ESG and Cybersecurity

What CISOs Need to Know (and Do)

Accenture Cybersecurity Forum
Global Executive Leadership Network

22 March 2023
Session Summary

From the Accenture Leadership

As we discussed the role of the CISO in supporting the enterprise's ESG aspirations at our latest Accenture Cybersecurity Forum, a comment from a Forum member underscored the topic's importance: "We don't have a choice."

We heard that CISOs are well-positioned to help improve their companies' environmental footprint, maintain society's trust in a digital world, and guide governance decisions. But we also heard that CISOs cannot go it alone. Senior management must make ESG a priority. The entire IT operation must contribute to reducing the environmental footprint. The expectations of rating agencies and insurers must be addressed with the help of legal counsel. But we are optimistic that CISOs can make a major contribution to ESG goals and even use their efforts to highlight the value of investments in security and resilience.

Thank you to all those who participated in the roundtable discussion. We hope you find the ideas and best practices that emerged from the conversation useful as you lead your enterprise towards a more cybersecure, resilient and ESG compliant future.

Cheers,

Paolo Dal Cin
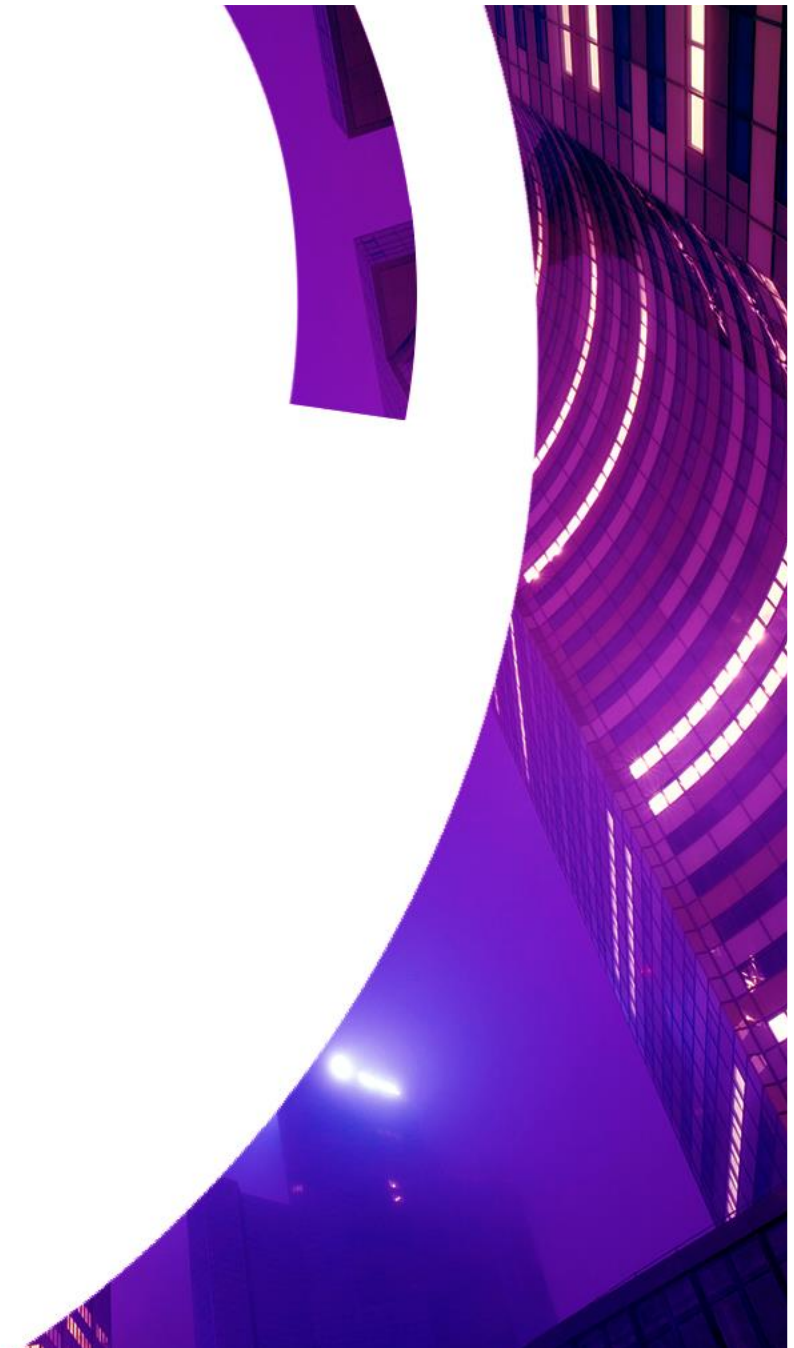Accenture Security Global Lead
ACF Executive Sponsor

LinkedIn

Kris Burkhardt
Accenture CISO
ACF Chair

LinkedIn

>

ESG and Cybersecurity: What CISOs Need to Know (and Do)

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, "ESG and Cybersecurity: What CISOs Need to Know (and Do)," on March 22, 2023. Forum members have expressed an interest in examining the connections between enterprise ESG (environmental, social and governance) and security priorities.

- Where is the intersection of interests for security and ESG?
- Where and how should the CISO be collaborating with other enterprise leaders regarding ESG?
- What best practices should CISOs consider?

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.
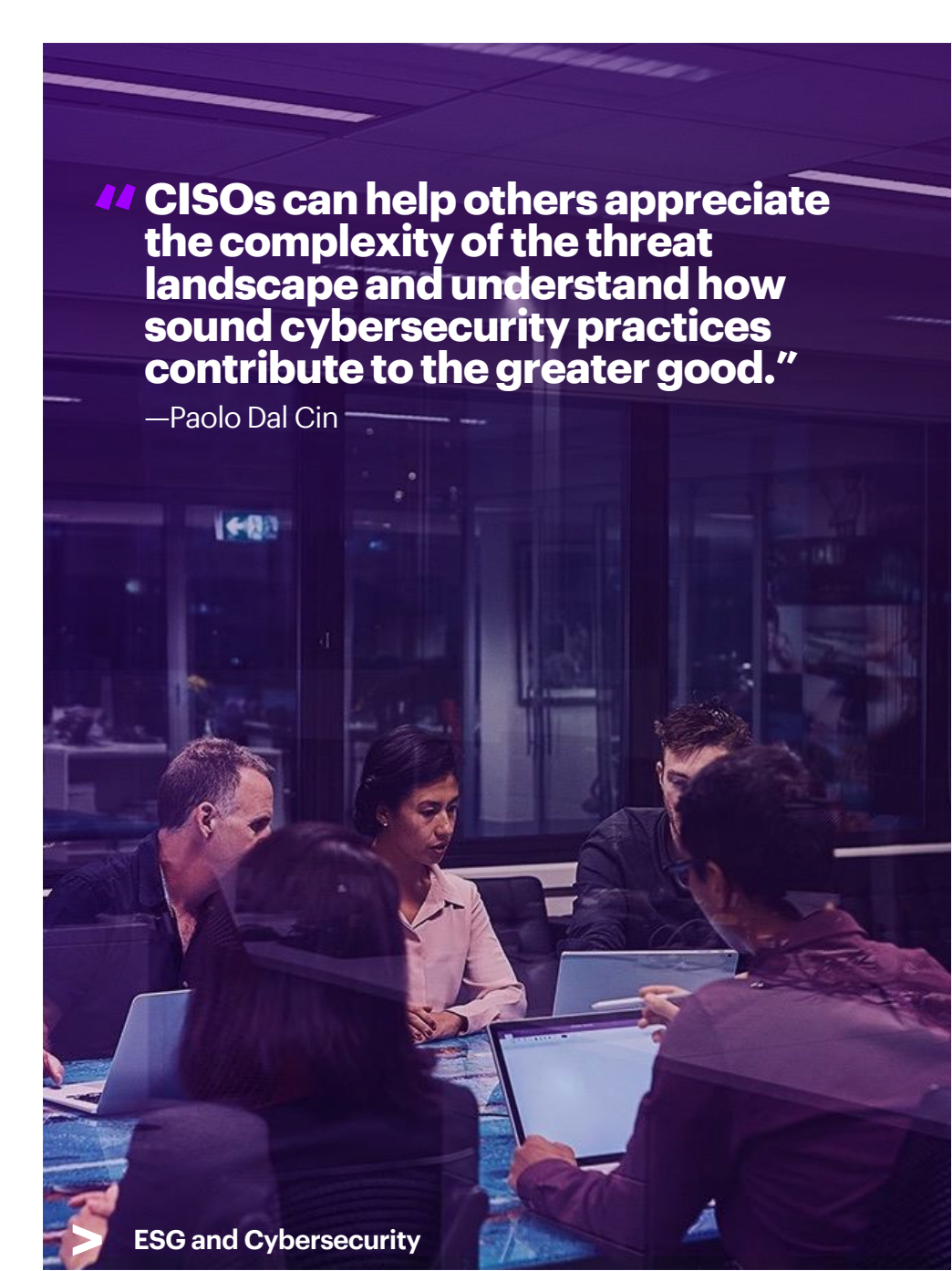
In this summary:

The intersection of security, resilience and ESG

Forum members agreed that CISOs have important responsibilities in helping their enterprises maintain appropriate ESG practices.

"Our work is central to the functioning of society," said a CISO. "Customers, regulators and the society we serve look to us to ensure a secure digital future. And we have to lead that conversation, not trying to stop regulations but helping shape smart regulations that don't overburden our businesses."

Measuring the impact of sound ESG-oriented cybersecurity is in the early stages. A CISO said: "On a maturity scale of one to 10, our ability to measure the impact of ESG initiatives is two." However, Forum members agreed that establishing metrics is a goal worth pursuing. "Financial accounting rules have emerged over hundreds of years and are still evolving," said a CISO. "We will have to develop metrics in the next few years." A range of metrics were discussed, from progress towards decarbonization, emissions from supplier processes, and energy usage by cloud service providers to the protection of customer personal information and the adoption of alternate energy sources such as wind and solar.

> **"CISOs can help others appreciate the complexity of the threat landscape and understand how sound cybersecurity practices contribute to the greater good."**
> —Paolo Dal Cin

Environmental best practices

- Moving from traditional enterprise data centers to the cloud can reduce an enterprise's energy footprint. A CISO said that cloud service providers should provide environmental impact metrics. Another CISO suggested evaluating the environmental footprint and ESG practices of SaaS security service providers.

- Close collaboration between the CIO, CTO and CISO can yield the greatest environmental impact. Reducing energy consumption is not a goal that can be addressed solely by the CISO.

- Consider the environmental impact across the supply chain. Understand where upstream emissions are coming from and work with suppliers who are aligned with your ESG goals. As an example, one CISO said that enterprises should push for purchasing carbon neutral laptops.

- Eliminating technology stack complexity can reduce the inefficiencies that contribute to higher energy consumption.

> **"Create communities to protect communities."** enough mind share is devoted to cybersecurity ... "
>
> —Member

Societal best practices

- Sharing threat intelligence serves the greater good. As a CISO said: "Create communities to protect communities." Another CISO pointed to the European Round Table for Industry, which include CEOs and Chairs from around 60 of Europe's largest companies in the industrial and technological sector, as a productive means of information sharing.

- Address the risks of interdependencies by conducting cross-sector threat simulations

- Stakeholders expect transparency. Look for opportunities to build trust with regulators, customers, shareholders and employees by demonstrating efforts to keep the enterprise secure and how performance is measured.

> **"It is incumbent on us as CISOs to have the metrics—and the courage—to be transparent about our contributions."**
>
> —Kris Burkhardt

Governance best practices

- Help drive consensus on risk tolerances. For example, the CISO of a multinational participates in a regular capital allocation review where country CEO input drives technology and security investment priorities.

- Translate ESG targets into actionable initiatives and invest accordingly in resilience capabilities, breach response, and other cyber priorities that are aligned with ESG.

- Monitor national, regional and global ESG goals such as the United Nations Sustainable Development Goals, the EU Taxonomy Regulation and trends in ESG prioritization among ASEAN countries.

- Monitor third-party providers. Determine if they are following sound ESG principles, including ethical, sustainable processes, in delivering high quality products and services.

- Address the risks of interdependencies by conducting cross-sector threat simulations

- Stakeholders expect transparency. Look for opportunities to build trust with regulators, customers, shareholders and employees by demonstrating efforts to keep the enterprise secure and how performance is measured.

"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.