WHITEPAPER

Risk and Resilience: What the C-Suite Needs to Know About Industrial Cybersecurity

MARK STACEY | DIRECTOR OF STRATEGY
DRAGOS, INC
JUNE 2025

TABLE OF CONTENTS

Introduction

Operational technology (OT) security breaches do not merely threaten data—they jeopardize physical operations, human safety, and organizational survival. For C-suite executives, the stakes could not be higher: a single OT security incident can trigger cascading consequences across safety systems, environmental controls, market reputation, financial stability, and regulatory compliance.

While operational technology risk is widely acknowledged as a critical concern for industrial organizations, there remains a dangerous disconnect in how various stakeholders comprehend and assess this risk. This inconsistency is particularly problematic in the insurance sector, where underwriters struggle to accurately evaluate and price OT cyber risk due to its unique characteristics that differ fundamentally from traditional IT environments. Unlike IT security incidents that primarily affect data confidentiality and availability, OT breaches can halt production, damage physical assets, create environmental hazards, and even endanger human lives—making standardized risk assessment frameworks inadequate.

The multi-dimensional nature of OT threats—affecting safety, environment, reputation, finances, and regulatory compliance—further complicates uniform risk assessment, creating critical gaps in understanding between operations teams, security professionals, and executive decision-makers. This misalignment frequently leads to investment decisions that fail to address the most consequential risks to the organization. Simultaneously, the regulatory landscape for OT security continues to evolve rapidly, introducing new legal implications that many organizations are unprepared to address. This evolution runs parallel to troubling changes in insurance policies, where exclusions are becoming more complex and less transparent. Asset owners face mounting uncertainty regarding which factors insurers consider when evaluating and pricing their policies, leaving them without clear guidance on how to effectively manage enterprise risk in response to these exclusions.

This ambiguity fundamentally challenges organizations' ability to develop comprehensive risk management strategies that account for both operational resilience and financial protection following an OT security incident. Building true resilience requires a methodical approach: identifying key risk considerations, developing practical metrics for measuring security posture, and implementing effective processes for continuous improvement. When communicated transparently to boards and partners like insurers, this resilience journey demonstrates a strategic commitment to sustainable risk management. Regular progress updates showcase your dedication to systematically reducing risk, potentially leading to more favorable terms with external stakeholders.

For today's industrial C-suite, understanding this evolving risk landscape isn't merely a technical concern—it's a fundamental business imperative that requires executive attention and strategic investment to ensure organizational resilience in an increasingly hostile threat environment.

Identifying Risk in Industrial Environments

Traditional risk assessment methods often fail to capture the intricacies of modern industrial environments, particularly in OT settings where the convergence of digital and physical systems creates unique security challenges.

Threat scenarios provide invaluable context by simulating real-world attack vectors against critical infrastructure, offering a more comprehensive understanding of risk than conventional approaches. By methodically modeling how threat actors might target industrial control systems, organizations can contextualize risks within their specific operational environments, considering both the likelihood of sophisticated attacks and the potential severity of impacts that could cascade throughout the organization and its broader ecosystem.

This scenario-based approach creates a common language between technical security teams, operational staff, and executive leadership, bridging communication gaps that typically hinder comprehensive security programs in industrial settings.

Threat scenarios excel at pinpointing vulnerabilities within OT systems that might otherwise remain obscured by the complexity of industrial networks, legacy systems, and proprietary protocols. Through the systematic simulation of

potential attack vectors, organizations can identify previously overlooked weaknesses at the critical intersection of IT and OT networks, enabling security teams to prioritize mitigation efforts based on business impact and allocate limited security resources more effectively.

These scenarios are particularly powerful in environments where traditional IT security approaches often fall short, transforming abstract cybersecurity concepts into concrete, relatable situations that demonstrate the direct connection between digital threats and operational safety, reliability, and business continuity. By revealing how sophisticated adversaries might exploit vulnerabilities to impact physical processes, threat scenarios provide industrial organizations with actionable insights to strengthen their security posture against increasingly targeted attacks.

Three Common Threat Scenarios Across Industrial Sectors

Sophisticated threat actors are investing significant resources in developing OT-specific attack capabilities, raising the stakes for industrial cybersecurity. These threat scenarios depict an evolution in OT-targeted attacks, demonstrating:

- Deep knowledge of specific industrial systems and protocols
- Ability and willingness to manipulate safety-critical systems, not just operational systems, which could result in physical harm
- Long-term persistence capabilities
- Modular malware frameworks adaptable to different industrial environments

Scenario	Description	Impact
Ransomware	Ransomware attacks against industrial organizations have increased dramatically. Modern ransomware campaigns specifically target OT environments, understanding that operational downtime creates enormous pressure to pay. These attacks often: • Enter through IT networks and pivot to OT systems • Target backup systems to prevent recovery without payment • Exploit IT/OT trust boundaries to gain access to critical systems • Deploy specialized malware with knowledge of industrial protocols	Ransomware attacks can halt operations, leading to significant revenue loss and operational downtime. The cascading effects can impact safety, disrupt dependent processes, and impact supply chains.

Scenario	Description	Impact
Nation-State Actors and Industrial Espionage	State-sponsored threat actors target industrial organizations for various strategic objectives: • Gaining competitive advantages for domestic industries • Developing capabilities for potential wartime sabotage • Establishing persistent access for future operations • Collecting intelligence on critical infrastructure • Testing and refining cyber weapons against real industrial targets	Nation-state actors can cause significant operational disruptions, safety hazards, and financial losses by manipulating control systems and processes. These groups can also remain undetected for long periods of time, collecting intelligence and increasing access for future campaigns.
Trusted Vendor Compromise	In trusted vendor compromise attacks, malicious actors infiltrate a vendor's software, which is then distributed to end users, compromising their systems.	This can lead to widespread data breaches and operational disruptions across various industries, given the interconnected nature of trade, commerce, and supply chains

Qualifying Risk: Conducting a Risk Analysis

The consequences of OT security incidents extend far beyond immediate technical concerns, creating complex business challenges across multiple dimensions. Organizations should develop a structured approach to risk evaluation that:

- Incorporates both likelihood and impact assessments
- Considers various attack vectors and scenarios
- Accounts for cascading effects across interconnected systems
- Evaluates impacts across multiple business dimensions
- Provides a framework for comparing and prioritizing risks

Risk Category	Impact Analysis Should Consider
Financial	• Direct costs of downtime and lost production • Recovery and remediation expenses • Potential regulatory fines and legal liabilities • Investment required to prevent recurrence • Long-term market impacts and customer confidence effects
Safety and Environmental	• Potential for personnel injury or loss of life • Environmental contamination or damage • Community health and safety concerns • Regulatory violations and associated penalties • Long-term environmental remediation costs

Risk Category	Impact Analysis Should Consider
Business Continuity	• Time to restore critical operations • Availability of manual overrides and backup procedures • Dependencies on external vendors for recovery • Communication challenges during incidents • Workforce impacts and operational constraints
Reputation Management	• Customer and partner confidence in reliability • Public perception of safety and environmental stewardship • Investor confidence and market valuation effects • Regulatory trust and relationship impacts • Industry reputation and leadership position
Ecosystem Impact	• Potential impacts on national security and defense capabilities • Supply chain disruptions affecting customers and partners • Potential product shortages in critical sectors • Price volatility in affected markets • Cascading failures across interdependent infrastructure • Coordination requirements with government agencies • Potential for escalated regulatory oversight

Qualifying Risk: Creating an Effective OT Cybersecurity Risk Register

An effective OT cyber risk register serves as the cornerstone of industrial cybersecurity governance, integrating several critical components into a unified management framework. At its foundation lies a comprehensive asset inventory that maps operational technology components according to the Purdue Enterprise Reference Architecture, identifying "crown jewel" assets that warrant enhanced protection. Beyond simple documentation, the register must incorporate OT-specific threat tracking mechanisms that prioritize availability and integrity concerns over traditional IT confidentiality priorities.

Key Components of an OT Cybersecurity Risk Register

Component	Description	Importance
Asset Inventory	Catalog of OT and IoT components, devices, and systems	Foundation for monitoring and assessing risk
Threat Scenarios	Analysis of potential attack vectors	Guides mitigation strategies
Risk-Based Vulnerability Management Program	Tracking and prioritization of vulnerabilities and compensating controls	Addresses unique OT patching challenges and provides context for decision making
Risk Scoring	Quantitative assessment based on business impact	Prioritizes mitigation efforts
Compliance Mapping	Links controls to relevant regulatory frameworks	Creates defensible audit trail

Maintaining an effective OT risk register requires systematic processes including regular review cycles—typically quarterly for high-risk systems—involving cross-functional teams of OT engineers, cybersecurity specialists, and business stakeholders. As environments grow more complex, organizations should leverage specialized tools that integrate with vulnerability scanners and threat intelligence platforms while maintaining clear governance structures with defined roles for risk management activities. When properly maintained, the register becomes a powerful tool for driving security investments by quantifying potential impacts in financial terms, transforming cybersecurity from a technical concern into a business risk management activity. This evidence-based approach builds credibility with executives, supporting continued funding while enabling comparative analysis of different mitigation strategies based on their effectiveness and implementation costs.

Beyond tactical decisions, the register should inform strategic security planning by identifying systemic issues requiring longer-term solutions, ensuring investments align with broader business objectives.

Once risk has been identified, qualified, and documented, the organization can evaluate available approaches to managing risk.

The Four Approaches to OT Risk Management

The ideal approach to any risk would be complete elimination, but this is rarely practical in OT environments. Different devices require different protection levels, not all vulnerabilities demand the same response, and not all risks need to be eradicated to maintain business continuity. Instead, organizations should demonstrate their understanding of risk by classifying their management approach into four distinct categories: elimination, transfer, acceptance, and mitigation.

Beyond tactical decisions, the register should inform strategic security planning by identifying systemic issues requiring longer-term solutions, ensuring investments align with broader business objectives. Once risk has been identified, qualified, and documented, the organization can evaluate available approaches to managing risk.

Elimination: Engineering Out Risk

Elimination represents the most desirable approach to risk management—completely removing the risk through software, hardware, or engineering changes to the network. While this sounds ideal in theory, elimination carries significant challenges in OT environments:

- **Patching Limitations:** While patching is often referenced as an elimination approach, it's important to recognize that patches change code on devices and may not truly eliminate risk. They can sometimes introduce new risks or may not be available at all. According to the Dragos Year in Review report, 26% of OT advisories had no patch available. Additionally, network administrators must confirm patches are deployed successfully across the entire network to be effective.
- **Technology Replacement:** In theory, removing vulnerable technologies seems straightforward. However, OT environments rarely allow for simple component changes without significant operational impacts. Removing technology typically requires implementing an alternative, which introduces new considerations that must be evaluated.
- **Validation Requirements:** OT operators are typically apprehensive about changing existing functional architectures. Any elimination strategy requires validation of its effectiveness and persistence, which demands comprehensive visibility across the network and alert functions for potential reappearance of risks.

Because true elimination is rarely achievable in OT environments, organizations must develop mature strategies for handling residual risk, often involving external partners and alternative approaches.

Transfer: Strategic Risk Allocation

Risk transfer has become a fundamental component of mature security programs, particularly for high-consequence scenarios with limited mitigation options. Cybersecurity insurance represents the primary mechanism for transferring risk to external parties, but this approach comes with its own challenges:

- **Evolving Insurance Landscape:** The cyber insurance market continues to develop more sophisticated Cyber-Property coverage policies, adapting exclusions, and partnering with subject matter experts to qualify impact. This evolution reflects the growing recognition of OT-specific risks.
- **Assessment Challenges:** Insurers struggle to accurately assess industrial risk exposures due to the unique characteristics of OT environments. Simultaneously, customers are often unclear about what influences coverage and what limitations exist in their policies.
- **Questionnaire Limitations:** Standard IT-based assessment questionnaires frequently fail to capture OT-specific risk factors. Underwriters struggle to quantify the risks they're accepting based on standard insurability questionnaires, and the time required to understand environmental contingencies doesn't scale well across multiple industries.
- **Proactive Documentation:** Organizations with well-documented risk management programs typically secure better coverage terms than those relying on standard form responses. This highlights the importance of transparent communication with insurers about both OT constraints and implemented controls.

Effective risk transfer requires organizations to clearly communicate their risk management approach, including both the constraints of their OT environment and the controls they've implemented to address those risks.

Acceptance: Acknowledging Residual Risk

Risk acceptance represents a practical approach when the potential impact is understood and deemed manageable. Some organizations choose not to carry cybersecurity insurance, anticipating that network compromises will be managed internally, and total impact will remain limited enough to maintain business continuity.

However, accepting risk is not an absolute decision and carries substantial implications:

- **Legal Implications:** Risk acceptance carries significant legal and regulatory considerations. As government agencies increase reporting requirements related to cyber breaches and disclosures, companies face additional public scrutiny when they know about a risk but take no action.
- **Public Perception Challenges:** Post-incident disclosures that reveal known-but-unaddressed risks can create significant reputational damage. This messaging may not be acceptable to the public and could position the organization poorly for litigation.
- **Dynamic Reassessment:** Accepted risks require periodic review as threats, regulations, and operational requirements evolve. As internal and external changes occur, risks need to be revisited to ensure acceptance remains the most appropriate position.
- **Documentation Imperative:** Formal risk acceptance decisions must be thoroughly documented with business justification and executive approval. This documentation helps protect the organization should an incident involve the accepted risk, providing context around the decision and staging reevaluation.

For high-consequence risks that threaten safety or critical operations—such as those that could cause mass injury or equipment destruction—acceptance may not be a viable option regardless of probability. Detection capabilities remain essential even for accepted risks, as acceptance reflects informed decision-making rather than ignorance.

Mitigation: Reducing Impact and Likelihood

When risks cannot be eliminated, organizations must implement controls that reduce either the likelihood or potential impact of security incidents. Mitigation techniques involve changes to the network, either removing or adding technology:

- **Network Architecture Controls:** Segmentation and access controls limit attacker movement without eliminating underlying vulnerabilities. These controls may make it more difficult to traverse network segments while not eliminating the ability.
- **Detection Capabilities:** For 47% of OT advisories, Dragos provided alternative mitigations when patching wasn't viable. This highlights the importance of having multiple approaches to addressing vulnerabilities.
- **Defense-in-Depth:** Multiple overlapping controls provide resilience against individual control failures. Adding security controls can facilitate not only early detection but add defense-in-depth against threats.
- **Risk Interdependencies:** Mitigation in one area often reduces risk in connected systems due to shared dependencies. When deploying active mitigations, organizations should recognize that additional risk may also be introduced. Any active capability added to the network may carry reliance or exposure not previously identified.

Mitigation should be viewed not as risk elimination but as strategic risk reduction to acceptable levels. Mitigations represent a practical approach to managing risks that cannot be completely removed from the environment.

Practical Approaches to Building Resilience in OT Environments

Business Resiliency and Dependencies in OT Environments

Of the four approaches, only Elimination and Mitigation reduce risk. Transfer and Acceptance acknowledge risk but do not reduce it. They are influenced by elimination and mitigation efforts but do not offer reciprocity.

The interconnected nature of industrial networks means risk is shared across systems. When a risk is eliminated or mitigated in one area, residual risk is reduced throughout connected systems. A vulnerability in one segment may not be present in another, but if traffic is allowed between segments, a vulnerability in one adds risk to the other.

This shared risk between reliant systems means that reduction in one area reduces risk in others. Organizations should consider this when evaluating total risk across their operations. If effective mitigations are implemented, the cost to transfer risk through insurance and the liability in accepting residual risk should both decrease.

This interconnection highlights the importance of sharing context around the risk management program and advocating completed work with external partners involved in managing organizational risk. A comprehensive approach that leverages all four pillars—elimination, transfer, acceptance, and mitigation—provides the most effective framework for increasing resiliency, given the unique challenges of OT security.

Practical Mitigations: Your OT Cybersecurity Journey

A structured approach to OT cybersecurity maturity progresses through three key phases.

MITIGATION PHASE 1:	IMPLEMENTATION OF CRITICAL CONTROLS

The implementation phase focuses on establishing the foundational elements of an OT security program:

- Working with operations teams to understand OT environments
- Deploying basic security controls with minimal operational impact
- Collaborating with OT security experts to establish best practices
- Establishing baselines for normal operations
- Developing initial incident response capabilities

During this phase, organizations focus on adopting the SANS ICS 5 Critical Controls, establishing the foundation for more advanced security capabilities.

MITIGATION PHASE 2:	OPERATIONALIZATION OF SECURITY PROCESSES

The operationalization phase builds on the foundation to create sustainable security processes:

- Executing core security use cases in high-priority sites
- Improving security designs and processes based on experience
- Integrating OT security efforts with existing IT security programs
- Building repeatable processes for security operations
- Developing the skills and knowledge needed for effective OT security

This phase moves beyond implementing controls to establishing ongoing operational processes that maintain security over time.

MITIGATION PHASE 3:	OPTIMIZATION AND CONTINUOUS IMPROVEMENT

The optimization phase refines the security program to maximize effectiveness:

- Executing advanced security use cases
- Maturing security designs and processes
- Expanding security coverage to medium-impact sites
- Establishing risk management frameworks for investment decisions
- Continuously improving based on new threats and lessons learned

This phase focuses on fine-tuning investments and continuously improving the security program based on evolving threats and operational experience.

A Roadmap for the Journey: The SANS ICS 5 Critical Controls

The SANS ICS 5 Critical Controls provide a focused framework for addressing the most prevalent attack vectors in OT environments.

Critical Control	Why it Matters
ICS Incident Response Planning	Effective incident response planning ensures organizations can quickly detect, respond to, and recover from security incidents while minimizing operational impact.
Defensible Architecture	A defensible architecture limits the ability of attackers to move within the network and access critical assets, even if initial defenses are breached.
ICS Network Visibility & Monitoring	Network visibility and monitoring enable organizations to detect threats before they impact operations and provides the data needed for effective incident response.
Secure Remote Access	Network visibility and monitoring enable organizations to detect threats before they impact operations and provides the data needed for effective incident response.
Risk-Based Vulnerability Management	Risk-based vulnerability management recognizes that not all vulnerabilities can be immediately patched in OT environments and provides a framework for making appropriate risk decisions.

Additional Considerations for Building Business Resilience

A successful OT cybersecurity program requires a strategic roadmap that balances security priorities with operational realities.

Roadmap Step	Considerations	Outcome
Determining Priority Sites	Organizations should identify high-priority sites based on: • Operational criticality to the business • Potential safety and environmental impacts • Regulatory requirements and compliance obligations • Interconnectivity with other systems and facilities • Current security posture and known vulnerabilities	Focusing initial efforts on high-priority sites maximizes security impact while managing resource constraints.
Developing Skills and Resources	Building the necessary capabilities requires: • Training IT security staff on OT environments and constraints • Educating OT personnel on security principles and practices • Developing cross-functional teams with both IT and OT expertise • Establishing clear roles and responsibilities for OT security • Creating governance structures that balance security and operations	The skill development process should focus on enabling teams to execute core security use cases effectively.

Roadmap Step	Considerations	Outcome
Improving Designs and Processes	Continuous improvement of security designs and processes involves: • Gathering feedback from security and operations teams • Analyzing the effectiveness of implemented controls • Identifying friction points in security processes • Streamlining workflows to reduce operational impact • Documenting and standardizing successful approaches	This iterative process ensures that security measures become more effective and less intrusive over time.
Integration Strategies for IT and OT Security	Effective integration between IT and OT security requires: • Establishing clear boundaries and responsibilities • Creating common security governance structures • Developing shared incident response procedures • Implementing compatible security technologies where possible • Maintaining regular communication between teams	Integration ensures coordinated responses to threats while respecting the unique requirements of each environment.
Advanced Use Case Implementation	As organizations mature, they should implement advanced use cases: • Threat hunting across IT and OT environments • Complex attack detection and response scenarios • Supply chain security monitoring and verification • Advanced analytics and anomaly detection • Comprehensive security posture assessment and improvement	These advanced capabilities build on the foundation established by the core security controls.
Expanding to Medium-Impact Sites	After securing high-priority sites, organizations should: • Apply lessons learned to medium-impact sites • Standardize security approaches across the organization • Scale security monitoring and management capabilities • Implement risk-appropriate controls at each site • Establish consistent security baselines across all facilities	This expansion ensures comprehensive security coverage while applying appropriate controls based on risk.

Helpful Advice: Don't think about risk as a snapshot in time; instead, look for opportunities to share your vision about the journey and what's next for your organization. This insight will help boards, insurers, legal representation, and other stakeholders understand your priorities and progress over time.

Conclusion

As industrial cybersecurity threats grow increasingly sophisticated, the gap between operational understanding and executive risk awareness has become dangerously untenable. For C-suite leaders, this is no longer just a technical concern but a fundamental business imperative requiring strategic attention and investment.

A balanced approach to risk and resilience begins with threat scenarios that provide the critical context missing in most boardroom discussions about OT security. By methodically modeling how threat actors might target industrial control systems—considering the multi-dimensional impacts to safety, environment, reputation, finances, and regulatory compliance—organizations can identify previously overlooked vulnerabilities and prioritize mitigation efforts based on true business impact. This approach directly addresses the stakeholder disconnect that currently undermines effective risk management.

The SANS ICS 5 Critical Controls provide a focused framework for addressing the most prevalent attack vectors, while the three-phase maturity model offers executives a clear roadmap for progressing from basic implementation to optimized security operations. This structured progression enables organizations to communicate their resilience journey transparently to boards and external partners—including insurers who, as we've seen, struggle to accurately evaluate and price OT cyber risk.

Effective risk management requires more than technical solutions; it demands a comprehensive understanding of your specific industrial environment and informed decision-making processes at the executive level. Organizations must proactively assess their operational environments, clearly identify the assets most critical to their operations, and systematically determine the appropriate strategies for addressing threats to those assets. This process cannot be an isolated exercise—it requires precisely the cross-departmental collaboration our introduction identified as lacking, along with unwavering executive leadership commitment and ongoing adaptation to the evolving threat landscape.

A documented risk management strategy—including a detailed risk register—provides the clarity and accountability currently missing across many organizations, from technical specialists through executive leadership. This documentation becomes especially crucial in navigating the rapidly evolving regulatory landscape and increasingly complex insurance policies. Partnering with vendors that have robust and established relationships across legal and insurance sectors can significantly enhance an organization's strategic positioning in this challenging environment. Such partnerships provide invaluable insights, streamlined risk-transfer mechanisms, and proactive legal guidance, enabling organizations to respond confidently in crises and maintain operational continuity. The selection of knowledgeable, connected, and reputable partners is pivotal to comprehensive OT risk management in today's uncertain insurance marketplace.

Most importantly, C-suite leaders must act now—don't wait until after an incident to learn that a risk that could have been mitigated was knowingly accepted. By implementing a strategic, documented approach to OT risk management—one that leverages realistic threat scenarios to identify and prioritize vulnerabilities—you position your organization to protect critical operations while maintaining the efficiency and reliability that your business depends on. Organizations that successfully implement this approach will be better equipped to navigate the challenges of securing industrial operations. More significantly, they will transform industrial cybersecurity from a technical challenge into a strategic advantage—demonstrating to stakeholders, regulators, and insurers alike that they understand the true dimensions of operational technology risk and have developed the resilience necessary to thrive despite them.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East. Learn more about our technology, services, and threat intelligence offerings: **request a demo** or **contact us**.