

The significance of ESG and the integration of security and privacy within its broader framework

By Dharmik Karania



According to the KPMG 2023 CEO Outlook, 69 percent of CEOs have integrated ESG into their business strategies as a means of creating value, and 50 percent are expecting substantial returns from these initiatives over the next three to five years. Though the environmental and social facets of the ESG agenda have received significant focus, governance components like cybersecurity and privacy have not received as much emphasis. With the rise in cyber threats and concerns regarding data privacy, Chief Information Security Officers (CISOs) must collaborate closely with their ESG counterparts. This collaboration ensures that in the event of an incident, operations remain resilient, and contingency plans are prepared for immediate activation.

By integrating cyber and privacy considerations into their social responsibility initiatives and safeguarding customer data, organizations can enhance their ability to preserve their reputations and earn trust from customers, even amidst a significant breach.

For Consumers who have shared their personal information with private and public sector providers, there is an expectation that their personal data will be safeguarded and the data will only be used for the purpose it was collected for. and At the same time, as the organization achieves its business objectives, there is an expectation that businesses will act in a responsible manner to support the local community, reduce the carbon footprint, ensure workplace equality and diversity, and also improve labour policies.

Addressing cybersecurity and privacy concerns particularly ESG largely have become leading priorities for the board. Executives uphold a massive responsibility to reassure customers, employees, and stakeholders that effective safeguards are implemented to protect their information assets and mitigate cyber threats. Furthermore, organizations face escalating corporate, legislative, and regulatory mandates, necessitating demonstrable efforts to appropriately manage and safeguard their information assets.

With the increasing scale and sophistication of cyber threats from both criminals and hackers, how can businesses quickly adjust their cyber capabilities to keep pace with the evolving security landscape and confidently encourage growth through business evolution, digital offerings, and services?

Insights to enable your business.

The KPMG Cyber Maturity Assessment (CMA) is a comprehensive risk assessment of your organization's readiness to prevent, detect, contain and respond to threats to information assets.

It provides insights to understand vulnerabilities, identify and prioritize remediation areas, and determine a strategic roadmap — outlining the cyber capabilities that require the board's focus and translating them into an operational, business-enabling function that supports the business and its technology objectives.

The CMA is an abstract of the KPMG Cyber Capability Framework that evolves traditional cyber maturity assessments. It looks beyond pure technical preparedness — taking a rounded view of people, process and technology.



In conclusion, integrating cybersecurity and privacy into the ESG framework is vital for creating value and growth. The KPMG 2023 CEO Outlook shows many CEOs prioritize ESG, yet often overlook cybersecurity and privacy. With rising cyber threats, CISOs must work with ESG teams to ensure resilience and effective contingency plans. Embedding cyber and privacy in ESG strategies protects data, maintains trust, and demonstrates responsibility. The KPMG Cyber Maturity Assessment (CMA) enhances cyber capabilities, aligns with business goals, manages risks, and builds trust. Incorporating these safeguards within ESG efforts supports compliance and drives long-term growth.

References

[Cyber Maturity Assessment - KPMG Global Cybersecurity considerations 2024 \(kpmg.com\) https://kpmg.com/xx/en/home/insights/2023/09/kpmg-global-ceo-outlook-survey.html](https://kpmg.com/xx/en/home/insights/2023/09/kpmg-global-ceo-outlook-survey.html)

Contact



Dharmik Karania
Senior IT Audit
KPMG East Africa
dkarania@kpmg.co.ke



It looks beyond pure technical preparedness — taking a rounded view of people, process and technology.

The views and opinions are those of the author and do not necessarily represent the views and opinions of KPMG