



Securing Critical Infrastructure

at the Speed of Digital Transformation

Accenture Cybersecurity Forum
Global Executive Leadership Network

17 November 2022
Session Summary





From the ACF Chair

When it comes to digital transformation, the CISO can be an accelerator, not a brake.

Members of the Accenture Cybersecurity Forum shared their experiences in convincing other business leaders that the right approach towards security can actually accelerate transformation, not slow it down.

Many of the suggestions had a motorsports racing theme.

- “Be in the passenger seat along with the business.”
- “Know how to drive the car, not just put on the brakes.”
- “Be prepared to move at the speed of the business.”
- “Plan and prepare so you don’t become a roadblock.”
- “The key is trusted relationships, not tools.”

We’ve all felt the pressure to squeeze costs, meet or beat deadlines and improve service delivery. Business leaders are no different, and when a game-changing digital transformation is on the line, the pressure can feel like driving a Formula 1 race car across the finish line ahead of the competition. **The CISO’s challenge is to ensure that the rest of team can advance safely, without sacrificing cybersecurity or enterprise resiliency.**

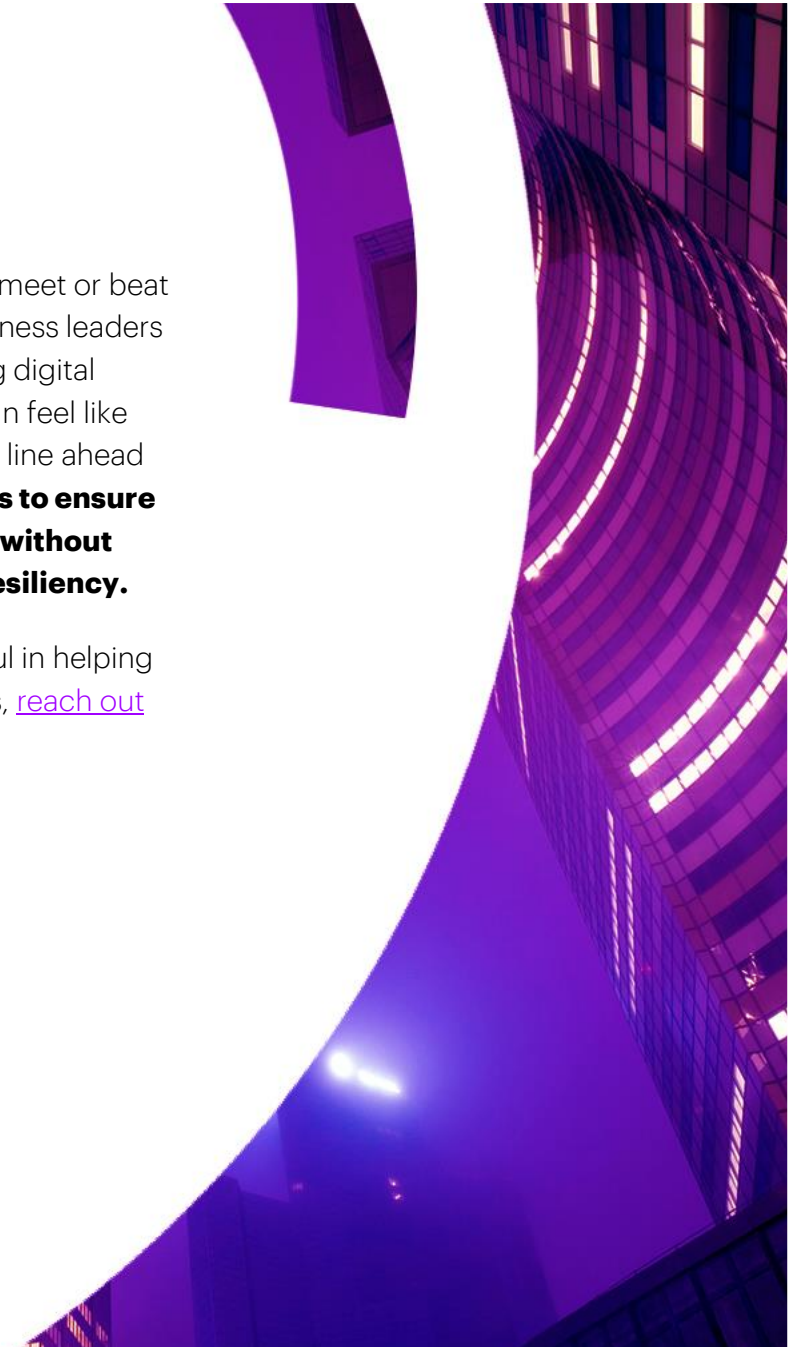
I hope you find these leading practices useful in helping your enterprise win their race. And as always, [reach out anytime](#) if you’d like to connect.

Cheers,

Kris Burkhardt

Accenture CISO, ACF Chair

LinkedIn: [Kristian Burkhardt](#)





Securing Critical Infrastructure

at the Speed of Digital Transformation

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “Securing Critical Infrastructure at the Speed of Digital Transformation,” on November 17, 2022. Members examined the challenges and opportunities for securing the enterprise during times of transformation with an eye toward defining a set of best practices that CISOs should follow to assure transformations are successful and secure.

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:

[Becoming a trusted advisor during digital transformation >](#)

[Leading practices >](#)

[Sample scorecard framework >](#)




“ Be in the passenger seat along with the business.”

Becoming a trusted advisor during digital transformation

Many of the enterprises represented by Forum members are undergoing a digital transformation, embedding technologies across their businesses to increase efficiency and greater business agility and, ultimately, unlock new value for employees, customers and shareholders. But despite efforts to adopt “security by design” and the CISO’s greater influence at the leadership table, members report that achieving secure digital transformation remains a challenge. In some cases, other business leaders see security requirements as a hindrance to achieving benefits quickly.

Forum members and subject-matter experts shared a variety of ideas for getting business leaders to appreciate that **addressing security upfront can actually accelerate time to value.**



“Be prepared to move at the speed of the business.”

Leading practices

- ❑ **Embed small security teams into business functions before they begin their transformation.** “Don’t wait until system testing to address cybersecurity requirements,” said a subject-matter expert. Having a small team of security pros working within each transformation team can eliminate the surprises that business leaders see as slowing their efforts to create new value.
- ❑ **Identify and engage with the drivers of digital transformation at the planning stage.** A CISO said an “Art of the Possible” planning session was an effective forum for raising cybersecurity issues with leaders who will be driving transformation initiatives.
- ❑ **Anticipate what leaders need to know about risk.** Get a head start in understanding what new business models are being considered. Have the security team ready before transformation begins. Be prepared to explain to the Board, CEO and transformation leaders how risk factors will change during and after a transformation.
- ❑ **Articulate the value proposition of cybersecurity in business terms.** Help transformation leaders appreciate what success looks like when the right security guardrails are in place, and what problems can occur when they’re missing. That clarity is critical in building the business case for cybersecurity.



“Plan and prepare so you don’t become a roadblock.”

Leading practices (cont.)

- ❑ **Don’t expect perfect compliance.** A Forum member said: “During a transformation you have to learn to be comfortable with variability. Get the baseline right, the SLAs, but don’t expect 100% compliance. A subject-matter expert added: Don’t create a requirement unless you know what good or done looks like, and then manage to operationally realistic SLAs
- ❑ **Assess the “state of readiness.”** Anticipate talent requirements, particularly when introducing new technology or migrating to the cloud. “In a transformation we’re talking about building a system of systems,” said a Forum member. “Specialists in one area may not have the breadth of skills required to adapt to a new, more complex system where the functionality they’re familiar must fit into a larger whole.
- ❑ **Digitally transform the security function.** Forum members said that an enterprise digital transformation can offer an opportunity to address the security debt and fund needed improvements. For example, with consolidation in the cybersecurity tools area, CISOs are finding opportunities to invest in platforms that replace disparate tools. A Forum member encouraged peers to set an example for the rest of the business for how digital transformation can occur rapidly.

“ A business transformation effort should be viewed as an opportunity to migrate to a platform and simplify cybersecurity operations.”

Leading practices (cont.)

- Use scorecards to drive behavioral changes and increase rates of adoption. Forum members acknowledge that dictating compliance isn't enough. Instead, take advantage of leaders' competitive nature by building scorecards that publicly identify the leaders from the laggards. "Peer pressure is a powerful force," said a Forum member. "Put data in front of everyone and let nature run its course. Nobody wants to see red when other departments are green." Below is a sample framework one CISO offered to share as an example:

Responsible Entity:	BU A	BU B
	Owner:	J. Doe
Issue w/Agreed Short-term Remediation Plans	#	#
Overdue Critical Issues	#	#
Overdue Standard Issues	#	#
Total Overdue Issues	#	#
External Facing Endpoints	#	#
Domains & Subdomains	#	#
Server & Network Devices	#	#
Cloud Objects	#	#
Scanned Applications	#	#
Container Image	#	#
Grade:	A	C



**“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 global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Technology and Operations services and Accenture Song — all powered by the world’s largest network of Advanced Technology and Intelligent Operations centers. Our 721,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at [accenture.com](https://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. Follow us [@AccentureSecure](https://twitter.com/AccentureSecure) on Twitter, [LinkedIn](https://www.linkedin.com/company/accenture-security) or visit us at [accenture.com/security](https://www.accenture.com/security).

View the entire suite of ACF roundtable summaries on our webpage – [here](#).

Copyright © 2022 Accenture All rights reserved.
Accenture, and its logo are trademarks of Accenture.