HILLSTRONG GROUP SECURITY

HILLSTRONG · THOUGHT LEADERSHIP

Stronger Together

Future-Proofing OT Cybersecurity

Chuck Tommey, P.E., CISSP, GICSP | Co-Founder and Chief Advisory Officer, Hillstrong Group Security, Inc.

Contents

Five chapters on building resilient OT cybersecurity through governance and cross-functional collaboration.

INTRODUCTION	Cybersecurity Is a Team Sport
CHAPTER ONE	Breaking Down Silos: Why IT and OT Must Work Together for Cybersecurity Success
CHAPTER TWO	Beyond IT/OT Convergence: Why True Collaboration is the Key to Operational Resilience
CHAPTER THREE	Cybersecurity as a Mission-Driven Imperative: Aligning Security with Organizational Goals
CHAPTER FOUR	Building a Culture of Collaboration and Resilience
CHAPTER FIVE	Preparing for the Future, Together: A Roadmap for Long-Term IT/OT Security Resilience
CONCLUSION	Resilience Requires Everyone
	About the Author
	About Hillstrong Group Security, Inc.

Cybersecurity Is a Team Sport

Cybersecurity in operational technology (OT) environments has never been more critical, or more complex. The convergence of IT and OT systems has opened up incredible efficiencies but also expanded the attack surface for increasingly sophisticated threats. In this new era, it's clear that cybersecurity is no longer the sole domain of IT. It's an enterprise-wide responsibility that must be embedded in the organization's culture, strategy, and mission.

This eBook is a practical guide for leaders, engineers, cybersecurity professionals, and operations managers who understand that technology alone isn't enough. You'll find five chapters originally published as a blog series, each exploring a core principle of resilient OT cybersecurity:

1. **Understanding IT/OT Dynamics:** Why recognizing shared goals is the foundation for cooperation.
2. **Going Beyond Convergence:** How true collaboration (not just integration) delivers real security.
3. **Cybersecurity as a Mission-Driven Imperative:** Ensuring that all security efforts support operational resilience.
4. **Building a Culture of Collaboration and Awareness:** Making your people a strategic advantage.
5. **Planning for the Future Together:** The role of an OT-specific GRC program in building lasting security and agility.

The central message across each chapter is clear: resilience is built through strong governance and cross-functional collaboration. Whether managing risk at the enterprise level or configuring control systems in the field, cybersecurity requires intentional alignment across functions, clear governance, and a shared commitment to protecting the mission.

This eBook will show you how to move beyond traditional, siloed approaches and build a sustainable cybersecurity strategy grounded in governance, risk, and compliance (GRC) powered by cross-functional teamwork.

HILLSTRONG GROUP SECURITY

STRONGER TOGETHER · CHAPTER ONE

Breaking Down Silos: Why IT and OT Must Work Together for Cybersecurity Success

Understanding IT/OT Dynamics and Shared Goals

For decades, Information Technology (IT) and Operational Technology (OT) have operated in separate domains, each focusing on different priorities. IT has been responsible for protecting data, ensuring network security, and maintaining compliance, while OT has been focused on keeping industrial processes running efficiently and safely.

But, in today's digital era, IT and OT systems are increasingly interconnected, and cyber threats now target industrial control systems (ICS) just as frequently as they target enterprise IT networks. This convergence presents both opportunities and risks.

The challenge? Merging IT and OT without disrupting operational resilience. The solution? True collaboration between IT and OT, built on a foundation of governance, risk management, and compliance (GRC) designed specifically for OT.

Cybersecurity in industrial environments must directly support the mission of the organization, whether that mission is producing pharmaceuticals, generating power, delivering clean water, or manufacturing critical infrastructure components. Every security initiative must enhance, not hinder, operational resilience.

Let's explore how IT and OT can break down silos, align on common goals, and work together to build a cybersecurity strategy that strengthens the mission instead of impeding it.

The IT Perspective vs. The OT Perspective: Why the Divide Exists

To truly collaborate, IT and OT must first understand each other's worldviews.

The IT Perspective: Securing Data and Networks

For most IT teams, cybersecurity is focused on data:

- **Confidentiality:** Protecting sensitive information from unauthorized access.
- **Integrity:** Ensuring that data isn't altered maliciously.
- **Availability:** Keeping systems online and responsive to support business operations.
- **Compliance:** Meeting regulatory or standards requirements such as HIPAA, CFR 17 229.106 (SEC reporting requirements), ISO 27001, and/or CMMC.

Because IT networks are constantly under attack, IT professionals are accustomed to rapid software patching, multi-factor authentication, and strict access controls. IT views cybersecurity as a technical discipline governed by strict policies and regular updates.

The OT Perspective: Keeping Operations Running

In contrast, OT professionals prioritize operational resilience:

- **Safety:** Protecting human lives and preventing catastrophic failures.
- **System Availability:** Ensuring production and operational processes never stop unexpectedly.
- **Reliability Over Change:** IT may update systems weekly, but OT systems cannot tolerate frequent changes without risk to operations.
- **Legacy Systems:** Many OT assets have 20+ year lifespans and were not designed with cybersecurity in mind.

In OT, uptime is paramount. A well-intentioned IT security patch could shut down an assembly line just as completely as a mal-intentioned cyber attack. Either way, a shutdown could lead to millions in lost production, reputational damage, and possible safety hazards. This is why OT has historically resisted IT-driven security initiatives.

The Shared Goal: Safeguarding the Organization's Mission

Despite their differences and whether they realize it or not, IT and OT are ultimately working toward the same overarching goal: Protecting the critical systems that enable the organization to fulfill its mission.

Whether it's delivering power, treating water, producing goods, or enabling public safety, IT and OT must align their cybersecurity efforts with the organization's core objectives.

A one-size-fits-all approach to cybersecurity does not work in OT environments: security initiatives must be tailored to industrial processes without sacrificing operational continuity.

A successful IT/OT collaboration strategy must:

- Balance security and operational uptime.
- Align cybersecurity with business and production goals.
- Use an OT-specific GRC framework to guide collaboration for the long-term.

How an OT-Specific GRC Program Can Align IT and OT

Governance, risk management, and compliance (GRC) frameworks help establish clear roles, responsibilities, and procedures for both IT and OT. However, when attempts are made to apply traditional IT GRC models directly into OT environments, it often ends up alienating the OT teams. This has led to a lack of formal OT GRC programs in OT environments and even a lack of cooperation between IT and OT. When both teams feel the other has no idea what is important to get the job done, they don't make time to resolve their differences.

This is where an OT-specific GRC program becomes essential. Frameworks like NIST CSF 2.0 can incorporate the structured guidance of OT-specific cybersecurity standards (e.g., NIST SP 800-82r3 and IEC 62443), moving the organization toward formally securing its industrial environments while maintaining operational integrity. When OT builds a GRC program, ideally with IT's assistance, both teams can better understand how to work together.

The Role of OT-Specific GRC in IT/OT Collaboration:

- **Governance:** Defines roles, responsibilities, and policies specific to OT security.
- **Risk Management:** Assesses vulnerabilities in OT systems and aligns risk mitigation with operational requirements.
- **Compliance:** Ensures cybersecurity efforts support regulatory needs without disrupting operations.

When properly implemented, an OT-focused GRC program serves as a bridge between IT and OT, creating a common framework for security initiatives.

Bridging the Gap: Steps to Align IT and OT

To move beyond IT/OT silos, organizations must intentionally foster collaboration between both teams.

Step 1: Establish a Shared Security Framework

Use NIST CSF 2.0, IEC 62443, and CMMI to create a common security language for IT and OT teams. NIST CSF encourages the creation of custom Organizational Profiles to better reflect the needs of highly diverse OT environments.

Step 2: Conduct Joint Risk Assessments

IT and OT must work together to:

- Identify vulnerabilities in industrial systems.
- Prioritize security fixes based on operational impact.
- **Implement layered security measures (such as network segmentation and access controls).**

Step 3: Build a Culture of Trust and Communication

Encourage regular cross-team meetings where IT and OT can:

- Discuss security concerns.
- Align on security goals that support operations.
- Share lessons learned from past incidents.

Step 4: Implement OT-Specific Security Policies

Standard IT policies often fail in OT environments. Instead, organizations should:

- Use compensating controls for unpatchable systems.
- Implement role-based access control (RBAC) specific to OT.
- Ensure network segmentation to isolate critical OT assets from external threats.

By integrating these steps into a formal OT GRC program, organizations can harmonize IT/OT efforts without jeopardizing production.

Chapter Conclusion: A Call for Partnership

IT and OT cannot afford to work in isolation: the growing number of cyberattacks on industrial environments demands a collaborative, risk-based approach to security.

The goal is not just cybersecurity. It’s operational resilience.

Every security initiative must support the organization’s mission.

An OT-specific GRC program can serve as the foundation for a well-functioning IT/OT partnership.

By breaking down silos, building trust, and aligning security with operational goals, IT and OT can work together to protect the systems that drive the organization forward.

HILLSTRONG GROUP SECURITY

STRONGER TOGETHER · CHAPTER TWO

Beyond IT/OT Convergence: Why True Collaboration is the Key to Operational Resilience

The Rise of IT/OT Convergence

The convergence of Information Technology (IT) and Operational Technology (OT) is a rapidly accelerating trend in industrial environments. The promise of convergence is enticing: integrated networks, cost savings, and streamlined management. However, while IT/OT convergence simplifies system integration and enhances visibility, it does not inherently strengthen cybersecurity or operational resilience. Without true collaboration, convergence can actually introduce new risks, leaving organizations vulnerable to cyber threats.

Cybersecurity in OT environments must be more than an add-on to IT security policies. Every cybersecurity initiative must directly enhance the mission of the organization, whether that mission is delivering power, managing water treatment facilities, or ensuring manufacturing continuity. This requires a mission-focused, risk-based approach as this is the best way to test how any cybersecurity initiative will affect organizational readiness. This is where IT/OT collaboration that goes beyond technology convergence and fosters genuine teamwork between the two disciplines becomes the critical enabler.

Why Convergence Alone is Not Enough:

While IT/OT convergence should bring significant benefits (such as improved data sharing, network visibility, lower tool count, and less training), it also presents unique security and collaboration challenges that cannot be solved through technology alone:

- **Increased Attack Surface:** More connected systems mean more potential entry points for attackers.
- **Cultural & Process Differences:** IT and OT operate under different priorities: IT values data confidentiality, while OT prioritizes safety and uptime.
- **Patching & Change Management Conflicts:** IT enforces frequent updates, whereas OT environments require stability and careful change control, often with regulatory implications.
- **Legacy System Security Gaps:** Many OT systems were designed without cybersecurity in mind and cannot be easily upgraded.

These challenges illustrate why convergence is just the first step: the real work lies in building collaboration between IT and OT teams to address these risks in a way that supports operational resilience.

The Power of True IT/OT Collaboration:

IT and OT must work together to establish a cybersecurity strategy that supports security and business operations. True collaboration means:

- **Joint Risk Assessments:** Both teams working together to identify and prioritize security risks based on operational impact.
- **Co-Designed Security Strategies:** Policies tailored to OT environments rather than applying IT security measures without modification.
- **Mutual Understanding & Respect:** IT understands the constraints of OT, and OT recognizes the importance of cybersecurity.

Without collaboration, IT-driven security initiatives may be seen as disruptive or unrealistic, while OT's focus on operational continuity may unintentionally neglect cybersecurity risks. The key is balancing both perspectives.

Building a Secure and Resilient IT/OT Partnership:

1. Establishing an OT-Specific GRC Program

A well-structured Governance, Risk, and Compliance (GRC) program tailored for OT provides a foundation for collaboration. Traditional IT GRC frameworks do not address OT's unique requirements, which is why standards, frameworks, and maturity models like IEC 62443, NIST CSF 2.0, and CMMI are crucial.

An OT-specific GRC program:

- Defines roles and responsibilities for IT and OT in cybersecurity.
- Ensures risk-based decision-making that prioritizes safety and uptime.
- Establishes compliance frameworks that meet regulatory and operational needs.

With a structured governance model, IT and OT teams can align security priorities without disrupting operations.

2. Developing a Joint Risk Management Strategy

Cybersecurity risks must be assessed in the context of operational impact. Instead of treating all vulnerabilities equally, IT and OT should collaborate to:

- Identify mission-critical systems and prioritize protections accordingly.
- Establish compensating controls when security patches are not feasible.
- Implement layered security controls that minimize risk without causing downtime and provide quick, non-disruptive mitigation opportunities.
- Scrutinize for indirect dependencies of OT processes on IT or other business functions.

3. Aligning Cybersecurity with the Organization's Mission

Cybersecurity should be an enabler of operational resilience, not an obstacle. To ensure security initiatives support the organization's mission, IT and OT must:

- Integrate cybersecurity into business continuity planning.

- Ensure security measures enhance, rather than hinder, uptime and productivity.
- Use cybersecurity frameworks (IEC 62443, NIST CSF 2.0) to align security with operational goals.

When security is viewed through the lens of mission success, IT and OT teams are more likely to work together effectively.

4. Strengthening Incident Response Collaboration

IT and OT must be aligned before a cyber incident occurs. Effective incident response planning includes:

- Defining IT/OT-specific response protocols.
- Running joint tabletop exercises and simulations.
- Ensuring clear communication pathways between IT and OT teams.

By preparing together, IT and OT can respond more efficiently to cybersecurity threats while minimizing operational impact.

Chapter Conclusion: Convergence is Just the Beginning

IT/OT convergence is an important step toward modernizing industrial environments, but it is not a cybersecurity solution on its own. Organizations must foster deep collaboration between IT and OT to truly enhance security and operational resilience.

- Technology alone cannot solve IT/OT security challenges: collaboration is essential.
- An OT-specific GRC program provides a foundation for well-functioning IT/OT relationships.
- Every cybersecurity initiative must enhance (not hinder) the organization's mission.

By moving beyond convergence and investing in true IT/OT collaboration, organizations can build a cybersecurity strategy that strengthens both security and operational resilience.

HILLSTRONG GROUP SECURITY

STRONGER TOGETHER · CHAPTER THREE

Cybersecurity as a Mission-Driven Imperative: Aligning Security with Organizational Goals

Cybersecurity is Not Just an IT Problem

Cybersecurity is often treated as a purely technical issue, an IT department responsibility that revolves around firewalls, patching, and access controls. But this narrow perspective misses a fundamental truth: cybersecurity is a business and operational imperative that directly impacts an organization's ability to fulfill its mission.

For critical infrastructure, manufacturing, and industrial organizations, cybersecurity is not just about compliance. In fact, we at Hillstrong would say it should never be, just about compliance. It should ensure uptime, protect workers and the environment, and enhance operational resiliency. Cybersecurity decisions must be made with an understanding of how they enhance, rather than hinder, the organization's core mission.

This chapter explores why cybersecurity must be integrated into the organization's overarching mission and how an OT-specific Governance, Risk, and Compliance (GRC) program can ensure that security enhances operational resilience rather than disrupts it.

Operational Resilience: The True Measure of Cybersecurity Success

Traditional IT security measures often focus on data confidentiality and integrity and using compliance to industry standards as a key measure of success. However, in an operational technology (OT) environment, an industrial processes' availability, reliability, and resilience are just as critical, if not more so. Cybersecurity strategies must be tailored to ensure operational resilience, preventing cyber threats from disrupting critical processes.

The Cost of Cybersecurity Failures

When cybersecurity is not aligned with an organization's mission, the consequences can be catastrophic:

- Production Downtime: Cyber incidents that cause unplanned shutdowns can lead to millions in lost revenue. The misapplication of standards-based cybersecurity controls has contributed to significant downtime in multiple cases.
- Safety Risks: OT systems control physical processes. Cyber attacks can cause equipment malfunctions, endangering workers and the local environment. A particularly vile subset of OT-focused malware actually targets automated safety systems in an attempt to cause more catastrophic effects, thus more downtime and more cost to the organization.

- Regulatory Fines & Reputation Damage: Non-compliance with cybersecurity standards like NIST 800-82r3, IEC 62443, and NERC CIP can result in lost customer trust and heavy penalties.

To prevent these disruptions, organizations must move beyond compliance checklists and adopt a mission-driven cybersecurity strategy that ensures business continuity.

Aligning Cybersecurity with Business and Operational Goals

Organizations should integrate security into business and operational decision-making rather than treating cybersecurity as a standalone or bolt-on function.

1. Cybersecurity as an Enabler, Not a Barrier

Cybersecurity initiatives should be designed to support, rather than hinder, operations:

- Security policies should prioritize uptime by implementing compensating controls for unpatchable systems or until a maintenance window allows patching.
- Access controls should be role-based and tailored to OT environments instead of rigid IT-driven authentication models.
- Incident response plans should consider operational continuity, ensuring production can continue even during a cyber event.

2. Leadership Buy-In and Cross-Department Collaboration

To align cybersecurity with mission objectives, leadership engagement is essential. Executives should:

- Establish clear security accountability across IT and OT teams.
- Involve cybersecurity leaders in business continuity planning.
- Ensure cybersecurity investments reflect the organization's risk landscape.
- Ramp up the communication with regular table-top exercises. Exercise those incident response and disaster recovery muscles!

A strong cybersecurity culture starts at the top, but it is maintained over time by continuous improvement and cross-functional engagement. When leadership prioritizes security as a business enabler, IT and OT teams are more likely to collaborate often and effectively.

3. Measuring Cybersecurity Success Beyond IT Metrics

Traditional IT security metrics (e.g., number of threats blocked, patching rates) don't always reflect the effectiveness of security in an OT setting. Instead, organizations should measure:

- Operational uptime improvements due to security investments.
- Reduction in risk exposure to critical industrial assets.
- Effectiveness of joint IT/OT security exercises and incident response drills.

Frameworks for Mission-Driven Cybersecurity

Several established frameworks can help organizations structure their cybersecurity strategy in a way that aligns with operational goals:

- IEC 62443: Focuses on securing industrial control systems while ensuring operational integrity.
- NIST Cybersecurity Framework (CSF 2.0): Provides a risk-based approach to cybersecurity that should be tailored to an organization's specific business objectives.
- CMMI for Cybersecurity Maturity: Helps organizations assess and continuously improve their cybersecurity posture.

An effective cybersecurity program combines these frameworks into a structured OT-specific GRC program that balances security, risk, and operational needs.

How an OT-Specific GRC Program Drives Cybersecurity and Resilience

1. Establishing Governance to Bridge IT and OT

A well-structured GRC program tailored for OT environments:

- Defines roles and responsibilities for IT and OT security.
- Ensures risk-based decision-making that prioritizes safety and uptime.
- Establishes compliance frameworks aligned with industry standards and customized to support the organization's mission.

2. Risk Management That Supports the Mission

A strong OT GRC program includes:

- Risk-based asset prioritization: securing critical assets and sites first.
- Layered and flexible security controls to minimize operational impact.
- Compensating or alternative security measures when standard IT security solutions are impractical.
- Strong policy and process-oriented framework that provides the long-term foundation

3. Security as an Ongoing Process

- Instead of treating cybersecurity as a once-a-year compliance effort, an OT-focused GRC program ensures continuous improvement of operational resilience.
- Continuous status updates from local sources give confidence that security is improving while aligning with operational realities.
- Security policies that evolve with technological and regulatory changes.

A well-implemented GRC framework fosters ongoing collaboration between IT and OT, creating a resilient security culture that strengthens mission readiness.

Chapter Conclusion: Making Cybersecurity a Strategic Advantage

Cybersecurity is not just a technical function. It is a core business imperative. When properly aligned with the organization's mission, cybersecurity:

- Enhances operational resilience.
- Enables business continuity.
- Enhances safety and compliance to fit-for-purpose frameworks without hindering productivity.

By leveraging OT-focused and organizationally specific GRC frameworks, ensuring leadership engagement, fostering close collaboration, and prioritizing cybersecurity as an enabler, organizations can build a security posture that supports their long-term success.

HILLSTRONG GROUP SECURITY

STRONGER TOGETHER · CHAPTER FOUR

Building a Culture of Collaboration and Resilience

How IT and OT Can Create a Cyber-Aware Workforce

Culture should be the First Line of Defense

Cybersecurity is not just a technology problem. It is also a people and process problem. Even the strongest security measures can be undone by a single click on a phishing email, poor communication between IT and OT teams, or lack of clear training on expectations and requirements. While organizations may invest in advanced security tools, those tools are only as effective as the people using them. A strong cybersecurity posture is built on awareness, collaboration, and shared responsibility.

For organizations that rely on Operational Technology (OT), such as manufacturing, utilities, and critical infrastructure, cybersecurity must be more than just an IT function. It must become a cultural priority embedded in day-to-day operations. IT and OT teams must not only work together during cyber incidents but proactively engage in training, awareness, and governance to prevent threats from taking hold in the first place.

A resilient organization is not one that never experiences attacks but one that detects threats early, mitigates risks effectively, and recovers quickly without significantly impacting operations and, most importantly, its customers. Operational resiliency, including OT cybersecurity, should always keep the mission front and center! Achieving this level of preparedness requires building a security-first culture where IT and OT collaborate, share knowledge, and jointly uphold cybersecurity best practices.

More importantly, properly trained and motivated employees can become a competitive advantage rather than a liability. When employees are trained to recognize anomalies, detect phishing attempts, and report unusual activity, they function as sophisticated human sensors in the cybersecurity defense system. Their awareness and vigilance provide an additional layer of protection that no software or firewall can replicate. This transformation from cybersecurity risk to cybersecurity asset is one characteristic that separates resilient organizations from vulnerable ones.

This chapter explores why cybersecurity culture matters, the unique IT/OT challenges in fostering it, and practical steps to create a cyber-aware workforce capable of defending against modern threats.

The IT/OT Divide in Cybersecurity Culture

Despite sharing the same overarching goal of securing the organization, IT and OT often approach cybersecurity from fundamentally different perspectives. IT departments focus on data confidentiality and

integrity, implementing strict access controls, encryption, and patching policies to mitigate risks. They view cybersecurity as a continuous process of updates, monitoring, and proactive threat detection.

OT, on the other hand, operates under a different set of priorities. The primary concern in industrial environments is the safety and availability of operational systems. A sudden update or security patch (common in IT environments) could disrupt production, leading to downtime, financial loss, or even safety hazards. Many OT systems were designed decades ago without cybersecurity in mind, making the integration of modern security measures a complex challenge.

These differing perspectives often lead to tension, with IT viewing OT as resistant to security protocols and OT perceiving IT-driven security measures as operational disruptions. Without deliberate efforts to bridge this gap, organizations remain vulnerable to cyber threats that exploit these misalignments.

Fostering a Cybersecurity Culture That Works for IT and OT

Building a cybersecurity-aware workforce requires more than policies and compliance checklists. It demands a shift in mindset. Organizations must create an environment where cybersecurity is not just a task for IT but an organization-wide priority.

Developing a unified cybersecurity vision that aligns IT and OT security strategies is one of the most critical steps in fostering collaboration. Leadership plays a pivotal role in setting this vision by clearly defining cybersecurity as a business enabler rather than an operational hindrance. A shared security governance structure, guided by frameworks such as NIST CSF 2.0 and IEC 62443, provides a structured approach to managing cybersecurity risks while ensuring that security measures do not compromise operational efficiency.

Beyond leadership support, organizations must also invest in cross-functional training programs. Done correctly, joint training will enhance mutual understanding between IT and OT. IT professionals should gain exposure to OT environments to understand how industrial control systems function, the impact of downtime, and the constraints of operational safety. Likewise, OT personnel should be educated on cybersecurity fundamentals, including phishing awareness, network segmentation, and secure remote access practices. Regular security drills, such as tabletop exercises, can help both teams prepare for cyber incidents and improve their ability to respond collaboratively.

Effective communication is another cornerstone of a strong cybersecurity culture. Cybersecurity threats often escalate due to a lack of clear communication between teams. To mitigate this, organizations should establish regular IT/OT cybersecurity meetings where security updates, emerging threats, and operational concerns are discussed openly. Cybersecurity should also be incorporated into daily operational meetings, ensuring that security awareness is integrated into routine workflows rather than treated as an afterthought. Operations teams should add cybersecurity topics to the ubiquitous daily safety briefings that most begin their shifts and/or meetings.

Additionally, cybersecurity training should be tailored to specific roles rather than applying a one-size-fits-all approach. IT personnel need to understand the unique cybersecurity risks in OT environments, including SCADA vulnerabilities and supply chain risks. At the same time, OT staff should focus on human-centric threats such as social engineering and insider threats. Meanwhile, leadership and executives should receive training emphasizing how cybersecurity directly impacts regulatory compliance, business continuity, and overall organizational resilience.

Organizations should consider implementing incentives for cybersecurity awareness to reinforce security best practices. Employees who identify and report phishing attempts, follow secure protocols, or actively contribute to cybersecurity initiatives should be recognized and rewarded. Gamification techniques, such as simulated phishing campaigns and interactive training modules, can further engage employees in developing a proactive security mindset.

Strengthening Cybersecurity Culture Through Governance

A strong cybersecurity culture does not emerge organically. It must be reinforced through governance structures that define clear responsibilities, policies, and continuous improvement processes. Industry frameworks such as IEC 62443, NIST 800-82r3, and the CMMI Cybersecurity Maturity Model provide organizations with structured approaches to integrating cybersecurity into both IT and OT environments.

Governance frameworks help standardize security policies, ensuring that both IT and OT operate under a common set of guidelines. By implementing risk-based decision-making, organizations can prioritize security investments based on the criticality of assets and their current level of maturity rather than applying blanket security controls that may not align with operational constraints. Regular security audits and continuous assessments ensure that cybersecurity policies evolve alongside emerging threats and regulatory changes.

By embedding cybersecurity into Governance, Risk, and Compliance (GRC) programs, organizations can create a security culture that is sustainable and adaptive to the ever-changing threat landscape.

Chapter Conclusion: Security is a Team Effort and a Competitive Advantage

Building a cybersecurity-aware workforce is not a one-time initiative but an ongoing commitment that requires leadership support, structured training programs, and continuous engagement. A strong cybersecurity culture does not aim to eliminate all cyber risks but to equip IT and OT teams with the knowledge, tools, and collaborative mindset necessary to detect, respond to, and recover from threats while minimizing the impact to operations.

Cybersecurity must be viewed as a business priority, not just a function of IT. When IT and OT teams work together, align security goals, and foster open communication, organizations can create a culture of cybersecurity resilience. Governance frameworks such as IEC 62443 and NIST CSF 2.0 provide the structure necessary to bridge gaps between IT and OT, ensuring that cybersecurity is integrated into operational processes rather than treated as an external compliance requirement.

More importantly, a well-trained workforce becomes a force multiplier for cybersecurity defenses. Employees who are empowered with cybersecurity awareness become human sensors, identifying threats before they escalate into major incidents. When cybersecurity is embedded into an organization's culture, it does more than protect operations: it creates a competitive advantage in a world where security and resilience are critical to long-term success.

HILLSTRONG GROUP SECURITY

STRONGER TOGETHER · CHAPTER FIVE

Preparing for the Future, Together: A Roadmap for Long-Term IT/OT Security Resilience

Why IT/OT collaboration (not just convergence) is the key to securing your future.

The Evolving Cyber Threat Landscape

Cybersecurity threats are growing in complexity, speed, and scope. From ransomware campaigns targeting industrial control systems to increasingly sophisticated supply chain attacks, organizations can no longer afford to rely on ad hoc defenses or siloed responses. The stakes are even higher for companies that operate critical infrastructure or rely heavily on operational technology (OT). A security incident can result in not only data loss but also physical damage, production halts, and even public safety risks.

In this dynamic threat environment, maintaining operational continuity while defending against cyber threats requires a future-proof approach to OT cybersecurity. At the center of that approach lies a powerful but often underutilized tool: a properly designed, implemented, and maintained OT Governance, Risk, and Compliance (GRC) program.

Why a Future-Proof Strategy Requires More Than Technology

Technology is an important enabler of cybersecurity, but it is not a solution in itself. Firewalls, endpoint detection, and intrusion prevention systems are only effective when they are part of a broader, strategic, and risk-aligned framework. Cybersecurity that is reactive, patchwork, or driven solely by IT will not scale or adapt as threats to your operational resilience evolve.

What's needed is a strategy that aligns with business goals, incorporates operational realities, and adapts to emerging risks. This is where an OT-specific GRC program becomes vital. GRC provides the structure needed to evaluate and manage risk, assign roles and responsibilities, ensure compliance with relevant standards, and (most importantly) create the conditions for continuous improvement.

A future-proof OT cybersecurity framework must be:

- Strategically aligned with the organization's mission and business continuity objectives.
- Risk-informed, based on real-world threats and asset or site criticality.
- Operationally practical, tailored to the constraints and priorities of industrial environments.
- Scalable, adaptable, and sustainable, capable of adapting to future technologies and threats.

These are exactly the goals a mature OT GRC program is designed to achieve.

The Central Role of an OT GRC Program

An OT GRC program serves as the foundation for resilient cybersecurity operations. By defining governance structures, managing risk consistently, and embedding compliance across people, processes, and technologies, it transforms cybersecurity from a series of technical controls into a business-aligned discipline.

A well-functioning OT GRC program:

- Establishes clear ownership and accountability for cybersecurity across IT, OT, and leadership.
- Aligns cybersecurity initiatives with operational and safety requirements.
- Enables risk-based decision-making, prioritizing protections for the most critical asset.
- Embeds compliance activities into daily operations to ensure ongoing adherence to frameworks like IEC 62443, NIST 800-82r3, and NIST CSF 2.0.
- Drives maturity through continuous assessment and improvement using models like CMMI.

Most importantly, GRC brings together the elements necessary for cross-functional collaboration, ensuring that cybersecurity is not just the responsibility of IT or security teams, but a shared priority for the entire organization

Collaboration Across Departments: The Key to Resilience

True cybersecurity resilience cannot be achieved in silos. While the partnership between IT and OT is critical, the future of cybersecurity depends on engaging the entire organization, including operations, safety, engineering, compliance, HR, procurement, and executive leadership.

For example:

- Engineering must be involved in system changes, configurations, and design decisions that affect cybersecurity.
- HR must support policies around user access, onboarding, and awareness training.
- Procurement plays a role in evaluating and selecting vendors that meet cybersecurity requirements.
- Legal and Compliance teams ensure that practices meet industry standards and regulatory mandates.
- Leadership must champion cybersecurity as a strategic imperative, not just a technical requirement. They must also provide the resources and organizational will to implement and incentivize the effort to sustain the program.

When cybersecurity is framed as a shared responsibility, supported by clear policies, consistent communication, and aligned incentives, every department becomes part of the organization's security posture. This integrated approach, supported by the governance structure of an OT GRC program, enables faster response to threats, more informed decision-making, and a stronger security culture.

Planning for the Unknown: Building Agility Into the Cybersecurity Program

One of the most important traits of a future-proof cybersecurity strategy is agility: the ability to adapt quickly to new threats, technologies, or business models. Agility is not possible without institutionalized learning and structured improvement processes.

A mature OT GRC program enables agility by:

- Regularly assessing the effectiveness of controls and updating policies, often resulting from cross-functional table-top exercises.
- Integrating lessons learned from incident response and threat intelligence.
- Identifying capability gaps and addressing them through workforce development and process change.
- Supporting scalable integration of new technologies, such as AI-driven threat detection or Zero Trust architectures.

This adaptive capacity ensures that the cybersecurity program remains relevant and effective, even as the organization and the threats it faces evolve.

Chapter Conclusion: Future-Proofing Starts Now

Organizations that treat cybersecurity as a technical afterthought or a compliance checkbox will find themselves unprepared for the threats of tomorrow. A properly designed, implemented, and maintained OT GRC program is not just a support function: it is the cornerstone of a future-ready cybersecurity strategy.

By embedding governance, risk management, and compliance into the fabric of operational technology environments, GRC enables organizations to align cybersecurity with business objectives, foster cross-functional collaboration, and continuously adapt to change.

In this future-proof model, cybersecurity is no longer the domain of a single department: it becomes an organization-wide commitment. And that's the only way to build lasting resilience.

The future is uncertain, but your organization can be operationally resilient when it has built a collaborative, enterprise-wide OT GRC foundation.

Resilience Requires Everyone

Cybersecurity is often discussed in technical terms: firewalls, zero trust, and endpoint protection. But beneath all of this lies a deeper truth: people, policies, and processes determine whether your organization can meet the challenges of the future.

A properly implemented OT GRC program does more than check regulatory boxes. It brings structure, accountability, and maturity to your cybersecurity efforts. More importantly, it creates the foundation for something technology can't provide on its own: enterprise-wide collaboration. When IT, OT, engineering, HR, legal, and leadership all work together with a shared mission, security becomes not just stronger. It becomes strategic.

In a constantly evolving threat landscape, a future-proof cybersecurity program must be agile, risk-informed, and aligned with business goals. That starts with building a culture where cybersecurity is everyone's responsibility.

You now have the roadmap. The next step is bringing your people together and leading from the front.

Cybersecurity isn't just a challenge. It's an opportunity to unite, protect, and lead. Stronger together.

About the Author



Chuck Tommey

Co-Founder and Chief Advisory Officer, Hillstrong Group Security, Inc.

With decades of experience in strategic operations, Chuck leads Hillstrong's growth initiatives and ensures alignment between cybersecurity best practices and our clients' business goals.

Chuck is a seasoned cybersecurity professional with over two decades of experience protecting critical infrastructure and industrial control systems. As a trusted advisor to global manufacturers, Chuck brings deep expertise in Operational Technology (OT) security, helping organizations build resilience, reduce risk, and navigate the evolving threat landscape. His passion lies in bridging the gap between IT and OT to create a safer, smarter, and more secure industrial environment.

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