#CS4CA

CYBER SECURITY FOR CRITICAL ASSETS

USA

Industrial CISO

PERSPECTIVES

Crafting a World-Class Security Program for your Unique Environment

Research

Shri Cockroft

Director IT Compliance and Disaster Recovery

Americold Logistics, LLC.

Enhancing OT Cybersecurity, Collaboration and Executive Engagement

> Takepoint:
>
> The intricacies of various markets present unique challenges in maintaining focus amidst critical duties such as saving lives or ensuring system reliability.

> From your extensive experience across different verticals, how do you perceive the role of security in facilitating these essential functions without hindering productivity or reliability?

Cockroft: My tenure of six years at my company has illuminated the dual necessity of facilitating job performance while ensuring security. In navigating the cyber insurance renewal process, I gained valuable insights into securing Operational Technology (OT) environments. My previous experience working in healthcare and building an Edge IT control framework from inception underscored the importance of cybersecurity in maintaining continuity of care and safeguarding against potential threats to implanted medical devices, and other doctor-owned blue-tooth medical equipment connected to the internet, thereby potentially affecting patient safety.

Based on experience, best practices focus on building partnerships with engineers who concentrate on customer-specific requirements, ensuring that there is collaboration and layered security in place, despite potential resistance due to the high stakes involved. Moreover, the distinction between IT environments and OT security underscores the challenges of integration, budgeting, and asset management, further complicated by vendor support and proprietary information.

The goal is to develop a world-class security program tailored to your unique environment. This involves taking inventory, completing a risk assessment, identifying gaps, building necessary security controls based on a roadmap and understanding regulatory requirements across industries. Emphasis on critical thinking is crucial, as common controls like air gapping or network isolation, and maintaining tight control over third-party support and contractual obligations, play pivotal roles in securing industrial environments.

> Takepoint:
>
> The challenge of ensuring third-party vendors not only agree to security measures in contracts but also fulfill these obligations is a significant concern, notably in large-scale operations involving critical infrastructure. With potentially hundreds of vendors and their personnel accessing systems daily, how do you manage and verify the granularity of their roles, responsibilities, and the execution of contracted tasks, particularly in terms of upgrades or maintenance activities?

Cockroft: The complexity of third-party management cannot be overstated, particularly in environments with substantial reliance on vendors for operational support. In my role, overseeing cloud vendors and involving myself in the security requirements of critical vendors are top priorities. Ensuring that security requirements and responsibilities within contracts are thoroughly documented and reviewed is just the first step. Equally important is making sure that vendor relationship owners understand their responsibilities—not only to adhere to the contract terms but also to actively monitor and verify the security posture of these vendors.

Tools and practices such as obtaining SOC reports, monitoring security vulnerabilities, and accessing security scorecards are fundamental in providing an overview of a vendor's security health. Despite these efforts, challenges persist in most organizations, including contracts signed outside of security review processes. To address this, it is important to work closely with engineering teams to establish controls that enhance the capability to monitor and ensure compliance with our security standards.

> Takepoint:
>
> With the evolving landscape of cybersecurity, particularly in OT, how does your approach to asset visibility and security, fit into your overall security strategy?

Cockroft: I can't speak specifically about my organization, but I recommend an allocation of funds specifically for the OT security budget, which is a significant step forward. This can be achieved by a heightened focus on security across the organization as a whole.

Since compiling an inventory of OT assets can be challenging, the strategy should involve a more sophisticated approach to asset identification, allowing a better understanding of the current landscape. It is recommended to make several investments into layered security for OT environments. Fostering closer partnerships with the Operational teams that own OT systems is crucial. This collaboration is aimed at delineating responsibilities: deciding what actions the cybersecurity team will undertake versus those that fall within the operational team's purview.

> Takepoint:

> Engaging operational teams in cybersecurity initiatives can be challenging due to their focus on core responsibilities. How have you succeeded in making them more attentive to cybersecurity, particularly by emphasizing the importance of reliability, productivity, and safety?

Cockroft: My experience in this area began in 2017 and involved starting with gaining a keen understanding of the organization's strategic objectives. Next, I found out what were the key goals and initiatives for the operational teams I was working with. With that, I began to map my security initiatives for their areas to their goals, along with the organization's strategy to gain their buy in.

The key to further engaging these teams lies in raising awareness. This effort includes learning from security practices in warehouses and other OT environments, where I discovered common challenges and innovative solutions, such as keeping operational systems completely segregated and using secure methods for updates and vendor interactions.

One inspiring approach shared with me by an OT security leader, who also happens to be a friend of mine, partnered with engineering teams and restricted updates where only a dedicated laptop is used for updates that never connects to the internet, favoring USB for firmware updates to maintain security. Vendors are not given access, but instead provide support by monitoring troubleshooting and guiding efforts of engineers. This level of security, where vendors are kept at arm's length from the systems, is ideal for certain environments.

When it comes to reliability, incident plans should include tabletop exercises specific to OT environments and be updated with lessons learned. Business Continuity Plans should cover OT systems, and backups for OT environments should include data attributes specific to them, such as PLCs.

> Takepoint:
>
> In the context of evolving technical solutions for cybersecurity, such as network segmentation and asset discovery, the persistent challenge appears to be the human element and organizational culture. Engineers, for example, may seek workarounds if security measures seem to hinder their workflow. How do you address this cultural challenge and ensure widespread awareness of cyber risks?

Cockroft: Addressing the cultural aspect of cybersecurity is pivotal in our strategy, especially given our reliance on vendors for supporting OT environments. To tackle this, we are refining our contractual language in collaboration with our legal

department, ensuring we have the appropriate mechanisms in place during vendor renewals to emphasize due diligence. This is crucial for our unique automation sites, where vendor support is vital yet presents potential cybersecurity risks.

> Takepoint:
>
> As the industry leans more towards advanced solutions like Multi-Factor Authentication (MFA) to combat phishing and credential theft, how is your organization adapting to these technological advances?

Cockroft: Our adaptation to these emerging technologies is demonstrated through the deployment of hardware security keys, such as YubiKeys, which introduce an additional layer of security by requiring physical possession of the key alongside a passphrase. This initiative is part of our broader strategy to enhance our cybersecurity posture in the wake of incidents that have underscored the importance of a robust and united approach to cybersecurity across the organization.

Moreover, the emphasis on reporting and demonstrating the tangible benefits of our cybersecurity investments is a critical aspect of our strategy. This not only involves securing the necessary funding but also proving that our efforts have led to a comprehensive and accelerated improvement in our security maturity, across all areas of the organization.

> Takepoint:
>
> In terms of accountability and progress within cybersecurity, how do you quantify your achievements? Are these measurements tied to the risk assessments you previously mentioned?

Cockroft: Indeed, our progress is closely monitored and quantified through regular risk assessments, but beyond that, we have a structured approach to reporting our advancements. We report to our board quarterly, underpinned by a detailed three-year roadmap that outlines our initiatives. This structure places significant pressure on us to not just implement but also to demonstrate tangible progress. It's about transforming the typical silo mentality into a unified effort—something I actively promote. For example, when discussing projects with engineers, my role extends

beyond oversight; I become an advocate and partner in their efforts, ensuring we align on security measures and incident response plans.

This collaborative approach has become especially critical following incidents that impacted our operations significantly, leading to a heightened awareness across the organization about the importance of cybersecurity.

> Takepoint:
>
> You mentioned that you were recently involved in renewing your cyber insurance policy. The insurance process often translates cybersecurity into financial terms, emphasizing the 'value at risk.' How does this financial perspective shape your cybersecurity strategy and stakeholder engagement?

Cockroft: The insurance process indeed casts cybersecurity in a stark financial light, making it a powerful tool for aligning perspectives across the organization. With insurance companies increasingly scrutinizing entities following numerous incidents, the risk of not being able to renew policies becomes a tangible concern. This scenario underscores the direct link between operational resilience, customer satisfaction, and ultimately, our bottom line.

Our approach to demonstrating value and securing buy-in revolves around the operational impact—how incidents can halt customer operations, leading to reputational damage and strained relationships. To address this, we recently organized a security roundtable with key customers, reinforcing our commitment to partnership and resilience in the face of shared cybersecurity threats.

By viewing our systems holistically and prioritizing risk assessment findings, we can methodically address vulnerabilities, reinforcing our security posture and ensuring continuous improvement in a landscape where threats are ever evolving.

> Takepoint:
>
> The trend towards transparency and communication with partners is becoming increasingly important in cybersecurity. Unlike some sectors that historically might have hesitated to share information, it seems that evolving regulations and the need for collaboration are shaping a new approach. How do you navigate these changes in your organization?

Cockroft: Our strategy emphasizes not only having the right tools in-house but also leveraging partnerships to enhance our cybersecurity maturity swiftly. A crucial step in this journey begins with securing executive support. Without leadership backing, both in terms of awareness and resources, meaningful progress in cybersecurity is challenging to achieve. This support is foundational, not just for initiating a cybersecurity program but for sustaining and scaling it across the organization.

Highlighting the necessity of executive buy-in, our approach includes regular engagement with leadership to align cybersecurity initiatives with the organization's strategic goals. This alignment ensures that OT security, which spans various operational areas, receives the attention and resources it needs.

> Takepoint:
>
> Considering the challenges smaller entities face, especially in sectors like critical infrastructure, how can they overcome resource and skill constraints to bolster their cybersecurity defenses?

Cockroft: My experience across healthcare and other sectors has taught me the importance of understanding the executive team's perspective. Each management team has its unique concerns and priorities. The key is to tailor your message, showing how cybersecurity aligns with their goals and the broader organizational objectives.

For smaller organizations, where resources are scarcer, this approach is even more critical. Understanding and articulating the value of cybersecurity in terms that resonate with leadership can lead to the necessary support and resources. This strategy involves not only securing initial buy-in but also maintaining a dialogue to ensure ongoing commitment to cybersecurity as an integral part of the business.

Moreover, recognizing that OT security is a collective responsibility rather than solely an engineering task helps break down barriers within the organization. This mindset shift is essential for fostering a culture where cybersecurity is valued and prioritized across all levels of the organization.

> Takepoint:

> Given the distinct challenges in industrial settings, such as critical infrastructure or manufacturing, how do you believe the role of a CISO in these environments diverges from more conventional sectors? How does one adapt from, say, a financial or healthcare background to address the unique needs of industrial cybersecurity?

Cockroft: The transition to industrial cybersecurity certainly presents unique challenges, not least of which include dealing with legacy systems that are often outdated and unsupported. This requires not just a technical adjustment but also a strategic shift towards securing funding and executive buy-in for necessary upgrades or replacements. Another critical aspect is the often encountered flat network architectures, where isolation alone is insufficient. Continuous patching and updates are essential, even for isolated systems, to mitigate vulnerabilities effectively.

The core difference in industrial settings is the need to understand and work closely with OT that supports proprietary systems. This demands a collaborative approach with engineers and operations teams to ensure that cybersecurity measures are effectively implemented without hindering operational efficiency. Building relationships and understanding the unique environment are crucial before proposing solutions or creating a cybersecurity roadmap.

> Takepoint:
>
> It appears that fostering trust and collaboration with engineering and operations teams, who may operate semi-autonomously within the organization, is vital. How do you approach building this trust and ensuring cybersecurity is integrated into their workflows?

Cockroft: Building trust with engineering and operations is indeed central to effectively managing cybersecurity in industrial contexts. It's about finding common ground and demonstrating that cybersecurity measures are not about imposing restrictions but about protecting the company and its customers. This involves understanding their priorities, communication styles, and the specific risks associated with their operations.

An additional layer to consider is the clear definition of roles and responsibilities (RACI matrix) among different stakeholders. This clarity ensures that everyone knows their part in maintaining security, which is particularly important when balancing operational productivity with cybersecurity requirements. Establishing

this understanding is foundational to creating a culture where cybersecurity is seen as a shared responsibility across all facets of the organization.

> Takepoint:
>
> Thank you for sharing your insights highlighting the importance of adapting cybersecurity strategies to fit the unique demands of industrial environments. It is clear That this adaptation not only involves technical solutions for legacy systems and network architecture but also emphasizes the significance of relationship-building, strategic communication, and clear delineation of responsibilities. These elements are key to integrating cybersecurity into the core operations of industrial organizations

About Takepoint Research

Takepoint Research is an exclusive analyst firm that specializes in delivering meticulous research and actionable insights for industrial enterprises and their cyber defenders. The firm's steadfast commitment lies in offering unequivocal, strategic counsel, tailor-made to cater to specific requirements, while steadfastly steering clear of biases and irrelevant distractions.

Industrial organizations use Takepoint Research's practical reports, blueprints, and advice to confidently navigate each stage of their industrial cybersecurity journey. The firm's core mission is to offer clarity and strategic vision, presenting a comprehensive current and future industry outlook, key players, regulatory focus, critical technologies, solutions, services, and industry-best practices.

Established in 2016, Takepoint Research's dedicated analyst team, composed of industrial cybersecurity professionals and veterans, prioritizes the safety, resilience, and productivity of organizations within the critical infrastructure and manufacturing sectors. Trusted by global industrial enterprises, Takepoint Research serves as a guide in creating a more secure and safer industrial future.

Recognizing that truly valuable advice is defined by its impact, we remain committed to delivering insights that make a meaningful difference.