COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023
ESG, Cyber, and Privacy: Bridging the Divide

By Lisa Beth Lentini Walker[1]

Why Are Cybersecurity and Privacy Now Important to a Broader Demographic?

The year 2020 was challenging for global organizations, with the adjusted average total cost of a data breach reaching $4 million per company.[2] Cyberattacks are also on the rise and their cost is increasing along with them. 2021 was one of the most active years for cyberattacks. According to Check Point Research, a provider of cyber security solutions to governments and corporate enterprises, in 2021 cyberattacks increased 50% year-over-year, with each organization facing an average of 925 cyberattacks per week globally.[3] This was compounded by remote workforces, which increase the surface area available to infiltrate an organization. Cybersecurity, data privacy, and governance are becoming significant topics for company management, global investors, and players from all industries. A far broader demographic is becoming increasingly concerned with cybersecurity and privacy's social and environmental impact, as well as governance and technological implications.

On top of privacy and cybersecurity's critical role in protecting systems, networks, programs, and data, it is now also regarded as a key environmental, social, and governance (ESG) concern, falling primarily under the "social" pillar but also touching upon governance and environmental.

Environmental

Cybersecurity and privacy protocols can absolutely have an impact on an organization's environmental posture. Collecting, storing, moving, and processing data requires energy and space. The more of these activities a company engages in, the more energy is required, and the more heat is generated by the equipment to support an organization. Excess collection of data can therefore have a negative impact on environmental factors, such as energy efficiency, carbon emissions, climate change, and electronic waste management. Additionally, companies have choices in whether they consider green energy usage as part of the cycle.

Social

Companies that collect data have a responsibility to protect information and respect the privacy of any impacted parties. Additionally, recognition of privacy as a human right is an important element of treating the data as a critical ESG imperative.

Governance

The governance factor combined the regulatory needs and ethical considerations of privacy and cybersecurity. Organizations must protect the confidentiality, integrity, and availability of information, including from unauthorized access and disclosure.

ESG frameworks are a tangible means of evaluating corporate behavior; by incorporating privacy and cybersecurity, a new dimension is added, giving insight into cyber behaviors, data governance, and risks which

form a critical part of the bigger ESG picture.

ESG standards have become critical metrics for corporate performance, reputation, and risk mitigation across stakeholder groups in recent years. Successful implementation of an ESG program not only affects a company's social and community profile but can also positively influence financial performance. Beyond well-known ESG issues covering carbon emissions, human capital development, diversity, and business ethics, privacy and cybersecurity are important topics for companies to address in their ESG programs and disclosures.