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

Think about how that breaks down on the other side of that equation – the damage in US Dollars caused by cyberattacks estimated for 2021[2]:

Figure 1: Global Cybercrime Damage Costs

$6 Trillion USD a **Year***
$500 Billion a **Month**
$115.4 Billion a **Week**
$16.4 Billion a **Day**
$684.9 Million an **Hour**
$11.4 Million a **Minute**
$190,000 a **Second**

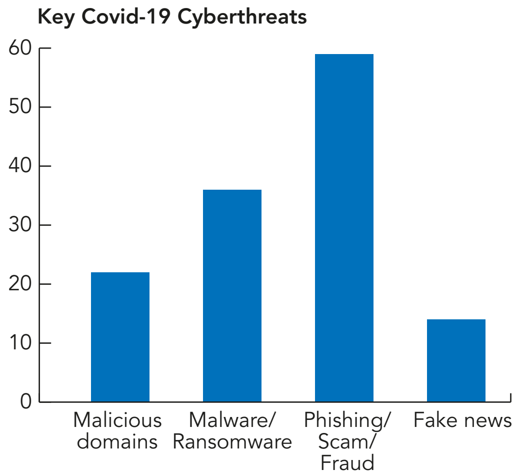
ALL FIGURES ARE PREDICTED BY 2021

CYBERSECURITY VENTURES

Source: **Cybersecurity Ventures.*

Add to this reality the fact that the Global Pandemic of 2020-21 has turbocharged cybercrime (as the Interpol chart below shows), targeting especially vulnerable sectors like hospitals, municipalities, healthcare, pharma and supply chain targets. What we now have is an unprecedented, constantly and rapidly morphing and exponentially growing global cyber-mess.

Figure 2: Distribution of the key COVID-19 inflicted cyber-threats based on member countries' feedback



Based on the comprehensive analysis of data received from member countries, private partners and the CFC, the following cyberthreats have been identified as main threads in relation to the COVID-19 PANDEMIC.

Source: *Interpol 2020.*

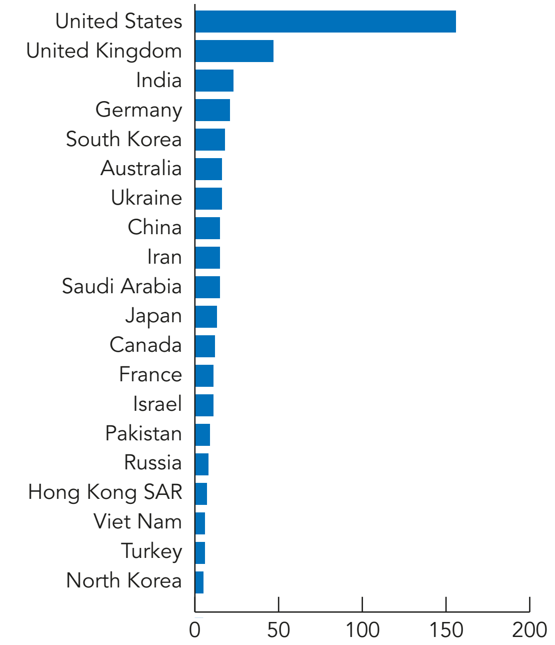
If those figures didn't paint a dire enough picture, WEF's 2021 Global Risks Report estimates that:

> "Organized cybercrime entities are joining forces, and their likelihood of detection and prosecution is estimated to be as low as 0.05% in the U.S."[3]

The bottom line is that cybercrime pays so much more than traditional crime, is so much easier to perpetrate and has so many other advantages to other types of crime (e.g., it's largely untraceable, logistically seamless, inexpensive to deploy and doesn't require a lot of investment in human capital). In other words, it pretty much can be perpetrated from someone's basement or bedroom. Ideal for our work-from-home pandemic times.

Meanwhile, though the Biden/Harris Administration has gotten off to a good start on rethinking and restructuring cybersecurity with more appropriate strategy, budgets and qualified personnel addressing both the public and private sectors, the FBI's cyber budget until now has been less than $500 million. And that's for the country – the United States – that has been most cyber-attacked in the World - see WEF chart below.

Figure 3: Significant Cyberattacks 2006-2020 (Total Number)



Source: *World Economic Forum 2020.*

[2] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/?_aiid=12699&trots=dGVuZzpnbztiZW5nOmI7ZGVuZzpjO2tlbmc6bmF0aW9uYWwlM

[3] http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

Think about the differential between the cybercriminal world currently drawing revenue of $2.2 Trillion versus that tiny FBI cybercrime enforcement budget in the country that is the most affected by cyber-crime and you get a picture of an upside-down, asymmetrical David and Goliath mega-problem confronting not just the US but the world in general where national governments oddly are David and the cyber-criminals sitting in their basement are Goliath (maybe).

As the leading cyber security expert, Larry Clinton, President of the Internet Security Alliance (and co-author of the NACD and WEF Cyber Risk Handbook), has stated:

> "The Cyber equation attack methods are comparatively cheap and easy to acquire, attackers have first-mover advantage, generate high profits with a great business model. Versus the defenders protecting an inherently vulnerable system (getting more vulnerable all the time), often "out-gunned" by attackers, virtually always in reactive mode and who get virtually no help from law enforcement."

III. Three Cyber Breach Cases: The Good, the Bad and/or the Ugly?

The following three cases (described in Boxes 1, 2 and 3) are meant to illustrate the vastness of the problem. Indeed, all three cases while not fully attributed to any nation state or criminal entity yet bear all the markings of both nation state and criminal gang activity. They are all far from resolved at the time of this writing.

The Microsoft Exchange case appears to have been started by China but once revealed publicly became the object of a vast criminal ecosystem feeding frenzy. Microsoft leadership's rection to this event has been consistent with its style of leadership under Satya Nadella its CEO – more transparent than opaque, and more collaborative than obtuse, but it is certainly a huge embarrassment that only a cyber-resilient organization like Microsoft can appropriately manage.

The Facebook case – despite Facebook's protestations to the contrary – reveals the soft underbelly of a company that is not known for protecting the privacy and data of its users – quite to the contrary, known for making user data (and everything that goes with it) the center of its wildly successful business model. This is another blow to the reputation of the company which does not appear to have deep cyber-resilience based on what we know publicly.

Finally, the SolarWinds case also bears the signature of Russia acting as a nation state perpetrator not only affecting US government agencies but also most of the Fortune 500 global companies. This case underscores the severe flaws and vulnerabilities that exist in the overall supply chain on a B2B level as well as between business and government with little attention paid to security at the inception and during the lifecycle of a software product. And for a company that has some of the most sensitive US government agencies as customers to allow its interns, reportedly, to enter passwords like "Solarwinds123" and then post the password on GitHub is a massive failure of cyber-resilience, specifically cyber-culture and risk management[4].

Box 1 - The Microsoft Exchange Hack[5]

> "Microsoft and DHS CISA announced the confirmed exploitation of several vulnerabilities in Microsoft Exchange Server which have allowed adversaries to access email accounts, exfiltrate data, move laterally in victim environments, and install additional accesses and malware to allow long-term access to victim networks. The exploitation of these vulnerabilities is described as a zero-day (or 0day), which means they were targeted and acted upon prior to the vendor knowing that the vulnerabilities existed. In other words, there were zero days for the vendor to implement a fix for the vulnerability before it was used in an attack. Microsoft detected multiple successful attacks against previously unknown vulnerabilities in Microsoft Exchange Server. Microsoft Threat Intelligence Center (MSTIC) has attributed observed activity with high confidence to a group they have named HAFNIUM, which they assess to be state-sponsored and operating out of China. The U.S. Government has not confirmed attribution at this time.

Box 2 - The Facebook 533 million User Breach[6]

> "After information from 533 million Facebook users was exposed to hackers, the company has tried to reassure users, saying that the data was

[4] https://www.zdnet.com/article/solarwinds-security-fiasco-may-have-started-with-simple-password-blunders/

[5] https://www.cisecurity.org/ms-exchange-zero-day/

[6] https://www.theguardian.com/technology/2021/apr/06/facebook-breach-data-leak

leaked years ago and has since been secured. But experts say the issue is still grave – whether it happened in 2021 or years prior – largely because of the nature of the leaked data. The dataset, first reported by Business Insider, contained information from 106 countries including phone numbers, Facebook IDs, full names, locations, birthdates and email addresses."

Cyber resilience is an organization's ability to sustainably maintain, build and deliver intended business outcomes despite adverse cyber events

Box 3 - The SolarWinds Sunburst Breach[7]

"On December 13, 2020, FireEye announced the discovery of a highly sophisticated cyber intrusion that leveraged a commercial software application made by SolarWinds. It was determined that the advanced persistent threat (APT) actors infiltrated the supply chain of SolarWinds, inserting a backdoor into the product. As customers downloaded the Trojan Horse installation packages from SolarWinds, attackers were able to access the systems running the SolarWinds product(s). This cyber-attack is exceptionally complex and continues to evolve. The attackers randomized parts of their actions making traditional identification steps such as scanning for known indicators of compromise (IOC) of limited value. Affected organizations should prepare for a complex and difficult remediation from this attack."

IV. Building Cyber Organizational Resilience: Partial and Imperfect but the Only Path Forward

All that is the bad news. Is there any good news? I think there is and it's this: businesses big, medium and small, can do something to protect themselves by building resilience and awareness within their organizations. However, without taking these key measures, businesses big, medium and small, are exposed and outgunned both literally and figuratively and at very high risk of a serious, material or even existential cyber-crisis.

Even being resilient doesn't guarantee cyber-success. But what it does do is provide greater confidence and trust to stakeholders (including importantly investors, regulators and the government) that management and the board are doing their utmost to safeguard the crown jewels of the company including people and assets (both digital and physical) as well as pursuing a mission, purpose and strategy that is both resilient and sustainable.

So, what is "cyber resilience"?[8]

"Cyber resilience is an organization's ability to sustainably maintain, build and deliver intended business outcomes despite adverse cyber events. Organizational practices to achieve and maintain cyber resilience must be comprehensive and customized to the whole organization (i.e. including the supply chain). They need to include a formal and properly resourced information security program, team and governance that are effectively integrated with the organization's risk, crisis, business continuity, and education programs."

And what is "organizational resilience"?[9]

"Organizational resilience is the ability of an organization to provide and maintain an acceptable level of operation, service, and performance in the face of challenging conditions, disruptions, risks and crises and to bounce back and recover quickly from them with minimal impact to the organization including to its reputation."

If we combine both terms to try to understand what cyber-organizational resilience is, I come up with eight key steps to building organizational cyber-resilience that is based on research and work I have done on cyber-governance, leadership, risk and resilience over the past 10 years.

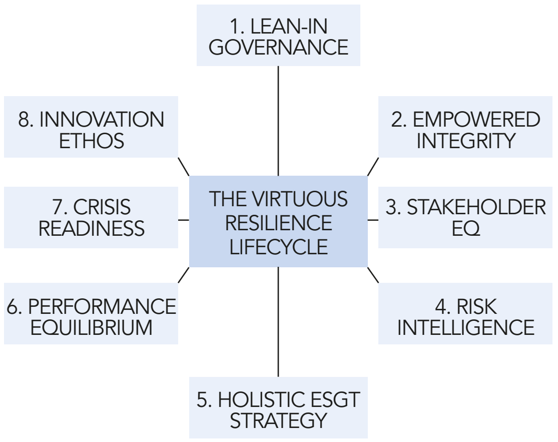
In my book, Gloom to Boom, I explore different types of organizational resilience with those having the "Virtuous" or "Responsible" types being the most equipped and able to deal with major incidents such as material cyber-attacks. See picture below.

[7] https://www.cisecurity.org/solarwinds/

[8] M. Bundt & A. Bonime-Blanc. Cyber Resilience ESG Reporting. Swiss Re & GEC Risk Advisory White Paper. 2020.

[9] A. Bonime-Blanc. Gloom to Boom: How Leaders Transform Risk into Resilience and Value. Routledge 2020.

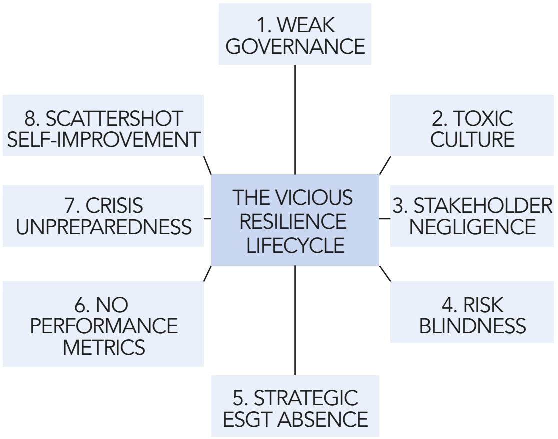
Figure 4:



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

In contrast those with a "Fragile" or "Vicious" Lifecycle (the worst kind) of organizational resilience are at a severe disadvantage when it comes to dealing with the pervasive and potentially existential threat of cyber insecurity. Just take a look at the graphic below for the Vicious Lifecycle type and you can draw your own conclusions.

Figure 5:


1. WEAK GOVERNANCE
2. TOXIC CULTURE
3. STAKEHOLDER NEGLIGENCE
4. RISK BLINDNESS
5. STRATEGIC ESGT ABSENCE
6. NO PERFORMANCE METRICS
7. CRISIS UNPREPAREDNESS
8. SCATTERSHOT SELF-IMPROVEMENT
THE VICIOUS RESILIENCE LIFECYCLE

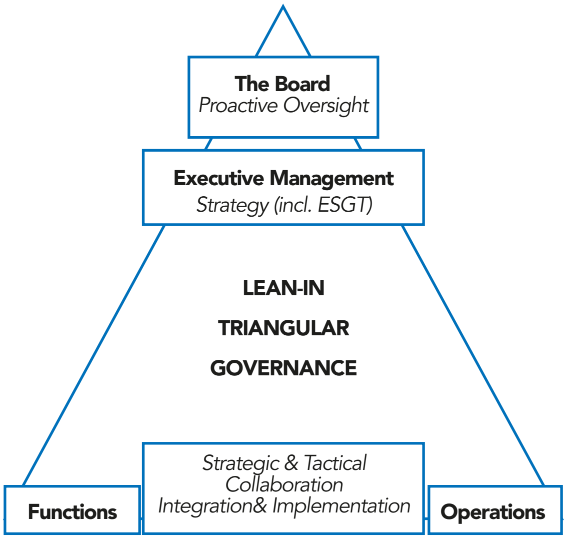
Source: *A. Bonime-Blanc. Gloom to Boom. Routledge 2020.*

Building on this model and focusing it exclusively on the construction of cyber-organizational resilience, I would distinguish the following 8 elements:

1. Lean in Cyber Governance and Leadership

This means that your board of directors and your c-suite understand the depth and breadth of the cyber challenge and are prepared to provide both the tone from the top and the resources and budget necessary to create lean-in, triangular cyber risk governance: where oversight by the board, strategy by the c-suite and front-line coordinated implementation by both functional and operational experts are in sync and operating smoothly together. See Graphic below.

Figure 6:



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

In the excellent March 2021 World Economic Forum, the Internet Security Alliance, PwC and the National Association of Corporate Directors publication "Principles for Board Governance of Cyber Risk", they distinguish the following key elements of the cyber-resilient organization from the governance perspective[10]:

- Cybersecurity is a strategic business enabler

[10] http://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf

- Understand the economic drivers and impact of cyber risk
- Align cyber risk management with business needs
- Ensure organizational design supports cybersecurity
- Incorporate cybersecurity expertise into board governance
- Encourage systemic resilience and collaboration.

2. Empowered Culture of Cyber and Information Hygiene

The culture that the tone from the top imbues the organization with is one that highlights, underscores, incentivizes and reinforces a culture of information hygiene and cyber hygiene where all concerned are trained and retrained regularly on pitfalls and best practices and are not afraid to speak up and when they do they are not ignored. A great example was provided by the Chief Information Security Officer of the World Health Organization, Flavio Aggio, in his keynote presentation at the Cyber Future Foundation/WHO Special Meeting held in April 2021 as follows[11]:

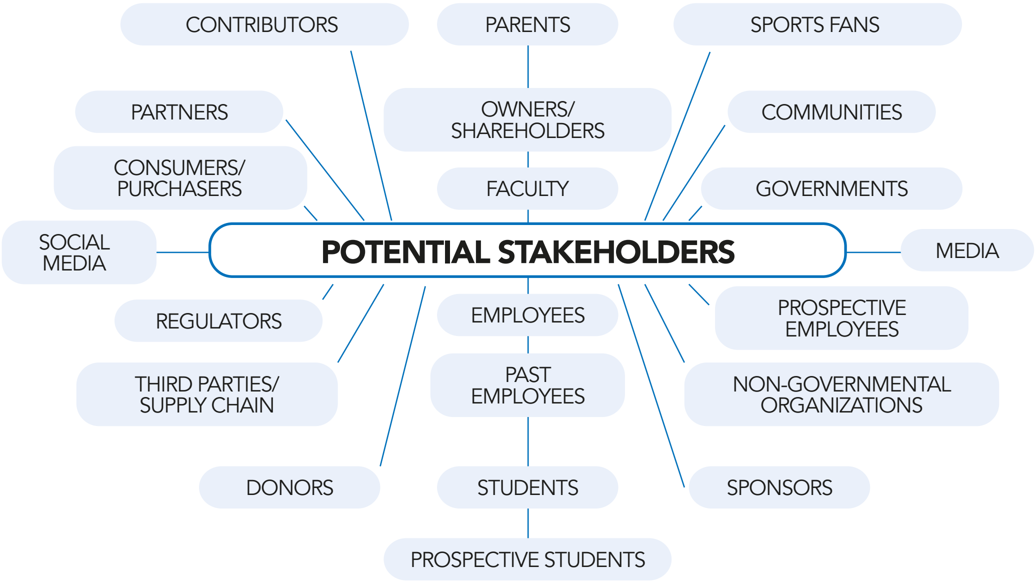
- Work hard to change the mindset that "IT ensures 100% security"
- Monthly Phishing exercises make users understand cyberattacks faster & better
- Communicate often but not too much
- Concentrate on "what's in it for me?"
- Collaborate and share information with external organizations
- Concentrate on human centric technology

3. Cyber-Stakeholder Emotional Intelligence

Each company needs to know where its cyber crown jewels are (assets – digital or physical that cyber-attackers might be interested in), understand how to prioritize and protect them and then understand

[11] Flavio Aggio, CISO, WHO, Keynote address CFF WHO Cyber Healthcare Special Meeting - https://www.youtube.com/watch?v=a1LW8w1SwQY&t=1955s

Figure 7: A universe of potential stakeholders



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

how their main stakeholders – owners/shareholders, customers, employees, other – may be negatively affected. A key part of this component of cyber-organizational resilience is to reach out and have close stakeholder relations and information sharing especially in the more vulnerable sectors with the greatest potential damage from cyberattacks (health, utilities, financial). That's why it is so important to have the right industry or sector collaboration as well as private public cyber-collaboration. See Graphic below for potential stakeholders.

4. Cyber-Risk Intelligence

It is absolutely crucial that cyber-risk management be a seamless part of a company's risk management system – fully integrated into enterprise risk management and risk mitigation and transfer opportunities such as cyber insurance. Part of a robust cyber risk management program is to have the right interdisciplinary, cross functional, multi-divisional group of experts internally (with access to outside experts) within your company. See graphic below for an illustration of this concept.

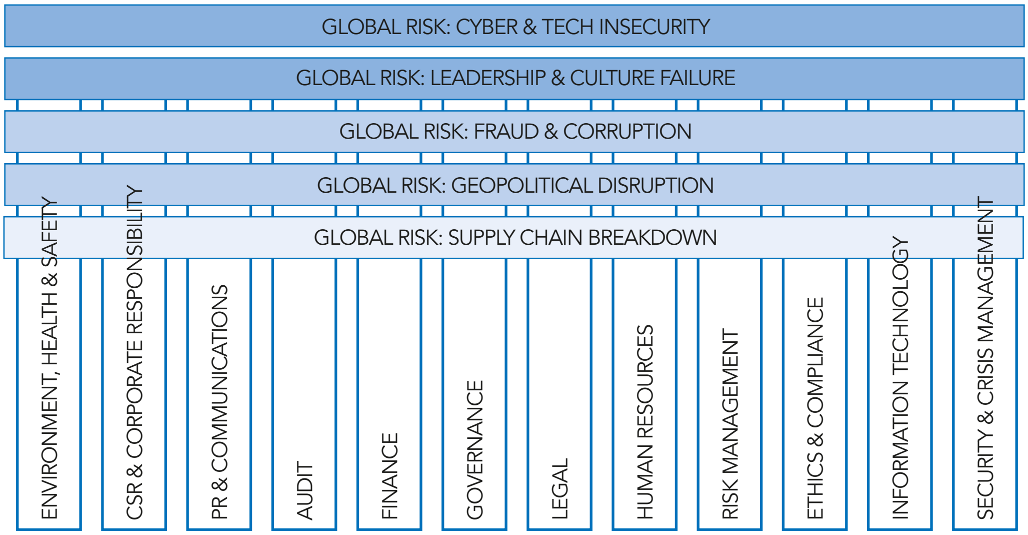
> It is absolutely crucial that cyber-risk management be a seamless part of a company's risk management system – fully integrated into enterprise risk management and risk mitigation and transfer opportunities such as cyber insurance

5. Strategic integration of key ESGT issues, risks and opportunities including cyber

No business will be cyber-secure or prepared if it does not integrate cyber-risk considerations into its business strategy. Period. There are way too many weak links in the chain of any business – whether it's the innovation stage, the product or services research and development chain, the supply chain, the mergers and acquisitions space, talent acquisition strategy (employee or contractors, subcontractors, etc.) or simple software updating protocols – if a company is not bringing cyber-vigilance into all aspects of strategy formulation, development

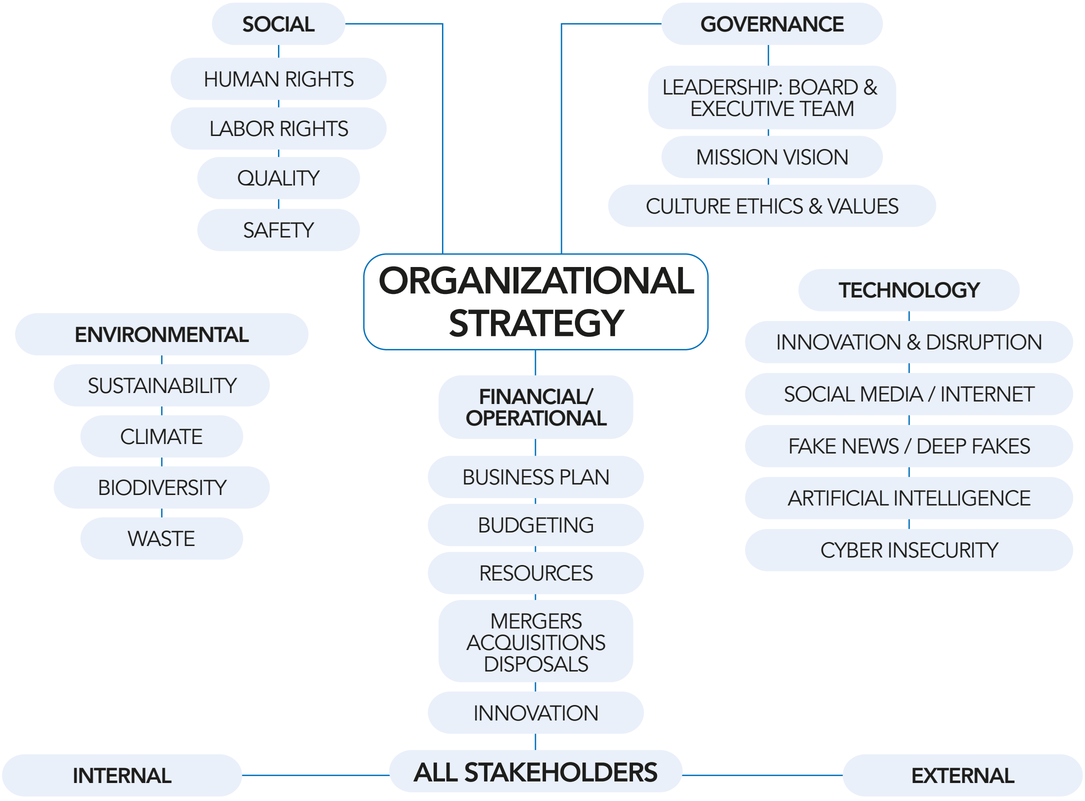
Figure 8:

THE RISK MANAGEMENT CROSS-FUNCTIONAL IMPERATIVE


GLOBAL RISK: CYBER & TECH INSECURITY
GLOBAL RISK: LEADERSHIP & CULTURE FAILURE
GLOBAL RISK: FRAUD & CORRUPTION
GLOBAL RISK: GEOPOLITICAL DISRUPTION
GLOBAL RISK: SUPPLY CHAIN BREAKDOWN
ENVIRONMENT, HEALTH & SAFETY
CSR & CORPORATE RESPONSIBILITY
PR & COMMUNICATIONS
AUDIT
FINANCE
GOVERNANCE
LEGAL
HUMAN RESOURCES
RISK MANAGEMENT
ETHICS & COMPLIANCE
INFORMATION TECHNOLOGY
SECURITY & CRISIS MANAGEMENT

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

Figure 9:



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

and execution it is once again exposing itself to major potential cyber damage not to mention losing out on serious opportunities for new business. See how cyber-insecurity is part of a broader ESGT strategy integration in the graphic below:

6. Performance metrics and incentive program including cyber-metrics

You cannot reward (or discipline I would add) what you cannot measure – is an important maxim in business. So the same goes for cyber-resilience – how do you measure cyber security internally? Do you have the right people, are they doing the right things, what is the profile of cyber-incidents, how quickly are they resolved, are we using the right technology solutions, training, communications, etc. And all this needs to be tied back to professional and executive compensation metrics and be properly reported to the board (who as we stated in #1 above should be leaning-in proact8uvely on cyber security oversight). Otherwise, no one will be properly incentivized. Below is a sample dashboard that attempts to capture some of such metrics.

7. Crisis Readiness including deep, broad cyber preparedness

Companies must have, in the first place, a crisis management team and plan that is ready at any given time, especially in. these crises-ridden times, to deal with a major crisis, including a cyber event. That means that the right people, resources and tools are ready and available and that proper scenario planning by an interdisciplinary team of high-level professionals, the executive team and the board should be addressing periodically. And all of the crisis management needs

Figure 11: What's on your board's cyber risk governance dashboard?

Architecture of cyber risk governance	Budget & resources
How is the company positioned, organized, and deployed for cyber risk management Is this the optimal approach?	What is being spent? What is needed for proper cyber risk management?
Threat matrix-substantive cyber-risk issues	**Toolkit & proactive measures**
Top issues Industry trends and benchmarking Technology trends and benchmarking Global heat map	Status report on the main policies and programs in place what is needed
Technology & liability defenses in place	**Internal technology talent & skills assessment**
Status report on what cyber defenses are in place: technological, assessments, audits, monitoring, testing, insurance	Review top expert executives Review C-suite and CEO performance on cyber-risk management
Incident reporting	**External experts used/needed**
Statistical overview of all incidents at company Specific mention of serious-to-material incidents	Are the right experts in place? Including for periodic board report
Cyber attack crown jewels	**Cyber actors & stakeholders matrix**
Know exactly what your company's crown jewels are what are the perpetrators and potential perpetrators after?	Who are the potential perpetrators? Who are the company stakeholders and potential victims?

Source: *Source: A. Bonime-Blanc. Emerging Practices in Cyber Risk Governance. The Conference Board 2016.*

to be seamlessly integrated with cyber savvy business continuity, backup and data management and preservation planning, of course.

8. Cyber - innovation ethos

Lastly but definitely not least, the same approach that companies give to their product and services innovation should be brought to cyber-security and risk management innovation. What does that mean?> It means thinking and acting outside of the box and learning lessons learned from both company incidents as well as sector and industry incidents that might have occurred. It means joining sector information sharing groups and public/private collaboration. It means doing deep dives, root cause analysis and adopting the important take-aways. It means that the cyber-security ethos must be one of continuous improvement and reinvention.

V. Conclusion

In closing, in mid-2021, I would propose that we revise Director Mueller's words quoted at the beginning of this article from 2012 to read as follows:

> There are only two kinds of organizations (whether government, business or NGO) – those that have been hacked and know it and those that have been hacked and don't know it yet. And the only way to be prepared for the future is to be cyber-resilient. ●