Cyber security: Don't report on ESG without it

2021

kpmg.com

For organizations across all industries, cyber security's connection to ESG includes not only governance, but social and environmental programs as well.

Mandates for environmental, social and governance (ESG) reporting are intensifying across all industries. Although sectors like retail and technology will likely soon face more stringent expectations, fintech companies, financial services, and oil and gas and public utilities are already under pressure from investors, boards of directors, and other stakeholders to be more transparent about their ESG efforts.

In addition to perennial concerns like anticorruption, clean water and climate change, cyber security is rising to the top of the ESG agenda. In a recent survey, 67.4 percent of respondents from the U.S., Canada, Europe, and Asia ranked cyber security as their top concern.[i]

Why now?

Socially conscious investing has already taken off with a focus on the environmental, diversity and social justice postures of potential investment targets. In light of recent security breaches like the ransomware attacks on the oil pipeline and a major meat production company, consumers of all kinds are becoming more and more savvy about potential cyber vulnerabilities at the organizations with which they connect and share data. As a result, there is a demand for transparency into how organizations use and protect the confidentially and integrity of personal data of everyday individuals. The consequences of failing to protect customer data can range from a devastating loss of assets; to eroded "trust" between the organization and its customers, employees, and third parties; to irreparable harm to the organization's reputation, brand, and bottom line.

How cyber security aligns with not only the "G," but also the "S" and the "E" in ESG

Governance: Customers want to know that the companies they invest in are doing everything they can to protect themselves against a potential breach, and that they have robust disaster recovery protocols in place in the event a breach occurs. As the world is still in the throes of pandemic recovery and rebuilding, demonstrating operational resilience and the flexibility to adjust to changing conditions is critical. When it comes to investing, using reporting to demonstrate cyber resilience—or the ability to keep delivering even when dealing with cyber security issues—gives investors a complete picture of an organization's operational capabilities prior to considering investment opportunities.

Reporting on cyber risk metrics can offer a window into overall corporate behavior. As such, these metrics should follow the same underlying principles as ESG ratings, i.e., reflecting what behaviors say about a corporation, for example how resilient an organization is to future adverse cyber events or future adverse business events in general. Further, there is an increasing belief that reporting on cyber security risk and resilience as part of ESG may soon be a regulatory requirement.[ii]

Social: At first glance, cyber security might not seem to have a strong connection to the social aspects of ESG. However, with high-profile data breaches, a company's relationship with its customers can be severely damaged if their personal data becomes public.

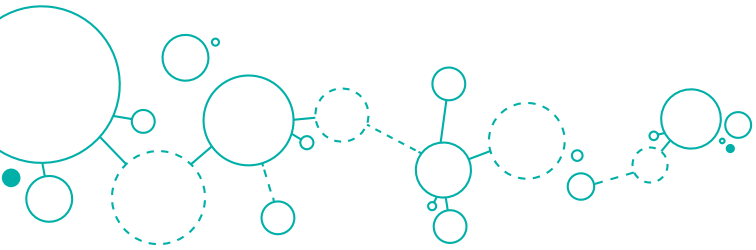
> "ESG provides organizations a unique opportunity to provide transparency into the significant cybersecurity investments they are making to earn and maintain stakeholder trust."
>
> **– Matthew P. Miller**
> Principal, Cyber Security Services

[i] 2019 RBC Global Asset Management Responsible Investing Survey.

[ii] Laura Deaner, There is a C in ESG, FS-ISAC, 2021

Further, the public has become increasingly concerned about what organizations are doing for society—from advancing diversity to reducing their carbon footprints. In the same vein, customers want to know that information protection and individual privacy rights are top of mind for an organization and that they can have confidence that their data won't be shared or sold to other organizations or retailers. To drive customer confidence, organizations should determine that access to sensitive customer data is carefully calibrated based on roles and responsibilities within the organization.

Environmental: Since a corporation's positive environmental policy/impact can potentially benefit those outside its corporate walls, it is considered a public good to contribute to clean air and water. In the same sense, the interconnectedness of today's world means that a corporation's cyber policy, compliance and risk metrics can have far-reaching impacts that can cascade throughout society. Organizations with robust cyber security programs—and reporting that gives stakeholders transparency into those programs—are well positioned to improve their ecosystems and safeguard their connections with other associations throughout the world. Organizations should determine they can clearly articulate the effectiveness of their operating models and supporting processes in terms of promoting security and risk awareness, as well as reporting on robust controls programs that protect stakeholder data.



Telling your cyber security story

In 2020, 66 percent of financial services directors (16 percentage points more than in 2019) reported that their confidence in their organization's ability to respond to a cyberattack was growing.[iii] However, when it comes to reporting on cyber security to the board, there is room for improvement—only 56 percent of CEOs, 53 percent of CIOs, and 45 percent of CISOs said they currently report to the board on cyber security, according to a recent study. The need to continue to enhance board communications is clear when you consider that boards that have three or more senior executives reporting on cyber security say they are more likely to be able to provide effective oversight than those with fewer executives reporting.[iv]

> "Organizations at any stage of their ESG journey should consider reporting on their cybersecurity posture to develop and sustain trust with their customers, employees and extended stakeholders."
>
> **– Prasanna Govindankutty**
> Principal, Cyber Security Services

[iii] NACD Public Company Governance Survey, 2020.

[iv] NACD Public Company Governance Survey, 2020.

Below are some key areas that should be included in cyber-security reporting and examples of actions corporations can take now:

Cyber-risk disclosure and reporting subcategories	Guidelines
Governance	Appoint and empower a senior executive responsible for cyber security risk
	Determine the appropriate frequency of cyber risk reporting to the board of directors
	Determine that the board comprises individuals with sufficient cyber security skill sets, expertise, and experiences
Security compliance approach	Stay abreast of evolving industry standards for control and disclosure frameworks, bearing in mind that World Economic Forum (ESG) and Task Force on Climate-Related Financial Disclosures (climate) disclosure frameworks are poised to become the future standards for disclosure and external reporting
	Consider the cyber security and privacy regulatory requirements in your organization's scope (e.g., Payment Card Industry, General Data Protection Regulation, The California Consumer Privacy Act)
	Determine if you should include business continuity frameworks in your reporting
	Assess and adjust your cyber insurance coverage on a regular basis
	Create a cadence of risk assessment involving third parties
Culture	Work toward ensuring that all personnel (from board members, to employees, to contractors) complete compulsory and continuous training programs to ensure investor confidence
	Increase the percentage of IT budget dedicated to cyber security and related initiatives
	Participate in industry knowledge sharing, particularly with companies known for mature cyber security protocols
Data privacy reporting	Report on the number of high-rated security incidents involving PII or how the numbers are trending
	Quantify the number of customers/employees whose data is used for secondary purposes
	Total up historic monetary losses associated with data breaches
	Include a publicly disclosed privacy or data protection policy in all reporting
	Determine the organization's security posture and develop a metrics and measurements program that consolidates disparate and sometimes inconsistent data
	Determine that internal reporting is wide-ranging and inclusive of all risk types
	Take a medium- to long-term outlook on not only cyber security, but also all ESG issues, since the effects can materialize much later than other risk types
	Be careful about giving too much away in terms of tools and capabilities used to manage cyber risk so that you don't disclose information that could be useful to attackers

Conclusion

It is already well established that embracing transparency can bring competitive advantages as it allows consumers, employees, investors, and other stakeholder groups to use data for targeted decision-making. Therefore, taking an ESG approach to cyber security reporting can promote digital trust in your organization. Cyber-reporting metrics should be based on data points your organization already has.

— **Our Cyber team delivers a range of services and change to approaches to enable your organization to share your Cyber and ESG story including:**

Cyber strategy and change to methodology

CISO reporting

Cyber GRC program implementation

Third-party security risk management

Privacy and data protection

Security awareness

Cyber resilience

Identity and access management

Contact

Prasanna Govindankutty
Principal, Cyber Security Services
E: pkgovindankutty@kpmg.com

Matthew P Miller
Principal, Cyber Security Services
E: matthewpmiller@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia