



# **OT Cybersecurity 2.0™**

**From Compliance to Operational Resilience**

**Thomas Jackson**

## **OT Cybersecurity 2.0™: From Compliance to Operational Resilience**

OT cybersecurity is at an inflection point. For years, many organizations have relied on assessments as the primary way to understand OT cyber maturity, establish a baseline, and demonstrate alignment with industry standards. Assessments became the language of progress useful for benchmarking, satisfying regulators, and framing early investment discussions.

Traditional OT cyber assessments are typically used to:

- Establish a baseline
- Measure maturity
- Demonstrate compliance
- Inform investment decisions

That approach served an important purpose in the early stages of OT cybersecurity. But it reflects an earlier era, OT Cybersecurity 1.0, where the primary objective was awareness and compliance. Today's OT environments are far more connected, digitized, and operationally interdependent. In that context, compliance alone no longer answers the most important question executives are asking:

“Can we continue to operate safely and reliably when something goes wrong?”

This is where OT Cybersecurity 2.0™ begins. Compliance may confirm that controls exist, but it does not validate whether they reduce downtime, protect safety, or enable rapid recovery. As operational risk increases and disruption costs rise, organizations must evolve from checklist-driven programs to resilience-driven operating models.

Because compliance is not cybersecurity and on its own, it is no longer sufficient.

### **The Limits of a Compliance-Driven OT Cyber model**

Traditional OT cyber programs rely heavily on:

- Control checklists
- Framework alignment
- Qualitative scoring
- Periodic point-in-time assessments

These tools provide structure and consistency, but they also create blind spots. Most compliance-driven assessments are:

- Qualitative, based on interviews and documentation
- Subjective, influenced by interpretation and self-reporting

- Static, quickly outdated in dynamic OT environments

As a result, organizations may appear compliant on paper while remaining exposed operationally. This creates a false sense of confidence and slows meaningful decision-making.

### **Why Compliance does not imply Cybersecurity**

Compliance answers an important question: “Are we aligned to a standard?”

Cybersecurity, especially in OT must answer a different one: “Can we continue to operate safely and reliably under adverse conditions?”

When OT cyber programs stop at compliance:

- Risk is measured in control gaps, not consequences
- Investment decisions lack operational context
- Leadership struggles to prioritize what actually matters

The outcome is predictable: cybersecurity becomes a checkbox exercise rather than a resilience capability.

### **Why the Data Supports a Shift Beyond Compliance**

Industry data consistently shows that while OT cybersecurity assessment and compliance activity has increased, operational resilience has not kept pace. This disconnect is a primary reason organizations struggle to manage real OT cyber risk using compliance driven models alone.

Several trends stand out:

Assessments are widespread, but execution maturity remains low.

Most industrial organizations report completing OT cybersecurity assessments aligned to standards such as IEC 62443 or NIST, yet far fewer report mature implementation of controls, continuous monitoring, or incident response capabilities. This reinforces the reality that assessment activity does not reliably translate into sustained risk reduction.<sup>12</sup>

OT cyber incidents continue to rise despite compliance efforts.

Reported cyber incidents impacting industrial operations including ransomware and operational disruption continue to increase year over year. These incidents frequently occur in environments that have already completed assessments, highlighting the gap between compliance and operational resilience.<sup>34</sup>

Limited OT visibility undermines effective risk management.

A significant percentage of organizations still lack comprehensive visibility into OT assets, communications, and vulnerabilities. Without objective, real-time insight, organizations rely on static

and qualitative assessments that quickly become outdated, limiting their ability to prioritize risk effectively.<sup>56</sup>

Executives respond to downtime and safety impact not control maturity scores. Studies consistently show that executive leadership prioritizes decisions tied to uptime, safety, and financial impact over abstract control alignment or maturity scoring. When OT cyber risk is not expressed in these terms, it struggles to influence investment decisions.<sup>78</sup>

Taken together, these data points reinforce a critical conclusion: compliance and assessments are necessary entry points, but they are insufficient for managing OT cyber risk in complex, interconnected environments. Operational resilience requires continuous, data-driven insight that connects cybersecurity directly to how the business operates.

### **The Shift to OT Cybersecurity 2.0™**

OT Cybersecurity 2.0™ represents a shift from control centric thinking to outcome-centric execution. It focuses less on whether a control exists and more on whether it actually reduces operational risk. This shift requires moving beyond traditional assessments and toward quantitative, objective insight drawn from the OT environment itself.

### **From Checklists to Operational Outcomes**

Instead of relying primarily on qualitative assessments, OT Cybersecurity 2.0™ emphasizes:

- Deeper network visibility
- Real-time assets and communication awareness
- Objective indicators of exposure and behavior
- Continuous validation of risk assumptions

This data provides a more accurate picture of:

- What is actually connected
- How systems communicate
- Where risk is accumulating
- Which failures would have the greatest operational impact

In other words, it replaces assumptions with evidence.

## **Metrics That Actually Matter**

For executives and decision-makers, OT cyber risk becomes actionable only when it is tied to operational outcomes.

The most effective OT cyber programs anchor decisions to metrics such as:

- Uptime and availability – What processes are most critical to continuous operations?
- Safety impact – Which failures introduce personnel or environmental risk?
- Recovery time – How long does it realistically take to restore operations?
- Decision speed – How quickly can leaders understand, prioritize, and respond?

Without these metrics:

- Risk discussions remain abstract
- Investment cases lack credibility
- Trade-offs are difficult to justify

With them, cybersecurity becomes a business decision, not a technical debate.

## **Why Data-Driven Insight Changes the Conversation**

When OT cyber leaders can show:

- Which assets support critical processes
- Which communication paths introduce exposure
- Which failures cascade across operations
- Which investments reduce downtime and recovery time

They change how leadership engages.

Cybersecurity shifts from:

“Do we comply?”

To:

“How do we reduce the most consequential operational risk?”

That shift is the foundation of resilience.

## **What This Means for Growth and Differentiation**

For organizations serving clients whether as operators, integrators, or advisors. OT Cybersecurity 2.0™ is also a differentiator.

Clients increasingly expect:

- Better data to support decisions
- Clear linkage between cyber investment and operational outcomes
- Programs that scale beyond assessments into execution and sustainment

Leaders who can deliver this don't just reduce risk they create long-term value and trust.

### **Closing Thought**

Compliance will always matter. Assessments will always have a role. But they are no longer the measure of OT cybersecurity maturity.

In today's interconnected and operationally dependent environments, maturity is defined by an organization's ability to understand operational risk in real time, make confident decisions under pressure, and sustain safe and reliable operations when disruption occurs.

OT Cybersecurity 2.0™ moves beyond checklists and point-in-time assessments. It focuses on evidence over assumptions, outcomes over controls, and resilience over compliance.

Organizations that make this shift don't just improve their security posture, they gain the insight needed to protect uptime, safeguard people, and enable the business to operate with confidence.

That is the evolution from compliance to operational resilience.  
And it is where the next generation of OT cyber leaders will differentiate.

*"Compliance proves alignment. Resilience proves readiness"*

### **References**

1. SANS Institute. *The State of OT/ICS Cybersecurity 2023*. SANS Institute, 2023.
2. Ponemon Institute. *The Global State of Industrial Cybersecurity*. Ponemon Institute, 2023.
3. Dragos, Inc. *ICS/OT Cybersecurity Year in Review*. Dragos, 2023.
4. IBM Security. *Cost of a Data Breach Report*. IBM, 2023.
5. Gartner. *Market Guide for OT Security*. Gartner Research, 2023.
6. CISA. *Cross-Sector Cybersecurity Performance Goals and Incident Trends*. Cybersecurity and Infrastructure Security Agency, 2023.
7. World Economic Forum. *Global Cybersecurity Outlook 2024*. World Economic Forum, 2024.
8. Deloitte. *Securing the Smart Factory: Cyber Risk in Manufacturing*. Deloitte Insights, 2023.

Tom Jackson is a senior OT/ICS cybersecurity executive with 20+ years of experience helping regulated and critical infrastructure organizations move OT cybersecurity programs beyond assessment into execution, resilience, and measurable business outcomes.