



New and Persistent Challenges Facing OT

Best Practice Approaches to Managing OT Security in Today's Environment

Accenture Cybersecurity Forum
Global Executive Leadership Network

27 June 2023
Session Summary



From the Accenture Leadership

Many enterprises are integrating industrial control systems and other OT assets with their IT environment in an effort to increase productivity and efficiencies. But ACF members recognize that those well-intentioned efforts add new vulnerabilities to the enterprise threat landscape.

Thanks to all those who participated in this roundtable discussion. While we heard that there are no quick fixes, ACF members report they are actively engaged with the means of production to protect enterprise assets and increase resiliency in the face of ransomware and other attacks.

We hope you find the shared experiences and best practices that emerged from the conversation useful.

Cheers,



Paolo Dal Cin

Global Head of Accenture Security
ACF Executive Sponsor

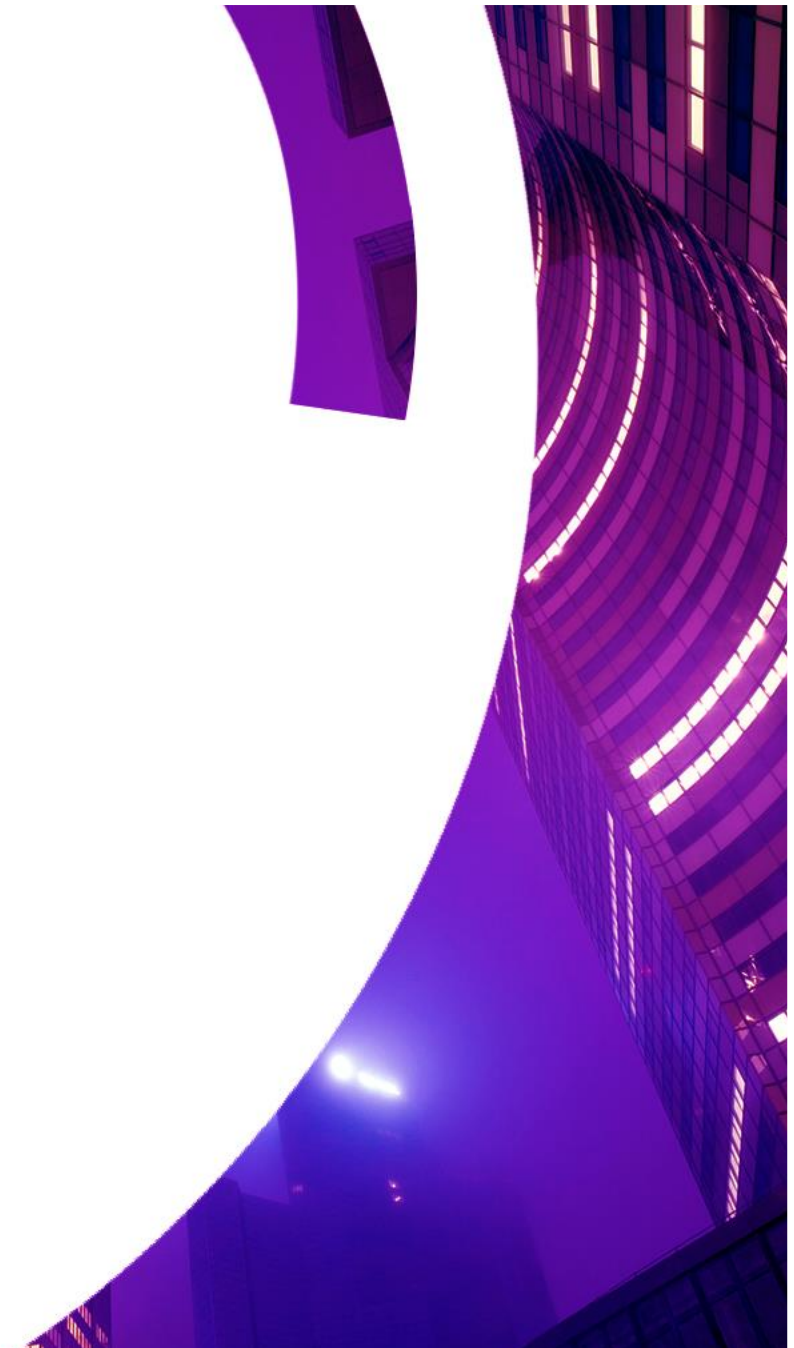
[LinkedIn](#)



Kris Burkhardt

Accenture CISO
ACF Chair

[LinkedIn](#)





New and Persistent Challenges Facing OT

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “New and Persistent Challenges Facing OT,” on June 27, 2023.

Forum members are concerned about the challenges of maintaining security of operational technology (OT) assets. In the face of supply chain issues, the rise of generative AI and a talent shortage, are there a set of security actions we should take? Are there any best practices we should follow?

This roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers, nor participants, is revealed.

In this summary:

[OT digitization drives complexity, which drives risk >](#)

[The value of architecture >](#)

[OT operator inertia >](#)

[Best practices >](#)



“ We have to cope with more bespoke solutions... We don’t have the opportunity to contract for \$5/node protection like we do in the IT environment.”

—ACF Member

OT digitization drives complexity, which drives risk

While OT technology matures and is integrated with the larger enterprise IT stack, CISOs are learning to adapt to new security demands. For example, an SME said: “Jargon and impact are very different than what most CISOs are familiar with, from standards like [IEC62443](#) and [ISO 27001](#) and impacts such as threats to worker safety and physical plant, versus data breaches.”

OT managed service providers “still have a way to go” in matching their traditional IT capabilities, said a subject matter expert (SME). Uncertainty remains about precisely which devices need to be secure, what protocols to apply and how to respond to threats.

The wide variety of disparate OT tools adds to complexity and risk, ACF members agreed. “We have to cope with more bespoke solutions,” said an ACF member. “We don’t have the opportunity to contract for \$5/node protection like we do in the IT environment.”



“ Know precisely when and where you can disconnect IT and OT to keep both environments secure.”

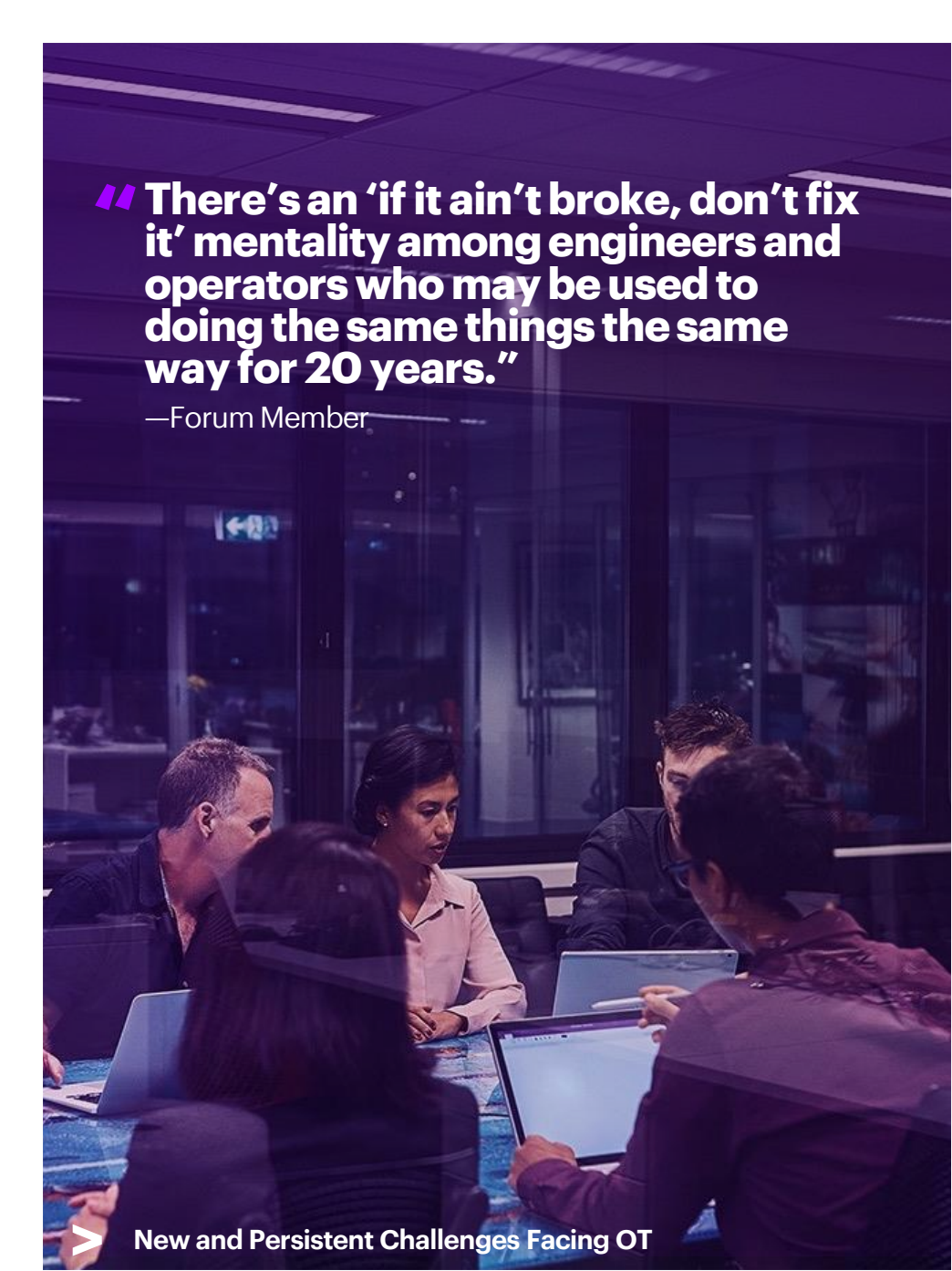
— Subject Matter Expert

The value of architecture

An ACF member said: “An OT SOC and managed security services are very difficult to operationalize. Without those foundations, architecture must provide the enabling points to minimize the attack surface and enable some basic cyber hygiene.”

Having an architecture for the entire OT environment, such as air conditioning, door locks and remote devices, can be useful in controlling access points, said an SME. Another SME added: “Know precisely when and where you can disconnect IT and OT to keep both environments secure.”

An ACF member added: “Naturalizing the convergence across IT and OT for detection will provide the full visibility across the entire kill chain vs. having an OT SOC-centric approach.”



“There’s an ‘if it ain’t broke, don’t fix it’ mentality among engineers and operators who may be used to doing the same things the same way for 20 years.”

—Forum Member

OT operator inertia

A Forum member said: “There’s an ‘if it ain’t broke, don’t fix it’ mentality among engineers and operators who may be used to doing the same things the same way for 20 years.”

Another ACF member said there is only one week a year when operations are suspended and there is an opportunity to upgrade security controls. “And you don’t have a chance to get it wrong when factory operations could be disrupted by a mistake or delay.”

In an operating environment such as a factory, which has been operating successfully for 20 years or more, it may not be realistic to implement sophisticated cloud-based security monitoring capabilities, said an SME. “We have to protect the new, and risk manage the old.”



“ Appreciate that ‘less is more’ when considering how much information OT operators require to understand and support security decisions.”

—Subject Matter Expert

Best practices

- **Get the basics right**—“The classic, old-school security controls still apply in the OT environment,” said a SME. “It’s OK that there may be an overlap between IT and OT tools.”
- **Overcome operator inertia**—Help OT operators, who already make safety a priority, understand, “If it’s not secure, it’s not safe.” Absorbing new technology takes time so a patient, step-by-step approach to change management is required. “Appreciate that ‘less is more’ when considering how much information OT operators require to understand and support security decisions.”
- **Actively collaborate**—“Build close connections between the corporate OT security team and operators in the field or factories,” said an SME. Informal connections, such as conversation over a drink, can go a long way in promoting collaboration and support for security priorities, said an SME.



“Your organization need to be prepared to say when to shut down operations and when it’s safe to go back online.”

—Member

Best practices (cont.)

- **Implement robust change control**—An SME said it is imperative to maintain rock solid control over who has access to the OT environment.
- **Preparedness drills**—Be creative and expansive in considering different threat scenarios. “The language of OT, the risks and the consequences are different than what the CISO typically encounters,” said an SME. At a minimum, analyze ‘game over’ scenarios and assess whether the right controls are in place. An ACF member added: “Your organization needs to be prepared to say when to shut down operations and when it’s safe to go back online.”
- **Clarify governance responsibilities**—“You need one person, not a committee, to make decisions when the environment is threatened,” said an ACF member. That person needs to understand both the OT and broader business implications of a cyber threat, and management needs to empower and protect that person.”



**“Let’s share what we know
to secure what we must.”**

— **Kris Burkhardt** Accenture CISO, ACF Chair

Work the network

Contact [our team directly](#)
for questions and member introductions.

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent and innovation led company with 738,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology with unmatched industry experience, functional expertise and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Accenture Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients succeed and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities. Visit us at www.accenture.com

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Visit us at accenture.com/security.

Copyright © 2023 Accenture All rights reserved.
Accenture, and its logo are trademarks of Accenture.