while defending against contemporary threats.

Benefits manifest concretely:

- Avoided remediation costs, which are typically three to four times higher post-separation when performed under production constraints and without the original architectural context.
- Systematic gap closure achieved during transformation phases, when resources are already mobilized for change rather than diverted by incident-driven firefighting.
- TSA milestones met without sacrificing foundational protections or extending timelines.
- Operational autonomy that reduces reliance on ParentCo infrastructure, tooling, and expertise no longer available after separation.
- Future-ready architectures that enable Industrial Internet of Things integration, Zero Trust adoption, and cloud-driven modernization—advancements often hindered by inherited technical debt.

Transitioning from inherited complexity to operational clarity requires deliberate design rather than hoping coherence emerges organically. Technology considerations in carve-out scenarios demand strategic approaches coordinating infrastructure separation, application dependencies, data migration, and cybersecurity architecture, recognizing interdependencies where failures cascade across domains [10].

Strategic questions confront leadership as separation accelerates:

1. How should identity boundaries be designed so SpinCo gains operational autonomy while still managing the temporary trust dependencies required during TSA, and what level of reliance on shared IT services remains acceptable for OT continuity?
2. Which legacy risks must transfer to SpinCo due to operational necessity, and which can be retired during separation to avoid carrying forward known vulnerabilities?
3. How well are interdependencies across applications, devices, networks, and security tooling understood and mapped, and where do undocumented or cross-domain dependencies introduce cutover risk?
4. Where do TSA timelines require trade-offs between security objectives and separation milestones, and which of those compromises can realistically be addressed through post-separation investments?
5. What technical and architectural conditions must exist for SpinCo to operate securely without inherited assumptions about ParentCo networks, identities, monitoring, or control tooling?

Clarity in these areas early enables focused execution, allowing security to stabilize organizational change rather than introducing friction or delay. Spin-offs aren't merely about protecting inherited assets; they fundamentally shape what new entities become, establishing architectural foundations enabling or constraining future capabilities.

Embedding security into separation architecture through structured frameworks helps organizations move faster toward operational independence, reduce risk earlier when mitigation remains cost-effective, and operate with clarity from day one regarding security posture, residual risks, and maturity roadmaps. This approach provides a framework, discipline, and practical guidance, transforming OT security challenges in corporate spin-offs into strategic advantages, positioning new entities for sustained success within increasingly hostile threat landscapes where operational technology has become the primary targeting focus

for sophisticated adversaries seeking to disrupt critical infrastructure and manufacturing operations. Success requires commitment, coordination, and recognition that security investments during separation windows generate returns far exceeding costs through avoided incidents, accelerated independence, and foundations supporting future growth.

Capability Domain	Implementation Focus	Security Benefits
Active Directory Management	Purpose-built directory infrastructure, clean organizational structures, validated policies	Identity autonomy, reduced inherited complexity, controlled interdependencies
Identity & Access Management	Account rationalization, least privilege alignment, service account governance	Eliminated shared credentials, traceable access, and reduced privileged exposure
OT Security Architecture Assessment	Baseline documentation, architectural pattern mapping, and deviation identification	Targeted remediation, reduced design risk, validated segmentation
Control Framework Realization	Foundational control deployment, gap assessment, POAM development	Risk-appropriate protections, audit readiness, sustained governance
Application Security Review	Inventory creation, dependency mapping, and security evaluation	Protected critical systems, validated configurations, governed access
PKI and Certificate Management	Certificate inventory, renewal workflows, trust validation	Prevented outages, enabled authentication, supported device identity
Asset Visibility and Monitoring	OT-native tool deployment, network mapping, detection tuning	Comprehensive awareness, anomaly detection, and incident response enablement
Firewall Policy Management	Rule redesign, segmentation implementation, and remote access restructuring	Least privilege enforcement, zone isolation, reduced attack surface
Threat Detection and Response	OT-specific playbooks, endpoint protection, triage workflows	Early threat identification, coordinated response, operational continuity

Table 4: Key Embedded Capabilities [9, 10]

Conclusion

The Cyber Factory Model represents a fundamental shift in how organizations address OT security during corporate spin-offs. It moves security from a reactive function to an architectural component of the separation itself. By treating cybersecurity as part of asset transfer—rather than an isolated workstream—the model positions new entities to begin operations with validated controls, a defensible posture, and a foundation that can support future modernization.

Prioritized risk reduction directs limited time and resources toward the issues most likely to disrupt production or compromise safety, grounding decisions in operational realities instead of theoretical maturity targets. Integrated capability deployment resolves identity, network, endpoint, and application dependencies as a cohesive system, closing the seams adversaries often exploit. Standardization for velocity converts one-off remediations into repeatable patterns that accelerate execution across sites. Operational independence by Day One gives SpinCo the ability to function without residual reliance on ParentCo identities, networks, or monitoring infrastructure.

Through architectural scaffolding, phased execution tied to business milestones, and embedded capabilities spanning identity management, segmentation, asset visibility, application security, and threat detection, the model produces measurable outcomes: reduced remediation effort, timely TSA exits, clearer understanding of inherited risk, and architectures ready for modernization. Security becomes part of the separation engine—shaping how information flows, how access is governed, and how operational boundaries are defined.

By integrating cybersecurity into conveyance activities rather than layering it on afterward, the Cyber Factory Model turns traditional spin-off constraints into opportunities to build cleaner, more sustainable OT environments. It reframes security not as a compliance cost but as an enabler of operational clarity, faster decision-making, and resilient performance within a threat landscape that increasingly targets industrial systems.

References

[1] KBV Research, "Global Operational Technology (OT) Security Market Size, Share & Industry Trends Analysis Report By Offering, By Vertical (Manufacturing, Energy & Power, Oil & Gas, BFSI), By Deployment Mode, By Organization Size, By Regional Outlook and Forecast, 2022 - 2028," 2022. [Online]. Available: https://www.kbvresearch.com/operational-technology-security-market/

[2] Fortinet, "2023 State of Operational Technology and Cybersecurity Report". [Online]. Available: https://www.content.shi.com/cms-content/accelerator/media/pdfs/fortinet/fortinet-062724-2023-state-operational-technology-cybersecurity-report.pdf

[3] MNA Community, "Cybersecurity mergers and acquisitions: Key deals and trends," 2024. [Online]. Available: https://mnacommunity.com/insights/cybersecurity-mergers-and-acquisitions-deals/

[4] Michael Fossati, "Cyber Security: The Key to a Successful Carve-Out," InfoGuard AG, 2025. [Online]. Available: https://www.infoguard.ch/en/blog/cyber-security-key-to-successful-carve-outs

[5] Claroty, "The Global State Of Industrial Cybersecurity 2023". [Online]. Available: https://web-assets.claroty.com/claroty-industrial-survey-report-dec-2023.pdf

[6] Dragos, "2024 Timeline of Cyber Events". [Online]. Available: https://www.dragos.com/ot-cybersecurity-year-in-review

[7] Fortinet, "5 Best Practices For Operational Technology (OT) Security". [Online]. Available: https://www.fortinet.com/resources/cyberglossary/ot-security-best-practices

[8] Bank of America, "The pivotal role of cybersecurity in mergers and acquisitions". [Online]. Available: https://business.bofa.com/en-us/content/cybersecurity-in-merger-acquisitions.html

[9] Ernst & Young, "Cybersecurity Due Diligence in M&A and Divestitures". [Online]. Available: https://www.ey.com/en_in/services/strategy-transactions/cybersecurity-mergers-acquisitions-divestments

[10] AvenData, "Tech Savvy Strategies: Navigating IT Considerations in Carve-Out Planning and Execution," 2024. [Online]. Available: https://avendata.hashnode.dev/tech-savvy-strategies-navigating-it-considerations-in-carve-out-planning-and-execution-1