HILLSTRONG GROUP SECURITY

HILLSTRONG · THOUGHT LEADERSHIP

The Roadmap to OT Cybersecurity Maturity

Roger Hill & Chuck Tommey | Hillstrong Group Security, Inc.

Contents

CHAPTER ONE	Assessing Your Current OT Cybersecurity Posture
CHAPTER TWO	Setting Goals and Benchmarks for Cybersecurity Improvement
CHAPTER THREE	Developing and Executing a Cybersecurity Roadmap
CHAPTER FOUR	Measuring Progress and Adapting to New Threats
CHAPTER FIVE	Achieving and Sustaining Cybersecurity Maturity
	About the Authors
	Ready to achieve Operational Resilience with Your OT Cybersecurity Program?
	About Hillstrong Group Security, Inc.

Assessing Your Current OT Cybersecurity Posture

How to Assess Your Current OT Cybersecurity Posture to Identify Strengths and Weaknesses?

Preventing Operational Technology (OT) cyberattacks against manufacturing systems starts with an organization's realistic grasp of its current security posture. Assessing your organization's cybersecurity protective capabilities, including perimeter security, adaptive controls, security operations capabilities, extent of monitoring visibility, incident response and recovery effectiveness, threat modeling, and overall governance is essential to stopping potential threats.

Manufacturing companies depend on OT systems like Industrial Control Systems (ICS), such as SCADA and PLCs, to run production and collect valuable data. However, these systems should never be connected directly to the Internet, which greatly increases the risk of intellectual property theft, malware, and ransomware attacks. For this reason, a robust network segmentation architecture with secure remote access, if required, is recommended.

Cyberattacks on ICS can cause severe problems in industries such as electric power, water, nuclear, manufacturing, infrastructure, transport, and oil and gas. Organizations should consult global standards like IEC 62443 and NIST SP 800-82 before moving forward with OT assessments.

Why Perform OT Risk Assessments?

Cyberattacks on manufacturing systems can lead to safety and operational issues. Attackers can manipulate control systems to cause physical impacts, such as explosions or the release of hazardous materials. These attacks can be numerous and widespread during military conflicts. Hackers, whether employed by nation states or acting patriotically, may target critical infrastructure like water facilities and power plants to disrupt operations and cause chaos.

Organizations operating in global manufacturing must know regional regulatory requirements for manufacturing security, which require them to comply with various mandates. Failure to meet these mandates often leads to fines and possible suspension from operating in a specific marketplace.

OT assessments provide valuable insight into creating supporting artifacts for the senior leadership team to invest in or delay additional security measures. Assessments offer detailed metrics to executives to make a well-informed decision to invest in new OT technology and quantify the level of risk if the decision is not to move forward. Ultimately, a 3rd party security assessment can be the most effective tool in building a case for investment in OT security.

> **Are you concerned about threats against your OT environment or long overdue for an assessment identifying potential vulnerabilities?**

Understand The Threat To Your Current OT Cybersecurity Posture

Outdated manufacturing systems are vulnerable to cyber-attacks because they lack secure-by-design security features, are difficult to patch, lack incident response capabilities, and lack vulnerability management programs. Cyberattacks on automated manufacturing and industrial operations facilities can cause significant revenue loss and downtime, making companies enticing and vulnerable targets.

Case Study: China and Taiwan Cyberattacks Against Critical Infrastructure

Tensions between China and Taiwan led to a rise in cyber espionage targeting industrial organizations in the Asia-Pacific region and the United States. These targets included chip manufacturing facilities in Taiwan, a military base in Guam, and industrial systems in the Philippines.

Case Study: Clorox Security Breach

In September 2023, a US-based consumer and professional products manufacturer, Clorox, announced that a cybersecurity attack that damaged its IT infrastructure and caused widespread disruptions to its manufacturing operations may significantly affect its first-quarter results. In 2024, Clorox updated the expected losses from the attack to total between $85 million and $95 million.

Assessing Critical Components Within Your OT Cybersecurity Infrastructure

Under IEC 62443-3-2, there are seven sections to completing an assessment for OT environments:

1. The first step is to map out all the systems in the OT environment and identify how they are connected. This step involves conducting asset discovery, inventory, and mapping the system's architecture and network components. Considering company policies, regulations, and acceptable risk levels is essential.
2. Perform Cybersecurity Risk Assessment. The company will assess its cyber risks by reviewing OT risk assessments and using an enterprise risk matrix to identify vulnerabilities and threats. This step is critical for establishing a reference point for future action.
3. Divide the System Under Consideration (SUC) Into Zones and Conduits. Break down the system into smaller parts and pathways for better risk management. Understand standards, policies, and supplier guidelines and analyze critical elements.
4. Evaluate the Current State of Risk. This step checks if the risk is okay for the company. We must take more steps to lower it if it's too high.
5. Execute a More Detailed Cybersecurity Risk Assessment. If there's a high risk, we need to do a detailed assessment to determine where risks could occur and devise ways to deal with them.
6. Continuous documentation is a must. Document the system's cybersecurity requirements. This document includes all assumptions, issues, and results and is a reference for security measures and audits.

7. Submit requests to the Change Control Board for Remediation Approval. Forward recommendations for implementing measures to resolve discovered vulnerabilities and exploits that could lead to a cybersecurity breach in the OT environment of the business or asset owner.

Defining The Tolerance for Risk

Understanding your organization's unique risks is the first step to building a solid security posture.

Organizations defining their various levels of concerns from current or future cyber attacks against your OT environment start with breaking down the considered risks into separate categories:

- Operational Safety Risk (Preventable): What would affect the organization's employees if a cyberattack shut down the various control units, including PLCs, SCADAs, and other critical infrastructure?
- Production Impact Risk (Strategic): What is the risk if a cyberattack disrupts production operations, material processing, or automation controls?
- Environmental Impact Risk (External): What is the risk to the facility and local environment if hackers successfully breach the various protection layers for chemicals, environmental safeguards, and other critical environmental systems?

What Risk Method Aligns With an OT Environment?

The NIST Cybersecurity Framework (CSF) 2.0 Manufacturing Profile helps industrial manufacturers manage cybersecurity risk in line with industry goals and best practices. It offers a voluntary, risk-based approach to cybersecurity for manufacturing systems, meant to work alongside existing standards and guidelines.

Manufacturing plants are vulnerable to cyber-attacks.

Implementing strong cybersecurity measures is essential to protect against disruptions and theft. NIST CSF 2.0 can help manage these risks effectively.

The CSF 2.0 framework is broken into six categories:

1. Identify: Enhance your knowledge to effectively handle cybersecurity risks related to systems, assets, data, and capabilities.
2. Protect: Establish and place necessary measures to guarantee the provision of essential infrastructure services.
3. Detect: Create and carry out activities to detect cybersecurity incidents.
4. Respond: Create and execute activities to respond to a cybersecurity incident.
5. Recover: Keep plans to bounce back from a cyber attack.
6. Govern: Adding governance to the CSF 2.0 framework will help resolve past disconnections between aligning the framework's enablement and the organization's much-needed commitment to a management structure with tighter alignment to CSF 2.0 and validating the relevance of their security policies.

The manufacturing profile complements existing cybersecurity standards and industry guidelines and does not replace them. It helps manufacturers prioritize cybersecurity investments to reduce and manage risks. It works alongside the Cybersecurity Framework but is not a one-size-fits-all solution. Each manufacturer will have unique risks and will implement security practices differently.

Manufacturing facilities should follow ISO 55000, 55001, and 55002 for asset management. It helps meet standards, reduce downtime, and boost productivity.

Remediation and Go Forward Cybersecurity Operations Strategy for OT Environments

By 2025, cyber attackers could harm people by hacking into OT environments. New laws and directives are making CEOs and CISOs responsible. Yet, most OT systems go unpatched or unprotected for extended periods. There are already multiple documented examples of hackers attacking the safety systems in refineries which if they had been fully successful, could have allowed catastrophic failures putting employees and the public in severe danger. Manufacturers are beginning to deploy digital twins providing a high-fidelity, simulated production system, allowing the organization to test critical security patches without causing an operations failure.

Installing network and end-point monitoring (IDS), extended detection and response (XDR) and threat hunting are the popular controls of today used to detect and stop cyberattacks. While important and generally effective if implemented in a cohesive systematic approach, these tools are classified primarily as reactionary, not proactive. OT organizations should proactively implement additional layers of controls, processes, and training to move their security postures forward.

Here are some recommendations to help

Threat Modeling and Detection

Detection and threat modeling are at the core of preventing cyberattacks against converged OT environments. Manufacturers should continue to invest in network detection and response (NDR), security information and event management solutions (SIEM), and extended detection and response (XDR) solutions giving attention to how AI might enhance their effectiveness. With these and all other solutions, manufacturing firms must continually assess if they are working as expected. OT SecOps teams may burn considerable time and effort chasing false positives and negatives without accurately reporting the real intrusions.

Effective Incident Response

Manufacturers will continue to become even bigger targets as more infrastructures become IP-enabled and globally accessible, and their data telemetry is processed with cloud-based analytics.

Even with sophisticated threat detection, reference architectures, and encryption, incident response is the most critical function converged OT manufacturing firms must assess. How OT organizations respond will either deter a hacker or encourage them to increase their velocity. Incident response is crucial in responding to future attacks and limiting impact.

Takeaway

Achieving OT cybersecurity maturity is a multi-faceted journey that begins with a thorough assessment of your current cybersecurity posture. By identifying strengths and weaknesses, you can lay a solid foundation for setting clear goals, establishing benchmarks, and developing a comprehensive and actionable cybersecurity roadmap. Each step builds upon the previous one, guiding your organization toward a resilient and adaptive cybersecurity posture.

As you progress through this journey, remember that cybersecurity is not a one-time effort but an ongoing process of continuous improvement and adaptation to new threats. Establishing a strong governance structure, investing in advanced technologies, and fostering a culture of cybersecurity awareness are crucial components of this journey.

Setting Goals and Benchmarks for Cybersecurity Improvement

The journey to OT cybersecurity maturity is a multi-faceted and continuous process. In the first chapter of this eBook, we discussed how to assess your current OT cybersecurity posture. Now, we move to the next critical step: setting goals and benchmarks for cybersecurity improvement. This phase is essential for guiding your organization toward enhanced security resilience and operational excellence. By establishing clear, measurable goals and benchmarks, you can systematically improve your OT cybersecurity posture, ensuring alignment with industry best practices and regulatory requirements.

Why Set Goals and Benchmarks?

Setting goals and benchmarks is akin to establishing a roadmap for your cybersecurity journey. Without them, efforts to enhance security can become fragmented, reactive, and ultimately ineffective. Goals provide direction and purpose, while benchmarks allow you to measure progress and make data-driven adjustments.

Key reasons to set goals and benchmarks include:

- Strategic Alignment: Ensuring that cybersecurity initiatives align with broader business objectives.
- Resource Optimization: Efficiently allocating resources to areas with the highest impact.
- Risk Management: Prioritizing actions that mitigate the most significant risks.
- Compliance: Meeting industry standards and regulatory requirements.
- Continuous Improvement: Establishing a culture of ongoing enhancement and resilience.

Defining Clear Cybersecurity Goals

When defining cybersecurity goals, it's crucial to consider your organization's unique needs and challenges. Goals should be Specific, Measurable, Achievable, Relevant, and Time-bound (SMART). Here are some example goals for an OT environment:

- Enhance Network Segmentation: Achieve complete segmentation of critical OT networks from IT networks within 12 months.
- Increase Patch Management Coverage: Within the next 18 months, ensure 95% of OT systems are in scope for regular risk mitigation and/or remediation.
- Improve Incident Response: Develop and test incident response plans for all major OT systems within six months.

- Conduct Regular Risk Assessments: Perform quarterly risk assessments and adjust security measures accordingly.
- Enhance Employee Training: Provide cybersecurity training to 100% of OT staff within the following year.

Establishing Benchmarks

Benchmarks serve as reference points against which performance and progress can be measured. They provide the data needed to assess the effectiveness of cybersecurity measures and inform strategic decisions.

Here are steps to establish effective benchmarks:

- Identify Key Performance Indicators (KPIs): Determine the metrics that best reflect your cybersecurity performance. Examples include the number of detected incidents, time to respond to incidents, percentage of systems mitigated or patched, and compliance scores.
- Set Baseline Measurements: Conduct an initial assessment to understand your current state. This baseline will serve as a comparison point for future measurements.
- Define Target Levels: Set target levels for each KPI based on industry standards, regulatory requirements, and organizational goals.
- Regular Monitoring and Reporting: Continuously monitor KPIs and report on progress at regular intervals. Use this data to adjust strategies and improve performance.

Common Benchmarks in OT Cybersecurity:

- Incident Response Time: The average time taken to detect, respond to, and mitigate a cybersecurity incident.
- OT Vulnerability Management Compliance: The percentage of OT systems with vulnerabilities mitigated or remediated with the latest security patches.
- Network Segmentation Effectiveness: The extent to which OT and IT networks are correctly segmented to prevent lateral movement by attackers.
- User Training Participation: The percentage of OT personnel who have completed cybersecurity awareness training.
- Vulnerability Management: The number of vulnerabilities identified, mitigated and/or remediated within a specified timeframe.

Case Study: Setting and Achieving Goals in a Manufacturing Environment

Consider a global manufacturing company that aims to enhance its OT cybersecurity posture. Here's how they might set and achieve their goals:

- Goal: Improve OT Vulnerability Management
- Current State: Only 50% of OT systems are in scope for the OT vulnerability management program.
- Target: Achieve 95% OT vulnerability management coverage within 18 months
- Steps:
- Conduct a comprehensive inventory of all OT assets.

- Develop an OT vulnerability management process and risk methodology
- Develop and implement an OT risk register
- Train OT staff on the importance and procedures of the OT vulnerability management process.
- Monitor and report OT vulnerability management progress monthly.
- Benchmark: Track the percentage of systems having mitigated and/or remediated vulnerabilities, aiming for incremental improvements.
- Goal: Enhance OT Incident Response
- Current State: OT Incident response plans need to be updated and tested.
- Target: Develop, test, and refine OT incident response plans for all critical OT systems within six months.
- Steps:
- Review and update existing incident response plans.
- Conduct tabletop exercises to simulate potential incidents.
- Establish a dedicated incident response team.
- Invest in advanced detection and response technologies.
- Benchmark: Measure the time to detect and respond to incidents during simulations and actual events.

Aligning with Industry Standards

To ensure your goals and benchmarks are robust and comprehensive, align them with established industry standards such as IEC 62443, NIST SP 800-82, and the NIST Cybersecurity Framework (CSF) 2.0. These frameworks provide guidelines and best practices tailored to OT environments, helping you build a resilient cybersecurity posture.

For instance, the NIST CSF 2.0 includes the categories Govern, Identify, Protect, Detect, Respond, and Recover, which can serve as a foundation for setting goals and benchmarks. You ensure a holistic approach to cybersecurity improvement by aligning your initiatives with these categories.

Continuous Improvement and Adaptation

Cybersecurity is not a one-time effort but a continuous process. Regularly review and adjust your goals and benchmarks to adapt to evolving threats, technological advancements, and organizational changes. Foster a culture of continuous improvement by encouraging feedback, conducting regular training, and staying informed about the latest cybersecurity threat intelligence, trends, and best practices.

Takeaways

Setting goals and benchmarks is crucial in the journey to OT cybersecurity maturity

Goals and benchmarks provide direction, facilitate resource optimization, and encourage continuous improvement. Manufacturing organizations can significantly enhance their cybersecurity resilience by establishing clear, measurable objectives and aligning them with industry standards. Remember, the path to cybersecurity maturity is ongoing, and staying committed to these principles will help you navigate the ever-changing cybersecurity landscape.

Developing and Executing a Cybersecurity Roadmap

As part of our journey towards OT cybersecurity maturity, we have evaluated our current posture, established measurable goals and benchmarks, and are now looking to create and implement a comprehensive cybersecurity roadmap. This roadmap will serve as a strategic guide to ensure that all cybersecurity initiatives align with our organizational goals and regulatory requirements, providing a clear path to enhance our OT security posture.

The Importance of Developing a Cybersecurity Roadmap

A well-defined cybersecurity roadmap helps in the following ways:

1. Strategizing Efforts: Aligning cybersecurity initiatives with business objectives and regulatory requirements.
2. Prioritizing Actions: Focusing on high-impact activities that mitigate the most significant risks.
3. Allocating Resources: Ensuring efficient use of resources across the organization.
4. Measuring Progress: Tracking cybersecurity measures' implementation and effectiveness.
5. Facilitating Communication: Providing a clear framework for communicating cybersecurity plans and progress to stakeholders.

Key Components of a Cybersecurity Roadmap

A robust cybersecurity roadmap typically includes the following components:

Vision and Objectives: Defining cybersecurity program's overarching vision and specific objectives that align with the organization's mission and strategic goals.

1. Risk Assessment: Conducting thorough risk assessments to identify and prioritize risks using established frameworks like IEC 62443, NIST SP 800-82, NIST CSF 2.0, and CMMI.
2. Strategic Initiatives: Identifying and outlining the key initiatives required to achieve cybersecurity objectives.
3. Resource Planning: Allocating the necessary resources (personnel, technology, and budget) to support each initiative.
4. Timeline: Establishing a realistic timeline for implementing each initiative, including milestones and deadlines.

5. Metrics and KPIs: Defining the metrics and key performance indicators (KPIs) that will measure each initiative's success.
6. Governance and Oversight: Establishing governance structures to oversee the roadmap's implementation, including defining roles and responsibilities and setting up regular review processes.

Developing Your Cybersecurity Roadmap

Define Your Vision and Objectives

Start by articulating your vision for OT cybersecurity. For example,

> **"To create a resilient and adaptive cybersecurity posture that safeguards our people, preserves our OT assets, and supports our business goals"**

Next, set specific, measurable objectives that align with this vision. For example,

> **"Achieve 95% OT cybersecurity compliance for all manufacturing sites within 18 months"**

Conduct a Comprehensive Risk Assessment

Utilize established frameworks like IEC 62443 and NIST SP 800-82 to guide your risk assessment. Identify critical assets, potential threats, and vulnerabilities and prioritize these risks based on their potential impact and likelihood.

Identify Strategic Initiatives

Identify the key initiatives required to address the highest priority risks based on your risk assessment. This could include:

- Enhancing network segmentation to prevent lateral movement by attackers.
- Developing and testing incident response plans for all major OT systems.
- Implementing an OT vulnerability management process and risk register.

Allocate Resources

Determine the resources needed to support each initiative, including personnel, technology, and budget. Ensure that you have the necessary expertise and tools to implement the initiatives effectively.

Establish a Timeline

Develop a timeline for implementing each initiative, including key milestones and deadlines to track progress. Ensure that the timeline is realistic and takes into consideration any potential challenges or delays.

Define Metrics and KPIs

Identify the metrics and KPIs that will be used to measure the success of each initiative, such as incident response time, percentage of systems patched, user training participation rates, and network segmentation effectiveness.

Set Up Governance and Oversight

Establish governance structures to oversee the implementation of the roadmap, defining roles and responsibilities and setting up regular review processes. Ensure clear accountability for each initiative and regular progress reporting to senior leadership.

Executing the Cybersecurity Roadmap

Execution is where the plans and strategies outlined in your roadmap are put into action. Here's how to effectively execute your cybersecurity roadmap:

Communicate the Plan

Clearly communicate the roadmap to all stakeholders. Ensure that everyone understands the vision, objectives, and their role in the implementation. Use regular updates and meetings to keep everyone informed of progress and any changes to the plan.

Implement Strategic Initiatives

Begin with the highest priority initiatives. Ensure that resources are in place and that there is a clear plan for implementation. Monitor progress closely and update as needed to stay on track.

Track Progress and Measure Success

Use defined metrics and KPIs to track progress. Regularly review performance data and adjust strategies as needed. Conduct regular status updates and reviews to ensure that initiatives are progressing as planned.

Foster a Culture of Continuous Improvement

Encourage feedback and open communication. Use lessons learned from each initiative to improve future efforts. Stay informed about the latest cybersecurity trends and best practices. Continuously update your roadmap to reflect new threats and opportunities.

Case Study: Executing a Cybersecurity Roadmap in a Manufacturing Environment

Consider a global manufacturing company that has developed a cybersecurity roadmap to enhance its OT security posture. Here's how they might execute this roadmap:

Initiative: Improve Network Segmentation

Objective: Achieve complete segmentation of critical OT networks from IT networks within 12 months for all manufacturing sites.

- Steps:
- Conduct a network audit to identify current segmentation gaps for sampling manufacturing sites.
- Implement network segmentation technologies and best practices.
- Monitor and test the effectiveness of segmentation measures.
- Metrics: Percentage of network segments compliant with security policies.

Initiative: Enhance Incident Response

- Objective: Develop and test incident response plans for all major OT systems within six months.

- Steps:
- Review and update existing incident response plans.
- Conduct tabletop exercises to simulate potential incidents.
- Establish a dedicated incident response team and invest in advanced detection and response technologies.
- Metrics: Time to detect and respond to incidents during simulations and actual events.

Initiative: Increase OT Vulnerability Management Program Coverage

- Objective: Within 18 months, ensure 95% of OT systems are included in the scope of the OT vulnerability management program.
- Steps:
- Conduct a comprehensive inventory of all OT assets.
- Develop OT Vulnerability Management Process & Risk Methodology
- Develop and implement an OT risk register
- Train OT staff on the process and risk management.
- Metrics: Percentage of systems patched monthly.

Takeaway

Developing and executing a cybersecurity roadmap is critical to achieving OT cybersecurity maturity. It provides a structured approach to enhancing your security posture, ensuring alignment with business objectives and regulatory requirements, and facilitating continuous improvement. By following the steps outlined in this chapter, manufacturing organizations can systematically improve their cybersecurity resilience and protect their critical OT assets.

Measuring Progress and Adapting to New Threats

As we continue our journey towards OT cybersecurity maturity, it's crucial to not only implement and execute our cybersecurity roadmap, but also to measure progress and adapt to new threats. This fourth step ensures that our cybersecurity initiatives remain effective and responsive to the ever-evolving threat landscape.

The Importance of Measuring Progress

Regularly measuring progress is vital for several reasons:

- **Validation:** Ensures that cybersecurity initiatives are effective and meeting their objectives.
- **Accountability:** Holds teams and individuals responsible for their roles in the cybersecurity plan.
- **Optimization:** Identifies areas for improvement and reallocates resources as needed.
- **Transparency:** Provides clear reporting to stakeholders on the status and effectiveness of cybersecurity efforts.

Key Metrics for Measuring Cybersecurity Progress

To effectively measure progress, it's essential to define and track key metrics. These metrics should provide insights into various aspects of your cybersecurity posture:

- Incident Response Time: Measure the average time taken to detect, respond to, and mitigate cybersecurity incidents. Faster response times indicate a more robust incident response capability.
- Patch Management Compliance: Track the percentage of OT systems that are up-to-date with the latest security patches. High compliance rates demonstrate effective vulnerability management.
- Network Segmentation Effectiveness: Assess the extent to which OT and IT networks are properly segmented to prevent lateral movement by attackers.
- User Training Participation: Monitor the percentage of OT personnel who have completed cybersecurity awareness training. High participation rates reflect a well-informed workforce.
- Vulnerability Management: Count the number of vulnerabilities identified, mitigated, and remediated within a specified timeframe. Effective management reduces potential attack vectors.

Tools and Techniques for Measuring Progress

- Dashboards and Reports: Use cybersecurity dashboards and regular reports to visualize and communicate key metrics. These tools provide real-time insights and help track progress over time.
- Audits and Assessments: Conduct regular internal and external audits to verify compliance with cybersecurity policies and standards. Assessments help identify gaps and areas for improvement.
- Penetration Testing: Perform regular penetration testing to simulate cyberattacks and evaluate the effectiveness of your defenses. This proactive approach helps uncover vulnerabilities before attackers can exploit them.
- Incident Reviews: After each incident, conduct a thorough review to analyze what happened, how it was handled, and what can be improved. Incident reviews provide valuable lessons and drive continuous improvement.

Adapting to New Threats

The cybersecurity landscape is dynamic, with new threats emerging regularly. To stay ahead, organizations must be agile and proactive in adapting to these threats.

- Threat Intelligence: Leverage threat intelligence services to stay informed about the latest threats and attack techniques. Use this information to update your defenses and response strategies.
- Regular Updates: Keep all systems, applications, and security tools up-to-date with the latest patches and updates. This reduces the risk of exploitation through known vulnerabilities.
- Continuous Training: Provide ongoing training and awareness programs for all employees. As new threats emerge, update training materials to ensure the workforce is prepared.
- Adaptive Security Policies: Regularly review and update security policies to address new threats. Ensure that policies are flexible enough to adapt to changing circumstances.
- Advanced Technologies: Invest in advanced cybersecurity technologies such as AI-driven threat detection, behavioral analytics, and automated response systems. These tools enhance your ability to detect and respond to new threats quickly.

Case Study: Measuring Progress and Adapting in a Manufacturing Environment

Consider a global manufacturing company that is focused on improving its OT cybersecurity posture. Here's how they measure progress and adapt to new threats:

- Metric: Incident Response Time
- Current State: Incident response time is averaging 6 hours.
- Target: Reduce incident response time to under 1 hour within the next year.
- Steps:
- Implement a Security Information and Event Management (SIEM) system for real-time monitoring.
- Establish a dedicated incident response team.
- Conduct regular incident response drills.
- Progress: Track and report response times monthly. Adjust strategies based on performance data.

- Adaptation: Emerging Ransomware Threats
- Current Threat: Increased ransomware attacks targeting OT systems.
- Response:
- Integrate advanced endpoint detection and response (EDR) tools.
- Update backup and recovery procedures to ensure rapid restoration of operations.
- Conduct ransomware-specific training for all employees.
- Outcome: Reduced impact of ransomware attacks through faster detection and response, and improved recovery capabilities.

Continuous Improvement & Feedback

Continuous Improvement is the key to effective cybersecurity. There is nothing static in cybersecurity, the people using the systems change, the network and devices change, the applications running on the systems change, the products change, the people protecting the systems change, and the threats are likely changing the fastest.

Takeaway

Measuring progress and adapting to new threats are crucial aspects of achieving operational technology (OT) cybersecurity maturity. Manufacturing organizations can significantly enhance their cybersecurity resilience by defining clear metrics, utilizing advanced tools and techniques, and remaining agile in the face of new threats. It's important to remember that the journey to cybersecurity maturity is ongoing, and adhering to these principles will help navigate the ever-changing cybersecurity landscape.

Achieving and Sustaining Cybersecurity Maturity

As we conclude our thoughts on the roadmap to achieving operational technology (OT) cybersecurity maturity, it's important to emphasize the significance of attaining and maintaining cybersecurity maturity. This final step ensures that the progress made is sustained and continuously enhanced, thereby protecting your organization against evolving threats.

The Importance of Cybersecurity Maturity

Attaining cybersecurity maturity is not just about reaching a milestone; it's about integrating cybersecurity into the fabric of your organization's culture and operations.

Cybersecurity maturity brings several benefits:

- Enhanced Resilience: Mature cybersecurity practices reduce the likelihood of successful attacks and mitigate the impact of any breaches.
- Regulatory Compliance: Meeting and exceeding regulatory requirements will become more manageable.
- Operational Efficiency: Streamlined processes and clear policies lead to more efficient operations and resource utilization.
- Stakeholder Confidence: Demonstrating a mature cybersecurity posture builds trust with customers, partners, and stakeholders.
- Reduced Overall Downtime: Better visibility and diagnostics as well as better familiarity and clearly defined roles with continuous monitoring all lead to quicker mean time to repair (MTTR) for cyber and non-cyber events.

Key Components of Cybersecurity Maturity

- Leadership and Governance: Strong leadership and governance serve as the foundation of a mature cybersecurity program. This includes executive support, clear policies, and an effective governance structure.
- Risk Management: A proactive approach to identifying, assessing, and mitigating risks is crucial. This involves regular risk assessments and adapting to new threats.
- Continuous Improvement: Cybersecurity is an ongoing process. Continuous improvement ensures that your cybersecurity posture evolves with the threat landscape.
- Employee Awareness and Training: Cybersecurity awareness should be part of the organizational culture. Regular training and updates keep employees informed and vigilant.

- Incident Response and Recovery: Robust incident response and recovery plans ensure that your organization can quickly and effectively handle any incidents.

Achieving Cybersecurity Maturity

Establish a Cybersecurity Framework:

- Adopt and adapt recognized frameworks such as NIST CSF, ISO, or IEC. These frameworks provide structured guidance and best practices.
- Ensure the framework aligns with your organizational goals and regulatory requirements.

Develop a Comprehensive Cybersecurity Policy:

- Create policies that cover all aspects of cybersecurity, including access control, incident response, and data protection.
- Ensure policies are clearly communicated and understood by all employees.

Implement Robust Risk Management Processes:

- Regularly conduct risk assessments to identify and prioritize risks.
- Develop and implement mitigation strategies to address identified risks.

Invest in Advanced Technologies:

- Utilize advanced cybersecurity technologies that provide benefits in threat detection, behavioral analytics, and playbook automation.
- Ensure that your technology stack is regularly updated and maintained.

Foster a Cybersecurity Culture:

- Promote cybersecurity awareness through continuous training and communication.
- Encourage a culture where cybersecurity is everyone's responsibility. Think like safety!

Measure and Report Progress:

- Use key performance indicators (KPIs) and metrics to measure the effectiveness of your cybersecurity initiatives.
- Regularly report progress to stakeholders and adjust strategies based on feedback and performance data.

Sustaining Cybersecurity Maturity

Regular Audits and Assessments:

- Conduct regular internal and external audits to ensure compliance with policies and standards.
- Utilize assessments to identify gaps and areas for improvement.

Continuous Training and Development:

- Provide ongoing training and professional development opportunities for your cybersecurity team.
- Update training programs to reflect new threats and best practices.

Adapt to Evolving Threats:

- Stay informed about the latest cybersecurity threats and trends through threat intelligence services.
- Regularly review and update your cybersecurity policies and practices to address new challenges.

Foster Collaboration and Information Sharing:

- Participate in industry forums and information-sharing initiatives.
- Collaborate with peers and industry experts to stay ahead of emerging threats.

Leverage Automation and Technology:

- Use automation to streamline repetitive tasks and enhance response times.
- Implement technology solutions to detect and deliver intelligence driven playbook automation to deliver guidance for response.

Case Study: Sustaining Cybersecurity Maturity in a Manufacturing Environment

Consider a global manufacturing company that has achieved cybersecurity maturity:

Leadership and Governance:

- The executive team actively supports and participates in cybersecurity initiatives, including regular training and table-top exercises.
- A dedicated cybersecurity governance committee oversees policy implementation and compliance.

Risk Management:

- Regular risk assessments are conducted, and mitigation strategies are continuously updated.
- Advanced threat intelligence services provide real-time insights into emerging threats.

Continuous Improvement

- The organization has established a continuous improvement program that integrates feedback from audits, assessments, and incident reviews.
- Regular updates to the cybersecurity roadmap ensure alignment with the latest best practices and threat landscape.

Employee Awareness and Training

- All employees receive mandatory cybersecurity training, with specialized training for high-risk roles.
- Cybersecurity awareness campaigns and phishing simulations are conducted to keep employees vigilant.

Incident Response and Recovery

- The incident response team conducts regular drills and simulations to ensure preparedness.
- Advanced recovery plans are in place to minimize downtime and data loss in case of an incident.

Securing our Future

Achieving and sustaining cybersecurity maturity requires continuous effort and adaptation. Manufacturing organizations can build a resilient cybersecurity posture by embedding cybersecurity into the organizational culture, leveraging advanced technologies, and fostering a proactive approach to risk management.

About the Authors



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.



Chuck Tommey

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

Chuck Tommey is dedicated to helping clients of Hillstrong Group Security architect and implement sustainable Operational Technology (OT) cybersecurity solutions that effectively reduce risk. With over 30 years of experience, Chuck's approach centers on understanding business needs before offering tailored cybersecurity strategies. His career spans innovative and cost-effective solutions for organizations ranging from Fortune 100 companies to startups.

Chuck's expertise extends to guiding companies in understanding OT-specific cyber threats and implementing risk-based cybersecurity programs that result in robust, supportable network architectures. He is a committed lifelong learner and an engaging communicator, frequently contributing to industry knowledge through publications, webinars, and speaking engagements. Chuck has presented at numerous notable conferences, including AUTOMATE!, Siemens Automation Summit, Hydrogen Technology Expo North America, and SANS ICS Security Summit, among others.

Ready to achieve Operational Resilience with Your OT Cybersecurity Program?

Roger, Chuck, and the entire Hillstrong team are ready to assist in your OT Cybersecurity transformation. Hillstrong was built to help manufacturing and critical infrastructure organizations maximize their operational resilience by creating and implementing the most effective and sustainable OT Cybersecurity Programs possible for their stage of maturity. Then we can go further and help elevate that level of maturity, unlocking more capability and reducing risk to the desired target level.

+1 (800) 820-8210 | info@HillstrongSecurity.com

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