THOMSON REUTERS
PRACTICAL LAW™

Expert Q&A on Aligning Cybersecurity and ESG Strategies

by Practical Law Data Privacy & Cybersecurity

Status: **Published on 26 Sep 2023** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **content.next.westlaw.com/w-039-5613**
Request a free trial and demonstration at: **tr.com/practicallaw-home**

An expert Q&A with Susan ("Suz") H. Mac Cormac, Miriam Wugmeister, and Stacey M. Sprenkel from Morrison & Foerster LLP discussing the intersection of Environmental, Social, and Governance (ESG) and cybersecurity programs. This Q&A addresses how organizations can potentially benefit from taking an integrated approach to their enterprise risk management (ERM), compliance, governance, and reporting activities across these high-profile areas.

Practical Law asked Susan ("Suz") H. Mac Cormac, Miriam Wugmeister, and Stacey M. Sprenkel from Morrison & Foerster LLP to discuss how organizations can potentially benefit from viewing cybersecurity through an Environmental, Social, and Governance (ESG) lens, despite the unique characteristics and risks of each area, and integrating their enterprise risk management (ERM), compliance, governance, and reporting activities.

Susan ("Suz") H. Mac Cormac co-chairs Morrison Foerster's ESG, Social Enterprise + Impact Investing, and Energy practices, focusing on late-stage financings, secondaries, and other corporate transactions for investors and on investments for some of the top impact-dedicated investors.

Miriam H. Wugmeister co-chairs Morrison Foerster's Global Privacy and Data Security group, regularly advises senior executives and boards of directors on incident response and has led the response to some of the largest cybersecurity incidents.

Stacey M. Sprenkel co-chairs Morrison Foerster's ESG practice, leads the firm's Global Ethics and Compliance practice, helps clients assess and mitigate a broad range of ESG and compliance risks across their organizations, and assists clients with internal investigations when issues arise.

Looking at Cybersecurity Through an ESG Lens

Let's do some level-setting. Can you start by telling us a little about ESG's history, evolution, and connection to cybersecurity issues?

As a term, ESG was first used in 2004 in the United Nations' Global Compact Initiative's Who Cares Wins report. The report was endorsed by 18 financial institutions from nine countries with over $6 trillion in assets under management. It concluded that companies that perform better on certain ESG metrics can increase shareholder value and deliver better risk-adjusted financial returns by managing risks, anticipating regulatory action, or accessing new markets, while contributing to sustainable development of the societies in which they operate. Following this report, corporations accelerated their adoption of ESG policies, often blending them into existing corporate social responsibility (CSR) initiatives and expanding ESG to include issues relevant to both stockholders and stakeholders, with cybersecurity falling in both categories.

Cybersecurity as an ESG consideration emerged as the world became interconnected by digitization, expanding cyber

incident impacts beyond the ecosystems or jurisdictions where they arise. The increasing interconnectivity and digitization of products and services, and human activities generally, have advanced cyber hygiene and governance as core responsible business practice considerations. Understanding cybersecurity and its governance through a holistic ESG lens addresses compliance with regulation, risk mitigation, and seeing around corners for developments or opportunities on the horizon, as well as designing governance around these issues. It can help organizations:

- Prioritize their cybersecurity efforts.
- Ensure that those efforts are:
  - coordinated with other compliance goals; and
  - aligned with their overall business goals.

Should cybersecurity be part of an organization's ESG program or separate and linked in other ways? Does the amount of personal data an organization handles change that?

Implementing an ESG-based cybersecurity strategy can be beneficial for many reasons. Specifically, it:

- Helps companies better understand their cyber exposures.
- Identifies critical areas for improvement.
- Creates measurable objectives for improving cybersecurity performance across an organization.

This strategy in turn allows for a more holistic and comprehensive approach to cybersecurity that can better protect businesses from today's threats.

The ESG approach also provides a framework to elicit information from and ensure compliance by counterparties in supply chains and elsewhere. Many organizations, whether companies or asset managers, have different teams within the organization focused on different counterparty risks. For example, one team assesses cybersecurity compliance risks, another team looks at trade compliance and sanctions, another looks at anti-corruption, another at climate, and yet another assesses human rights risks. This siloed approach to dealing with counterparty compliance can:

- Present real risk to organizations.
- Result in blind spots or forum shopping for approvals.

Treating cyber risk as a core part of a holistic compliance approach, like anti-bribery, anti-money laundering, sanctions, and other areas, also aids in preparing for:

- The Securities and Exchange Commission's (SEC) increased focus.
- Growing regulations across different jurisdictions.
- Technological proliferation across all endeavors.

Further ways that an ESG perspective can be helpful include:

- Identifying potential risks early.
- Ensuring that practices align with company values and goals.
- Increasing coordination and decreasing duplication when securing information and compliance from supply chain members and customers.
- Mitigating potential financial losses.

The amount of personal data that a company handles creates varying degrees of risk for them. Additionally, cybersecurity considerations in an ESG program vary for private and public companies and asset managers. Private and public companies may think of how cyber vulnerabilities may affect customers and their bottom line. Cybersecurity is also a growing compliance issue for public companies subject to certain disclosures, such as the SEC rules on cybersecurity and the EU's Corporate Sustainability Reporting Directive (CSRD), among others. Asset managers, on the other hand, consider cybersecurity part of complying with certain disclosure regulations, such as the EU's Sustainable Finance Disclosure Regulation, or as part of deal screening and diligence, as well as portfolio company management.

Enterprise Risk Management (ERM)

What does it mean for organizations to take a holistic versus siloed view of risks? How can that help them?

A holistic approach to ERM involves taking an integrated, top-down and bottom-up posture to risk assessment efforts across all functions and personnel within the organization. This includes both:

- Identifying the key existing and emerging risks an organization faces.
- Ensuring that relevant parties have a clear understanding of:
  - how risk hotspots interact; and
  - the roles and responsibilities they play in a collective effort to build resilience into ERM strategies.

A holistic approach to risk is important to ensure:

- Coordination between all relevant teams and functions within an organization on incident response and risk mitigation efforts.
- There is a risk-based approach to resource allocation for compliance and other risk mitigation activities.

It creates a full picture of risk and potential pitfalls, equipping companies with information to design strategies that thoroughly address vulnerabilities and exposures. Taking a holistic and integrated approach also:

- Provides decision makers with a clear picture for designing ERM plans.
- Equips investors with a clear picture of a company's risk exposure, potential vulnerabilities, blind spots, and efforts to mitigate and eliminate risk exposure to inform investment decisions.

How does that holistic approach affect the way organizations view cybersecurity risks?

Increased technology proliferation and digitization advance interconnectivity. Consequently, cybersecurity risks or exposures are not solely the IT department's problem. Instead, they:

- Have far-reaching consequences.
- Require quick responses.
- Make a core understanding of cybersecurity risk and response everyone's responsibility within an organization.

A holistic approach to risk management equips every member of an organization with an understanding of their role in a collective effort to reduce exposures and mitigate cybersecurity risks.

Single and Double Materiality

What is single materiality versus double materiality? How do they apply to ESG and cybersecurity programs?

Businesses traditionally have viewed cybersecurity on a single materiality basis, that is, in terms of the economic value to the organization. A single materiality approach to ESG examines risks through the company value lens and no more. It asks the question: how would a cybersecurity incident affect financial value?

The double materiality approach, on the other hand:

- Examines risk from both financial value and impact perspectives.
- Recognizes a cybersecurity incident's potential impact on society, rather than only on the company.

The single materiality approach may be a top priority, but it does not provide a true account of the company's value. With the threat of malicious actors and increased global regulation, a double materiality approach is essential. Cyberattacks and security incidents can have significant effects on lives and livelihoods. In a world that is becoming more and more interconnected, organizations must both:

- Consider how they can protect potentially affected external parties, including employees, customers, consumers, key stakeholders, and vendors.
- Protect the organization itself.

This need reinforces the case that a company's true value and impact are best understood if it analyzes its behavior and hygiene from both a company value and an impact perspective. A double materiality lens approach is important to create a true picture of a business's performance on cybersecurity as a part of its broader ESG picture.

Weak cybersecurity can result in severe reputational damage and loss of trust. Deals may be lost if a minimum level of trust is not achieved. A good ESG framework, implemented using a double materiality lens, is a company's way of alerting its customers and society at large that beyond a business need for their trust, the company cares about the impact of its activities on everyone within its ecosystem. Good ESG practice enables shareholders and stakeholders to trust companies with their data and gives them the confidence to be associated with the company. On the company side, reputational risks cause shareholders and stakeholders to disassociate from the company. This affects long-term customer retention and loyalty.

These are global concerns for many organizations. How do jurisdictions outside the US view these issues and obligations differently?

The EU largely views ESG risk through a double materiality lens. Corporations must consider and disclose how sustainability related issues affect them both from an inside-out perspective and from an outside-in

perspective. For example, the new EU CSRD requires in-scope companies to report sustainability-related risks and opportunities from an impact materiality and a financial materiality perspective. Impact materiality assesses a company's actual or potential positive or negative material impacts on people or the environment over the short-, medium-, and long-term. Financial materiality highlights information that is useful to investors, lenders, and other creditors when they assess the effects of sustainability matters on a company's cash flows, development, performance, position, cost of capital, or liquidity access.

In the US, SEC-proposed and adopted rules, and widely adopted voluntary standards or best practices, largely assess materiality from the financial materiality standpoint, taking a single materiality approach. For example, a cybersecurity incident is examined for its impact on corporate value as opposed to how it may affect others.

We anticipate a convergence in how different jurisdictions approach ESG reporting. We are increasingly seeing regulations with ripple effects, such as the CSRD, emerge. Since these regulations mandate certain disclosures that companies may otherwise not consider, best practices and compliance with reporting likely will:

- Gradually evolve to accommodate regulatory requirements that may affect them.
- Ultimately mandate a double materiality approach to reporting ESG and sustainability-related risks.

Governance, Reporting, and Disclosure

Cybersecurity laws and regulations increasingly call for board-level oversight, incident reporting, and risk disclosure. What can cyber learn from ESG and vice versa? What trends do you see in regulatory enforcement?

ESG, as a term in common use today, is extremely broad and includes different components, including compliance and ERM. ESG materiality assessments include:

- Inquiring into a company's exposure to ESG risks, including cybersecurity.
- Identifying hotspots.
- Prioritizing risks to inform strategy and operational alignment.

Narrowing this down to cybersecurity, assessing cyber vulnerabilities, risk posture, and response readiness through an ESG lens may help companies evaluate cybersecurity risk as a core risk. Ownership, including board-level oversight and assigning responsibility at varying degrees throughout the organization, ensures an all-hands-on-deck approach for identifying and addressing cybersecurity risk and vulnerabilities.

The SEC rules regarding ESG, including the cybersecurity rules, focus on processes, ownership, and disclosures (see Legal Update, SEC Adopts Cybersecurity Risk Management and Incident Disclosure Rules). This trend throughout ESG-related regulations signals a consistent regulatory approach to ensuring that overall corporate strategies and operational alignment converge to address and communicate ESG risk and opportunities, including cybersecurity risks. Since cybersecurity is part of a company's ESG program and compliance with regulation is mandatory, building internal strategies for compliance into an ESG program:

- Integrates the key elements of a successful ESG program.
- Ensures a cost-effective and cost-efficient approach to complying with regulations on the horizon.

On enforcement, the SEC is taking an all-agency approach to ESG, prioritizing transparency and accuracy in disclosures and proactively identifying misconduct in ESG-related disclosures. As companies develop processes and strategies to preempt, prevent, and mitigate cyber risks, heightened focus should be on transparency, accuracy, and consistency in cyber-related processes, ownership, and disclosures.

What does good governance look like from ESG and cybersecurity perspectives? Are there differences? What about board-level expertise?

Industries are quickly changing, as are risks. Companies need to put a governance structure in place that allows the business to:

- Continually monitor risks.
- Move with developing requirements.

Companies should identify who is responsible for and processes key data, understand where data is stored and how it is processed, transferred, stored, and deleted, and ensure that good data management is in place and complies with the numerous data protection laws.

On disclosure, the SEC cybersecurity rules require organizations to report on a number of cybersecurity requirements relating to governance. Specifically, the rules require companies to disclose, among other things:

- Board oversight of risks from cybersecurity threats.
- If applicable, the board committee or subcommittee responsible for oversights of risks from cybersecurity threats.
- Management's role in assessing and managing material risks from cybersecurity threats.
- Processes by which the board or the appropriate committee is informed about risks from cybersecurity threats.
- Processes for the assessment, identification, and management of material risks from cybersecurity threats.

In disclosing management's role in assessing and managing material risks from cybersecurity threats, companies are required to disclose, among other things:

- Whether and which management positions or committees are responsible for assessing and managing those risks and the relevant expertise of those persons or members to a level of detail as necessary to fully describe the nature of their expertise.
- The processes by which those persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents.
- Whether those persons or committees report information about those risks to the board of directors, a committee, or a subcommittee of the board of directors.

Good governance as it relates to cybersecurity should model the ESG approach to governance. Some companies establish a risk committee or a technology committee. However, some organizations may find it more effective to include cybersecurity in the ESG mandate of all its committees, including:

- The governance and nominating committee, to establish the best framework for management and the board to coordinate cybersecurity and ESG matters, and to ensure that there is requisite expertise at the board level to exercise a duty of care.
- The audit committee, to provide oversight regarding disclosure and risk assessments.
- The compensation committee, to integrate ESG factors, including cybersecurity, into the company's compensation framework.

Voluntary guidance and standards abound in ESG and cybersecurity. What are some pros and cons of adopting these frameworks, especially as mandates increase?

Voluntary standards and guidance are beneficial for many reasons, including creating a baseline for identifying risks and opportunities, and facilitating disclosures. Voluntary standards also bridge the gap where regulation is absent or during intervening periods before regulations are enacted, giving companies a working roadmap to design their ESG programs and prepare for compliance. Industry-specific voluntary standards are also helpful in creating an appropriately tailored but consistent approach to identifying and disclosing ESG risks and opportunities as they present in specific industries.

As mandates increase, we are seeing a trend of regulations adopting existing standards to facilitate disclosures and compliance. For example, the SEC's proposed climate rules largely model the Task Force on Climate-Related Financial Disclosures (TCFD). The EU's CSRD and European Sustainability Reporting Standards (ESRS) are designed to ensure some level of alignment and interoperability with global standards, such as the International Sustainability Standard Board's (ISSB) IFRS S1 and S2 standards, TCFD, and Global Reporting Initiative standards, to ensure uniform, cost-effective, and cost-efficient reporting, given the CSRD's global application. These developments lend credence to the importance of standard-setters facilitating ESG disclosures.

One of the cons of voluntary standards has been fragmentation, given the multiplicity of standard-setters. However, we are increasingly seeing a trend of aggregation by the standard-setters to advance uniformity. Examples include the ISSB's inaugural S1 standards on sustainability-related disclosures, including data privacy and data security under the Sustainability Accounting Standards Board disclosures. Second, voluntary standards require businesses to report their operations to several parties demanding data on the businesses' performance on certain metrics. This adds another layer of exposure to cyberattacks and data leaks. Responsible cybersecurity practices when complying with ESG performance requests must rise to the top of the board's agenda to integrate cybersecurity considerations into its voluntary disclosure considerations.

Cybersecurity in Today's Interconnected Digital Ecosystem

How have cyber defense models changed, and does that align with ESG trends? What does it mean to be part of an interconnected digital ecosystem?

As our digital world becomes more interconnected, the cybersecurity hygiene of one organization can have significant consequences for stakeholders across the digital ecosystem. Incidents at one organization can impact the sensitive data of customers halfway around the world, and as data becomes easier to accumulate and store, the consequences of a security incident can quickly multiply. In this context, the ESG framework offers one lens through which we may view cybersecurity to create a more sustainable and responsible business model.

Application of the ESG umbrella can help organizations:

- Prioritize their cybersecurity efforts.
- Ensure that they are both coordinated with other compliance goals and aligned with their overall business goals.

How do successful organizations manage third-party supply chain risks?

Addressing supply chain risks requires having a coordinated program to ensure that vendors are not the weak link in a company's cybersecurity defenses. It is vital that organizations think not solely about their own network perimeter, but also about those of trusted vendors. Organizations that have been successful in mitigating supply chain risks have done so by creating a robust supply chain risk management program that includes:

- Policies and procedures.
- Adequate resources and training.
- Management buy-in.
- Measurable controls for mitigating risk.

An ESG perspective is helpful to increase coordination and decrease duplication when securing information and compliance from supply chains and customers. Vendors' ESG disclosures can be an important source of information for assessing supply chain risk.

Key Takeaways

What should organizations and their counsel be doing now to lean into these issues and build trust?

ESG is not new and is an aggregation of material issues within a company's anatomy that may pose risks and opportunities. A great starting point to lean into potential ESG issues, including cybersecurity, is to:

- Look within existing policies, procedures, and compliance programs.
- Build on them to account for the core elements of a successful ESG program.

Considerations around ownership, especially from a bottom-up approach, getting employees to understand their role in the collective effort to develop a successful program, and creating synergy from the bottom-up and top-down can culminate in a resilient and trustworthy program.

Lastly, companies must ensure a robust cybersecurity program in their ESG-related communications to build trust and reduce exposure to litigation, enforcement, and reputational risks.

Smaller or less-resourced companies should take a similar approach by:

- Building on existing policies and understanding regulatory considerations that are size-specific.
- Considering adopting existing best practices and standards, such as the Responsible Innovation Labs' roadmaps for founders, to build resilience and trust, especially in how they adopt technology and address cybersecurity risks and opportunities.

Overall, an integrated approach to risk management, combining the key elements of a successful ESG program, is a cost-effective and cost-efficient strategy to:

- Enhance cybersecurity and other compliance strategies.
- Create well-designed programs not only for strict regulatory compliance, but also for broader risk management.
- See around corners for developments and opportunities on the horizon.