



Beyond the OT Cyber Assessment: Why OT Cyber Risk Still Struggles to Get Funded

**Translating Technical Risk Into Business
Impact for Executive Decision Making**

Thomas Jackson

Beyond the OT Cyber Assessment: Why OT Cyber Risk Still Struggles to Get Funded

Most organizations today acknowledge that OT cybersecurity risk is real.

Many have completed assessments aligned to IEC 62443, NIST 800-82, NIST CSF, or sector-specific regulations. The findings are documented, risks are ranked, and roadmaps are produced. And yet, OT cyber risk still struggles to secure sustained funding. This is not a technology problem. It is not a framework problem. It is a decision-making problem.

OT Cyber Risk Isn't Framed in Business Terms

The core challenge is simple: OT cyber risk is rarely presented in terms that align with how executives allocate capital.

Most assessments describe:

- Control gaps
- Architecture weaknesses
- Vulnerabilities and exposures

What executives need instead is clarity on:

- Operational downtime
- Safety impact
- Production loss
- Revenue and recovery implications

When risk remains framed in technical language, it competes poorly against projects with clear operational or financial returns. As a result, OT cyber often becomes “important but not urgent.”

Standards Are a Starting Point, Not a Funding Strategy

Frameworks such as NIST 800-37 RMF, OT risk registers, and even OT HAZOP-style analyses provide valuable structure. They help organizations identify hazards, threats, and control gaps. But these artifacts still operate one level deeper than most executives need.

From the boardroom perspective:

- Risk registers do not equal risk decisions
- Control mappings do not equal investment cases
- Compliance alignment does not equal resilience

Standards help define *what* needs attention—but they do not explain *why now*, *what happens if we wait*, or *where investment* actually reduces business risk.

The Missing Link: Operational Impact Narratives

OT cyber risk becomes fundable only when it is connected to how the business actually runs. This requires shifting the conversation from abstract risk to operational narratives, such as:

- Which production processes would be impacted by a cyber event
- Which systems take the longest to recover
- Which failures cascade into downstream outages
- Which disruptions affect safety, quality, or regulatory compliance

When leaders can see how cyber risk interrupts operations, decisions change.

Mapping Risk to Downtime and Recovery Reality

One of the most effective shifts OT cyber leaders can make is mapping risk to process-level downtime and recovery complexity.

Key questions executives understand immediately:

- If this system goes down, what else stops?
- How long would it realistically take to restore?
- What is the cost per hour of that outage?
- Are there safety or regulatory consequences?

This reframes cyber investment as:

“Reducing the likelihood and duration of operational disruption” not as “improving security posture.”

What the Data Shows

Industry data consistently reinforces why OT cyber funding stalls when risk is not operationalized:

- Funding remains misaligned with risk exposure
While OT cyber incidents continue to rise, many organizations report that OT security initiatives struggle to secure consistent funding without clear operational justification.^{1,2}
- Executives prioritize downtime over vulnerabilities
Studies show executives respond far more strongly to quantified downtime, safety impact, and production loss than to control maturity scores or vulnerability counts.^{3,4}
- Visibility gaps undermine confidence in investment
A significant percentage of organizations still lack complete visibility into OT assets and communications, making it difficult to justify where investment will actually reduce risk.^{5,6}

- Incidents continue to drive reactive spending
Despite increased assessment activity, disruptive OT cyber incidents—including ransomware—continue to increase, often triggering funding *after* disruption rather than before.^{7, 8}

The conclusion is consistent across sectors: OT cyber risk struggles to get funded until it is framed as an operational and financial problem.

From Risk Awareness to Investment Decisions

This is where OT cyber leadership becomes a differentiator. Cyber leaders who succeed in securing funding do not just report risk they:

- Translate risk into business and operational outcomes
- Align remediation to production and safety priorities
- Sequence investments to reduce the most consequential downtime scenarios
- Communicate trade-offs executives can act on

In other words, they convert risk insight into investment decisions.

What Hiring Leaders Should Be Looking For

As OT cyber programs mature, organizations need leaders who can do more than assess.

They need leaders who can:

- Bridge OT engineering, cybersecurity, and executive decision-making
- Translate technical findings into funded, executable programs
- Align cyber investments with operational resilience and growth
- Build repeatable models clients and organizations will sustain

This capability is increasingly what separates strategic OT cyber leaders from technical specialists.

Closing Thought

OT cyber risk does not struggle to get funded because executives don't care about security. It struggles because risk is too often presented without context, consequence, or clarity. When cyber leaders connect risk to downtime, safety, and operational continuity, funding conversations change and resilience follows.

“OT cyber funding follows operational impact, not technical findings.”

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