

This site uses cookies to deliver website functionality and analytics. If you would like to know more about the types of cookies we serve and how to change your cookie settings, please read our [Cookie Notice](#). By clicking the "I accept" button, you consent to the use of these cookies.

[I accept](#)

8 steps to starting a cybersecurity virtuous cycle



Only 0.5% of cybercriminals are convicted – so businesses must build their own cyber-resilience.

Image: Getty Images/iStockphoto

26 May 2021

Andrea Bonime-Blanc

Founder and CEO, GEC Risk Advisory

AUDIO: LISTEN TO THE ARTICLE



12:15 A small black speaker icon with sound waves.



This is an experimental feature. Some words or names may be mispronounced. Does it sound good? [Yes](#) / [No](#)

In the face of an unprecedented and exponentially growing global cyberthreat matrix, there must be a call to arms to all businesses – big, medium and small – to build cyber-organizational resilience.

According to Verizon, 86% of all cyber breaches are financially motivated. The World Economic Forum has estimated revenues from cybercrime will be at around \$2.2 trillion this year – likely to grow almost five times to \$10.5 trillion by 2025.

Even when businesses do all the right things, they will still be at a severe disadvantage because, unlike many other operational risks, cyber-risk is primarily a frontierless criminal activity where only 0.5% of criminals get prosecuted and/or a nation-state, geopolitical level one, for which businesses are completely outgunned.

One of the few things within a company's cyber-control is building organizational cyber-resilience. Here's an eight-step plan to get this done.

Building organizational cyber-resilience

Even being resilient doesn't guarantee cyber-success. But what it does do is provide greater confidence and trust to key stakeholders that the company is doing its utmost to safeguard the crown jewels of the company, including people and assets, as well as pursuing a mission, purpose and strategy that is both resilient and sustainable.

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 programme, team and governance that are effectively integrated with the organization's risk, crisis, business continuity, and education programmes.

It slots into the broader context of organizational resilience, which 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.

This is the best possible "Virtuous" organizational resilience life-cycle (as opposed to the "Vicious", depicted beneath it):



Figure 7.2 The Virtuous Resilience Lifecycle.

Source: Author and GEC Risk Advisory.

The Virtuous resilience life-cycle Image: A. Bonime-Blanc



Figure 7.14 The Vicious Resilience Lifecycle.

Source: Author and GEC Risk Advisory.

The Vicious resilience life-cycle Image: A. Bonime-Blanc

Let's review the eight elements as they apply to cyber-resilience:

1. Lean-in cyber governance and leadership

Your leaders understand the depth of the cyber challenge and are prepared to provide tone from the top and necessary resources and budget to create lean-in, triangular cyber-risk governance where board oversight, C-suite strategy and front-line functional and operational coordination of cyber policy take place.

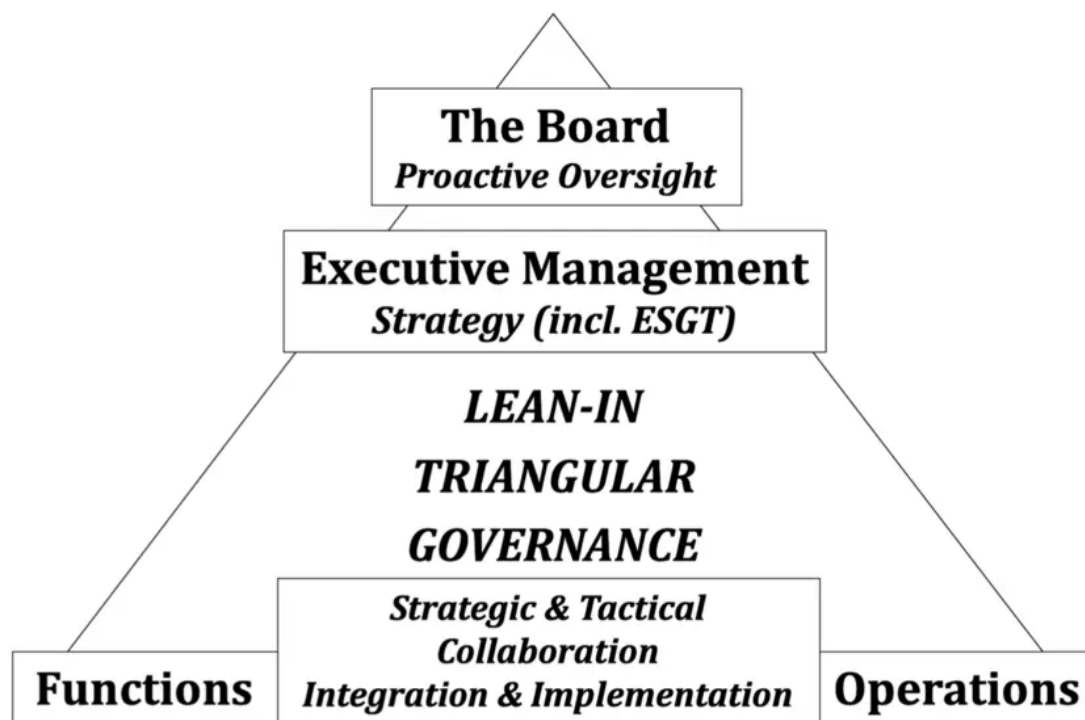


Figure 7.3 Lean-In Triangular Governance.

Source: Author and GEC Risk Advisory.

A healthy cyber culture stems from the top down Image: A. Bonime-Blanc

In this World Economic Forum, ISA, PwC and the National Association of Corporate Directors publication, these resilience elements are underscored:

FIGURE 3 Consensus principles visualized



Characteristics of a cyber-resilient organization Image: World Economic Forum

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 regularly on pitfalls and best practices. Employees are not afraid to speak up, and when they do they are not ignored. Here's a great set of approaches from the [Chief Information Security Officer of the World Health Organization, Flavio Aggio](#):

- Work hard to change the mindset that “IT ensures 100% security”
- Monthly phishing exercises make users understand cyberattacks faster and 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 cyberattackers might be interested in), understand how to prioritize and protect them and then understand 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).

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 programme is to have the right interdisciplinary, cross-functional, multi-divisional group of experts internally (with access to outside experts) within your company.

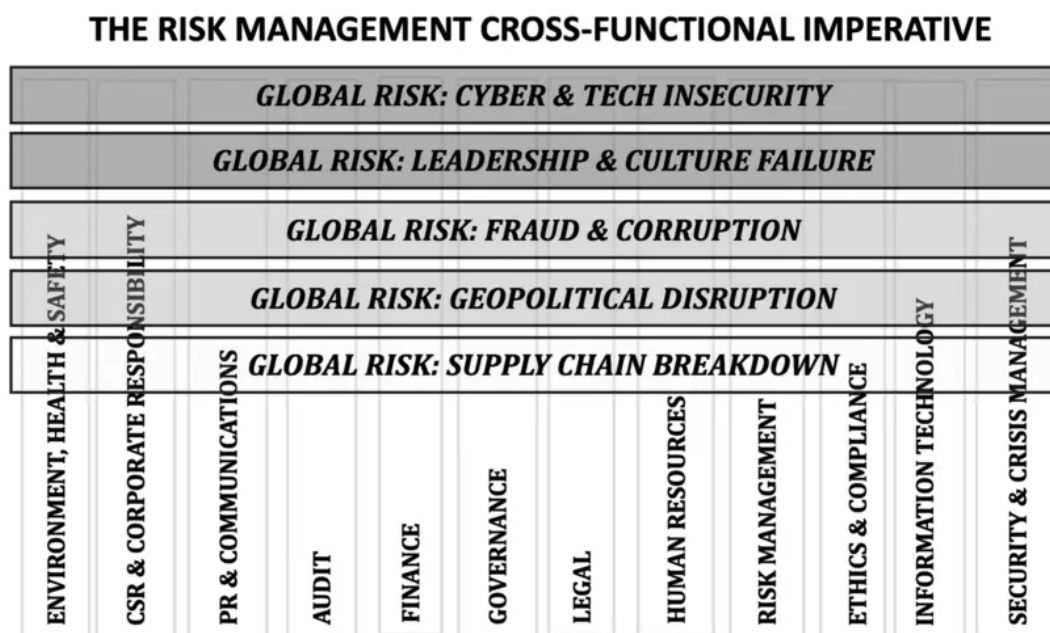


Figure 7.11 The Risk Management Cross-Functional Imperative.

Source: Author and GEC Risk Advisory.

Cyber-risk management must extend across an organization's functions Image: A. Bonime-Blanc

5. Strategic integration of cyber into ESGT

No business will be cyber-secure or prepared if it does not integrate cyber-risk considerations into its business strategy. Period. There are too many weak links in the chain – whether at 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 vigilance into all aspects, it exposes itself to potential cyber damage and lost opportunities.



Figure 7.12 An ESGT integrated organizational strategy.

Source: Author and GEC Risk Advisory.

Fully integrating cybersecurity into an organization's business strategy is also crucial

Image: A. Bonime-Blanc

6. Performance metrics and incentive programme, including cyber-metrics

You cannot reward what you cannot measure. The same goes for cyber-resilience – how do you measure it? Do you have the right people, doing the right things, with the right resources, budget and reporting? All of it tied back to professional and executive compensation metrics and properly reported to the board?

Figure 1 **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: Andrea Bonime-Blanc. 2015 Conference Board Emerging Practices in Cyber-Risk Governance, © GEC Risk Advisory LLC 2016. All rights reserved.

Metrics help with measuring progress on cybersecurity Image: A. Bonime-Blanc

7. Crisis readiness, including cyber preparedness

Companies must have a crisis management team and plan that is ready at any given time, especially in these turbulent times, to deal with a major crisis, including in the cyber realm. 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 is being addressed periodically. All this seamlessly integrated with business continuity and data management.

8. Cyber innovation ethos

The same approach that companies give to their product and services innovation should be brought to cybersecurity and risk-management innovation. This means thinking and acting outside of the box and integrating 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 takeaways. It means that the cybersecurity ethos must be one of continuous improvement and reinvention.

What is the World Economic Forum doing on cybersecurity

Show

While there are no guarantees in the rapidly changing and explosive world of cyberattacks, business has the responsibility to at least build resilience – and these eight steps will go a long way.

- Andrea Bonime-Blanc is the author of Gloom to Boom: How Leaders Transform Risk into Resilience and Value. This piece is based on a longer feature article, published in Spain's [Actuarios Magazine Spring 2021 edition](#).

License and Republishing

Written by

[Andrea Bonime-Blanc](#), Founder and CEO, GEC Risk Advisory

The views expressed in this article are those of the author alone and not the World Economic Forum.

UpLink - Take Action for the SDGs

Take action on UpLink



Explore context

Cybersecurity

Explore the latest strategic trends, research and analysis



Subscribe for updates

A weekly update of what's on the Global Agenda

© 2021 World Economic Forum [Privacy Policy](#) & [Terms of Service](#)

