#ESGT Impact

Andrea's Quick Take On All Things...

ESG & TECHNOLOGY

June 2, 2021

8 Steps to a Cyber Resilience Virtuous Cycle

Subscribe to #ESGT Impact

Colleagues and friends,

You may ask yourself - what in the world is a "cyber resilience virtuous cycle"? Sounds like an oxymoron?? Well, maybe it is or maybe it isn't - read on and you decide.

I just wrote two articles on this concept:

- A short piece called "8 Steps to Starting a Cybersecurity Virtuous Cycle" for World Economic Forum Agenda
- A long, feature piece called "Cyber Organizational Resilience is a Business Imperative: Eight Steps to Get There" for the spring edition of Spain's Actuarios Magazine with a lot more detail.
- If you missed last month's #ESGT Impact and haven't yet downloaded a free copy of The ESGT Megatrends Manual: A Blueprint for Navigating Risk and Opportunity in Tectonic Times what are you waiting for? Download it here.
- Watch my latest presentation to the Wall Street Green Summit 20th Anniversary summit on, what else, an "ESGT Strategy for Sustainable Organizational Resilience" here.

Most of my resilience work borrows heavily on the 8-step model of organizational resilience that I outlined and developed in Chapter 7 of my book Gloom to Boom: How Leaders Transform Risk into Resilience and Value.

Overall organizational resilience is necessary to combat some of the truly material and even existential threats of our times, to protect stakeholders and to preserve and create value. And this applies to all types of entity - whether business, government or social - everyone must build internal resilience to deal with not only cyber-insecurity but climate, pandemics, social injustice, misinformation and other critical issues of our times.

Until the next time, stay healthy, stay well and stay connected!

All the best,

Andrea

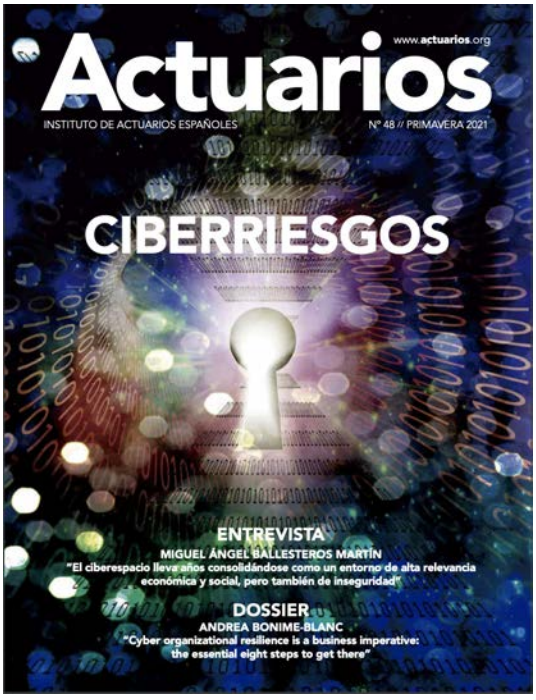
Subscribe to #ESGT Impact

WORLD ECONOMIC FORUM AGENDA SHORT PIECE: Eight Steps to Starting a Cybersecurity Virtuous Cycle

WORLD ECONOMIC FORUM

8 steps to starting a cybersecurity virtuous cycle

ACTUARIOS MAGAZINE - "Cyber Organizational Resilience is a Business Imperative: The 8 Essential Steps to Get There"



Primavera 2021 // nº 48 // DOSSIER

Cyber organizational resilience is a business imperative: the essential eight steps to get there

ANDREA BONIME-BLANC
CEO, GEC Risk Advisory, Board Member, Global Strategist, Ethicist, Author

I. Introduction

This article is a call to arms to all businesses – big, medium and small – to build cyber organizational resilience in the face of an unprecedented and exponentially growing global cyber threat matrix. Even governments are unable to cope with the cyber-onslaught which means that everyone – from individuals to corporations – must do their part to protect lives, assets, value and stakeholder interests.

This article begins by presenting some highlights of the current, dark cyber-picture that is upon us. We then shine the spotlight on three ongoing mega-cyber breach cases and conclude with an eight-step plan for building cyber-organizational resilience.

This is the bottom line for business: ignoring the cyber problem could become one of the costliest potentially existential) crises you've ever faced. Paying attention to it now will protect people, assets and profits and give your business the opportunity to not only survive financially but thrive reputationally. Building cyber organizational resilience is the only sustainable stance that businesses can take to the ever-expanding universe of cyber-malevolence.

Even when businesses do all the right things, they will still be at a severe disadvantage because, unlike many other business risks, cyber-risk is primarily a turbo-charged, frontier-less criminal risk where only 5% of the criminals get prosecuted and/or a nation-state, geopolitical risk for which businesses are completely outgunned (literally and figuratively). In both cases, business needs the help of government and in both cases so far business hasn't gotten much help (or looked for it, frankly). It's time to seriously address and fix these problems.

II. A Global-Mega-Cyber-Problem

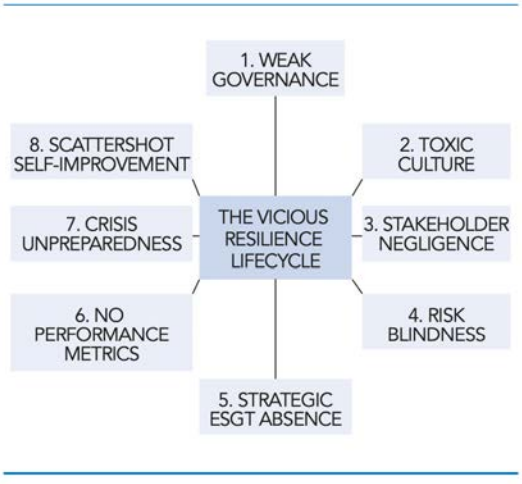
"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again".

Prophetic words in 2012 uttered by then FBI Director Robert S. Mueller at what now can only be called the dawn of modern-day cyber-attacks before they became as huge, widespread, diversified and accelerated as they are now, especially since Covid19 hit in early 2020.

When Director Mueller said those words almost a decade ago, we had no idea how pervasive, complex, multi-dimensional, disruptive, exponential and frightening the world of cyber-attacks would become in the following years. According to Verizon, 86% of all cyber breaches are financially motivated. The World Economic Forum (WEF) has estimated revenues from cybercrime to be at around US$2.2 Trillion this year - likely to grow almost five times to US$10.5 Trillion by 2025.

1 https://en.wikiquote.org/wiki/Robert_Mueller

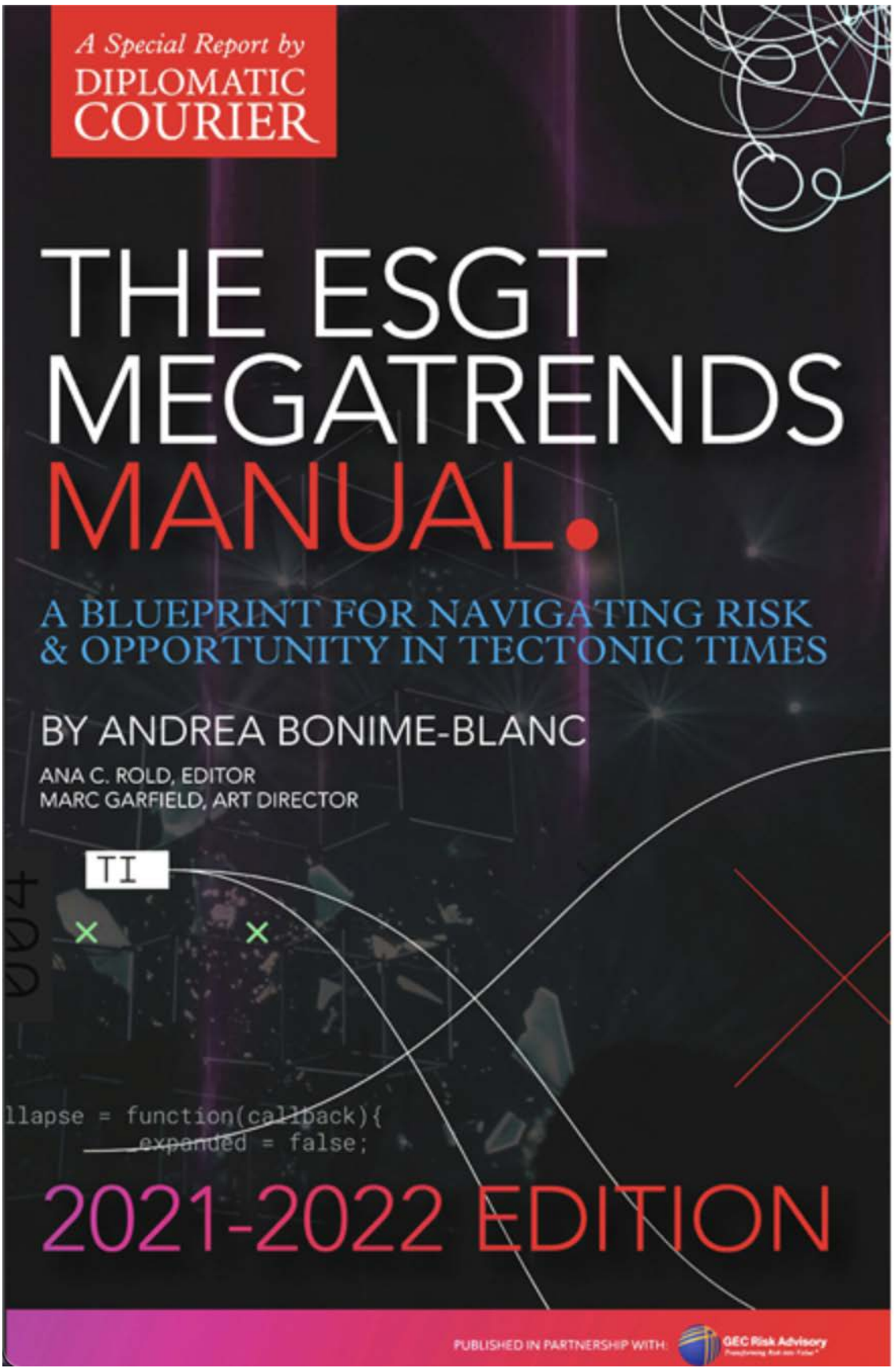
Source: *A. Bonime-Blanc. Gloom to Boom. Routledge 2020.*



Source: *A. Bonime-Blanc. Gloom to Boom. Routledge 2020.*

WATCH PRESENTATION ON DEVELOPING AN ESGT STRATEGY FOR SUSTAINABLE RESILIENCE

DOWNLOAD YOUR COMPLIMENTARY COPY OF THE ESGT MEGATRENDS MANUAL



Subscribe to #ESGT Impact

Learn more about Gloom to Boom

Twitter Website Email

Tweet Forward Share

Our mailing address is:
GEC Risk Advisory LLC
P.O. Box 231351
NEW YORK, NEW YORK 10023 USA