



# CISO Liability Issues

**Accenture Cybersecurity Forum**  
Global Executive Leadership Network

November 16, 2023  
Session Summary



## From the Accenture Leadership

APAC ACF members are keenly aware that in certain circumstances they can be held personally responsible and potentially liable for how they act and carry out their role—especially during and after an incident.

During this session, members, along with a seasoned attorney, shared a variety of situations and best practices for avoiding legal peril. One key observation: When it comes protecting themselves from liability claims, the CISO's most important asset may be a moral compass.

Our thanks to all the participants who shared questions and valuable insights on CISO liability issues.

Cheers,



**Paolo Dal Cin**

Global Head of Accenture Security  
ACF Executive Sponsor

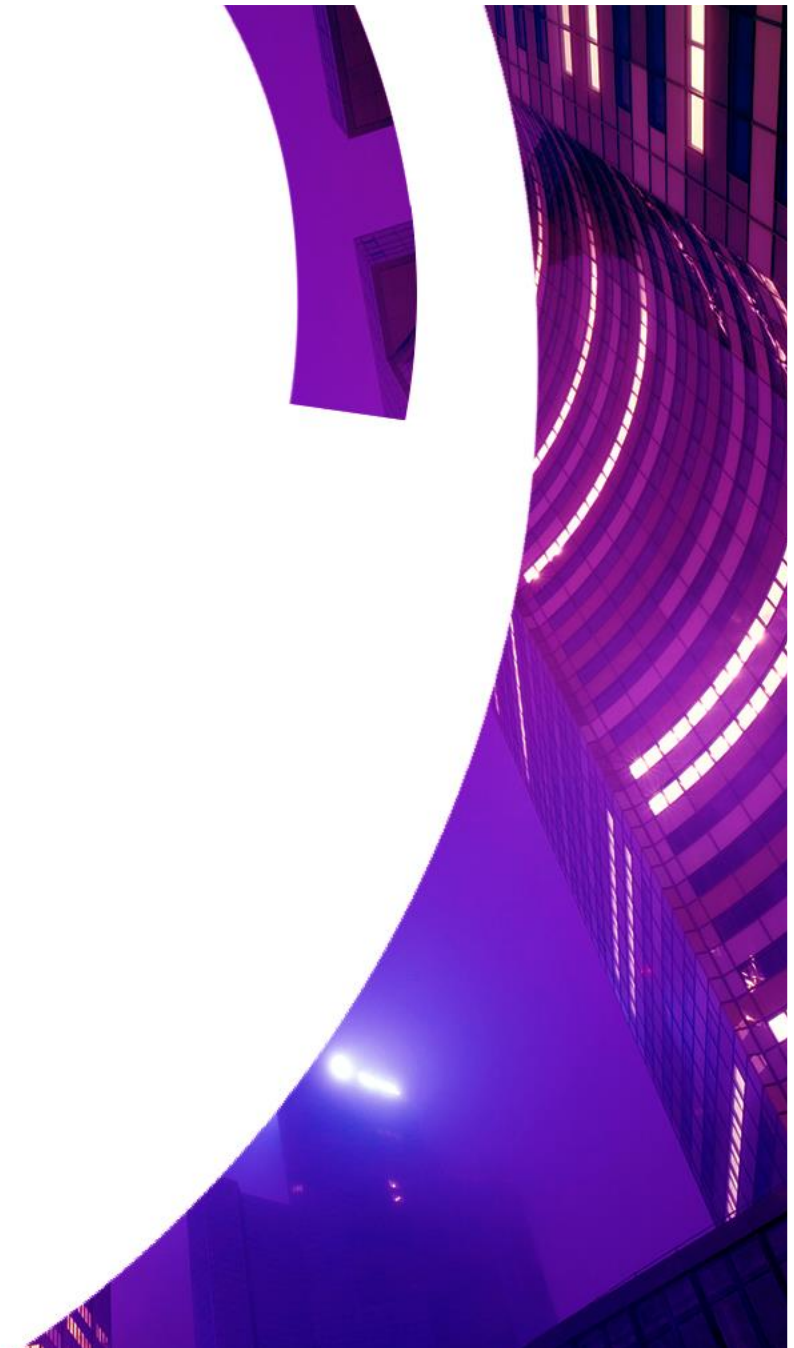
[LinkedIn](#)



**Kris Burkhardt**

Accenture CISO  
ACF Chair

[LinkedIn](#)



# CISO Liability Issues



The Accenture Cybersecurity Forum APAC membership convened a virtual roundtable titled “CISO Liability Issues” on November 16, 2023.

ACF members must play a collaborative leadership role within the enterprise in the event of a major cyber incident. And, in light of increasing oversight and compliance requirements, the CISO must maintain a degree of independence, objectivity and responsibility to assure that enterprise stakeholders are protected.

The discussion focused on two broad questions:

- In light of evolving regulation and compliance requirements, what should CISOs be alert to as they conduct themselves on behalf of their enterprises to limit both enterprise and individual risk? What are the friction points? What actions create risk and how can risk be mitigated?
- Are there a set of generalized “best practices” that CISOs should follow to protect the enterprise without incurring individual risk?

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:**

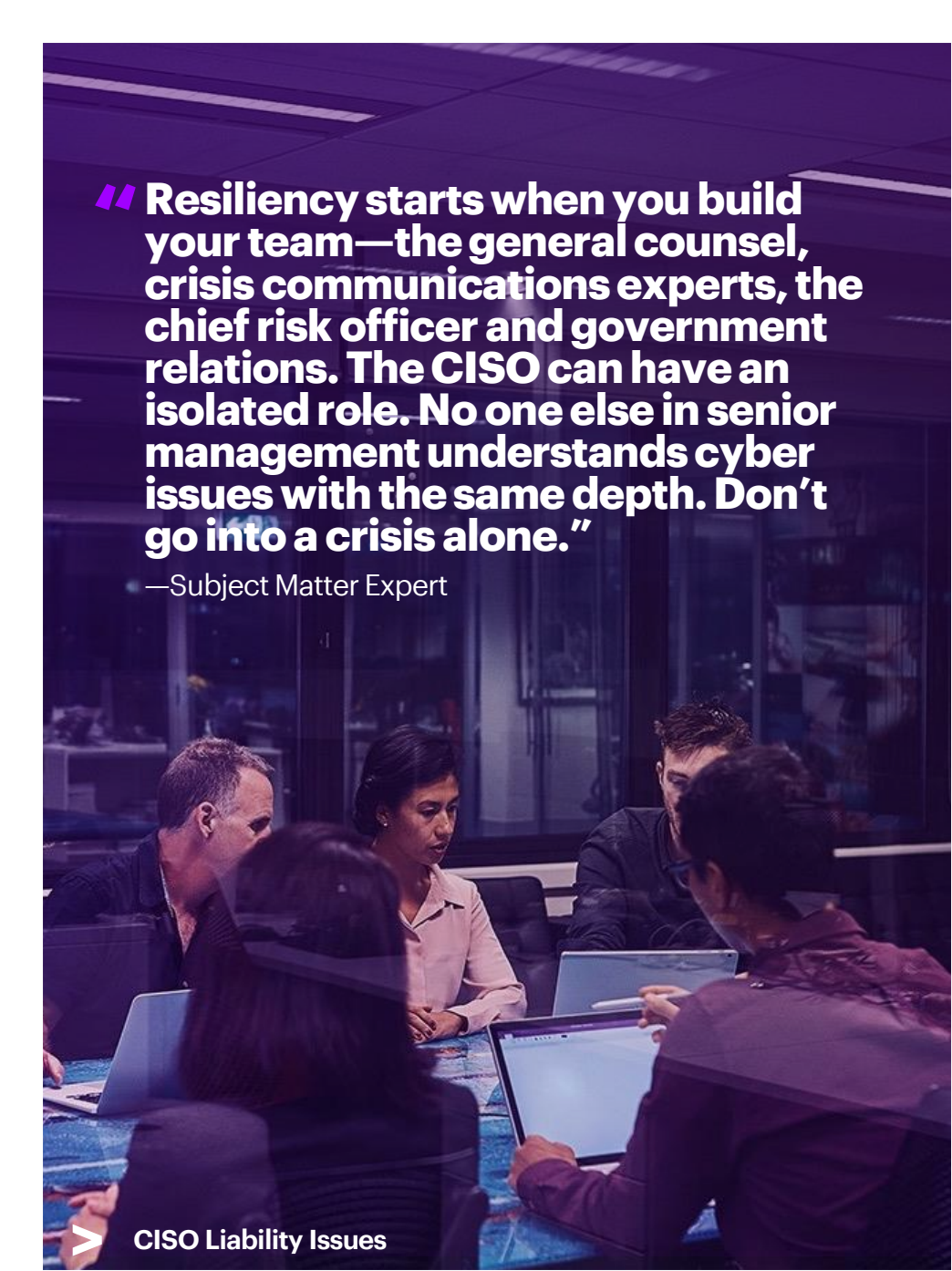
---

[New regulations call for new partnerships >](#)

---

[Best practices >](#)

---



**“Resiliency starts when you build your team—the general counsel, crisis communications experts, the chief risk officer and government relations. The CISO can have an isolated role. No one else in senior management understands cyber issues with the same depth. Don’t go into a crisis alone.”**

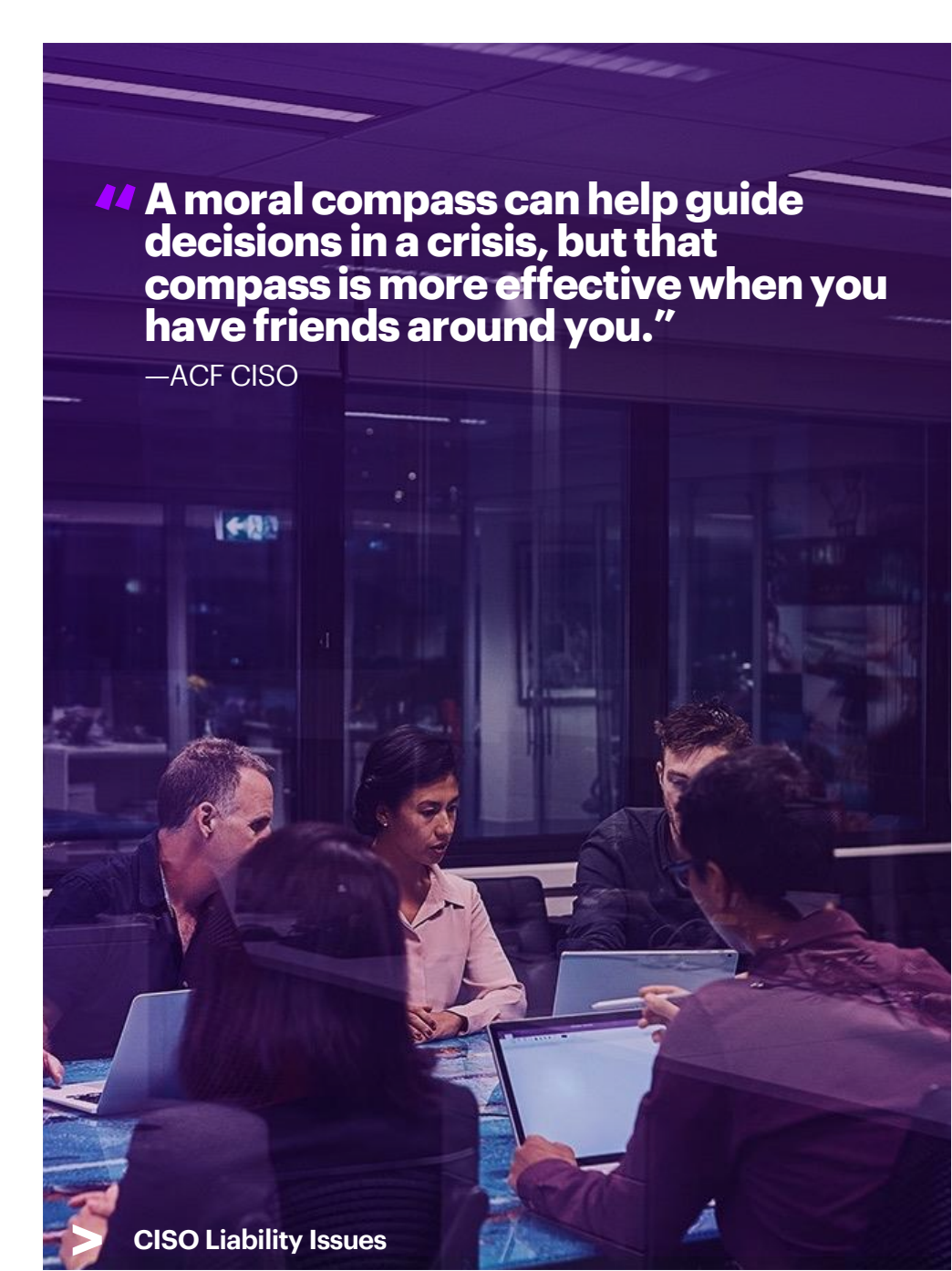
—Subject Matter Expert

## New regulations call for new partnerships

New [SEC rules](#) have reframed the role and responsibility of the CISO. At companies listed on US stock exchanges, CISOs will be responsible for responding to a material incident, but may also be called upon to report that incident and make an official regulatory disclosure.

An expansion of the industries covered by Australia’s Security of Critical Infrastructure ([SOCI](#)) Act, means that even more companies must report a material event to the relevant Commonwealth body as soon as practicable, and in any event within 12 hours after the entity becomes aware.

The legal subject matter expert (SME) said that as the threat of liability increases, so does the importance of a team approach to cybersecurity. “Resiliency starts when you build your team—the general counsel, crisis communications experts, the chief risk officer and government relations,” the SME said. “The CISO can have an isolated role. No one else in senior management understands cyber issues with the same depth. Don’t go into a crisis alone.”



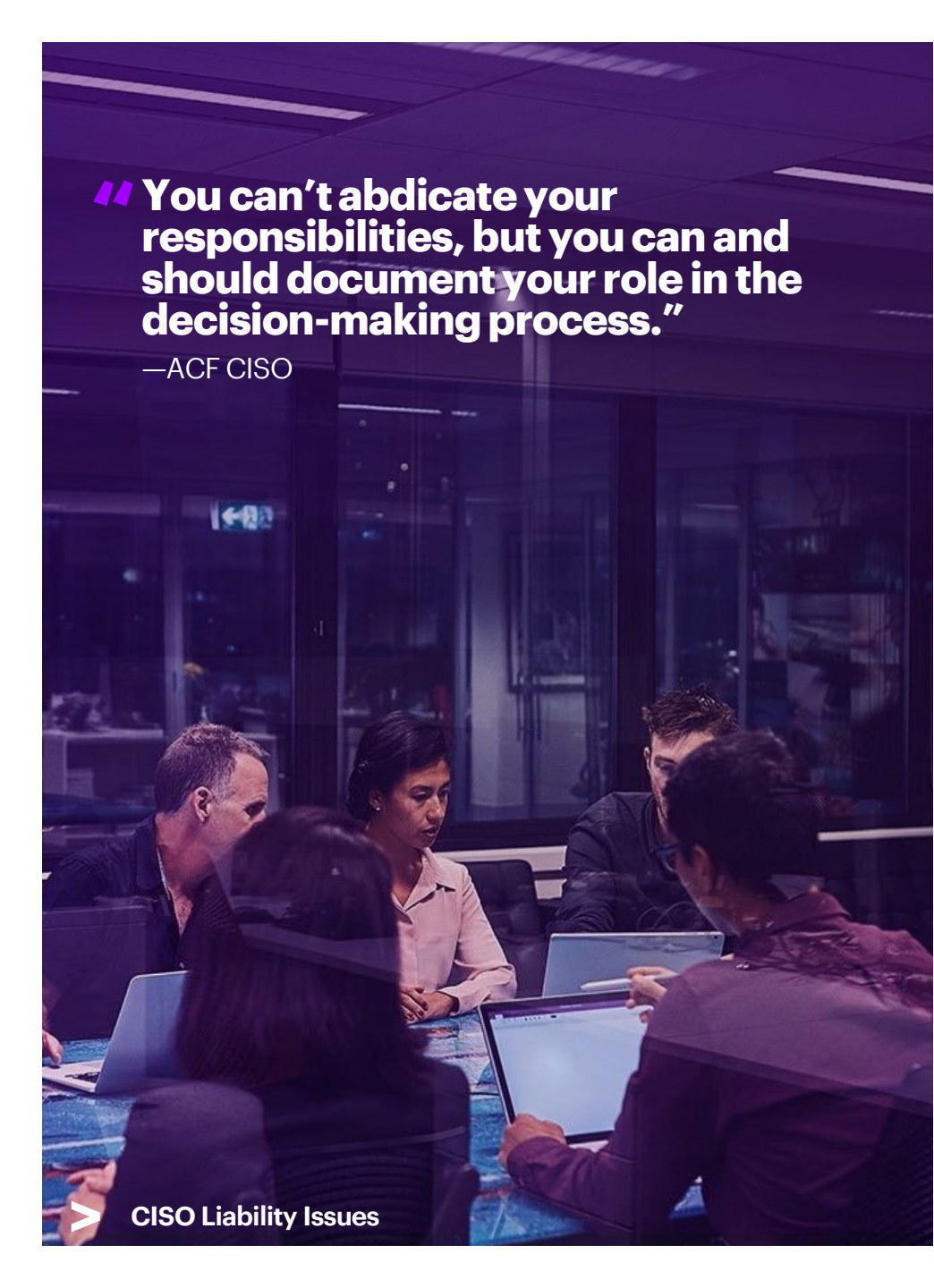
**“A moral compass can help guide decisions in a crisis, but that compass is more effective when you have friends around you.”**

—ACF CISO

# Best Practices

Forum members identified the following best practices:

- Avoid situations where you are called upon to publicly misrepresent a cyber attack. The pressure to do so can be intense. Set boundaries well in advance and work with legal counsel to avoid risks. After all, a lawyer engaging in fraud can lose their license.
- “A moral compass can help guide decisions in a crisis, but that compass is more effective when you have friends around you,” said a CISO. Another CISO said: “The CISO should help others think through their decisions during and after an event.”
- Include the entire team—legal, crisis communications, government relations, the CEO—in tabletop exercises to test public responses to cyber attacks.
- The timing of communications is critical. In a dynamic crisis situation, where conditions are constantly changing, it pays to be cautious about public statements. It is perfectly acceptable to say: “We are aware of the situation. We are investigating now and will let you know when we learn more.”
- Ask to be covered by Directors and Officers (D&O) insurance but know that it does not apply to criminal activity.



**// You can't abdicate your responsibilities, but you can and should document your role in the decision-making process."**

—ACF CISO

## Best Practices (cont.)

Forum members identified the following best practices:

- Governance matters. Establish agreement on your CISO responsibilities. Are you a "decision facilitator" who advises the CEO or a decision maker who might be held to a higher standard of liability in a lawsuit? A CISO said: "You can't abdicate your responsibilities, but you can and should document your role in the decision-making process."
- Keep the CEO and board fully and accurately informed during and after a breach. Be transparent and choose your words carefully. "You're walking a tightrope," said a CISO. "Consistently have those conversations."
- Document the rationale for decisions. Compile a paper trail that can be referenced when called upon in the event of a lawsuit. Documentation can also be useful in after-action reviews.
- Require the security team to characterize vulnerabilities in terms of non-compliance with the company's norms and policies.





**“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](http://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](http://accenture.com/security).

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