HILLSTRONG GROUP SECURITY

HILLSTRONG · THOUGHT LEADERSHIP

Bridging Gaps

A Pragmatic Approach to OT Cybersecurity

Roger Hill | CEO, Hillstrong Group Security, Inc.

hillstrongsecurity.com

Contents

CHAPTER ONE	Building Consensus
CHAPTER TWO	Scaling Security
CHAPTER THREE	Mastering Regional Regulations in a Global Compliance Framework
CHAPTER FOUR	Turning Audit Results into Actionable Security Improvements
CHAPTER FIVE	Bringing the Board on Board
CLOSING THOUGHTS	OT Security as a Strategic Advantage
	About the Author
	About Hillstrong Group Security, Inc.

HILLSTRONG GROUP SECURITY

BRIDGING GAPS · CHAPTER ONE

Building Consensus

Making the Business Case for OT Security

Operational technology (OT) security has moved beyond being just a technical concern: it's a critical business priority. For CISOs and CIOs, the challenge isn't just identifying risks; it's building the internal consensus needed to secure investments, align strategies, and drive meaningful change. Success hinges on connecting OT security to business value, operational goals, and long-term resilience.

This chapter delves into how to make a compelling case for OT security, framed in terms that resonate with C-suite stakeholders. By emphasizing the operational mission and aligning security initiatives with core business drivers, CISOs and CIOs can bridge organizational silos and drive effective collaboration.

Framing OT Security as Business-Critical

To build consensus, the conversation must move away from technical jargon and focus on what matters most to the organization: ensuring safety, sustaining operations, and protecting revenue. OT security must be framed as integral to the company's operational mission, which typically includes:

- **Human Safety:** Protecting employees and contractors from harm caused by compromised systems or malicious actors.
- **Environmental Stewardship:** Ensuring systems remain secure to prevent incidents that could result in ecological damage or regulatory penalties.
- **Production Continuity:** Safeguarding uptime to avoid disruptions impacting supply chains and customer commitments.
- **Product Integrity:** Protecting the quality of goods and ensuring they meet standards to avoid recalls or reputational harm.
- **Data Protection:** Ensuring operational and production data remain secure and accurate to maintain decision-making integrity.

A critical part of this narrative is showing how OT security protects these pillars. For example, could you highlight how segmentation prevents ransomware from propagating through the network, safeguarding production schedules, and protecting sensitive data? By tying technical controls to tangible business outcomes, security leaders can make OT security relatable to their peers in operations and finance.

Engaging Stakeholders Across the Organization

For CISOs and CIOs, stakeholder engagement is not optional: it's foundational. Building consensus means meeting leaders where they are, addressing their concerns, and framing security as a shared responsibility. Key stakeholder groups include:

- **CFOs:** Focused on ROI, cost efficiency, and avoiding unplanned financial hits. For them, emphasize the cost of inaction (lost revenue, regulatory fines, or reputational harm) compared to the investment in proactive measures.
- **COOs and Plant Managers:** Concerned with uptime, productivity, and efficiency. Highlight how OT security minimizes operational disruptions and enables sustained production.
- **Compliance Officers:** Tasked with meeting regulatory mandates and avoiding penalties. Tie OT security to frameworks like NIST CSF or NIS2 and explain how it streamlines compliance efforts.
- **IT and OT Teams:** Balancing performance and security. Show how a collaborative approach can strengthen the IT-OT relationship, reducing friction and delivering better outcomes.

Tailor the messaging when engaging these groups. For example, financial models should be used when presenting to CFOs, but operational scenarios should be used when talking with COOs. Case studies and real-world examples can bridge gaps, showing how similar organizations have successfully navigated OT security challenges.

Quantifying Risks and Benefits

Boards and executives respond to data. To drive home the importance of OT security, quantify risks and opportunities with hard numbers:

- **Risk Quantification:** Calculate the potential financial impact of an attack. For instance, a ransomware event that halts production at a critical facility for 24 hours could result in millions in lost revenue, delayed shipments, and damaged relationships with key customers.
- **Opportunity Quantification:** Demonstrate the upside of investing in security. For example, implementing predictive maintenance tools tied to OT security could reduce unplanned downtime by 30%, yielding substantial savings.

Beyond immediate impacts, emphasize systemic risks. Discuss how vulnerabilities at one facility could cascade across the supply chain, amplifying financial and reputational damage. Present these dynamics using visual aids, like risk heatmaps.

Collaborating on a Strategic Roadmap

Collaboration is essential for alignment. Building a strategic roadmap allows stakeholders to see a clear, actionable plan that ties security investments to measurable outcomes. Key components include:

- **Clear Objectives:** Define goals, such as achieving compliance with a specific standard, reducing response times, or implementing segmentation across critical sites.
- **Prioritized Milestones:** Break the roadmap into phases, focusing on high-impact areas first. For example, start with vulnerability assessments at strategic sites, then scale to smaller facilities.

- **Resource Allocation:** Be transparent about what's needed (budget, personnel, and tools) and explain how these investments support the business.

Involve cross-functional teams in roadmap development to foster buy-in. Engaging operations, finance, and compliance leaders ensures the plan is practical and aligned with broader business priorities. When stakeholders see their input reflected in the strategy, they're more likely to support it.

Communicating the ROI of OT Security

Securing investment requires translating technical initiatives into business value. CISOs and CIOs must connect the dots between security measures and financial outcomes. Strategies include:

- **ROI Models:** Show how proactive investments reduce long-term costs. For instance, the expense of deploying advanced monitoring tools can be compared with the financial losses avoided by preventing a significant incident.
- **Scenario Analysis:** Use hypothetical or real-world examples to illustrate risks. Explain how a phishing attack targeting OT systems could escalate into a supply chain disruption, costing millions.
- **Benchmarking:** Compare the organization's security posture to industry peers, highlighting gaps and opportunities to lead rather than follow.

Visuals like dashboards, cost charts, and trend analyses can make complex information digestible. Tailor these materials to the audience, ensuring they align with their decision-making style and priorities.

Takeaways for CISOs and CIOs

Building consensus for OT security requires more than technical expertise. It demands strategic communication and alignment. By framing security as a business enabler, quantifying its value, and effectively engaging stakeholders, CISOs and CIOs can secure the buy-in needed to drive meaningful change.

Remember, the goal isn't just to secure funding. It's to foster a culture where OT security is considered integral to the organization's mission. With clear messaging, actionable roadmaps, and a collaborative approach, OT leaders can position security as a safeguard and a strategic advantage, ensuring resilience in an increasingly complex threat landscape.

HILLSTRONG GROUP SECURITY

BRIDGING GAPS · CHAPTER TWO

Scaling Security

Tailoring Programs for Distributed Organizations

Scaling an operational technology (OT) cybersecurity program across a global enterprise requires balancing a centralized strategy and localized execution. For CISOs and CIOs, the challenge extends beyond deploying tools or meeting regulatory requirements: it's about ensuring business continuity, strengthening operational resilience, and safeguarding revenue streams on a large scale. Each site within a global organization has distinct risks, operational dynamics, and maturity levels, necessitating a tailored and strategic approach to security.

This chapter explores how leaders can create scalable OT security programs that address the complexities of diverse, geographically distributed operations while aligning with strategic business objectives.

Establishing a Centralized Strategy with Localized Flexibility

At its core, a scalable OT security program begins with a strong centralized framework. This framework provides consistency in governance, policy, and oversight while allowing individual sites to adapt implementation based on their unique contexts.

Centralized strategies should focus on:

- **Universal Policies:** Core requirements such as access control, network segmentation, and incident response protocols must be standardized across the organization.
- **Governance Models:** Clear lines of accountability, with central oversight ensuring alignment while empowering local teams to act within defined boundaries.
- **Standardized Toolsets:** Deploy a standard suite of monitoring, detection, and compliance management tools to simplify integration and provide uniform data visibility.

Flexibility is equally critical. A European production plant adhering to the NIS2 Directive may require a different compliance timeline than a Southeast Asian site focused on supply chain efficiency. Allowing localized customization within a centralized framework ensures that security measures are practical and effective.

Mapping and Prioritizing Operational Risks

CISOs and CIOs must map the organization's operational landscape to scale effectively, categorizing sites based on their criticality and risk profiles. This process involves:

- **Tiering Sites:** Segment facilities into strategic, supportive, and peripheral tiers based on their operational and financial importance. For example, a strategic site producing unique components for a global supply

chain demands advanced threat detection capabilities, while peripheral sites may require only baseline controls.

- **Interdependency Analysis:** Document interdependencies between sites. For instance, a ransomware attack on a peripheral facility could cascade into delays at a strategic plant reliant on shared systems.
- **Risk Modeling:** Conduct scenario planning to assess the potential impact of disruptions, such as downtime costs, safety incidents, or regulatory penalties. Quantifying these risks enables data-driven prioritization.

By aligning resources with each site's criticality, security leaders can ensure that investments deliver the most significant operational and financial impact.

Leveraging Technology to Enable Scalability

Technology is critical in scaling OT security programs, but success requires selecting tools that align with the operational realities of OT environments. While certain technologies are supportive, others take center stage in addressing unique OT challenges. The following strategies reflect these realities:

Centralized Visibility:

- Tools like Security Information and Event Management (SIEM) platforms offer value as ancillary controls, providing a unified view across IT and OT environments. However, in OT systems, particularly at Level 2 with embedded or RTOS devices, most assets lack the event capability to support SYSLOG. This limitation makes SIEMs insufficient as standalone solutions for detecting security events. Instead, they should complement more OT-specific technologies. In addition, OT security correlation rules should be much more operational-centric vs. DNS-centric.
- **OT Network Threat Detection:** Industrial networks demand specialized threat detection solutions to characterize, understand, and identify risks. These tools analyze communication patterns, protocols, and device behaviors unique to OT environments. Organizations can detect anomalies and threats even in systems where endpoint telemetry is unavailable by focusing on network-level visibility.
- **Mitigation Over Automation for Patching:** Automation for patch management in OT remains impractical given the lack of tools that understand OT-specific contexts, such as compatibility with unique configurations or vendor-required testing cycles. Instead, mitigation through alternative controls (such as network segmentation, compensating measures, or robust vulnerability management frameworks) offers a more realistic and practical approach to reducing risk. Having a robust OT vulnerability management process is crucial.

Robust training programs must support the adoption of these technologies. Centralized training initiatives should educate local teams on how to use tools effectively, detect and respond to threats, and implement mitigation strategies tailored to their environments. Empowering teams with these skills ensures that technology investments translate into actionable improvements in security.

Addressing Cultural and Regional Differences

Scaling across global operations requires sensitivity to cultural and regulatory nuances. Resistance to centrally mandated security measures often stems from misalignment with local priorities. To navigate this challenge:

- **Engage Local Leaders:** Involve site managers and regional teams in designing and rolling out security initiatives. Their input ensures measures are practical and builds buy-in.
- **Tailored Training:** Develop region-specific training programs that address local regulatory requirements, such as GDPR compliance in Europe or CISA guidelines in the U.S.
- **Localized Communication:** Translate policies and resources into local languages and contexts, demonstrating respect for regional differences and fostering understanding.

Building trust at the local level is essential for successful implementation. Regular site visits by central teams and collaborative workshops can bridge gaps and reinforce alignment.

Establishing Feedback Loops and Continuous Improvement

A scalable security program isn't static; it evolves. Embedding continuous feedback mechanisms ensures the program adapts to emerging risks and operational changes.

- **Metrics and Reporting:** Establish KPIs that measure program effectiveness, such as time to remediate vulnerabilities, compliance rates, and incident response times. Use these metrics to inform strategy adjustments.
- **Local Feedback Channels:** Create forums or committees where site teams can share challenges, successes, and lessons learned. This bottom-up feedback is invaluable for refining policies and identifying gaps.
- **Audit Cycles:** Regularly audit sites to assess policy adherence and identify improvement opportunities. Audits should prioritize high-risk or strategic sites and cycle through supportive and peripheral locations.

Investing in a continuous learning culture supported by data-driven insights ensures the program remains resilient and responsive.

Takeaways

Scaling an OT security program across distributed operations requires more than deploying tools and policies. It demands strategic alignment, adaptability, and collaboration. CISOs and CIOs who succeed in this endeavor focus on:

- Building a centralized framework that allows for local flexibility.
- Prioritizing investments based on site criticality and operational risk.
- Leveraging technology to provide visibility and automation at scale.
- Addressing cultural differences and engaging local teams as partners.
- Embedding continuous improvement mechanisms to adapt to evolving challenges.

The result is a secure operational environment and a more resilient and efficient organization. By balancing consistency with adaptability, CISOs and CIOs can ensure their OT security programs are scalable, sustainable, and aligned with the organization's strategic goals.

HILLSTRONG GROUP SECURITY

BRIDGING GAPS · CHAPTER THREE

Mastering Regional Regulations in a Global Compliance Framework

CISOs and CIOs managing OT cybersecurity for global enterprises face an immense challenge: aligning a patchwork of regional regulations with the organization's overarching compliance strategy. While compliance often begins as a reactive necessity, successful leaders use it as a strategic enabler to enhance security, drive operational excellence, and maintain access to critical markets.

This chapter provides a roadmap for navigating the complexities of regional regulations, integrating them into a cohesive global strategy, and ensuring alignment with business goals. By understanding regional nuances, building scalable frameworks, and embedding flexibility, CISOs and CIOs can turn compliance into a competitive advantage.

Understanding the Global Regulatory Patchwork

Each region approaches OT security and compliance with unique priorities. North America, for instance, emphasizes risk-based frameworks like NIST 800-82, which offer flexibility for critical infrastructure sectors. The NIS2 Directive mandates prescriptive measures in Europe, including incident reporting and cross-border collaboration. Asia often prioritizes supply chain security, reflecting the region's role as a global manufacturing hub.

For CISOs and CIOs, navigating this patchwork begins with thoroughly mapping regulatory requirements across operating regions. This involves:

1. **Identifying Core Requirements:** Catalog the specific mandates of each regulation, such as reporting timelines, technical controls, or audit expectations.
2. **Comparing Overlaps and Gaps:** Determine where existing policies meet multiple regulations and where adjustments are necessary.
3. **Aligning With Business Priorities:** Ensure compliance efforts support broader goals, such as maintaining uptime, accessing new markets, or enhancing customer trust.

Regional nuances also play a critical role. For example, Europe's focus on data protection stems from its strong privacy and regulatory culture, while North America prioritizes operational resilience. Tailoring compliance strategies to reflect these nuances helps balance regulatory adherence with operational feasibility.

Building a Centralized Compliance Framework

A centralized compliance framework forms the foundation of a scalable OT security program. It provides consistency across global operations while allowing localized adaptations to meet specific regulatory demands.

Key elements of a robust framework include:

- **Risk Management Protocols:** Regularly assess vulnerabilities and allocate resources based on risk severity and site criticality.
- **Unified Policies and Standards:** Establish baseline controls for network segmentation, access management, and incident response.
- **Continuous Monitoring:** Deploy tools with real-time visibility into compliance performance across all sites.

While centralization ensures consistency, rigidity can backfire. Flexibility is essential. For instance, adapting the framework to meet NIS2's incident reporting timelines in Europe without disrupting global consistency ensures compliance and practicality.

Technology enables operationalizing these frameworks. Centralized compliance platforms can automate policy updates, streamline reporting, and aggregate insights into unified dashboards. These tools empower CISOs and CIOs with the data needed to make informed, timely decisions.

Addressing Infrastructure Maturity Across Sites

Global operations often include sites with vastly different levels of infrastructure maturity. Modern facilities may have advanced cybersecurity measures, while legacy sites struggle with outdated systems. Addressing these disparities is critical for achieving consistent compliance outcomes.

Steps to address infrastructure maturity include:

1. **Conducting Site Assessments:** Evaluate each facility's current capabilities, categorizing them as modern, intermediate, or legacy.
2. **Prioritizing Investments:** Direct resources toward high-risk sites with the most significant potential impact on overall operations.
3. **Phased Modernization:** Implement foundational controls at legacy sites (such as segmentation and access controls) before deploying advanced solutions like predictive analytics.

Investments in modernization are not just technical decisions. They're strategic imperatives. Demonstrating how these upgrades mitigate risks and support business objectives strengthens the case for funding.

Incorporating Capability Models: IOC and FOC

Capability models like Initial Operating Capability (IOC) and Future Operating Capability (FOC) provide a structured approach to scaling compliance and security measures across diverse sites.

IOC: Focuses on establishing foundational controls, such as basic segmentation, access management, and incident detection capabilities. Achieving IOC ensures all sites meet baseline compliance requirements, mitigating the most immediate risks.

FOC: Builds on the IOC foundation, advancing security measures with advanced monitoring, predictive analytics, and automated risk assessments. FOC ensures continuous improvement and positions the organization as a leader in operational resilience.

By defining clear milestones for IOC and FOC, CISOs and CIOs can prioritize investments, allocate resources strategically, and measure progress effectively. This phased approach ensures scalability without overwhelming local teams.

Maintaining Consistency Without Micromanagement

Balancing global consistency with local autonomy is one of the most significant challenges in scaling compliance. A rigid, top-down approach risks alienating local teams and stifling innovation. Conversely, too much independence can lead to fragmentation and inconsistencies.

Decentralized governance offers a middle path. This approach establishes:

- **Clear Global Standards:** Define non-negotiable policies for critical areas like incident reporting and vendor management.
- **Localized Adaptations:** Empower regional teams to tailor implementation based on local regulations and operational realities.
- **Transparent Oversight:** Use centralized platforms to track adaptations, ensuring deviations are well-documented and justified.

Regularly engaging regional leaders fosters collaboration and trust. For example, hosting quarterly compliance forums where teams share challenges and successes ensures alignment and continuous learning.

Navigating Cultural and Operational Differences

Compliance is not just a regulatory exercise. It's a cultural one. Local resistance often stems from a perceived disconnect between centrally imposed mandates and site-specific priorities. Overcoming this requires empathy, collaboration, and clear communication.

Effective strategies include:

- **Involving Local Leaders:** Engage site managers early in compliance to incorporate their insights and build buy-in.
- **Region-Specific Training:** Tailor training programs to address cultural and regulatory differences, ensuring relevance and accessibility.
- **Celebrating Local Wins:** Recognize and share examples of sites that excel in compliance, fostering a culture of shared success.

By respecting regional nuances, CISOs and CIOs can strengthen relationships and drive more effective implementation.

Future-Proofing the Compliance Program

Regulations constantly evolve, driven by technological advances, geopolitical shifts, and emerging threats. Futureproofing ensures the organization's compliance program remains resilient and adaptable.

Key strategies include:

- **Proactive Monitoring:** Stay ahead of regulatory changes through industry partnerships, conferences, and advisory services.
- **Feedback Loops:** Regularly gather input from site teams to refine policies and address gaps.
- **Adaptive Tools:** Use cloud-based platforms that seamlessly incorporate new requirements, reducing the burden of manual updates.

Embedding flexibility and continuous improvement into the compliance framework positions the organization to navigate future challenges confidently.

Takeaways

Mastering regional regulations in a global compliance framework is a complex but achievable goal. Organizations can create a scalable and resilient compliance program by understanding the regulatory landscape, building a centralized yet flexible framework, and addressing infrastructure disparities.

Equally critical is the human element. Engaging local teams, respecting cultural differences, and fostering collaboration ensure compliance becomes an integrated part of operations rather than a disruptive mandate. Future-proofing efforts, supported by adaptive technologies and continuous feedback, position the organization to thrive in an ever-evolving landscape.

For CISOs and CIOs, the opportunity lies in transforming compliance from a cost center into a driver of operational excellence and strategic advantage. They can ensure adherence and enduring success by aligning regulatory efforts with business goals.

HILLSTRONG GROUP SECURITY

BRIDGING GAPS · CHAPTER FOUR

Turning Audit Results into Actionable Security Improvements

Audits often evoke a sense of compliance-driven obligation. However, for CISOs and CIOs, audits can be powerful tools to uncover opportunities to enhance OT security and operational resilience. When viewed strategically, audit results become more than a checklist: they catalyze meaningful, scalable improvements across a distributed enterprise.

This chapter explores transforming audit findings into actionable insights that align with the organization's business objectives. By prioritizing risks, engaging stakeholders, and embedding continuous improvement, CISOs and CIOs can ensure that audit results drive measurable impact and long-term value.

Interpreting Audit Findings in a Strategic Context

Audit findings include critical gaps, minor oversights, and systemic inefficiencies. Interpreting these findings strategically begins with understanding their potential business impact. For CISOs and CIOs, this involves mapping findings to operational priorities and aligning remediation efforts with site criticality.

- **Strategic Sites:** A vulnerability at a strategic site (such as a plant producing high-value components) might pose a significant risk to supply chain continuity. Addressing such findings should take precedence.
- **Supportive Sites:** Findings at supportive sites often reveal opportunities to standardize processes, such as implementing uniform OT vulnerability management or access control protocols.
- **Peripheral Sites:** Issues at peripheral sites may have limited direct impact but can still expose the organization to cascading risks. These findings should focus on efficiently achieving baseline compliance.

Using a risk-based framework helps prioritize findings by their potential to disrupt operations, incur financial losses, or violate compliance mandates. For instance, consider the economic and reputational implications of a ransomware attack on a strategic site versus the administrative inefficiencies uncovered at a smaller facility.

Developing a Targeted Remediation Plan

An effective remediation plan addresses immediate risks while laying the groundwork for long-term improvements. This requires clear prioritization of audit findings and actionable steps to resolve them.

1. **Critical Vulnerabilities:** Implement immediate fixes for high-impact findings, particularly at strategic sites. Examples include improving segmentation to prevent lateral movement or deploying anomaly detection tools for real-time monitoring.
2. **Process Standardization:** Establish uniform practices at supportive sites to address systemic issues. Standardizing incident response protocols across sites ensures consistency in handling threats.
3. **Scalable Solutions:** Focus on cost-effective, scalable measures such as automating compliance reporting or implementing cloud-based monitoring solutions for peripheral sites.

Each remediation effort should be tied to measurable outcomes, such as reducing the time to detect and respond to threats or achieving compliance with specific regulations. Establishing timelines and accountability ensures that the plan drives results without overburdening teams.

Communicating Findings and Gains to Leadership

Audit findings must be communicated in terms that resonate with the board and C-suite to secure executive buy-in for remediation efforts. This involves translating technical details into business-relevant narratives.

- **Quantify Risks:** Highlight the potential financial and operational consequences of inaction. For example, a critical vulnerability can be framed as a possible $5 million downtime risk supported by industry benchmarks or historical data.
- **Emphasize ROI:** Show how addressing audit findings delivers value, such as avoiding regulatory penalties or improving production uptime. Use case studies from similar organizations to reinforce your message.
- **Provide a Clear Plan:** Present a prioritized action plan that aligns with business goals, including timelines, budgets, and expected outcomes. Dashboards and visual tools can help simplify complex findings.

Engaging leadership through these narratives secures funding and positions the CISO or CIO as a strategic partner in driving organizational resilience.

Embedding Continuous Improvement Across Sites

Audits should not be isolated events. Instead, they should feed into a continuous improvement cycle that strengthens the organization's OT security posture over time.

- **Regular Audits:** Conduct audits on a rotational basis, prioritizing high-risk sites while ensuring all locations are reviewed periodically. This provides sustained oversight.
- **Feedback Loops:** Create mechanisms for local teams to share challenges and successes in implementing audit recommendations. This bottom-up feedback informs policy adjustments and identifies best practices.
- **Metrics and Monitoring:** Establish KPIs to track progress, such as the percentage of findings resolved within a set timeframe or improvements in compliance scores. Regularly review these metrics to assess program effectiveness.

For example, a site that successfully implements a new access control measure could share its approach with other locations, accelerating organizational improvements. Encouraging cross-site collaboration fosters a culture of shared learning and accountability.

Leveraging Technology for Scalable Auditing

Technology is a force multiplier for scaling audit improvements across a distributed enterprise. Tools that automate key aspects of the audit process enable consistency, efficiency, and scalability.

- **Automated Compliance Management:** Deploy platforms that track audit findings, assign remediation tasks, and generate real-time progress reports.
- **Predictive Analytics:** Use technology tools to identify patterns and predict risks before they become critical issues. For instance, predictive maintenance software can preemptively address equipment risks tied to OT systems.
- **Integrated Dashboards:** Centralized dashboards provide a unified view of compliance and risk metrics, enabling leadership to make data-driven decisions.

Adopting these technologies ensures that audit programs remain agile and capable of addressing the complexities of global operations.

Fostering a Culture of Accountability and Engagement

The success of any audit-driven improvement program hinges on organizational culture. Building a culture that values accountability and proactive security requires:

- **Leadership Commitment:** Senior leaders must champion audit-driven improvements, emphasizing their importance during town halls, strategy meetings, and performance reviews.
- **Incentives and Recognition:** Recognize teams that excel in implementing audit findings through formal awards or public acknowledgment. This motivates others to follow suit.
- **Training and Development:** Equip local teams with the skills needed to address audit findings effectively, from technical training on new tools to workshops on regulatory changes.

Embedding accountability into performance metrics ensures that security becomes a shared responsibility rather than a siloed function.

Takeaways

Turning audit results into actionable improvements requires more than technical fixes. It demands a strategic approach that aligns remediation efforts with business objectives, engages leadership, and leverages technology to scale solutions globally.

For OT Security leaders, audits are not just checkpoints: they are opportunities to drive operational resilience, enhance compliance, and secure the organization against emerging threats. By fostering a culture of continuous improvement and aligning efforts with site criticality, security leaders can ensure that audit results translate into long-term value and competitive advantage.

HILLSTRONG GROUP SECURITY

BRIDGING GAPS · CHAPTER FIVE

Bringing the Board on Board

How to Communicate OT Risk and Compliance

For CISOs and CIOs, effectively engaging the board on operational technology (OT) security and compliance is a strategic imperative. Boards now understand the importance of cybersecurity, but the challenge lies in translating complex technical risks into actionable insights that resonate with their priorities. Successful communication secures funding and elevates OT security to a business-critical priority.

This chapter outlines strategies for engaging the board, aligning security efforts with business objectives, and ensuring their commitment to long-term OT resilience.

Framing OT Risk in Business Terms

To connect with the board, OT risks must be framed regarding their impact on business operations and financial outcomes. For example, instead of describing a "vulnerability in an industrial control system (ICS)," explain how exploiting that vulnerability could halt production at a flagship plant, resulting in millions of dollars in lost revenue.

The focus should be on translating risks into measurable impacts:

- **Revenue Impact:** Highlight potential losses due to downtime or supply chain disruptions.
- **Regulatory Fines:** Quantify penalties associated with non-compliance.
- **Reputation Damage:** Discuss how breaches could erode customer trust or damage brand value.

Data-driven narratives resonate best. Use scenarios and metrics to articulate risks. For instance, "A ransomware attack targeting our strategic plant could result in a $5 million loss over 24 hours, plus $500,000 in recovery costs. Implementing enhanced segmentation and monitoring tools would reduce this risk by 80%."

Aligning Compliance with Strategic Objectives

Compliance is often seen as a regulatory requirement but can also be considered a competitive advantage. Boards care about growth, efficiency, and resilience, and aligning compliance with these goals ensures their attention.

- **Operational Continuity:** Emphasize how compliance measures reduce unplanned downtime and ensure consistent production schedules.
- **Market Access:** Highlight how meeting international standards like NIS2 or CISA requirements enables operations in key markets.

- **Brand Reputation:** Demonstrate how proactive compliance strengthens customer trust and differentiates the organization in competitive markets.

Tie compliance investments to tangible outcomes. For example, explain how automating compliance reporting reduces manual effort by 40%, allowing teams to focus on strategic initiatives. Case studies from industry peers can reinforce the value of these efforts.

Building a Clear Action Plan for Investment

Boards need clarity on where their investments will go and what outcomes they will drive. A structured action plan helps bridge this gap.

- **Prioritize by Impact:** Categorize security initiatives based on their potential to mitigate risks or enable strategic goals. Focus initial efforts on high-impact areas, such as implementing advanced threat detection at strategic sites.
- **Define Measurable Outcomes:** Set clear goals, such as reducing incident response times by 50% or achieving compliance certifications within six months.
- **Create a Timeline:** Outline a phased approach with quick wins to demonstrate immediate value while building toward long-term objectives.

Visual tools like dashboards and roadmaps simplify complex plans, making them accessible to board members and reinforcing confidence in the strategy.

Crafting Compelling Narratives for Engagement

Boards respond to stories that illustrate both risks and opportunities. Crafting a compelling narrative involves blending data with relatable scenarios.

For instance, present a hypothetical “day in the life” scenario of a cyber incident. Walk the board through:

1. **The Attack:** A phishing email that compromises a system supporting OT, spreading ransomware through the network.
2. **The Impact:** Production halts, delaying shipments and resulting in contractual penalties.
3. **The Resolution:** Contrast the prolonged recovery from unpreparedness with the swift containment enabled by proactive measures.

Use visuals like risk heat maps and cost-impact graphs to reinforce the narrative. These tools make abstract risks tangible and emphasize the value of proposed investments.

Building Long-Term Engagement Through Metrics and Updates

Securing board support is not a one-time effort. It requires ongoing engagement. Regular updates and clear metrics ensure continued alignment.

- **Track Progress:** Share metrics like vulnerability reductions, compliance score improvements, or ROI on security investments. For example, “Since implementing enhanced monitoring at our strategic sites, we've reduced downtime incidents by 35%, avoiding $1.2 million in potential losses.”

- **Report Emerging Risks:** Keep the board informed about new threats and how the organization prepares to address them. Highlighting proactive measures reinforces confidence in the program.
- **Celebrate Successes:** Showcase milestones, such as achieving compliance certifications or mitigating a significant threat. This demonstrates progress and builds momentum for future initiatives.

Boards value transparency and measurable results. Consistent updates position the CISO or CIO as a trusted advisor and ensure a sustained commitment to OT security.

Fostering Board-Level Champions for OT Security

The goal is to turn board members into advocates for OT security. Achieving this requires trust, education, and alignment with their priorities.

- **Education and Awareness:** Conduct workshops or site visits to provide firsthand insights into OT risks and the importance of security measures.
- **Tailored Messaging:** To secure support and address individual board members' priorities (such as cost control for CFOs or operational resilience for COOs).
- **Recognition of Impact:** Highlight how board-approved investments have driven measurable improvements, such as enhanced compliance or reduced downtime.

By aligning OT security with the board's strategic vision, CISOs and CIOs can ensure sustained investment and elevate security to a core business priority.

Takeaways

Engaging the board on OT security requires a mix of strategic insight, clear communication, and measurable outcomes. By framing risks in business terms, aligning compliance with organizational goals, and providing actionable plans, CISOs and CIOs can secure the investment and commitment needed to drive meaningful change.

Ongoing engagement builds trust, reinforces progress, and positions OT security as a cornerstone of the organization's resilience and growth. With these strategies, OT leaders can gain the board's support and transform security into a competitive advantage.

OT Security as a Strategic Advantage

Operational technology (OT) security is no longer just a matter of technical controls or regulatory compliance; it is an essential pillar of modern business resilience and growth. For CISOs and CIOs, this journey requires more than managing threats. It involves shaping the narrative, fostering alignment, and driving transformative change across the organization.

This series has explored the critical elements of building and scaling effective OT security programs. From establishing the business case to aligning with compliance frameworks and engaging the board, every chapter emphasized the strategic role of OT security in safeguarding operations, protecting revenue, and enabling long-term innovation.

The key takeaway for leaders is that OT security must be framed as a business enabler. When risk reduction is tied to operational uptime, supply chain reliability, and market competitiveness, it moves beyond IT discussions and into the boardroom as a core element of business strategy. CISOs and CIOs can secure the trust and investment necessary to drive meaningful impact by quantifying risks, presenting actionable roadmaps, and continuously engaging stakeholders.

Success also demands adaptability. The threat landscape will continue to evolve, shaped by emerging technologies, geopolitical tensions, and the increasing convergence of IT and OT systems. Leaders must remain agile, leveraging predictive analytics, AI-driven tools, and cloud-based solutions to stay ahead of threats. Simultaneously, fostering a culture of accountability and security across all levels of the organization ensures that improvements are sustainable and scalable.

Finally, remember that OT security is not an endpoint but an ongoing journey. The most successful leaders combine technical expertise with strategic vision, positioning their organizations to withstand risks and thrive in a complex and interconnected world. By aligning security initiatives with business goals and communicating their value effectively, CISOs and CIOs can elevate OT security from a compliance mandate to a competitive advantage.

As you move forward, take the strategies outlined here as a foundation but tailor them to your organization’s unique challenges and opportunities. With the right approach, OT security can become a driving force for resilience, innovation, and growth, ensuring your organization is prepared for today’s challenges and tomorrow's opportunities.

About the Author



Roger Hill

CEO, Hillstrong Group Security, Inc.

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

Throughout his career, Roger 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 insights and 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