The OT Governance Gap

Addressing These Hidden Risks Could Save Your Company

Facilitated by:

Chuck Tommey, P.E.

CISSP, GICSP, ISA Cyber Expert

HILLSTRONG GROUP SECURITY

My Tech Conference

Seattle, Washington

October 22, 2025

What IS OT/ICS/IIoT or Operational Technology?

My Definition

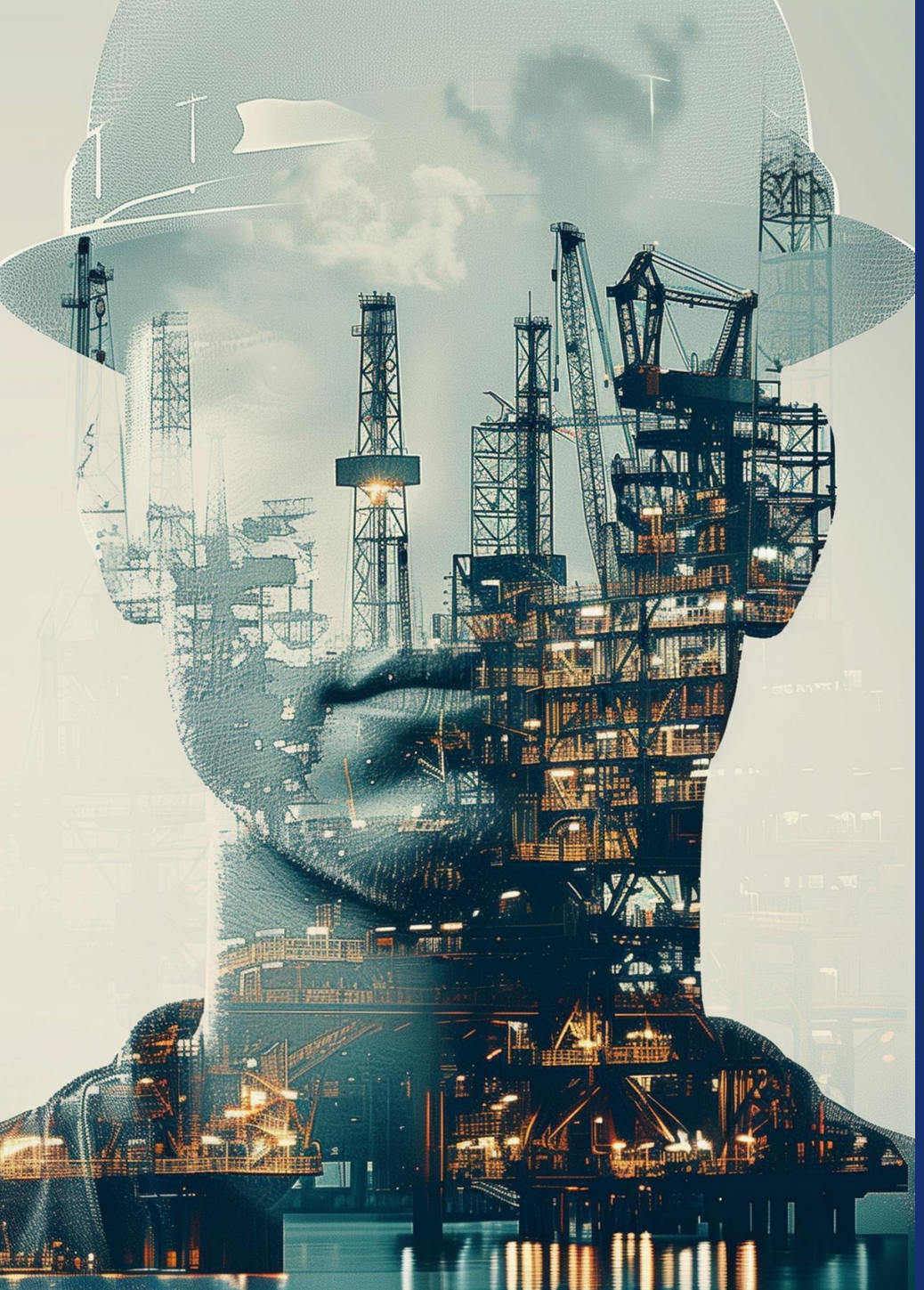
Anything that looks, sounds, feels, smells, or tastes like IT **AND** interacts with the physical world

Simple Interactions

Measuring temperature, speed, quantities, or device status indicators

Complex Controls

Full industrial control systems: controllers, HMIs, data historians, recipe management



Who is Responsible for OT Cyber?

Trick question: Everyone has OT systems, whether you know it or not — and everyone shares responsibility

Today's Agenda

01

Where Can You Find OT in Your Organization

02

Why & How OT Cyber Is Different

03

The OT Governance Gap

04

OT-specific Guidance from Industry & Government

05

Lessons Learned from the Field

OT Exists Everywhere

Beyond Industrial Plants

- HVAC systems keeping buildings comfortable
- Elevator and escalator controls
- Smart lighting and energy management
- Physical access control systems
- Warehouse logistics and automation

OT Cyber Wake-up Calls

1

Target (2013)

HVAC vendor credentials stolen — 40M credit cards compromised

2

Ukraine Electrical Grid (2015-16)

Power safety systems (breakers) attacked — 230,000 customers lost electricity

3

Casino Fishtank (2017)

“Smart” thermometer for lobby fishtank hacked — high-roller database exfiltrated

4

Colonial Pipeline (2021)

IT order tracking down — couldn't move product, paid ransom and still took weeks to recover

5

MGM Resorts (2023)

Door locks compromised — 2-3 weeks to restore normal operations

Recent OT Horror Stories

1

Clorox

August 2023 — Social engineering attack (service desk pw reset), lost production, product scarcity ~$429 Million in losses

2

Bridgestone Americas

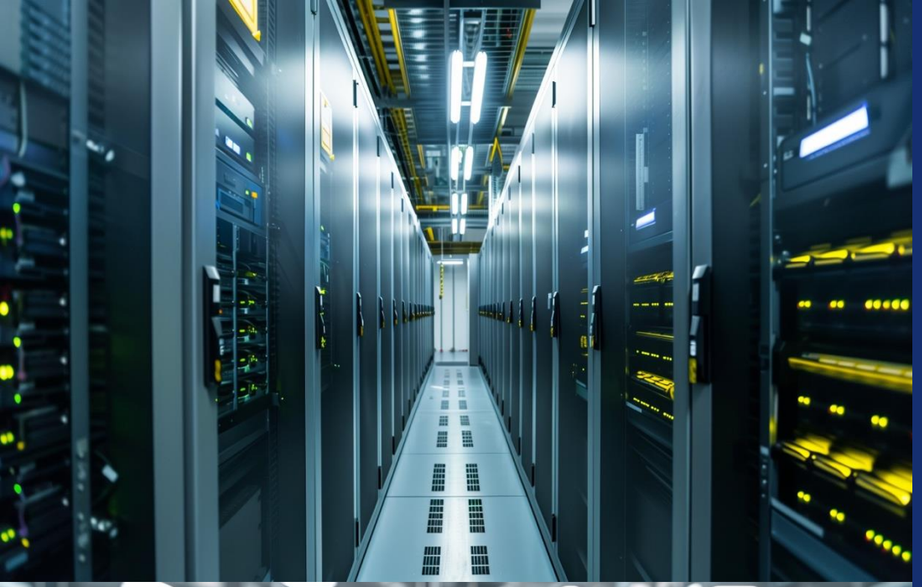
September 1, 2025 — Tire manufacturing disrupted, production halted across multiple facilities

3

Jaguar Land Rover

September 2, 2025 — Invoice payments and logistics down, manufacturing suspended for 5 weeks, £1.5 B gov loan guarantee

In 2024, ransomware attacks on OT/ICS environments increased significantly, with a surge of 87% in industrial sector attacks compared to 2023, making manufacturing the most affected industry.



Why OT Cyber Is Different

IT is Fully Digital

IT Priorities

- **Confidentiality** first
- Data protection focus
- Rapid patching cycles
- Regular system updates

Report to CIO

8 x 5 work week

Computer Science

- Networks & Cyber Savvy

OT is Physical & Digital

OT Priorities

- **Safety & Availability** first
- Physical process protection
- Change control windows
- System uptime critical

Report to COO

Rotating Shifts (24 x 7)

Engineering

- Process & Controls Savvy

OT Cyber Risks Are Physical

Safety Incidents

Equipment malfunctions causing injury or environmental damage

Production Downtime

Manufacturing halts costing millions per hour

Physical Damage

Systems destroyed requiring weeks or months to replace

The OT Governance Gap

IT infrastructure on one side...
OT operations on the other

Traditional IT governance, risk, and compliance models don’t always bridge the divide

Why IT GRC Models Don’t Always Fit OT

Common OT Governance Failures

No OT-Specific Policies

Organizations apply IT policies without adapting to OT realities

Missing Proper Stakeholder Buy-In

COO, VP Manufacturing, and Engineering never engaged or consulted

Invisible OT Metrics

Board-reported cyber metrics tend to exclude OT data

Misaligned KPIs

MTTR and patching metrics don't reflect OT constraints

No OT Processes and Playbooks

Incident response and recovery processes don’t include most OT systems

Excluded from Exercises

Plant managers and facilities teams rarely included in tabletop exercises

Why GRC Is MORE Critical for OT

Tall Organizational Silos

CIO/CISO vs. COO vs. CFO vs. Engineering
- requires Board/C-suite supervision

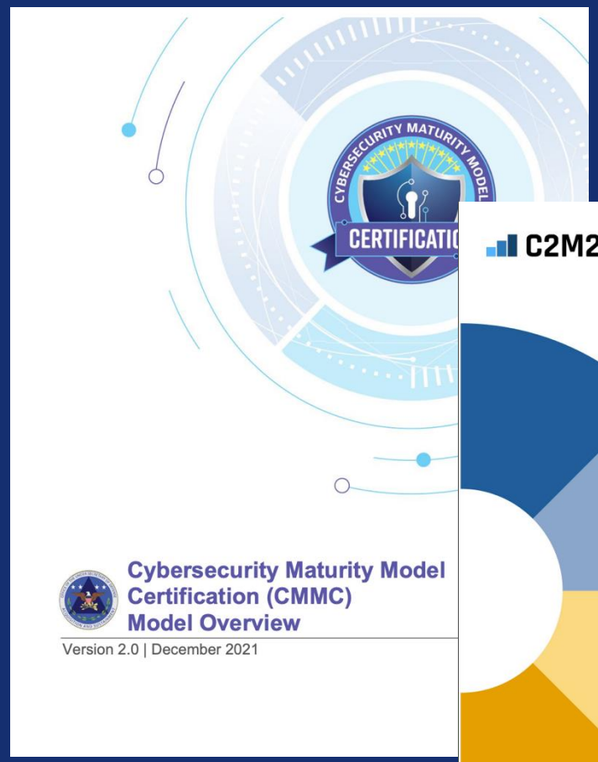
Recovery Time Disparity

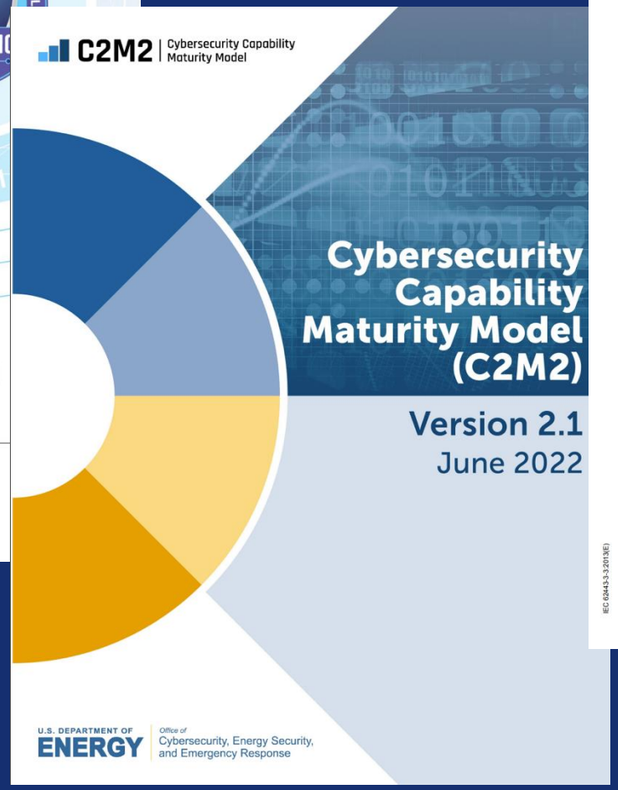
Email server: hours or days. Production line or plant: weeks or months

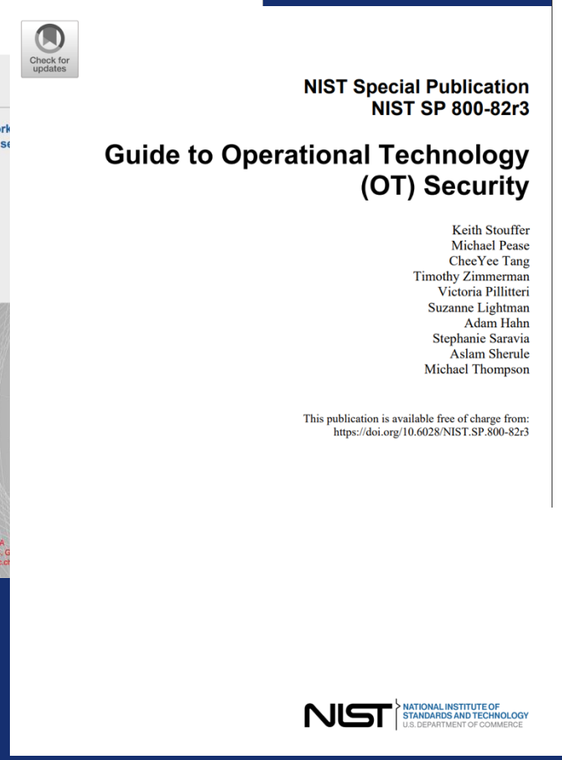
Economic Impact Scale

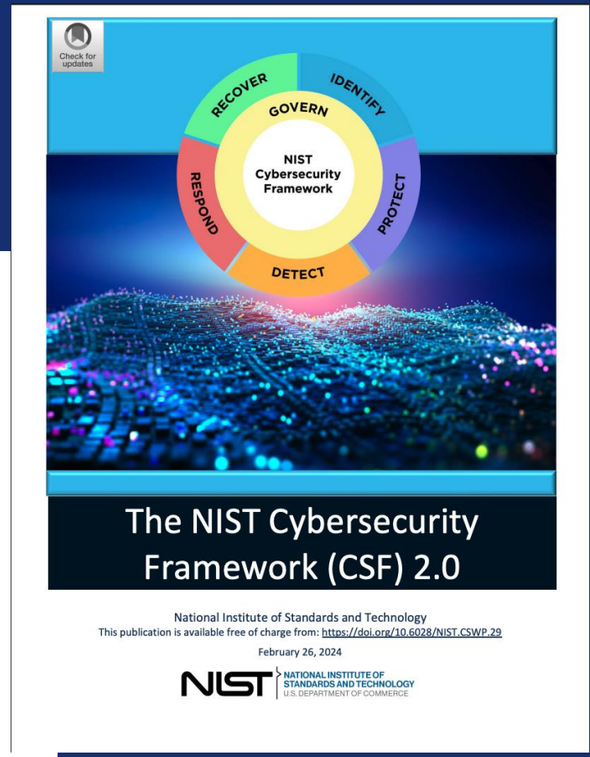
IT outage: inconvenience. OT outage: business-threatening financial loss

OT-Specific Standards & Frameworks









Industry and government have created **comprehensive guidance** specifically designed for OT environments

Key OT Guidance Explained

NIST CSF 2.0

Updated with dedicated **Governance** function — applies to all sectors, now OT-inclusive

IEC 62443

International OT-specific standard with **risk-based approach** and security levels

NIST SP 800-82

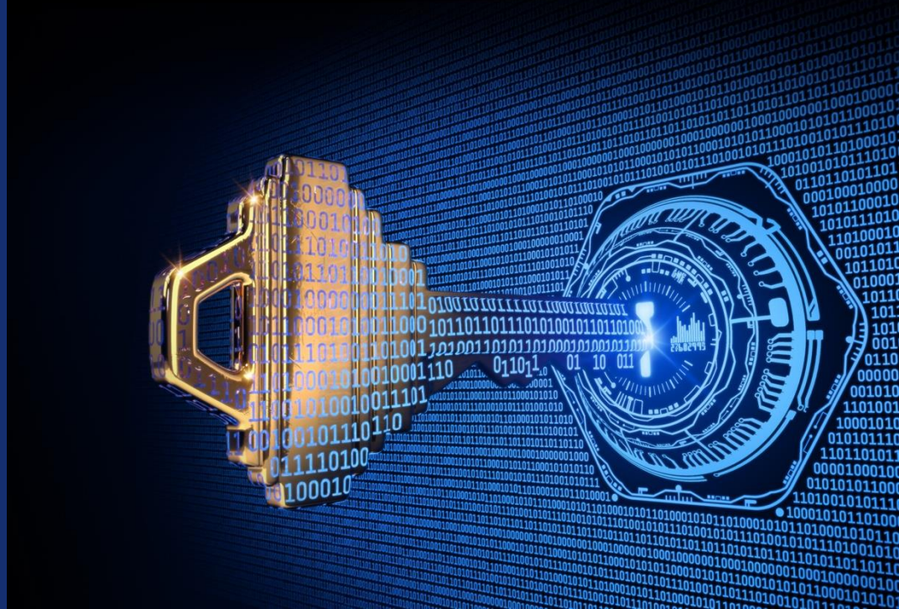
Extends IT control framework (SP 800-53) with **ICS-specific guidance**

C2M2

DOE critical infrastructure maturity model focused on **capability domains**

CMMC 2.0

DOD requirement for defense contractors — **3-year phase-in** starting Nov 10, 2025



Lessons Learned from the Field

OT Governance Pitfalls

Complete Hands-Off Approach

Zero collaboration between IT and OT teams creates dangerous blind spots

Treating OT Like IT

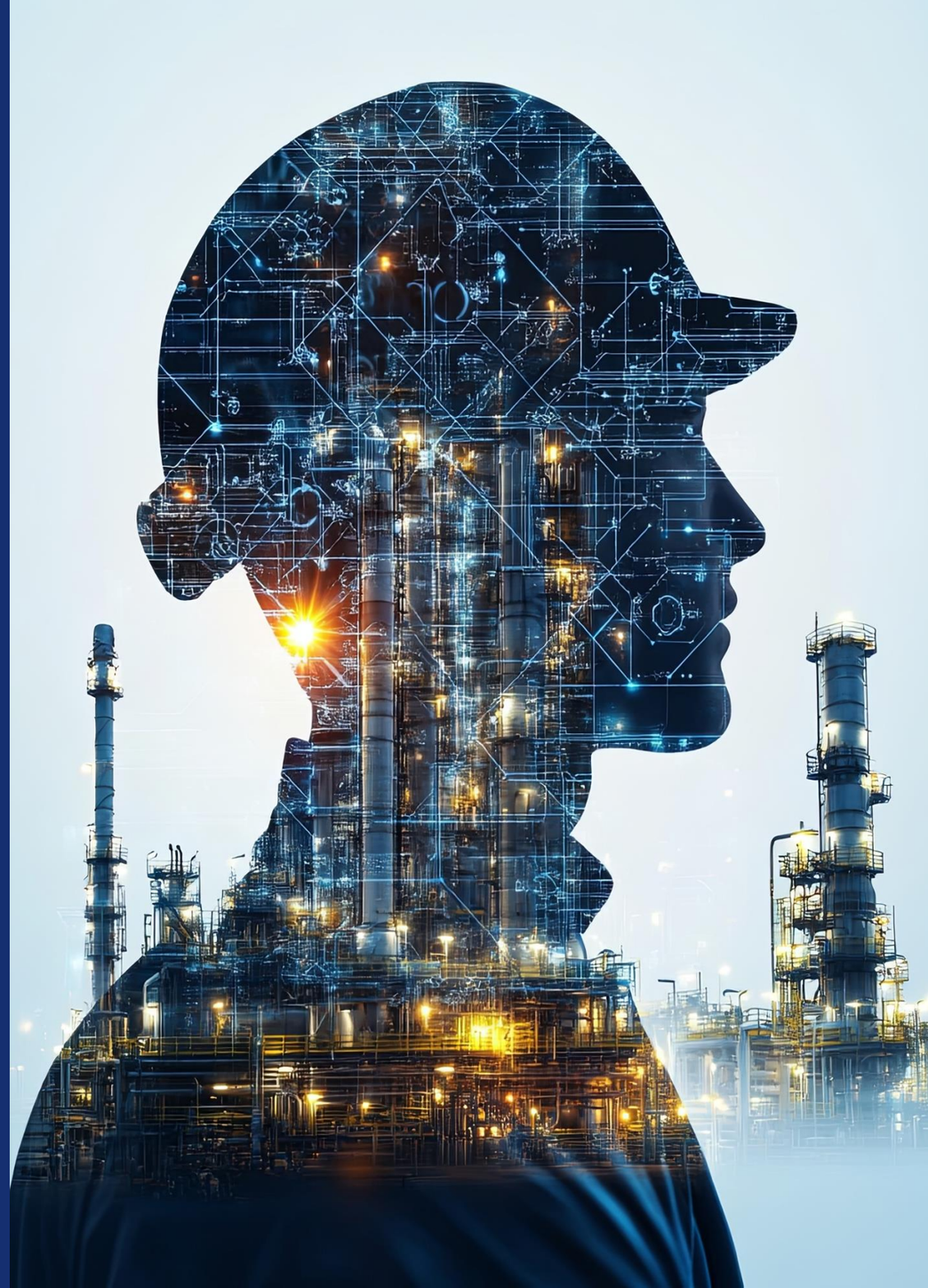
Forcing IT controls onto OT without adaptation causes operational failures

No Incident Response Planning

Lack of OT-specific playbooks and training leaves teams unprepared

Ignoring Third-Party Vendors

HVAC contractors, system integrators, and service providers create entry points



Lessons Learned from the Field

Success Factors for OT Governance

Senior Sponsorship

C-suite sets budget and priorities — Board oversight is essential

OT/IT Collaboration

Leverage IT expertise while respecting OT constraints and requirements

Risk-Based Roadmaps

Phased implementation prioritized by actual risk, not convenience

Change Management

People and process transformation, not just technology deployment

Field Lessons: Chemical Manufacturer

The Context

- $2.5B annual revenue
- 22 manufacturing sites globally
- 4 global regulatory regions
- Multiple peer cyber incidents

What Worked

- CIO/CISO and corporate engineering engagement
- Created OT-specific policies
- Talented teams already started efforts

What Didn't Work Well

- **Budget constraints** stalled progress
- **"Value engineering"** by sales bypassed internal standards
- **Uneven deployment** created appearance without substance
- **Weak monitoring** obscured real security posture

Field Lessons: Grid-Scale Battery OEM

The Context

- $2.7B annual revenue
- Global installations
- Customer certification requirements

What Worked

- CISO and product engineering engagement
- Complete OT policy framework
- Enthusiastic cross-functional participation

What Didn't Work Well

- **Product development priorities** created delays
- **Regional differences** difficult to reconcile
- **Legacy vs. new products** required careful balance

Key Takeaways

- OT is EVERYWHERE in EVERY Organization
- OT is a BIGGER RISK than most realize
- GOVERNANCE maturity is the KEY to solutions
- A WEALTH of OT-specific GUIDANCE exists
- Learn from PEERS, not HARD knocks
- IT/OT COLLABORATION is critical
- Look for OT DEPENDENCIES on non-OT systems

“The next era of cybersecurity leadership isn’t about bigger firewalls—it’s about BROADER VISION.

The leaders who understand and GOVERN their OT will define what RESILIENCE means for the next decade.”

Chuck Tommey, P.E., CISSP, GICSP, ISA Cyber Expert

Hillstrong Group Security, Inc.

chuck.tommey@hillstrongsecurity.com

(704) 984-0593

https://hillstrongsecurity.com

https://Resilion.io