#CS4CA
CYBER SECURITY FOR CRITICAL ASSETS
APAC

#APAC
CYBER SUMMIT

Industrial CISO

PERSPECTIVES

From Vulnerabilities to Strategy: Transforming Industrial Cybersecurity Management

Research

Justin Nga

Cybersecurity Manager
CitiPower and Powercor

Dealing with OT cybersecurity landscape

> Takepoint:
>
> Can you describe your role within the organization and how it influences your approach to cybersecurity, particularly in terms of strategic planning and addressing vulnerabilities?

Nga: I am the cybersecurity manager for my organization reporting to the Technology and Security Manager. My daily responsibilities revolve around strategizing for both the present and future states of our business, specifically focusing on our cybersecurity infrastructure and controls that manage our cyber risk. This also includes management and board reporting, providing updates on our program of work, threat landscape, metrics in terms of control coverage and effectiveness, and overall security posture. Additionally, we also provide security governance and architecture reviews for projects through the architecture review board, alongside the other domain architects. Essentially, security-related queries or concerns are directed to our team.

My background is in industrial control systems, a field I was involved in before the term 'operational technology' (OT) was coined. This has helped provide me a unique perspective on cybersecurity challenges in industrial environments. Back then, the concept of integrating security from the early stages of development was not as emphasized as it is today. This historical context highlights the evolution towards a 'shift left' approach towards cybersecurity and underscores the importance of adapting to this paradigm to address contemporary security challenges effectively.

We are committed to ensuring that we drive a 'shift left' culture, focusing on "secure by design" principles before deployment, rather than productionizing and then addressing security design weaknesses and vulnerabilities as an afterthought. This approach avoids the need for makeshift solutions to secure the product post-deployment. From there, a vulnerability management program manages the operational patching. This perspective is central to our strategy and aligns with the proactive stance we take towards security.

> Takepoint:
>
> Can you describe the composition and expertise within your cybersecurity team, and how does this diversity contribute to your strategic objectives?

Nga: Our team is a diverse blend of technical and risk management expertise and evolving skill sets, reflecting a broad spectrum of experiences and backgrounds. At the core, each member brings a strong technical foundation, having transitioned from hands-on roles to more strategic positions encompassing risk management, product management, governance, and architecture design and deployment.

Among us is a PhD in IP networks, who brings a deep understanding of complex network and infrastructure challenges.

Another team member adds to the mix his background in IT operations and infrastructure, providing a solid base in the technological underpinnings of our cybersecurity technology platforms.

The latest addition to our team is an analyst who, despite being newest, brings a valuable new perspective from his previous organization. He has swiftly developed his ability to analyze data, learning to decode numbers and statistics to uncover cybersecurity patterns and insights that aid in our risk assessments

My expertise lies in control systems, reflecting a journey from the operational to the strategic across OT and IT. I started as a control systems engineer before specializing in industrial ethernet networks when it became more pervasive in different industrial verticals like process control, discrete manufacturing, power and transportation.

My team works in tandem with the Security Operations, Risk and Assurance and the Architecture teams.

Together, we possess a well-rounded set of skills, ready to tackle challenges with a blend of technical knowledge and strategic foresight.

> Takepoint:
>
> Considering past cybersecurity incidents, how do you perceive the evolving landscape of threats, particularly regarding OT, and what lessons can be drawn from these developments?

Nga: It's intriguing to discuss trends in cybersecurity, particularly how they impact OT. Let's look back in history. Many would have forgotten the cyber incident at the Maroochydore Shire sewage treatment facility. It was a hot topic due to an attack on OT systems by a disgruntled employee of the system integrator that worked on the plant. When you look beyond the "OT cyber-attack" hype and get to root cause, this was a supply chain risk of an internal disgruntled employee combined with a failure to deprovision the identity and access in a timely manner. This underscores the importance of looking beyond the surface to understand the root causes of cybersecurity incidents, which often point back to foundational security hygiene practices.

Initially, I too focused on the distinct aspects of OT and IT, but I've come to realize the interconnectedness and the overarching theme of cyber risk management across OT and IT. Best practices apply equally across both domains, but their application and deployment may have specific nuances.

> Takepoint:
>
> How do you view the relationship between risk management in IT and safety in OT, especially with the ongoing convergence of these fields?

Nga: Cybersecurity in IT and safety in OT both fundamentally revolve around managing risk. The challenge we face with convergence isn't just about network convergence, which tends to be usual focus, but also about the convergence of the technology stack itself. IT technology, infrastructure, resources and protocols are increasingly used in OT environments. This includes common operating systems, applications, databases and network equipment, which introduces IT originated vulnerabilities into OT settings. Another critical issue often overlooked is the disparity in cybersecurity skills and resources between IT and OT. Even though organizations have a head start in their IT cybersecurity program and execution, incidents and breaches are still on the rise. This reality challenges the OT assumption that only adopting certain tools or technologies can fully safeguard against threats. It is important to realize that you cannot drive risk to zero. What should be done is a continuous process of cyber risk assessments against the threat landscape and pivoting to prioritize new controls or leveraging existing controls to manage the risk instead of focusing on the 'silver bullet' technology.

TP Analysis:

As industry analysts observing the cybersecurity sector, we have noticed a tendency to overlook important issues, such as control system vulnerabilities, due to a legacy of IT-centric approaches and vendor interests. Risk management is a universal concept across various sectors, such as manufacturing, power distribution, and oil and gas. Engineers have always engaged in risk assessment as part of their operational duties, treating cyber risk as another dimension of operational or engineering risk. However, the source of risk is less important than its potential impact, as it can affect production or contracted services.

The challenge lies in people rather than technology, as industry professionals have varying attitudes towards connectivity and integration. Despite

technological solutions and response plans, a significant barrier remains - a reluctance to engage in open discussions about risk management strategies. This reluctance highlights the need for greater collaboration and communication within the industry.

Creating an environment where diverse perspectives on risk can be shared and understood is crucial for developing effective cybersecurity measures responsive to modern industrial operations. Facilitating these discussions will help bridge gaps and foster a more holistic approach to cybersecurity in the industrial sector.

Covering cybersecurity concerns with the Board

Takepoint:

Can you share how you approached the board with your cybersecurity strategy when you first started, specifically given the prevalent fears about cyber-attacks?

Nga: When I first joined the team four years ago, I was tasked with developing a comprehensive cybersecurity program. At that time, there was significant concern among board members and management about potential cyber-attacks, fueled by warnings that adversaries could shut down operations. While completely justified, I aimed to shift the focus from these concerns to a more rational and actionable approach centered on risk management. I proposed a program that detailed how we would prioritize and allocate funding to manage risks that were specific to our organization over a period of three years.

Takepoint:

What strategy did you employ to secure board approval and funding for your cybersecurity measures?

Nga: I began by extrapolating the standard risk management model of Likelihood and Consequence into (Threat and Vulnerability) and Consequence. The Threat could be both an insider (accidental or malicious) or malicious outsider, and vulnerabilities could be known or unknown. By focusing on areas we could influence, such as accidental insider threats, vulnerability discovery and

management, and detection and response to reduce consequences, I outlined how targeted investments in these areas could reduce overall cybersecurity risks specific to our organization. For example, implementing an email security filtering system would reduce the likelihood of accidental clicks on malicious links by insiders. In addition, I emphasized the importance of a layered defense strategy, including cyber culture training, architectural defenses, and vulnerability management. This approach helped the board and management understand the rationale behind each proposed investment, the impact in reducing threat, vulnerability or consequence, thus leading to the support and approval of the funding. More importantly, it helped to shift discussions from only focusing on external malicious threat actors, which we can do little to influence, to focusing on areas within our control where we could reduce the risk.

> Takepoint:
>
> How do you handle the ongoing concerns of the board regarding cybersecurity, in light of the evolving threat landscape?

Nga: Every time there's a newsworthy cyber incident, it inevitably raises concerns among the board members and management. I address these concerns by deconstructing the incident based on the foundational risk model we established before. This method helps to remove hype from the news and allows us to assess pragmatically whether and how such an incident could impact us, what controls could apply, and guiding our discussion back to the principles of risk management. This consistent focus on risk has significantly aided in maintaining their support and understanding, proving essential for the ongoing success and funding of our cybersecurity initiatives. Even now, as I prepare for the second phase of our plan, the same principles of risk management continue to guide our strategy and discussions.

TP Analysis:
It's quite intriguing how the usual clarity and decisiveness seen in building business cases for addressing specific risks or investments seem to vanish when it comes to reacting to the latest cybersecurity breach. Essentially, the process should be straightforward: construct a solid business case, and if it holds merit, the necessary funds are allocated based on the anticipated value to the organization. This is a routine decision-making process at the executive level.

> However, the complexity of cybersecurity seems to introduce a unique challenge, possibly due to a lack of understanding of the technical details. Yet, it's worth noting that executives often make informed decisions in areas outside their technical expertise by relying on insights from their teams, making the hesitancy around cybersecurity decisions particularly curious.
>
> There is a need for a deeper comprehension of the human factors at play in (industrial) cybersecurity. Reflecting on the IT industry, its evolution has been relatively gradual, allowing for a more measured adaptation to changes. In contrast, the field of industrial cybersecurity is experiencing a rapid shift, akin to leaping across a vast chasm after years of complacency. This sudden awakening to a new reality necessitates a significant, almost quantum leap in approach and understanding, marking a fascinating phase in the industry's development.

Addressing survivable architecture across OT environments

> Takepoint:
>
> Can you elaborate on the concept of survivable architecture in OT and its significance?

Nga: Cybersecurity emphasizes building a defensible architecture. I view a survivable architecture in OT as one that emphasizes the ability of a system to continue operating even when certain components are compromised or disconnected, potentially due to a cyber incident response for zone isolation. For instance, if a Human-Machine Interface (HMI) in the control room is disconnected, a properly designed control system can still function because the essential logic and control mechanisms should be located at the edge, not in a separate zone or centralized cloud. This principle underlines the importance of local control and the inherent risks of relying too heavily on cloud-based solutions for critical control functions. It is important to understand the layers of availability control and safety protection in any OT design. The key takeaway here is that just because we have the capability to move controls to the cloud or further away from the edge or process, it doesn't necessarily mean it's the best course of action for maintaining operational resilience. And if it should be necessary to do so, the risk should always be assessed, and residual risks clearly articulated, understood and approved.

> Takepoint:
>
> How do you view the relationship between adopting new technologies and the inherent cybersecurity risks, notably with the necessity of internet connectivity for Industry 4.0?

Nga: The adoption of new technologies, particularly those integral to Industry 4.0, undeniably requires more OT to IT, and internet connectivity, which introduces significant cybersecurity challenges. The fundamental issue lies in understanding and evaluating the associated risks. It's a bit of a seductive notion to believe we can make internet facing assets entirely secure; the reality is that connecting to the internet exposes us to greater risks and the changing threat landscape. Businesses must therefore adjust their risk appetite, accordingly, weighing the benefits of new technologies against the potential cybersecurity threats. Cybersecurity should be a business enabler, and our role here with any technological innovation that pushes traditional OT boundaries that impact availability and safety, should be to articulate the risks clearly so that it is understood by the organization.

> Takepoint:
>
> Can you share an analogy that helps explain the concept of risk appetite in the context of OT cybersecurity?

Nga: I often use the evolution of car brake systems to illustrate this point. Traditional cars had a hydraulic master-slave cylinder system for braking, complemented by a mechanical cable operated handbrake. Modern vehicles, however, increasingly rely on electronic systems for braking by wire, including features like autonomous braking, which are controlled by an Electronic Control Unit (ECU). While these advancements offer numerous benefits, such as improved efficiency and safety features, they also introduce new risks.

For example, I referenced a video where a modified car lost all braking capability due to an ECU failure resulting from an engine fire, highlighting the absence of a mechanical backup like the traditional handbrake. This scenario underscores the trade-offs between embracing technological advancements and accepting the potential risks. Whilst one can argue that the likelihood of this scenario occurring is low, it does not preclude the fact that the consequence of this could be catastrophic, and the risk should still be assessed and documented as such. It's not about avoiding progress but about understanding and preparing for the risks

involved, ensuring that organizations are ready to make informed decisions about their cybersecurity risk appetite.

TP Analysis:

Facilitating open discussions and fostering collaboration across IT and OT divisions is crucial for addressing organizational risks effectively. Historically, IT personnel have often been viewed as outsiders in production and operational environments, creating a divide that hinders cooperative risk management efforts. However, there's a growing recognition that such segregation is counterproductive. The emerging consensus suggests a shift towards a more collaborative approach, where the distinction between OT and IT blurs, moving towards a unified technology (T) framework. This evolution is partly driven by generational changes and the realization that collective action is essential for safeguarding the organization and its customers, chiefly within critical infrastructure sectors.

The dialogue around integration and collaboration is gaining momentum, though challenges and resistance persist. Some industry professionals hold onto biases that discourage open dialogue on how to advance together. Yet, the necessity for such discussions is increasingly acknowledged, driven by external pressures like geopolitical events and the push towards Industry 4.0, which emphasizes the benefits of IT-friendly practices in manufacturing and beyond.

Critical infrastructure environments have shown resistance to this shift, often maintaining a siloed approach to IT and OT. However, the imperative to adapt is becoming undeniable. Conversations with many OT experts reveal a frustration with outdated attitudes that resist connectivity and integration, emphasizing the need to focus on current realities and proactive risk management. The stance of avoiding connection is no longer viable; the priority must be on finding solutions to manage and mitigate risks in an already connected and integrated technological landscape.

Inherent challenges of dealing with organizational cyber risk

> Takepoint:
>
> Can you share how your team assesses and communicates risk levels within the organization?

Nga: Typically, we run risk assessments for new projects and solutions, security exemptions, modifications to existing environments and industry threat intelligence. We use the same risk principles to identify and quantify the threat, vulnerability and consequences for inherent risk, the controls that can apply and the resultant residual risk. A consistent format is used to clearly articulate the risk and ensure that it is understood by all stakeholders, including shared responsibilities for specific controls if applicable.

> Takepoint:
>
> How do you navigate the challenges of sharing cybersecurity practices, both internally and externally?

Nga: Internally, fostering an open dialogue about cybersecurity practices can sometimes be challenging. I find a critical skill is to be able to deliver the information in a way that demystifies cybersecurity topics for different audiences. It's potentially even more complex when addressing external audiences. There's always a concern about disclosing too much intellectual property or not enough that can benefit the audience. A good litmus test is to ensure the information shared is both timely and creates a 'no harm' outcome for the organization or the industry. I try to keep an open mind that a rising tide lifts all boats, and there is always a sense of achievement if someone goes away learning how to be more secure in this rapidly changing cyber world.

> Takepoint:
>
> How do you assess and prioritize risks, chiefly considering the potential for internal versus external threats?

Nga: Our risk assessment strategy considers the likelihood of threats materializing from different vectors. We consider the outside-in and inside-out vectors. Outside-in, for example, is any asset that is internet facing, which will always be at a higher risk and priority than an internal network that has zones and is securely segmented. Inside-out however, we still need to consider the potential of an internal malicious or accidental threat, or the breach of credentials, and treat those risks **accordingly**.

TP Analysis:

While there's a growing interest in technologies like attack path analysis, breach attack simulation (BAS) and automated penetration testing, we maintain that understanding the consequences and critical assets upfront is essential. Without this foundational work, the rest becomes noise. It's crucial to focus on the most significant risks and not get distracted by every potential vulnerability.

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.