HILLSTRONG GROUP SECURITY

HILLSTRONG · THOUGHT LEADERSHIP

From Signals to Strategy

Executive Briefings on OT Risk

Roger Hill | CEO, Hillstrong Group Security, Inc.

hillstrongsecurity.com

Contents

Five executive briefings on making operational technology risk visible, measurable, and strategic.

CHAPTER ONE	The OT Risk the CFO Can't See
CHAPTER TWO	The Value Gap in OT Security
CHAPTER THREE	The Silent Drift
CHAPTER FOUR	12 Plants, 12 Programs: Why Site-Level Risk Can't Scale
CHAPTER FIVE	What Is Operational Risk Costing You?
	About the Author
	About Hillstrong Group Security, Inc.

HILLSTRONG GROUP SECURITY

FROM SIGNALS TO STRATEGY · CHAPTER ONE

The OT Risk the CFO Can't See

Why operational cyber risk still escapes financial oversight, and how innovative leaders are fixing it.

> **"What gets reported gets funded. And if your OT risks aren't reported in business terms, they don't exist at the executive table." If your CFO asked for your top 3 OT cyber risks, could you answer in dollars?**

There's a silent disconnect in boardrooms today. While enterprise leaders obsess over ransomware headlines, OT security teams are fighting a different kind of war and losing budget battles they never got to join.

Why? Because the language of OT risk still doesn't translate into the language of executive action. We don't have a visibility problem. We have a framing problem.

The Problem We're Not Talking About

OT risk rarely appears on the enterprise risk register. It doesn't align neatly with traditional IT metrics and often lacks the storytelling power needed to win airtime in executive discussions.

The metrics we use are operational, not strategic:

- Patching stats
- Asset uptime
- Scan counts

None tells a CFO what an unpatched PLC might cost in lost production.

None of it tells the board how vendor credential drift could trigger a compliance failure and spike insurance premiums.

So OT teams report to CISOs, who report to CIOs, who don't own the asset producing the revenue.

And that means the risk, while very real, never enters financial planning conversations.

This misalignment limits visibility, weakens OT's ability to secure funding, prioritize investments, and establish a business case for modernization, and turns legitimate concerns into what the board perceives as “technical noise.”

When OT Risk Finally Got Noticed

We worked with a multi-site industrial client who completed all the right paperwork. Their GRC program was mature on paper: policies were reviewed, risk matrices were defined, and exception logs were diligently maintained.

However, the badge system hadn't been audited in one of their highest-throughput plants in 14 months. A long-tenured contractor still had physical access, despite their contract expiring three quarters earlier. That same credential was used to plug a laptop directly into an unmanaged switch on the process control network.

The result? Not malware, not espionage, but a manual system override during peak operations, which forced a halt to ensure personnel safety. The downtime ripple effect spanned four sites and delayed customer shipments across two continents.

Impact: $3.1 million in late penalties and expedited logistics costs.

The CFO didn't get that story from a vulnerability scanner.

They understood when the supply chain director asked, “Why are we eating costs to make up for a plant error?”

That's when the risk got noticed.

Why Technical Metrics Aren't Enough

Most OT cybersecurity reports resemble a service log: vulnerabilities discovered, patches deployed, devices scanned, risks accepted. They're often detailed, but not decision-ready.

CFOs and COOs don't operate from that lens. They look for exposure, trends, investment justification, and revenue impact. When OT cybersecurity conversations fail to cross that divide, funding dries up.

That's why reporting tools aren't the solution: translation is.

What does this control gap mean in terms of uptime exposure? What's the estimated cost of delaying this upgrade? Which sites are most likely to trigger fines or lost contracts?

Boards don't care how many devices have been scanned. They care about what happens when one of them fails in production.

What Smart Organizations Are Doing Differently

They're changing the conversation.

Instead of reporting activities, they're telling stories of exposure and consequence:

What happens if this site goes offline?

What's the cost of a failed audit?

Where is our coverage weakest?

They're moving from site-by-site spreadsheets to comparative frameworks that allow them to prioritize by risk tier and impact.

They're incorporating business stakeholders into risk reviews, creating accountability across disciplines. Cybersecurity isn't siloed as “IT” or “compliance” anymore; it becomes part of how the company talks about operational resilience.

Some organizations are even embedding OT cyber metrics into enterprise KPIs and executive dashboards, not as a separate track but as part of business continuity, revenue protection, and audit readiness.

Because when OT risk is translated into business language, it finally earns a seat at the table.

What You Can Do

If you're an OT leader: Stop reporting vulnerabilities. Start reporting exposure. Connect system health to operational consequences.

If you're a CISO or GRC lead: Don't assume the board understands OT risk. Quantify it regarding operational downtime, compliance impact, and financial exposure. Establish a recurring executive briefing cadence.

If you're a CFO or COO: Ask your teams to bring you their top 3 OT risks, in business terms. If no one brings you a number, you don't have a handle on the risk, just a hope.

You can't manage what you don't understand. And you can't fund what you don't see.

A Final Thought

Operational risk is a board-level issue hiding in plain sight. It shows up after the event but lives upstream: in ignored exceptions, outdated inventories, and risk reports that speak the wrong language.

The question isn't whether OT cyber risk matters. Why hasn't it been included in the financial playbook yet?

It's time it did.

Your Turn

What would it take for OT cyber risk to earn a seat at your next board meeting?

Let's move the conversation forward.

HILLSTRONG GROUP SECURITY

FROM SIGNALS TO STRATEGY · CHAPTER TWO

The Value Gap in OT Security

From Telemetry to Trust

Why more data hasn't made us safer, and what actually builds confidence in cyber-informed decisions.

> **The real problem isn't a lack of visibility. It's a lack of context.**

We're drowning in telemetry.

Device scans. Asset inventories. Traffic anomalies. Risk scores.

The issue for most OT security teams isn't data collection, it's data translation.

CISOs and COOs are increasingly asked to justify spending, prove coverage, and demonstrate readiness. But what they get from the field is a raw signal.

The value gap? It's not technical. It's relational. Contextual. Strategic.

And the broader the gap, the harder it is to build trust in risk decisions.

The Illusion of Visibility

Ask any OT security vendor what they do best, and you'll hear it: visibility.

"We can see your assets." "We can scan your traffic." "We can alert on threats."

What few vendors talk about is what happens next:

Who interprets the data?

Who decides what matters?

Who connects it to operations?

We've created a paradox: More data, less confidence.

Executives don't want another dashboard. They want a decision. They want to know what action is needed, what happens if they wait, and what it will cost to get it wrong. Visibility without prioritization is noise. And OT risk doesn't just live in devices, it lives in decisions made without context.

The Meeting That Changed the Question

A regional manufacturing leader once shared this with me:

"Our OT visibility platform told us we had 280 high-risk findings. My COO asked which ones could shut down production. I didn't have an answer."

Not the findings. Not the score. ***The question.***

That's when they realized they didn't have a visibility problem. They had a framing problem. So they changed the lens.

They stopped asking, "What did we detect?" They started asking, "What can this risk disrupt?"

And that shift became contagious. Risk reviews became cross-functional.

Findings were sorted by consequence.

Vulnerabilities were mapped to operational zones, not just asset IDs.

It didn't just improve reporting. It changed how security spoke to the business.

What Trust Looks Like

Trust isn't just seeing everything. Trust is knowing what matters.

In OT, that means:

- Understanding criticality, not just count
- Knowing the impact of action vs. inaction
- Measuring risk in terms of availability, safety, and cost

Trust also means confidence in timing. Not every fix is urgent, but some can't wait. Executives don't want to be overwhelmed, they want clarity.

Teams that build trust do more than scan. They synthesize.

They contextualize findings against:

- Operational zones
- Downtime thresholds
- Known failure modes
- Compensating controls

And they present options that speak in tradeoffs, not alerts.

This is how security earns trust at the executive level.

This is how technical insight becomes business intelligence.

The Pivot: From Raw Signal to Operational Insight

Here's what high-functioning OT risk programs are doing differently:

- Tiering by consequence
- Overlaying controls
- Time-bounding decisions

- Translating for stakeholders

This is what maturity looks like: not a dashboard full of data, but a conversation anchored in consequence.

The False Comfort of Compliance

One of OT's most significant sources of friction is the illusion that compliance equals confidence.

But checklists don't capture nuance. They don't account for:

- Outdated threat models
- Misleading scan results
- Human error in exception approvals

We've seen fully compliant facilities hit with outages, safety shutdowns, and reputational damage, not because they didn't do what was required, but because they failed to challenge what was relevant.

Compliance is the floor. Operational resilience is the ceiling.

And that difference is often found in the value layer: how well your risk data supports real-world decisions.

What You Can Do

If you're a site or OT lead: Map your top risks to production, not just to assets. Rank by consequence, not just likelihood. Highlight the controls already in place, and where they're missing.

If you're a CISO or enterprise risk lead: Ask whether your visibility tools are decision-grade. Sit with operations to pressure test your top 5 alerts. Prepare your next board slide around tradeoffs, not threats.

If you're a COO: Challenge your team to tell you what data matters, and what they can safely ignore. Ask how many findings actually drive action. Request risk briefings that include downtime impact, not just CVSS scores.

A Final Thought

OT security doesn't earn trust by showing up first in a crisis. It earns trust by helping leaders make confident calls before the crisis hits.

That's the difference between visibility and value.

Because you can't measure security maturity just by counting alerts. You measure it by how quickly and confidently decisions are made when it matters.

That's the real goal.

Your Turn

How does your OT telemetry actually support executive decisions?

If it doesn't, you're not falling behind in security. You're falling behind in strategy.

HILLSTRONG GROUP SECURITY

FROM SIGNALS TO STRATEGY · CHAPTER THREE

The Silent Drift

Operational Gaps That Compound Into Crisis

Why the most significant risks to your OT environment aren't sudden threats: they're slow, silent shifts in process, behavior, and control.

> **Most major OT failures don't begin with a breach. They begin with something quietly neglected.**

Some risks make headlines. Others build in silence.

In operational environments, security incidents rarely start with a bang. They start with an exception that never gets reviewed, a shared credential that wasn't revoked, or a workaround that becomes standard practice.

These aren't anomalies. They're symptoms of something more profound: operational drift.

The slow erosion of process, governance, and enforcement, in ways that most dashboards never see.

And because this kind of drift accumulates invisibly, many organizations only become aware of it *after* a triggering event.

What Drift Looks Like in the Field

It doesn't announce itself. It accumulates.

A contractor is granted persistent remote access for "troubleshooting" and never removed.

A temporary exception to a firewall rule is approved for one urgent maintenance task, and forgotten.

An aging asset that can't be patched is quietly decoupled from vulnerability reporting to avoid triggering constant alerts.

A disconnected sensor logs to a buffer that hasn't been checked in six months.

An HMI is updated through a USB workflow that bypasses centralized change tracking.

Each one feels like a workaround. A shortcut. A necessary exception.

None of these causes an incident on their own. But together?

They form a foundation of fragile assumptions, a web of unexamined trust. One small trigger (a new hire, a missed audit, a threat actor scanning for footholds) can turn drift into downtime.

Drift is not just about what breaks. It's about what no longer operates as designed.

A Case That Didn’t Start as a Crisis

One industrial facility we assessed had a strong compliance record.

They had:

- An updated inventory
- A well-documented patch policy
- A high maturity rating on their last audit

But something didn’t sit right.

As we walked through the access logs, we noticed something strange: an inactive vendor account had successfully authenticated to the network three weeks prior.

It turns out that the account belonged to a retired contractor who had helped commission the site years ago. Although he no longer worked for the company, his VPN access and stored credentials were still live.

He hadn’t done anything malicious; he was doing someone a favor. But it was a window left open. If it hadn't been flagged, it might have stayed open until someone else found it.

And that “favor” could have turned into a foothold.

This wasn't a breach. It was a **signal**. A proof point that drift had accumulated and would have remained invisible without scrutiny.

Why Dashboards Miss Drift

Drift doesn’t always show up in logs, isn’t scored by vulnerability scanners, and rarely makes it into compliance reports.

Because drift isn’t about policy.

It’s about practice.

It hides in the difference between what a procedure says and what people actually do.

This is the unmeasured domain of:

- Operator habits
- Workflow workarounds
- Process improvisation under pressure
- Ad hoc control changes that “just work”

These patterns are often undocumented, informal, and embedded in daily routine.

Most programs don’t track these changes.

And yet, this is where resilience is built or broken.

Security engineers often say, “Assume breach.” In OT, we might also say: “Assume drift.”

Because unless you're actively surfacing it, it's probably already there.

The Cost of Drift: More Than Security

When left unaddressed, drift doesn't just introduce cyber risk. It undermines:

- **Audit readiness:** Discrepancies between written procedure and real practice invite findings.
- **Process integrity:** When improvisation becomes standard, troubleshooting becomes guesswork.
- **Training and onboarding:** New staff learn undocumented behaviors, propagating the drift.
- **Safety culture:** The normalization of deviation erodes procedural discipline.

Organizations that experience chronic drift tend to have higher variance in outcomes, which affects not just uptime but also quality, safety, and customer trust.

Drift turns complex systems into unpredictable ones.

And unpredictability is the enemy of resilience.

What Smart Organizations Are Doing Differently

Leaders who take risks seriously treat risk as more than technology. They build feedback loops into the human and procedural layers.

What that looks like in practice:

1. **Behavioral monitoring, not just system monitoring**

They regularly check for unapproved workflows, peer-to-peer knowledge transfer, and shadow procedures. They validate behavior through interviews, walk-throughs, and even ethnographic audits. 2. **Exception lifecycle governance**

Every temporary rule, account, or change gets a timebox and an owner. Nothing lingers by default. Some use automation to expire exceptions if not reviewed. 3. **Risk validation through walk-throughs**

Not every risk can be found from behind a console. Site visits and interviews reveal gaps that dashboards miss. They ask fundamental questions: “When's the last time this control was actually tested?” 4. **Drift tracking as a KPI**

Monitor deviation from SOPs over time. Treat procedural decay as a leading indicator of broader security gaps. Some organizations include this in monthly site-level health reports. 5. **Embedded ownership**

Rather than assigning all governance to GRC or security teams, they assign drift accountability to local leaders who know the context. 6. **Feedback loops with frontline workers**

They turn workers into sensors, inviting them to share where policy breaks down or gets bypassed, not to punish but to learn.

This is security as **continuous alignment**.

What You Can Do This Week

If you’re a plant or OT leader:

- Review your exception list. What’s still active? Who owns it?

- Ask operators what they do when the procedure doesn't work. Document it.
- Walk the site and spot the unofficial shortcuts. Don't assume they're wrong. Assume they're trying to adapt.

If you're a CISO or enterprise security leader:

- Include drift scenarios in tabletop exercises.
- Audit at least one high-trust access pathway (VPN, RDP, vendor tunnel) for credential sprawl.
- Add drift review to your incident post-mortems: what didn't go as expected?

If you're a COO:

- Ask your teams where process friction leads to shortcuts.
- Support efforts to embed feedback into frontline workflows, before audits expose the gaps.
- Consider drift exposure as a financial risk, because when it triggers an outage, it will be.

A Final Thought

The most dangerous vulnerabilities in OT aren't just digital.

They're procedural.

They're cultural.

They're the choices people make when no one's watching.

When left unchecked, those choices create fragility that no patch can fix.

The absence of a breach isn't proof of protection.

It might just be a sign that drift hasn't hit a tripwire yet.

If you don't track how practice diverges from policy, you're not managing risk. You're documenting hope.

Your Turn

Where in your operations might drift be silently accumulating?

And what would it take to surface it before it becomes your following incident?

HILLSTRONG GROUP SECURITY

FROM SIGNALS TO STRATEGY · CHAPTER FOUR

12 Plants, 12 Programs: Why Site-Level Risk Can't Scale

Enterprise OT resilience demands more than strong sites: it demands unified governance.

Every plant has a story. However, not every plant should have its own program.

> **"You don't need twelve programs. You need one model that flexes."**

In OT security, site-level autonomy has its place. Operational nuances, local vendor ecosystems, and legacy constraints shape risk management.

But the problem is that every site manages cyber risk differently, and leadership loses the ability to compare, prioritize, or act.

Twelve plants. Twelve scorecards. Twelve definitions of "done."

That isn't oversight. It's fragmentation. When a risk event occurs, there's no typical response, escalation path, or investment baseline.

What Fragmentation Looks Like in Practice

- One plant tags vulnerabilities by CVSS, another uses risk matrices, and a third uses a color-coded spreadsheet from 2018.
- Site A treats remote access as a business function, Site B treats it as an exception, and Site C has no idea who has access.
- Some sites log asset changes weekly as part of their management of change process (MOC), while others never do. One plant manually updates a Visio diagram after each project.

From HQ, the dashboard looks healthy. But underneath, it's a patchwork of workflows, standards, and assumptions.

Which means you can't answer:

- Where was the greatest exposure?
- Which sites need help first?
- Where should we invest?

And if you can't answer those questions, you're not managing your risk. You're reading plant-status reports. Even worse, you're implicitly telling your readership that there is no shared scale for risk across the business.

A Moment That Reframed the Problem

One manufacturing client told us, “We had five plants in the same country reporting completely different OT maturity levels, and the CISO had no idea who was right.”

The problem wasn’t dishonesty. It wasn't consistent.

Each plant was graded against a different rubric. One had a local consultant, another had a checklist from an old audit, one site’s OT lead was a former IT manager, and another had no security resource at all.

So when it came time to justify a capital request for upgrades, no one could defend the prioritization.

The board asked, “Which sites are most at risk?” No one could answer.

That’s when the CISO realized that maturity doesn't mean much without a unified lens for comparison. If every plant defines progress differently, there’s no credible way to defend investment, show improvement, or model enterprise risk.

The Cost of Inconsistency

A fragmented governance model carries real risk:

- **Inefficient spending:** Money goes to sites that advocate best, not those most at risk.
- **Audit exposure:** Without consistent documentation, global audits become site-by-site battles.
- **Cyber insurance complexity:** Underwriters struggle to evaluate program effectiveness without enterprise baselines.
- **Incident response delays:** Every incident is reinvented locally without standard escalation paths.
- **Lost trust:** When senior leaders realize that scorecards aren’t apples, they lose confidence in all of them.

Fragmentation creates a perception of maturity without the reality of coordination. And when leadership starts questioning the data, OT risk becomes more challenging to fund, defend, and improve.

Why Site-by-Site Doesn’t Work

Running OT security as twelve independent programs might seem workable in the short term. Each plant has its own budget, its own preferences, its own way of doing things. But this approach doesn’t scale. It fragments oversight, fractures trust, and prevents the organization from gaining any cohesive understanding of enterprise-wide exposure.

Over time, it creates:

- **Redundant tooling**
- **Inconsistent controls**
- **Unverifiable claims**
- **No roll-up view of enterprise exposure**

And when a centralized function (legal, finance, audit) asks for clarity, there’s no normalized way to provide it.

Worse, site-level independence creates hidden inequities:

- Sites with strong leaders get support.
- Sites with weak governance fly under the radar.
- Sites with low maturity avoid scrutiny by reporting success in local terms.
- Sites with unofficial tools and shadow-IT setups bypass standard protocols altogether, introducing risk that's invisible to enterprise oversight.

Shadow-IT often starts with good intentions, a local engineering team solving a problem fast. But over time, these unapproved systems create data silos, inconsistent practices, and security gaps that can't be seen, let alone managed.

Without enterprise alignment, those gaps become permanent.

That's not a strategy. That's *organizational drift*.

What Smart Organizations Are Doing Differently

The most mature organizations aren't forcing uniformity. They're defining a real model.

Here's how it works:

1. **Here are the sites by criticality and risk**

Define 3–4 archetypes based on impact, complexity, and sensitivity. For each tier, define what good looks like. 2. **Assign operating expectations by tier.**

Tier 1 sites might need complete segmentation of the process control network from the control system network, always-on monitoring, and quarterly audits. Tier 3 sites may focus on hardening and response preparedness. 3. **Centralized assessment, decentralized action.**

Use shared tools and metrics to assess risk consistently. Let sites own execution within guardrails. 4. **Create an enterprise control plane.**

Consolidate reporting, risk scoring, and escalation into a shared environment. Normalize, compare, and prioritize risk across all sites. 5. **Use the same metrics everywhere.**

Every site reports in the same terms: exposure, consequence, coverage. Not local flavors. 6. **Provide support where it's needed.**

Shared services, regional support teams, or embedded OT security leads provide programmatic help to high-risk, low-maturity sites.

This is how governance scales, not by dictating every controversy but by harmonizing how risk is understood.

And that understanding enables strategic decisions:

- Where to invest
- What to defer
- Who to empower

What You Can Do This Week

If you're an OT lead:

- Ask how your plant compares to others. Are you speaking the same language?
- Push for shared definitions of risk, impact, and readiness.
- Volunteer your site for a pilot of the tiered governance model.

If you're an enterprise risk lead:

- Inventory your governance models. How many different “programs” are you really running?
- Draft an OT site tiering model with 3–4 risk-based categories.
- Define core metrics every site must report, then validate with plant leads.

If you're a COO, push for a unified view of OT risk across your facilities.

- Prioritize investment based on tier, not noise.
- Set a 12-month target to align all sites to a common reporting framework.

A Final Thought

Enterprise resilience isn’t about being perfect. It’s about the site being understood and every risk being measurable, comparable, and actionable.

You don’t need twelve programs. You need one framework that flexes.

Because if you can’t scale your model, you can’t scale your protection.

And if you can’t compare sites, you can’t protect them equally.

Your Turn

How many different OT security programs are you really running?

And what would it take to unify them without losing local control?

HILLSTRONG GROUP SECURITY

FROM SIGNALS TO STRATEGY · CHAPTER FIVE

What Is Operational Risk Costing You?

Why is treating OT cyber risk as a budget-neutral technical problem costing you far more than you think?

> **"If OT risk isn't on your balance sheet, you're not managing it. You're absorbing it."**

Operational risk is expensive.

But not in the way most people *think*.

It's not just about breach response, hardware upgrades, or insurance premiums. Those are the visible costs. The ones that show up in budget cycles and project justifications.

The real cost of operational risk is hidden in:

- Downtime you can't predict
- Premiums you can't negotiate
- Contracts you can't win
- Brand damage you can't unsee

And the longer risk goes unquantified, the more it compounds quietly, invisibly, until it surfaces, often *too late*.

What Operational Risk Really Looks Like

Let's get specific.

It looks like:

- A five-hour outage at a regional plant that missed its shipping window triggered $1.2M in expedited logistics and penalties.
- A quarterly review where no one could explain the difference between patch coverage at Plant A and Plant B, so the board held funding.
- A missed opportunity to bid on a government contract because the OT environment lacked documented segmentation and control audit review processes.
- An external audit from a global supplier flagged inconsistent security controls between two similar plants. That finding delayed a multimillion-dollar contract renewal by six weeks, as procurement teams had to manually review every OT site's security posture. The lost time (and the perception of immaturity) resulted in a pricing concession and a downgrade in vendor risk score.

These are the costs that don't show up in your cybersecurity line item. But they're real. And they add up *fast*.

Why You're Not Seeing the Cost

Most organizations don't consider OT risk because they've never *had* to.

Risk has traditionally been viewed as a compliance function: something to check, document, and pass. However, that lens is outdated as threat actors get smarter and regulatory environments get stricter.

Today, OT risk is:

- A financial liability
- A procurement blocker
- A reputational exposure
- A board-level concern

But most dashboards still measure vulnerabilities.

Most scorecards still show maturity.

Very few convert risk into impact.

That's the *problem*. Until OT risk is translated into financial language, financial leaders won't *prioritize* it.

A Real-World Flashpoint

We worked with a global food and beverage company operating 19 plants. Their OT security leader was sharp, engaged, and diligent. He'd built strong controls at four flagship sites and pushed for broader investment.

But every time he went to the CFO, he got the same response:

"We haven't been hit. Why spend *now*?"

Then came a supply chain disruption at a Tier 2 plant. What looked like a brief system slowdown turned out to be unauthorized remote access that had gone unnoticed for weeks. It wasn't a breach. But it triggered a shutdown, a root cause investigation, and weeks of cleanup.

Final cost? Over $3.8 million.

When the board reviewed the incident, they asked: "Why wasn't this flagged?"

The answer wasn't lack of *data*. It was lack of financial *framing*.

The Five Cost Categories of OT Risk

To elevate OT risk to the boardroom, move beyond threat severity and discuss exposure cost.

Here are five categories every OT leader should know:

1. Downtime & Production Loss
2. Safety & Incident Response
3. Compliance & Insurance
4. Contract & Market Risk

5. Reputation & Recovery

How to Start Costing Risk

If you're not ready to model all of this in dollars, start with something *simpler*:

Identify the top 5 most critical OT assets or processes:

- Estimate what an hour of downtime costs for each
- Map known risks to those systems
- Ask: "What's the probability of disruption over the next year?"
- Multiply that by the estimated impact

Congratulations. You now have a risk-adjusted exposure estimate.

It's not perfect. But it's better than a red-yellow-green heatmap that no one believes.

From there, you can refine. Add historical incident data. Factor in compensating controls. Incorporate time to recover.

The point isn't precision. The point is conversation.

What Smart Organizations Are Doing Differently

The most forward-leaning teams are integrating OT cyber into their enterprise risk quantification models.

They're not just asking "What might go *wrong*?

They're asking:

- "What would that *cost* us?"
- "What's our exposure delta if we delay investment by six months?"
- "How does this plant compare to others on cost-weighted risk?"

They present OT risks in the same framework as capital projects, regulatory liabilities, or environmental exposures.

And suddenly, OT isn't a silo. It's a *strategic* lever.

What You Can Do?

If you're an OT or site lead:

- Identify your plant's top revenue-generating processes
- Document potential risks to each, and estimate the downtime impact
- Present that to your plant manager in dollars, not alerts

If you're a CISO or enterprise risk lead:

- Meet with finance and operations to align on risk costing assumptions
- Develop a cross-functional task force to build exposure models across high-risk sites

- Prepare your next board update with risk quantified in cost, not color codes

If you're a COO or CFO:

- Ask your teams for a dollarized view of your top 3 OT risks
- Use that data to inform your next budget, insurance, or M&A decision
- Start treating OT resilience as a financial discipline, not just a technical one

A Final Thought

You can't manage what you can't *measure*.

And right now, most organizations are mis-measuring OT risk by measuring activity instead of impact.

The board doesn't care about how many devices were scanned. They care about what it would cost to lose the line.

If we want OT cyber to be taken seriously at the executive level, we need to speak the language that moves budgets, changes minds, and protects what matters most.

And that language is value.

Your Turn

What is operational risk really costing you today?

And how much longer can you afford not to know?

About the Author



Roger Hill

CEO, Hillstrong Group Security, Inc.

Roger brings over 30 years of experience in industrial automation and cybersecurity. His extensive background in OT security has positioned him as a trusted advisor to CISOs across various industries. His expertise lies in developing and implementing robust OT GRC programs that address the unique challenges faced by global manufacturing operations.

Throughout his career, he has been dedicated to helping organizations achieve operational resilience through strategic security initiatives and pragmatic solutions. His commitment to excellence and deep understanding of the intricacies of OT systems have earned him a reputation as a pioneer in the field. Roger's methodologies continue to drive the development of secure and compliant OT environments for leading manufacturing companies worldwide.

HILLSTRONG GROUP SECURITY

About Hillstrong Group Security, Inc.

Hillstrong Group Security, Inc. is an operational-technology cybersecurity consultancy helping industrial and critical-infrastructure operators build security programs that hold up across their regulatory, product, service, and grid obligations. Blending OT, IoT, and ICS expertise, Hillstrong partners with companies in energy, manufacturing, water, chemicals, food and beverage, automotive, and other essential sectors to achieve operational resilience. Every engagement starts on the plant floor, hands-on and on-site, not on a remote scan.

Our Core Services

- OT Security Maturity Assessments
- OT Risk & Vulnerability Analysis
- OT Program Design & Governance
- Expert-Level OT Security Engineering
- Fractional CISO & Advisory Support
- OT Governance, Risk & Compliance (GRC) as a Service
- OT Staff Augmentation & Contract Specialists
- Resilion.io, AI Execution Engine for OT Cybersecurity

Resilion.io is Hillstrong's AI-powered OT cybersecurity platform, delivering continuous visibility, risk quantification, and program execution (build, execute, manage), so assessment findings translate into measurable resilience.

www.hillstrongsecurity.com · Based in Atlanta, GA · Solving cybersecurity challenges globally