Whitepaper
UNITED NATIONS SCIENCE-POLICY-BUSINESS FORUM

December 4, 2021

OVERVIEW

AUTHOR

Dr. Jonathan R. Everhart, CPA, Esq.
Chairman & CEO
Global ReEnergy Holdings

AFFILIATIONS

UN environment | SCIENCE POLICY BUSINESS FORUM

BROWN
Institute at Brown for Environment & Society

IoD Inspiring business
Institute of Directors

CISI
CHARTERED INSTITUTE FOR SECURITIES & INVESTMENT

CYBERSECURITY + ESG FOR THE GLOBAL CAPITAL MARKETS

IMPLEMENTING CYBERSECURITY WITHIN THE NASDAQ ENVIRONMENTAL, SOCIAL, AND GOVERNANCE (ESG) FRAMEWORK

This whitepaper discusses cybersecurity from the corporate governance standpoint and explores why Nasdaq's ESG Reporting Guide, which is used by many public and private companies globally, should implement cybersecurity into the framework. The intersection of a company's cybersecurity and ESG is a new corporate governance model. Cybersecurity has become a prevalent issue, specifically in the context of the digital economy, as corporate stakeholders require cyberattacks and security breaches to be proactively measured and mitigated in governing enterprise-wide risk management. Additionally, cybersecurity has gained wider attention due to increasingly impactful data breaches (i.e., SolarWinds) and the shift to remote working environments. As companies prioritize ESG, the inclusion of cybersecurity into their ESG governance framework is critical to manage the risks posed by cybersecurity to their ESG efforts. Nasdaq's ESG Reporting Guide is a leading standard within the global capital markets for companies implementing ESG policies and metrics. This whitepaper provides a use case demonstrating the implementation of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework into the Nasdaq ESG Reporting Guide. This can aid in encouraging more enhanced cybersecurity governance and improvements for the global capital markets.

WHY IS CYBERSECURITY CRITICAL TO AN ESG FRAMEWORK?

OPTIMIZING ESG THROUGH CYBERSECURITY GOVERNANCE

Since the inception of ESG practices, cybersecurity has not been considered an associated component of ESG. However, with the increase in high-profile data breaches, the acceleration of the global digital economy, and the shift to remote working environments, cybersecurity has quickly become strongly connected to ESG. Leading institutions, like JPMorgan, suggest that considering cybersecurity as an ESG metric is a relatively new model, however all evidence points to continued interest of this new model by organizational stakeholders across the board.[1] For instance, a 2019 survey by RBC Asset Management on investing concluded that 67% of investor respondents from the U.S., Europe, Asia, and Canada ranked cybersecurity as a top concern.[2] Core cybersecurity spending reached $68 billion in 2020, consisting of major spending in infrastructure protection, network security equipment, integrated risk management, and application security.[1] A Bloomberg report estimates cybersecurity spending to surpass $200 billion annually by 2024.[3] Given the rising importance of cybersecurity to a company's operational and financial performance, it is absolutely an ESG issue and should be implemented within a company's ESG practices.

Company stakeholders–including employees, investors, customers, regulators, and supply chain partners–are now more attentive to potential cybersecurity vulnerabilities and data management practices by companies. For example, the U.S. Securities & Exchange Commission requires public companies to disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky.[4] At the same time, these stakeholders have also required companies to adopt an ESG governance model as a means of operating more consciously towards environmental, social, and governance areas. Incorporating cybersecurity within the ESG framework is a natural evolution of technology's importance in managing enterprise-wide risks and strategic value creation for ESG. The general consequences of cybersecurity vulnerabilities associated with ESG include loss of critical assets; erosion of trust between the company and its customers, employees, and third parties; and irreparable harm to the company's reputation, brand, and bottom line.[5] To illustrate this further, cybersecurity plays a role in each area of the ESG framework as follows:

- Environmental: The interconnectedness of global economies means that a company's cybersecurity policies, compliance, and risk metrics can have far-reaching impacts on the environment. Companies with robust cybersecurity programs are better positioned to improve their environmental footprints, without interruptions and cyber threats to their environmental efforts. Companies should be able to clearly describe the effectiveness of their environmental operating models and the supporting cybersecurity processes, in terms of promoting security and risk awareness and reporting on cybersecurity metrics.[5]

- Social: Cybersecurity is important to the social aspects of ESG, as the public has become more concerned with the protection of personal data. Cybersecurity has risen to the level of other areas that the public is concerned about regarding what companies are doing for society (i.e., advancing diversity, human rights, etc.). Additionally, the public wants to know that the data they share with companies is protected. A commitment to cybersecurity drives customer confidence and promotes a company's proactiveness to protect against cyber threats.

- Governance: Reporting on cybersecurity risk metrics provides key insights into a company's overall corporate behavior and risk management oversight. Cybersecurity metrics should follow the same underlying principles as those used in ESG ratings, for instance, how resilient a company is to potential cyber events.[5]

To demonstrate how cybersecurity can fit within an ESG framework, the next sections explain Nasdaq's ESG Reporting Guide–a leading ESG framework which is used by companies globally–and how it can implement the NIST Cybersecurity Framework as a new ESG measure.

NASDAQ'S ESG REPORTING GUIDE

A LEADING ESG FRAMEWORK FOR THE GLOBAL CAPITAL MARKETS

Nasdaq established an ESG Reporting Guide through its Corporate Sustainability Program. The Guide was created primarily for public and private companies, however investors, stock exchanges, regulators, and other capital market stakeholders have significantly contributed to it.[6] In creating the Guide, Nasdaq engaged with stakeholders across the global capital markets, including public and private companies, investors, standards-setters, regulators, and stock exchanges. The first ESG Reporting Guide was launched in March 2017 as a pilot project, focused on business intent and regional socioeconomic scope.[6] Nasdaq used this pilot project as a request for information and comments from the abovementioned stakeholders. The interchange was based on the role of emerging ESG practices and key data that should be used to measure ESG performance by companies.

The Guide has gone through several updates to reflect the current ESG performance metrics that companies of all sizes and in all sectors are seeking to adopt. The current version of the Guide is intended to meet the following objectives: (1) Eliminate and revise uncommon or impractical metrics; (2) Incorporate new developments in the marketplace (such as TCFD, SDGs, GRI Standards, EU NFR Directive, and others); (3) Simplify and standardize guidance, labels, and calculations; (4) Improve ESG engagement for small- and medium-sized business enterprises; and (5) Cover all Nasdaq markets–including the U.S. equities market–in a single document.[6]

The Guide centers on companies considering the long-run strategic value of adopting ESG practices into their operations and transparency in reporting their ESG data. To meet this objective, the Guide focuses on economic principles and specific data because financial impacts are more direct and actionable by companies, as opposed to moral or ethical arguments.[6] The Guide also fosters a focus on ESG as a way for companies to obtain more efficient and sustainable governance practices. ESG is becoming a way to improve operations and corporate strategy, broaden corporate risk management, and engage with new investors. Nasdaq does not require its listed companies, by rule or practice, to disclose ESG data. However, Nasdaq encourages companies to reference the Guide's information as companies evaluate the best way forward within their operations relative to ESG.

Environmental (E)	Social (S)	Corporate Governance (G)
E1. GHG Emissions	S1. CEO Pay Ratio	G1. Board Diversity
E2. Emissions Intensity	S2. Gender Pay Ratio	G2. Board Independence
E3. Energy Usage	S3. Employee Turnover	G3. Incentivized Pay
E4. Energy Intensity	S4. Gender Diversity	G4. Collective Bargaining
E5. Energy Mix	S5. Temporary Worker Ratio	G5. Supplier Code of Conduct
E6. Water Usage	S6. Non-Discrimination	G6. Ethics & Anti-Corruption
E7. Environmental Operations	S7. Injury Rate	G7. Data Privacy
E8. Climate Oversight / Board	S8. Global Health & Safety	G8. ESG Reporting
E9. Climate Oversight / Management	S9. Child & Forced Labor	G9. Disclosure Practices
E10. Climate Risk Mitigation	S10. Human Rights	G10. External Assurance

GLOBAL CAPITAL MARKETS USE CASE

IMPLEMENTING NIST'S CYBERSECURITY FRAMEWORK WITHIN NASDAQ'S ESG REPORTING GUIDE

Cybersecurity should be added as a central element to Nasdaq's ESG Reporting Guide. To demonstrate this concept, this section demonstrates a use case implementing the NIST Cybersecurity Framework within the Guide. This paper and use case will be presented to Nasdaq and their Sustainability Division for consideration to implement, as Nasdaq is actively soliciting feedback to improve its ESG Reporting Guide.

The NIST Cybersecurity Framework incorporates industry standards and best practices to assist organizations in their cybersecurity risk management.[7] The Framework was created in cooperation with private and government sector experts and released in 2014. The Framework is a risk-based approach to cybersecurity risk management. It includes five core areas:[7,8]

- Identify: Assists organizations in developing an overall risk management approach to cybersecurity by understanding their critical assets, business environment, governance model, and supply chain.
- Protect: Assists organizations in putting important defensive controls in place based on their critical assets, risk tolerance, and other input from the Identify core area. This area focuses on managing identities, securing access, protecting data, and training users.
- Detect: Assists organizations in shortening the time to discovery by spotting anomalies, investigating events, continuously monitoring, and other detection processes.
- Respond: Assists organizations in taking the right action immediately through incident response planning, analysis, mitigation, communication, and ongoing improvement.
- Recover: Assists organizations in restoring operations through recovery planning, continuous improvement, and communications.

Through these areas, organizations are equipped with a cybersecurity governance framework that guides them on understanding their cybersecurity threats, vulnerabilities, and impacts, and how to mitigate these risks using proactive measures.

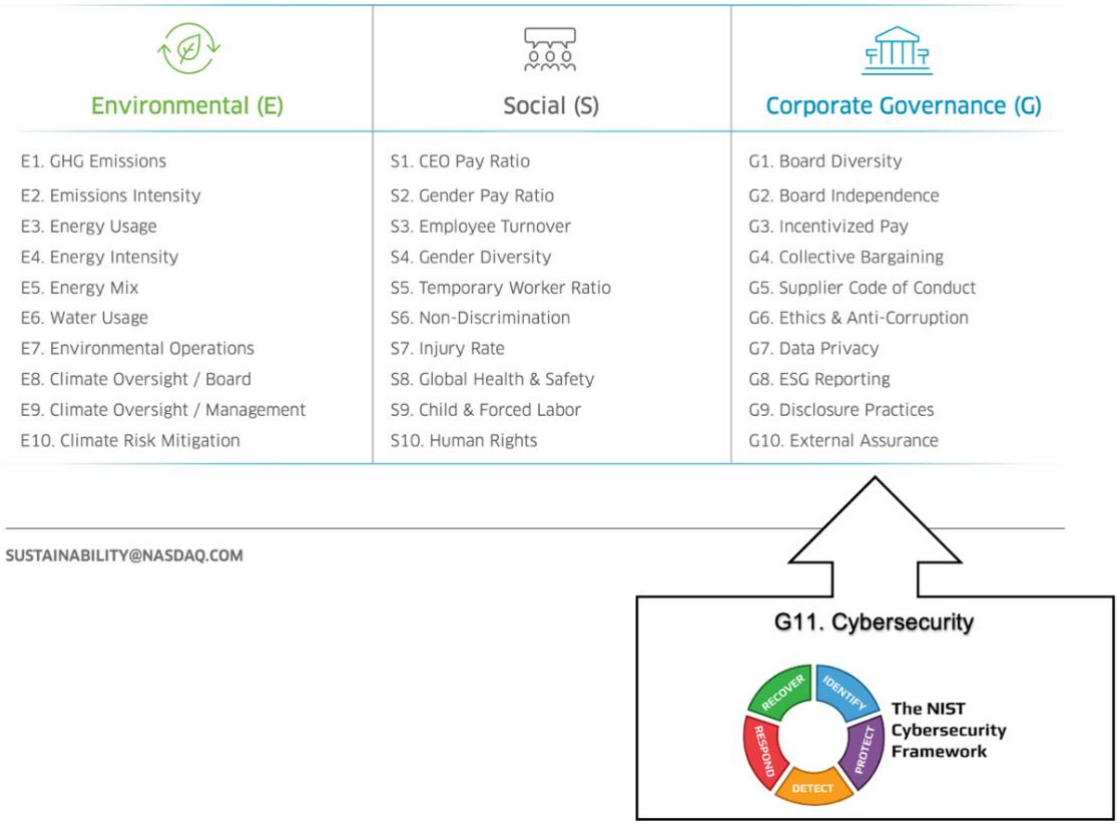
Nasdaq's ESG Reporting Guide currently includes 33 core ESG metrics divided into each ESG subsection, with a focus on driving market valuation to the most meaningful, practical, and achievable metrics that companies and stakeholders consider in ESG reporting.[6] Each of these ESG metrics includes several related insights, which are:[6] (1) Why is it measured; (2) How is it measured; (3) Why is it disclosed; and (4) How is it disclosed. Additional information is provided to assist companies in evaluating each ESG data point, including: existing connections to prominent ESG reporting frameworks, the relative percentage of Nasdaq-listed companies reporting this data (when known), and links to underlying calculation methodologies.[6] Figure 1 outlines a sample cybersecurity ESG metric, created by the author of this whitepaper, based on the NIST Cybersecurity Framework and in accordance with the criteria used by Nasdaq's ESG Guide to report each of the other 33 metrics.

Figure 1. Sample Cybersecurity ESG Metric Using Nasdaq's ESG Reporting Guide Criteria

G11. Cybersecurity G11.1) Does your company follow a cybersecurity risk management framework? Yes/No G11.2) Does your company's board of directors and executive management regularly assess cybersecurity risk management? Yes/No	
Why is it measured?	Cybersecurity has become a prevalent issue, specifically in the context of a digital economy; many stakeholders assert that cyber attacks and security breaches should be vigorously mitigated, and they use this metric to measure the sophistication of a company's enterprise-wide cybersecurity risk management protocols.
How is it measured?	Companies that create, publish, and periodically update a policy document that covers this subject may affirmatively respond
Why is it disclosed?	Stakeholders use this metric to evaluate the efficacy and scope of enterprise risk management (ERM)
How is it disclosed?	As text, with appropriate links to public content
Connections to Frameworks	UNGC: Principle 9 National Institute of Standards and Technology's Cybersecurity Framework
Percentage of Companies Reporting?	N/A
Notes & Sources	Cite specific frameworks used See also: Internet Governance Forum: We must act now to tackle the threats of cyberspace (United Nations, 2019)

In incorporating a cybersecurity ESG metric using the NIST Framework, Nasdaq's ESG Reporting Guide can include it within the governance section–as number G11.–which is shown below in Figure 2.

Figure 2. NIST's Cybersecurity Framework Incorporated within Nasdaq's ESG Reporting Guide



Cybersecurity has become an ESG issue and should be included within a company's ESG governance framework. Cybersecurity awareness, investment, and impact will continue to increase as economies become more digitized and interconnected. Incorporating the NIST Cybersecurity Framework within Nasdaq's ESG Reporting Guide is a key step to accelerating the implementation of this new governance model for the betterment of the global capital markets.

References

[1]JPMorgan, "Why is Cybersecurity Important to ESG?," *JPMorgan*, August 19, 2021. [Online]. Available: https://www.jpmorgan.com/insights/research/why-is-cybersecurity-important-to-esg

[2]RBC Global Asset Management, "2019 Responsible Investing Survey Key Findings," *RBC Global Asset Management*, 2019. [Online]. Available: https://global.rbcgam.com/sitefiles/live/documents/pdf/rbc-gam-responsible-investing-survey-key-findings-2019.pdf

[3]Nasdaq Investment Intelligence, "Cybersecurity: Industry Report & Investment Case – HUR," *Nasdaq*, 2021. [Online]. Available: https://indexes.nasdaqomx.com/docs/HUR_Research.pdf

[4]Division of Corporate Finance – Securities & Exchange Commission, "CF Disclosure Guidance: Topic No. 2 Cybersecurity," *Securities and Exchange Commission*, Oct. 13, 2011. [Online]. Available: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[5]KPMG, "Cyber security: Don't report on ESG without it," *KPMG*, 2021. [Online]. Available: https://advisory.kpmg.us/articles/2021/cyber-security-report-on-esg.html

[6]Nasdaq, "Nasdaq ESG Reporting Guide," *Nasdaq*, 2021. [Online]. Available: https://www.nasdaq.com/docs/2019/11/26/2019-ESG-Reporting-Guide.pdf

[7]National Institute of Standards and Technology, "NIST Cybersecurity Framework," *National Institute of Standards and Technology*, 2021. [Online]. Available: https://www.nist.gov/cyberframework

[8]Cisco, "What Is the NIST Cybersecurity Framework?," *Cisco*, 2021. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-nist-csf.html