



#ESGT Impact

Andrea's Quick Take On All Things...

ESG & TECHNOLOGY

September 14, 2020

Cyber. Pandemic. Resilience. Interconnected.

Dear Friends,

I hope that you and yours are healthy and safe. If you're in the Northern Hemisphere, I hope you had a good summer - if in the Southern Hemisphere - I wish you a good start to spring.

Are cyber, resilience, ESG interconnected? Well of course they are and especially in our pandemic times. To make my case, today's issue features:

- My new piece on "[How Relevant is Cyber Resilience to ESG?](#)" for [Crisis Response Journal's](#) latest fall issue. It's borne out of a series of pieces I have co-written with my friend Maya Bundt, head of digital and cyber for Swiss Re:
 - Here is our [original White Paper for the Swiss Re Institute](#)
 - here is [our piece for the World Economic Forum Agenda](#)
- Also, please join me for a complimentary NACD panel on "ESG and Cybersecurity: How Boards Can Respond to Investor Concerns" on September 17th from 2-3pm Eastern. [Register here.](#)
- Thanks to my friends at UK-based Emergency Planning Society who produced a summary report from a co-presentation I did with the head of the British Red Cross on "[Organizational Resilience in our Pandemic Times](#)" recently.

I'm also sharing [my latest LinkedIn post on Boeing's continued leadership, culture and quality travails](#). I don't know why this particular post struck such a nerve but it blew up and is at 73,000+ views and counting...

Until next time. Please get a safe start to the new "work & school" season wherever you are - stay vigilant, take care of your neighbors and do something to make the world a better place.

[Andrea](#)

NACD CYBER & ESG WEBINAR - COMPLIMENTARY SIGN UP



The banner features the NACD logo in the top left corner. To the right of the logo is a navigation menu with links: NACD NXT, Podcast, Chapters, Membership, About, Contact, and a search icon. Further right are 'Login' and 'JOIN' buttons. Below the navigation menu is a horizontal bar with links: CERTIFICATION, INSIGHTS, ANALYTICS, BOARD SERVICES, COURSES & EVENTS (highlighted in blue), and CREDENTIALS. The main content area of the banner has a background image of hands typing on a keyboard. Overlaid on this image is the text: 'ESG & Cybersecurity: How Boards Can Respond to Investor Concerns'. Below this title, it says 'September 17, 2020 | Online' and '2:00-3:00 pm (EDT)'. At the bottom of the banner is a horizontal bar with links: CALENDAR, FOUNDATION COURSES, SUMMIT, PEER TO PEER, VIRTUAL LEARNING, and SPECIAL EVENTS.

Contact Us.

Connect by phone: 844-245-2363

ESG & Cybersecurity: How Boards Can Respond to Investor Concerns

September 17, 2020 | Online
2:00-3:00 pm (EDT)

Complimentary

[REGISTER NOW](#)

READ "HOW RELEVANT IS CYBER RESILIENCE TO ESG?"

How relevant is cyber

With the global pandemic continuing to rage, malign cyber actors – sensing a world of opportunity in the chaos – are deploying their weapons in an even more amplified and depraved way than before. Organisations must therefore be cyber resilient, writes **Andrea Bonlime-Blanc**

We are experiencing a convergence of major cyber risks, including a labour shift, as work has migrated from the more cyber resilient, relatively centralised workplace to the less secure, decentralised home office environment. There are new opportunities for cyber criminals, with a rise of actors looking to get rich via ransomware attacks on healthcare targets, or steal Covid-19 healthcare and pharmaceutical intellectual property. Another risk involves geopolitical instability, as the current unstable scene allows for even greater nation state and criminal cyber activities designed to exploit chaos.

The convergence of these risks makes it much more critical for every type of organisation to develop resilience, including in cyber. Increasingly, investors and other stakeholders are demanding transparency into the environmental, social and governance (ESG) profile of companies and it is a matter of time before they demand cyber resilience transparency – or what I term ESG-T resilience – for technology, including cyber.

To explore the relevance of cyber resilience to ESG, Maya Boud and I crafted a definition for the term in a recent white paper, *Cyber-Resilience ESG Reporting: Transparency Imperative or Security Nightmare?* – “an organisation’s ability to sustainably maintain, build and deliver intended business outcomes, despite adverse cyber events. Organisational practices to achieve and maintain cyber resilience must be comprehensive and customised to the whole organisation (including the supply chain). They need to include a formal and properly resourced information security programme, team and governance that are effectively integrated with the organisation’s risk, crisis, business continuity and education programmes.”

Net benefits for businesses and investors

After interviewing 20 global executives and board members, we found that the vast majority of respondents – 19 in fact – agreed that cyber resilience external ESG-style reporting would deliver a net benefit, not only to the investor, but to the company itself.

According to the 2019 RBC Global Asset Management Responsible Investment Survey of almost 800 investors surveyed in the USA, Canada, Europe and Asia, 57 per cent of the world’s institutional investors are concerned about the impact of cybersecurity threats on their investments.

considered four categories of cyber disclosure that are important to investors: Cyber risk identification, governance, context, and implementation. I says, “Companies with best practices have solid incident anticipation and damage control processes in place. We also expect that best practice companies have cyber security integrated at the product level early in product development and are managing their cyber assets and costs effectively.”

The World Economic Forum has carried out useful research on the topic and offers five principles of due diligence: Incorporate a cyber risk tolerance; conduct cyber due diligence; determine appropriate incentive structure; secure integration and development; and regular review and collaboration.

The above examples give us what ESG reporting is intended to do for environmental, social and governance issues. ESG reporting is here to stay – even in the US, a latecomer to the party.

This July, CNBC reported on the increase in ESG investment in 2020 despite, or maybe owing to, the pandemic. It highlighted that 14 out of 17 ESG-focused exchange traded funds (ETFs) outperformed the S&P 500 – one of the most followed stock market indices for large US companies – from January 1 to May 15. In addition, financial services firm Morningstar says that 23 new ESG funds were launched this year and it anticipates a record number of launches in 2020. US sustainable funds hit record net flows in 2019; this year is already on track to surpass these figures.

In the EU, a well-established ESG regime has emerged over the past couple of decades, originally encouraged by a wide array of stakeholders and then embraced by regulators via EU Directive 2014/95, which requires

– age, gender, educational and professional backgrounds. Even the US Government has recently embraced ESG. The US Securities and Exchange Commission (SEC) requires the investment community to create more rigour around what it means to be an ESG investment fund. When the US Department of Labor issued a proposal for public comment suggesting that pension funds should focus exclusively on financial metrics and forget about ESG ones, the idea was met with a wall of criticism from the vast majority of the investor community and others.

The US ESG conversation was recently enlivened by a surprisingly useful US Government Accountability Office research report issued in July 2020, which evidenced the further mainstreaming of these issues in the American business and policymaking contexts.

You might notice, however, that cyber and technology reporting do not seem to factor highly or even in the ESG agenda of any jurisdiction. Indeed, if lucky, data privacy and protection may enter the ESG lists, but they are not given much prominence, despite the importance of cyber and other technology issues, such as AI ethics and diversity concerns. These emerging and widely replicating technology risks and opportunities have deep implications for business strategy just to mention society as a whole.

This is partly why I wrote my book, *Gloom to Boom*, to highlight the need for businesses and their stakeholders to incorporate emerging tech risks and opportunities into the ESG analysis, strategy and reporting discussion by considering including technology into a broader ESG-T framework (see CFI ESG).


Currently, we need to extrapolate ESG reporting best practices, since required public cyber resilience reporting doesn’t yet exist. The best an outside stakeholder can glean is when things go wrong, that is material cyber risk reporting when major negative events occur. For example, in the US, regulators are starting to require small elements of greater cyber transparency, but this is mostly related to material negative events.

In 2018, the US SEC released cybersecurity guidelines to listed companies, which essentially revolved around ensuring that they have the right policies in place to protect against insider trading on adverse non-public cyber news. In 2020, the SEC also issued guidelines requiring publicly listed companies to report on material technology risk events involving intellectual property theft.

This is a step in the right direction. However, investors and other stakeholders are still unable to evaluate fully how well prepared – how cyber-resilient – an organisation may be, despite the fact that cyber risk is at an all-time high.

One of the few organisations that has carried out work on the idea of cyber resilience reporting is Principles for Responsible Investment (PRI), a UN-supported international network of investors. Table one (p8) summarises its eight categories, along with 14 indicators, of what cyber resilience reporting might consist of in its 2019 research report, *Stepping Up Governance on Cyber Security: What is Corporate Disclosure Telling Investors?*

The PRI document is a good start and asks questions that should be factored into the



What cyber reporting could look like – an early example from a study by PRI

Legal compliance	Does the company publicly commit to complying with relevant laws, including those related to cyber and data protection?
Policy	Does the company publicly disclose a privacy and/or data protection policy? Does the policy explicitly cover its entire operations, including third parties?
Senior management and board accountability	Does the company identify a named person at senior management or executive committee level with overall responsibility for information management and cybersecurity? Is the board or board committee responsible for cybersecurity issues?
Board communication	Does the company communicate cyber risks to the board – and how, by who and how often? Does the board receive detailed information about the company’s cyber or information security strategy, including what information it receives and how it assesses this information?
Skills and resources	Does the company disclose that it has a cyber or information security team and/or dedicated budget? Does the company state that it works with relevant industry initiatives on cybersecurity and/or has access to internal or external expertise on cybersecurity? Does the company actively seek cybersecurity skills when appointing directors?
Training	Does the company provide training on information or cybersecurity requirements to all employees?
Assessment	Does the company conduct audits of information or cybersecurity policies and systems?
Business continuity and risk management	Has the company established an incident management plan, including disaster recovery and business continuity? Has the company disclosed information or cybersecurity as a key part of its risk assessment or business continuity plan?

READ THE EPS SUMMARY REPORT ON ORGANIZATIONAL RESILIENCE



CONVERSATION THREE:
**ORGANISATIONAL RESILIENCE &
THE RESILIENCE PROFESSIONAL
AND 'NEW' EMERGENCIES**

Speakers:
Michael Adamson
Jehangir Malik OBE
Dr Andrea Bonime-Blanc

Thursday 16th July 2020

SUMMARY REPORT



**ADD YOUR OPINION TO
THE LINKEDIN POST**

**Andrea Bonime-Blanc**

Founder • CEO • Board Director • ESG • Ethics • Cyber • Technology • Stra...

4d • 🌐



Here we go again with **Boeing** & its **#quality #health #safety #risks** ...

It's about the **#leadership**

It's about the **#governance**

It's about the **#culture**

it's about not making **#ESG** & **#ESGT** (+ **#technology**) **#stakeholder**
expectations central to your long term business **#strategy**

It's about not having/caring about **#organizational #resilience**

I talked about this with **Cheddar Inc.** TV on the **NYSE** trading floor on March 12th
- the day the market crashed & the day before we began to quarantine in NYC -
<http://bit.ly/2TLCLNa>

https://lnkd.in/gX8i_nx

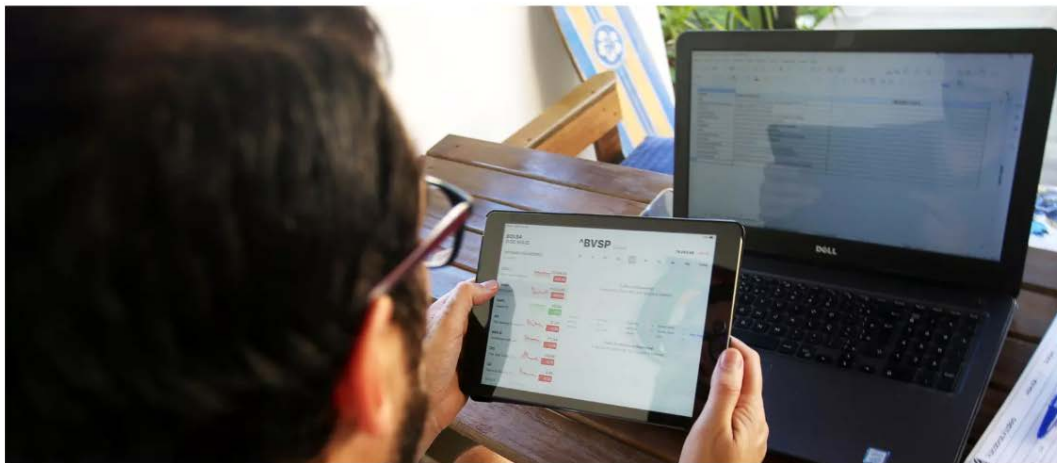


WSJ News Exclusive | Production Problems Spur Broad FAA Review of Boeing Dreamliner Lapses

RELATED RESOURCES

[Global Agenda](#) | [Cybersecurity](#) | [Cybercrime](#) | [The Digital Transformation of Business](#)

Cyber resilience is critical for organizations' survival. Thoughtful reporting can help build it.



In an era of strategic risk, thoughtful cyber-resilience reporting is important to creating overall cyber resilience.

Image: REUTERS/Rahel Patrasso

07 Jul 2020

Andrea Bonime-Blanc



Founder and CEO, GEC Risk Advisory

Maya Bundt

Head, Cyber and Digital Solutions, Swiss Re


- The COVID-19 pandemic has highlighted the importance of cyber resilience to organizations' stability, productivity and survival.
- Cyber-resilience reporting can increase transparency, enhance reputations and foster an organizational culture to combat cyber risk.

[READ THE WORLD ECONOMIC FORUM AGENDA BLOG](#)




In partnership with

Transparency Imperative or Security Nightmare?
Cyber Resilience "ESG" Reporting



Maya Bundt, Swiss Re, and
Andrea Bonime-Blanc
coauthor White Paper for the
Swiss Re Institute



**"Cyber Resilience ESG
Reporting: Transparency
Imperative or Security
Nightmare?"**

[Click Here](#)

[DOWNLOAD THE WHITE PAPER](#)

GLOBAL GOVERNANCE

FUTUREPROOFING POST-PANDEMIC GOVERNANCE

BY ANDREA BONIME-BLANC


[READ THE ARTICLE](#)
[ADDITIONAL RESOURCES](#)

GEC Risk Advisory
Transforming Risk into Value®

HOME SERVICES RESOURCES GLOOM TO BOOM BOOK 2020 ANDREA'S BOOKS EVENTS THOUGHT LEADERSHIP TEAM & CONTACT

Gloom to Boom Book Reviews are rolling in

Directors & Boards BOOK REVIEW
View Here

FROM GLOOM TO BOOM: BUILDING RESILIENCE BOOK REVIEW
View Here

INACD Directorship BOOK REVIEW
View Here

COMPLIANCE WEEK BOOK REVIEW
View Here

[Visit the GEC Risk Advisory Website](#)



Learn more about [Gloom to Boom](#)



Twitter



Website



Email



Tweet



Forward



Share

Copyright © 2020 GEC RISK ADVISORY LLC. All rights reserved.

Our mailing address is:

GEC Risk Advisory LLC

P.O. Box 231351

NEW YORK, NEW YORK 10023 USA

[unsubscribe from this list](#) [update subscription preferences](#)