

A hand holding a pen is positioned over a server rack. The scene is illuminated with a strong blue light, creating a futuristic and technical atmosphere. The server rack is filled with various components, and the background is slightly blurred, emphasizing the hand and the pen.

# CISO Liability Issues

**Accenture Cybersecurity Forum**  
Global Executive Leadership Network

---

February 21, 2024  
Session Summary



## From the Accenture Leadership

The legal ramifications of high-profile breaches have CISOs asking important questions about the risk that they can be held personally and professionally liable for as they carry out their role—especially during and after an incident. In this ACF session members, along with a seasoned attorney, shared a variety of situations and best practices for avoiding personal legal peril.

One key observation: When it comes to documentation, stick to the facts, avoid hyperbole and leave marketing to the marketers. As one ACF member said: “Your job is not to document. Your job is to do the work.”

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 (ACF) convened a virtual roundtable titled “CISO Liability Issues” on February 21, 2024.

ACF members must play a collaborative leadership role within the enterprise in the event of a material cyber incident. And, considering increasing oversight and compliance requirements, the CISO must maintain a degree of independence, objectivity and responsibility to assure that enterprise stakeholders are protected. How should the CISO balance enterprise and individual risk and liability, especially in light of evolving regulations and stakeholder expectations?

Our discussion focused on two broad questions:

- 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?
- How should CISOs do their jobs so they avoid legal peril, and what steps can they take now to protect themselves from legal liability?

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 pressure >](#)

---

[Best practices >](#)



**“CISOs typically say they’re on a journey because they know things are always changing. CISOs recommend, they don’t decide how much money the company will spend on cyber. They should not be engaging in external-facing communications. Why should the CEO be out front?”**

— Legal Subject Matter Expert

## New pressure

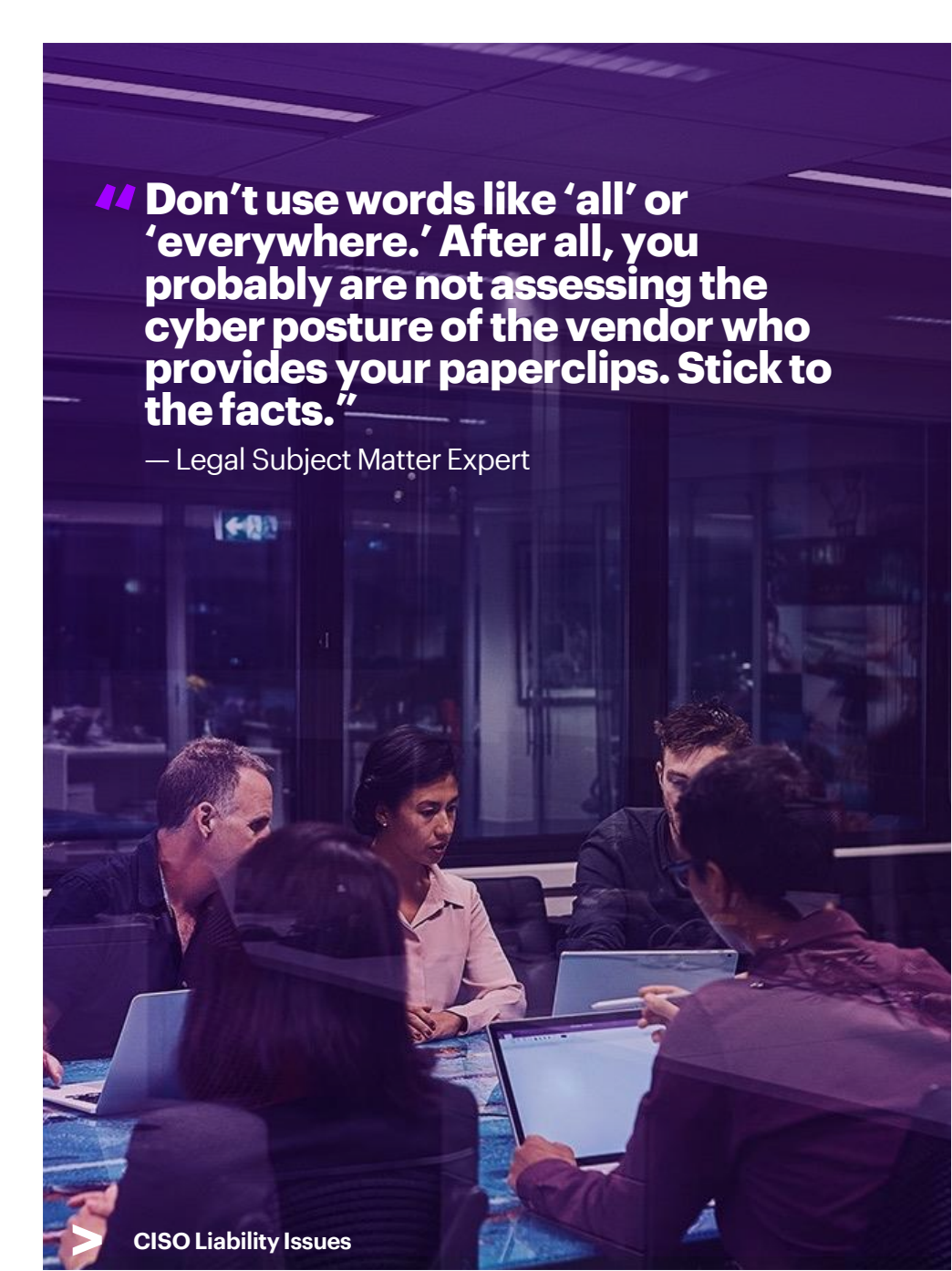
Recent [SEC rules](#) have reframed the role and responsibility of the CISO. At companies listed on US stock exchanges, CISOs will be responsible for responding to a material incident but may also be called upon to report that incident and make an official regulatory disclosure. The U.S. Office of the Comptroller of the Currency requires a bank to notify the OCC no later than 36 hours after the bank determines that a computer-security incident that rises to the level of a notification incident has occurred.

The legal subject matter expert (SME) said these kinds of legal requirements put the CISO in a difficult position. “CISOs typically say they’re on a journey because they know things are always changing. CISOs recommend, they don’t decide how much money the company will spend on cyber. They should not be engaging in external-facing communications. Why should the CEO be out front?”

The SME noted three promising trends regarding CISO engagement and liability considering increasing pressure:

- CISOs seem less willing to participate in external-facing activities.
- They are less willing to whitewash communications with the board of directors.
- Increasingly, board members are seeking to be educated about cybersecurity.

An ACF member added that there is actually a silver lining to new regulatory requirements. “As CISOs we bring a strategic perspective on risk and how to manage it. The challenge gives us an opportunity to elevate our influence.”



**“Don’t use words like ‘all’ or ‘everywhere.’ After all, you probably are not assessing the cyber posture of the vendor who provides your paperclips. Stick to the facts.”**

— Legal Subject Matter Expert

## Best practices (part 1)

Forum members identified the following best practices:

- “Follow your company’s policies,” the SME said. “In-house attorneys should be your best buddies. Talk to them and understand what’s expected of you.”
- 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. “Think carefully about whether or not you put your name on documentation, and how much you want to be associated with marketing messages.” the SME said.
- Avoid adjectives and adverbs in 10-Ks and other public communications. “Don’t use words like ‘all’ or ‘everywhere.’ The SME said. “After all, you probably are not assessing the cyber posture of the vendor who provides your paperclips. Stick to the facts.”
- “CYA documentation is not the answer,” the SME said. “You don’t need to document everything. Remember, the SEC is using e-mails as evidence. ‘She said, he said’ documentation is not helpful.”



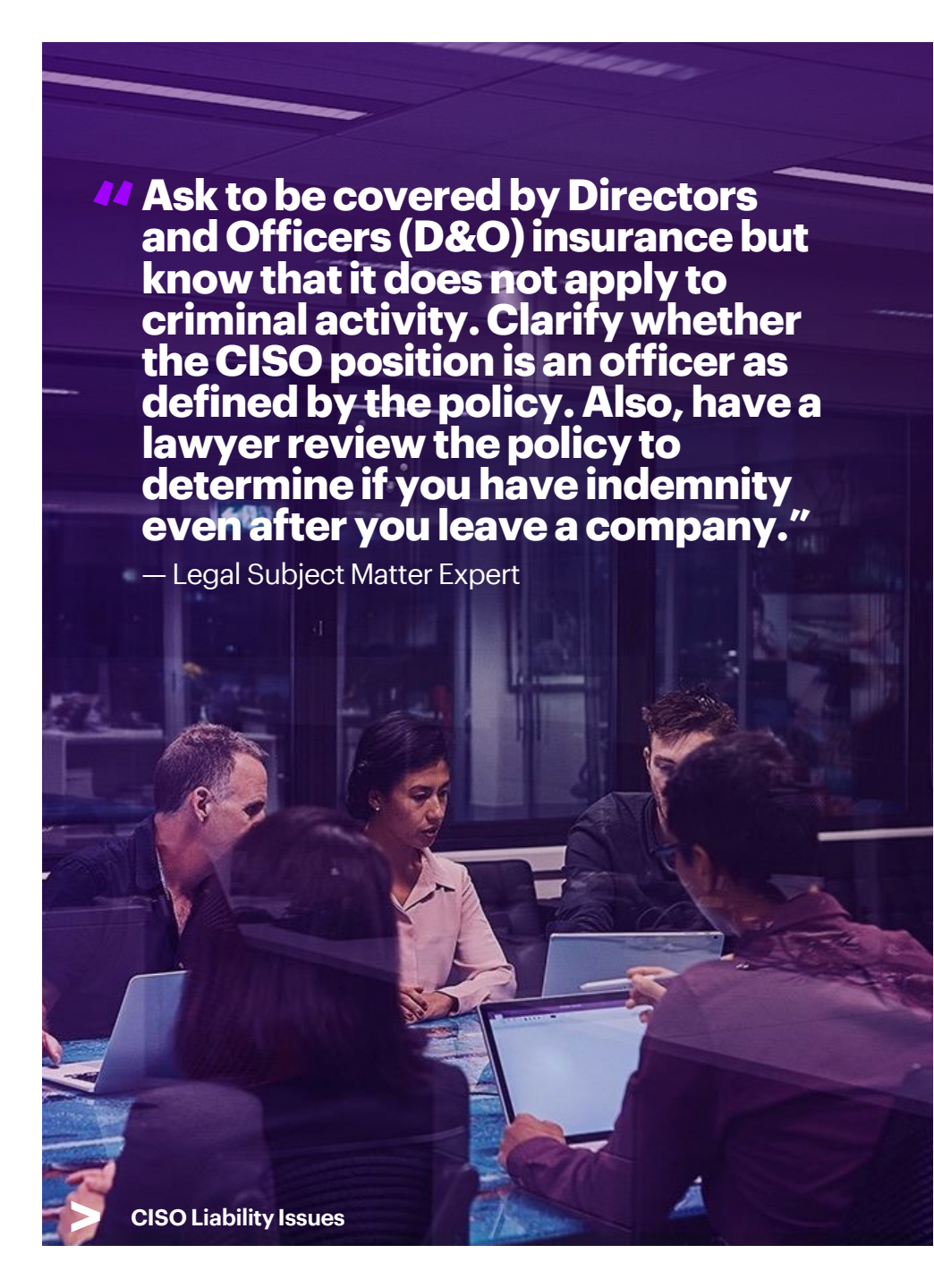
**“When budgets are being cut, it is in your interest to document what won't be able to be implemented without that funding.”**

— ACF Member

## Best practices (part 2)

Forum members identified the following best practices:

- “When budgets are being cut, it is in your interest to document what won't be able to be implemented without that funding,” said an ACF member. Another member agreed: “There is a need to communicate the impact of reductions in funding for committed outcomes or progress timelines.” The SME said: “Make sure you document the ramifications of those decisions.”
- Don't over rely on claims of attorney-client privilege. “Labeling everything as privileged doesn't help,” said the SME. “Privilege only applies when seeking legal counsel.”
- Context matters when speaking to the board. “In many cases, the dashboards you are showing to the board are incomprehensible. They don't know what good looks like. You must give them context.”
- Several ACF members spoke of the value of private conversations with board members to help them have a deeper understanding of cyber risks. “Private sessions with the board allow for unfiltered conversations.” said an ACF member.



**“ Ask to be covered by Directors and Officers (D&O) insurance but know that it does not apply to criminal activity. Clarify whether the CISO position is an officer as defined by the policy. Also, have a lawyer review the policy to determine if you have indemnity even after you leave a company.”**

— Legal Subject Matter Expert

## Best practices (part 3)

Forum members identified the following best practices:

- Consider asking the board to observe tabletop exercises to test enterprise responses to cyber attacks. “Have them sit in the back of the room and hear the upside and downside of the process,” said an ACF member. “And use it as a learning opportunity.”
- Ask to be covered by Directors and Officers (D&O) insurance but know that it does not apply to criminal activity. Clarify whether the CISO position is an officer as defined by the policy. Also, have a lawyer review the policy to determine if you have indemnity even after you leave a company.
- “Secondary personal insurance is probably too expensive and too difficult to obtain,” said the SME. “But if you do pursue it, ask your employer to pay for it.”
- Governance matters. Establish agreement on CISO responsibilities relative to the Disclosure Committee. CISOs are typically not a permanent member of that committee but rather a decision facilitator. “You can share the facts, but the Committee should have a solid process for determining if an event is material,” the SME said. “You should not be expected to override decisions by the Committee.”
- An ACF member asked: “What new skills do CISOs need to meet the moment. Are there new things CISOs need to grow or master?” The SME said: “CISOs in my view need to now be educators. The board and management need to be brought along on the path to understanding the ramifications of their decisions.”



**“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 © 2024 Accenture All rights reserved.  
Accenture, and its logo are trademarks of Accenture.

