THE EMERGENCE OF CYBERSECURITY IN ESG

Cybersecurity rising on the ESG radar, with investors leading the way

CONSERVICE® ESG

DRAWBRIDGE

ESG (Environmental, Social, Governance) topics are now firmly at the top of the business agenda, amid the unprecedented changes unleashed by the COVID-19 pandemic and stakeholders' rallying cry for business to do more to contribute to sustainability.

Stakeholders are pushing for companies to show that they are as serious about ESG performance as they are about financial performance, as the world grapples with challenges from climate change to plastics pollution to deforestation to poverty, inequity and more.

And now cybersecurity has a central role in the S and G, consistently ranking as one of the most pressing ESG issues in investor surveys. The growing number of cyberattacks are leaving companies as well as governments and other institutions feeling undefended.

This latest ESG issue is rising to the fore amid the pandemic, which was already pushing ESG to the forefront with its huge health, social, and economic costs. COVID-19 exposed the risks of low-probability, high-impact events like global pandemics. Planning for the longer term is seen as more critical than ever.

The cost of inaction on ESG could be severe. In a June 2021 survey from PwC, 76% of consumers said they will discontinue relations with companies that treat employees, communities, and the environment poorly. And 86% of employees prefer to support or work for companies that care about the same issues they do.

Customers, consumers, and employees alike want to see accountability and transparency in how companies approach societal and environmental issues, how they care for workers, customers, and neighbors, and how they govern themselves in an ethical way (including protecting data privacy and warding off cyberattacks).

While climate change has long been a top concern, the "S" aspect of ESG is now gaining attention, with "social" jumping in ranking from number three to number one as the most important ESG factor in the U.S.

Investors driving demand for robust ESG actions

Investors are among the most vocal in pushing for greater actions around ESG. A growing number of investment firms now consider sustainability critical to operations and performance.

Investors directed $51.1 billion to sustainable funds in 2020, more than doubling investments within a year, according to industry reports. In 2021, about 77% of professional fund selectors and 75% of institutional investors considered ESG factors an integral part of sound investing, Nasdaq reports.

Increasingly, institutional investors are aligning their portfolios toward companies demonstrating better ESG performance. And they do it with increasing rigor. Of the 98% of investors surveyed who assess ESG, 72% carry out a structured review of ESG performance, compared with just 32% in the previous survey conducted two years earlier, a 2020 survey found.

This charge is being led by some of the biggest financial players. BlackRock, the world's largest asset manager, has called sustainability its "new standard" for investing and informed CEOs that "climate change has become a defining factor" in their companies' long-term prospects.

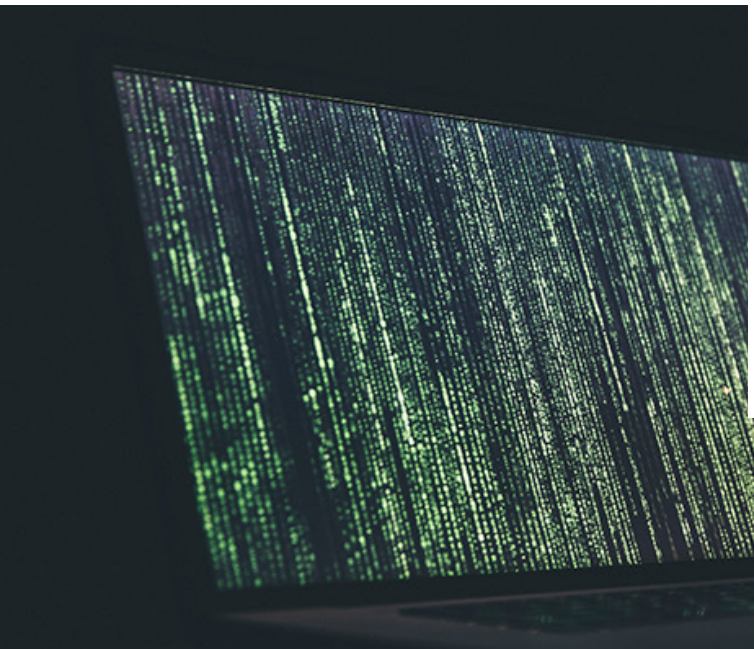
In short, ESG investing has reached critical mass & cybersecurity is quickly rising on investors' radar.

Benefits of shifting from reactionary to proactive

Forward-thinking companies are responding to investors and other stakeholders, recognizing the many advantages of leading on ESG. Some 91% of CEOs believe companies must act on ESG issues.

Companies that are proactive on ESG gain numerous benefits, from climate resiliency to employee and customer trust and loyalty to attractiveness to investors, who are aligning their portfolios towards better ESG performance. Prioritizing sustainability also contributes to more proactive regulatory compliance.

And there are direct financial benefits to superior ESG performance, studies have shown. BlackRock found that 81% of a globally representative selection of sustainable indexes outperformed their parent benchmarks. As BlackRock CEO Larry Fink put it in his 2021 CEO Letter: “It’s not just that broad-market ESG indexes are outperforming counterparts. It’s that within industries—from automobiles to banks to oil and gas companies—we are seeing another divergence: companies with better ESG profiles are performing better than their peers, enjoying a ‘sustainability premium.’”



Those who want to be leaders in the space need to shift from a reactionary approach to ESG to a strategic, value-add approach. In fact, experts have warned that an ESG reckoning is coming for firms that offer commitments that are not authentic or sincere, or when they overpromise transformation, according to the Harvard Business Review.

ESG central to risk mitigation

Not least, incorporating an ESG framework into business operations and processes is a smart form of risk mitigation.

Risks related to climate change impacts, environmental management, workers' health and safety, respect for human rights, anti-bribery and corruption practices, and compliance with relevant laws and regulations are growing in importance in a company's overall risk profile.

Companies that ignore these risks or make a misstep could face substantial economic costs that threaten the ability to earn long-term, sustainable profits. To reduce that probability, companies are wise to minimize their ESG-related risks and enhance their sustainable competitive advantages.

As cyberattacks mount, vulnerabilities are exposed

And certainly, a growing risk, and opportunity to demonstrate leadership, is cybersecurity. The FBI's cyber crimes unit has seen a 400% increase since the start of the COVID-19 pandemic. Experts note that cyberattacks are becoming more sophisticated and malicious, finding new ways to compromise the IT software supply chain to infiltrate government and enterprise networks.

Microsoft's Digital Defense Report noted that it blocked over 13 billion malicious and suspicious emails in 2019, including 1 billion that were URLS set up to launch phishing attacks. The incidence of cyberattacks has only grown in the past two years.

No business is immune. Recorded Future, a security firm that tracks ransomware attacks, estimated that there were 65,000 successful ransomware attacks last year, or one every eight minutes. As businesses automate their core operations, the prospect of more ransomware attacks grows. The average cost of a data breach in the U.S. is $8.64 million and the ransom demand can turn into six figures with some of the more notorious ransomware gangs.

The attacks are becoming more brazen. In May 2021 the cyberattack on Colonial Pipeline, a main artery of the U.S. fuel supply, focused overdue attention on whether oil and gas (and businesses across other industries) are adequately prepared to mitigate cyber risk and safeguard against vulnerabilities. Colonial paid 75 Bitcoin, or roughly $5 million, to hackers to recover its stolen data. A sophisticated cyberattack shut down hundreds of businesses around the world including one of Sweden's largest grocery chains in July 2021, and experts believe it may be the same Russian cybercriminal group that the F.B.I. has said is behind the hacking of the world's largest meat processor, JBS, in May.

Cybersecurity failure ranks as the fourth likeliest critical threat to the world within the next two years, behind infectious diseases, livelihood crises, and extreme weather events, according to the World Economic Forum's Global Risks Report 2021.

Investors see cybersecurity as top issue

No wonder, then, that cybersecurity ranked as the most pressing ESG issue for 67% of institutional investors surveyed by RBC Global Asset Management in 2019.

And in June 2021, a new Architas ESG report found data protection and cybersecurity to be the second most pressing ESG issue for retail clients in 8 out of 11 markets it surveyed.

Governance specialists with the Principles for Responsible Investment (PRI) warned in a report last year that "[c]ompanies can only ignore these threats at their peril." They recommended that governance structures and processes incorporate cybersecurity and data privacy elements if a company is serious about identifying, addressing, and resolving these issues, which can impact every stakeholder. Cybergovernance is seen as a proxy for cyber resilience.

Business shows lacks of preparedness against cyberattacks

Business leaders are clearly looking for guidance, with one survey in February 2021 showing that 78% of senior IT and IT security leaders lack confidence in their firm's cybersecurity readiness, leading to 91% raising their 2021 budgets.

And 2020 EY research into 76 Fortune 100 companies found that the frequency of cybersecurity reporting, active preparedness, and ties to executive compensation among the largest companies in the US remains dismally low.

Best practices for cyber resiliency

What can be done to protect against cyberattacks and manage this increasingly pressing ESG topic?

An S&P Global Ratings report urged that "energy infrastructure needs to become more cyber resilient," with improved data security procedures for investments and to prioritize new cybersecurity solutions where weaknesses are identified.

Awareness and continuous monitoring are vital. PRI recommended that investors continually press boards of directors to actively monitor cyber issues, integrate cybersecurity into corporate strategy, and improve disclosures. Other experts urged a robust approach to cybersecurity reviews, training, and outcomes, urging that as much attention be paid to an organization's network and information as its core IT infrastructure and endpoint devices.

In the U.S., the White House has urged companies to adopt many of the defensive steps that the federal government requires of its agencies and contractors, according to the New York Times. Anne Neuberger, the deputy national security adviser for cyber and emerging technologies, in an open letter in June 2021, suggested that companies separate corporate business functions and manufacturing/production operation to avoid an attack on business records, such as emails or billing operations, cutting off critical production and supply lines.

Further suggestions from Neuberger included multifactor authentication, a process that forces employees to enter a second, one-time password from their phone, or a security token, when they log in from an unrecognized device. And, while it may seem obvious, companies were urged to regularly back up data, and segregate those backup systems from the rest of their networks to make them more difficult for cybercriminals to find. Another tip was "penetration testing," which simulates an attack on a company's systems to identify vulnerabilities. And not least, companies need to plan their response should they face a ransomware attack.

Banks and payment companies are taking the cue, using an increasingly militarized approach to respond to cybercrime, hiring former government cyberspies, soldiers, and counterintelligence officials for their security teams and opening up "fusion centers," a term loaned from the Department of Homeland Security to coordinate intelligence gathering. With these intelligence hives, the banks have pinned their hopes on detecting patterns in the data they collect to ward off future attacks.

SEC takes more aggressive ESG stance

If companies don't step up, regulators will step in. After the Colonial hacking, the Transportation Security Administration (TSA) made it a requirement for companies that operate pipelines to alert the government whenever they suffer cyberattacks. And thousands of employees in the past two years have been sent on government-mandated cyber and information security courses.

Meanwhile, the Securities and Exchange Commission (SEC) is putting increased emphasis on ESG issues. It appointed its first-ever head of ESG in February 2021. And its Spring 2021 rulemaking list included regulations that would enhance ESG-related disclosures for public companies in areas like climate change, board diversity, human capital management, and cybersecurity risk governance.

Acting Chair Allison Herren Lee said in March 2021 that the agency "has begun to take critical steps toward a comprehensive ESG disclosure framework aimed at producing the consistent, comparable, and reliable data that investors need."

As part of that effort, the SEC formed the first-ever Climate and ESG Task Force within the Division of Enforcement. The Task force will work to proactively detect climate and ESG-related misconduct, including identifying any material gaps or misstatements in issuers' disclosure of climate risks under existing rules and analyzing disclosure and compliance issues relating to investment advisers' and funds' ESG strategies.

What's next

2021 is expected to be a decisive year for both increased awareness of and action on ESG, and cybersecurity will continue to be a hot topic. Any post-COVID recovery will be closely tied to ESG, with scrutiny on how companies prepare for complex systemic risks, such as the potential effects of climate change.

There will be a greater push, not least from investors, for clearer ESG standards that are unified and harmonized into a single consistent framework applicable across different sectors and industries.

ESG activism will not dissipate any time soon, both from activist investors and regular citizens. The coming months and years are seen as an opportunity to rebuild economies with ESG priorities, corporate purpose, and sustainability at the forefront.

The social aspect of ESG will continue to rise in importance, and financial markets data firm Refinitiv expects that 2021 will see the emergence of new technologies, new approaches, and new players, as well as a renewed focus on ESG integration driven by data.

On the cybersecurity front, expert Chuck Brooks writing in Forbes predicted that attacks will cast a wider web, encompassing remote work, the Internet of Things (IoT), and the supply chain. Ransomware will remain the cyber weapon of choice. And finally, threats to critical infrastructure through industrial control systems and operational technology will converge, posing ever greater threats against critical infrastructure.

"Like most issues in cybersecurity, it comes down to people, vigilant processes, and technologies coupled with risk factors constantly being reviewed," according to Brooks.

With growing investor demand for action on cybersecurity among many ESG concerns, "vigilance" is a mantra that companies are well advised to make their own in 2021 and in the years to come.

CONSERVICE® ESG

Conservice is the most intelligent, comprehensive, and intuitive solution for ESG management. We help businesses establish, monitor, and communicate ESG initiatives that provide an imperative to attract and retain capital, accelerate sustainable and responsible growth, and mitigate enterprise risk.

ESG.CONSERVICE.COM

DRAWBRIDGE

Drawbridge Partners is the premier cybersecurity software and services firm providing solutions to the alternative investment space. We not only protect our clients from cyber breaches but we also meet the demands of institutional investors and the regulatory bodies.

DRAWBRIDGECO.COM