HOW TO ENSURE DIGITAL TRUST IN OUR SHARED DIGITAL ECONOMY?

Daniel Dobrygowski

Our interconnected, global economy is increasingly indistinguishable from what was once referred to as the digital economy. The immense scale, scope, and complexity of the Fourth Industrial Revolution has touched all aspects of economy and society.[1] Over the past decades, every economic sector has faced pressures to digitize and to face the significant challenges that such digitization brings with it - including risks to security. These pressures have only increased as digitalization became the solution to business continuity and social connectivity during the Coronavirus pandemic.

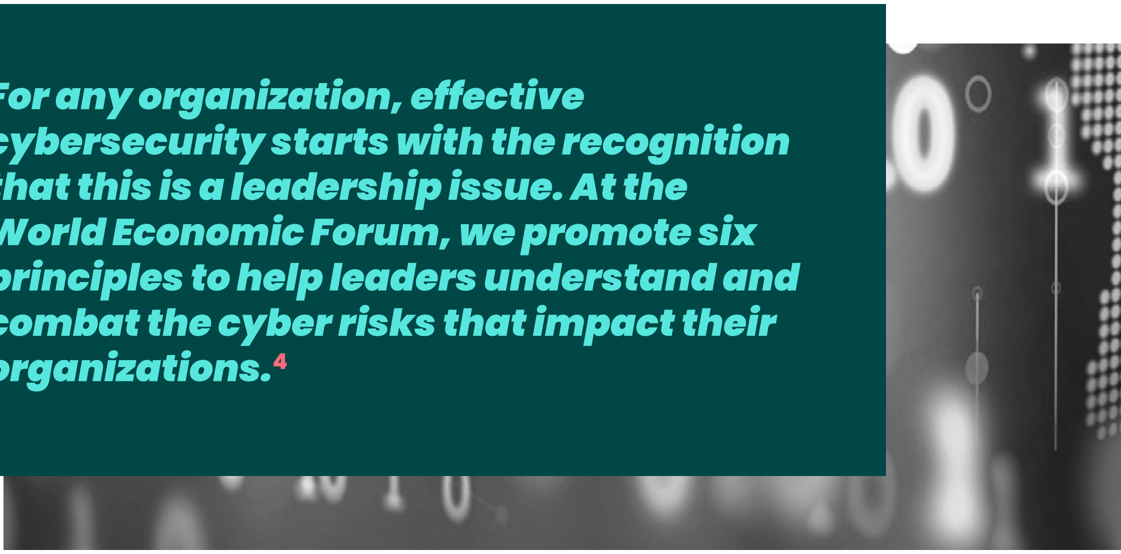
At the same time, our digital economy is beset by another set of risks, those of cyber insecurity and digital mistrust. Cybersecurity failures, hacks and breaches of sensitive information currently represent the top human-caused risk facing business and economic leaders.[2] Partially due to this insecurity, as well as a lack of adequate governance of and accountability for new technology, public trust in technological innovation is at an all-time low.[3]

In order to ensure the sustainability of our digital economy, we must come back from this precipice by cooperating, across sectors and industries, in support of our shared security and take action to guarantee our technologies are trustworthy. These issues are fundamentally questions for leaders across the economy.

> ***Therefore, leaders must take every opportunity to build both security and trust into their strategies and cooperate to ensure a secure and trustworthy technological basis for our shared growth.***

Imagem: AdobeStock.com

PROMOTING CYBERSECURITY



> ***For any organization, effective cybersecurity starts with the recognition that this is a leadership issue. At the World Economic Forum, we promote six principles to help leaders understand and combat the cyber risks that impact their organizations.***[4]

These principles are:

- **Recognize that cybersecurity is a strategic business enabler:** this means that organizational cybersecurity directly contributes to both value preservation and new opportunities to create value for the enterprise and larger society.

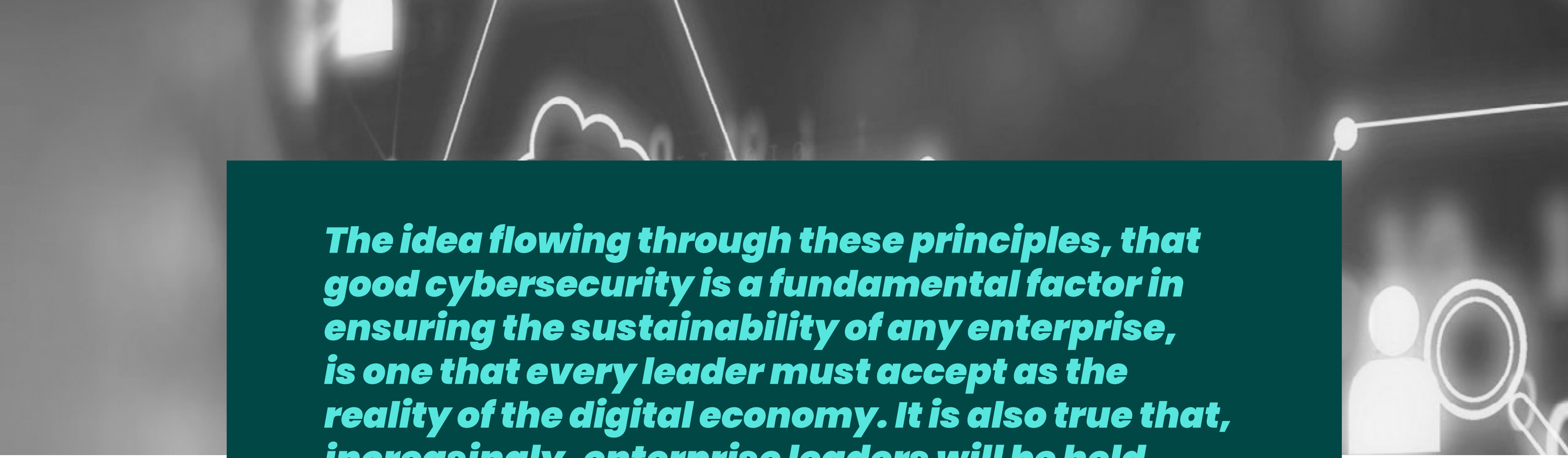
- **Understand the economic impact of cyber risk:** this means that in order for organizations to make effective business decisions, risk determinations should focus on the financial impact to the organization, including trade-offs between digital transformation and cyber risk.

- **Align cyber risk management with business needs:** this means that effective governance of any enterprise requires clear alignment between cyber-risk management and business objectives across every facet of decision-making.

- **Ensure organizational design supports cybersecurity:** this means that organizations should design an internal governance structure that addresses cybersecurity on an enterprise-wide basis.

- **Incorporate cybersecurity expertise into board governance:**this means that leaders must avail themselves of diverse sources of cybersecurity expertise and knowledge.

- **Foster systemic resilience:** this means that leaders must recognize the interconnected nature of cyber risk and encourage unified responses to it.



The idea flowing through these principles, that good cybersecurity is a fundamental factor in ensuring the sustainability of any enterprise, is one that every leader must accept as the reality of the digital economy. It is also true that, increasingly, enterprise leaders will be held accountable, by their shareholders, by regulators, and by their customers for ensuring good cybersecurity.

Practically, good cybersecurity requires those in leadership and on the front line to continually focus on identifying and protecting their most vital assets and develop cyber-aware business continuity practices to ensure the organization can withstand the most likely cyber attacks.[5]

ENSURING RESPONSIBLE TECHNOLOGY

While vital to ensuring trust, cybersecurity only protects against external malicious attacks on technology and systems.

We must also ensure that those systems are trustworthy in their planned implementation and use.

In order to bolster trust, which is vital for a sustainable digital economy, we must implement both good security and good policies and governance.[6] This is where questions of responsibility, ethics, and accountability come in. In order to build a sustainable digital economy, we must ensure that it's technological underpinnings serve the purposes of society as a whole.

Previously, the negative implications of new technologies – erosion of privacy, application of bias, and other ills – have been regarded as mere "externalities", irrelevant to the technologies themselves. In order to build a truly sustainable digital economy, these negative aspects must be recognized as flowing from human decisions in the development and application of a diverse set of technologies.

This means that new rules and norms must be put into place to govern technologies and guide responsible innovation. At the very least, this includes assessments of how these technologies adhere to generally recognized ethical responsibilities. Trustworthy technology must also include adequate protections for shared values, for example privacy, before those technologies are implemented and adopted. Further, new accountability mechanisms must be in place to ensure that errors or violations of shared expectations have effective remedies.

Ultimately, this will require leaders in the digital economy to adopt a human-centric approach to technological innovation.

But we have more to gain than to lose in such an approach. Already, human-centric approaches to data use have shown how all stakeholders can thrive under such strategic and policy decisions.[7]

COOPERATING FOR A TRUSTWORTHY DIGITAL ECONOMY

Throughout the digital economy, its benefits and its challenges are highly interconnected. Therefore, solutions to those challenges and our efforts to shape the digital economy to benefit the entirety of human society must begin with cooperation. From working to combat cybercrime[8] to increasing the trustworthiness of internet-connected devices,[9] we have already begun the shared process of bolstering trust in the digital economy. It is incumbent on every leader and every technologist to continue these efforts.

If we are to protect the digital economy and expand its benefits to include every stakeholder, from the companies to government to citizens, we must offer both security and trustworthy technology. In order to do so, we must choose to take cybersecurity seriously and choose to keep technological innovation accountable in service to the goals of humanity. We must make the choice for digital trust.

Imagem: AdobeStock.com

Daniel Dobrygowski

Daniel Dobrygowski is the Head of Governance and Trust for the World Economic Forum's Centre for Cybersecurity. An attorney and educator with two decades of experience at the intersection of technology, civil rights, law, and policy, he oversees projects and research relating to cybersecurity, cyber risk and corporate governance, and digital trust. As one of the founders of the Forum's Centre for Cybersecurity, he leads teams responsible for efforts to understand and shape global cybersecurity norms, law, regulation, and standards. Daniel also advises the Forum on legal and policy matters related to cybersecurity and privacy. He sits on the board of the Cyber Risk Institute and was recognized by the National Association of Corporate Directors in 2021 in its NACD Directorship 100 as one of the most influential leaders in the corporate governance community.

Daniel holds an MPA from Harvard University's Kennedy School of Government, a JD from the University of California, Berkeley, School of Law where he was an editor of the Berkeley Technology Law Journal, and a BA from the Johns Hopkins University. Prior to coming to the Forum as a Global Leadership Fellow, Daniel practiced law in San Francisco and Washington, DC, counselling clients on antitrust/competition, consumer protection, and privacy matters. Daniel shares his expertise in appearances online and in-person and he has been published by global think tanks as well as leading publications including Harvard Business Review and Wired.

NOTES AND REFERENCES

[1] World Economic Forum. 2021. The Global Risks Report, 16th edition. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

[2] World Economic Forum. 2021. The Global Risks Report, 16th edition. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

[3] Haerpfer, C., Inglehart, R., Moreno, A., Welzel, C., Kizilova, K., Diez-Medrano J., M. Lagos, P. Norris, E. Ponarin & B. Puranen et al. (eds.). 2020. World Values Survey: Round Seven - Country-Pooled Datafile. Madrid, Spain & Vienna, Austria: JD Systems Institute & WVSA Secretariat. doi.org/10.14281/18241.13 ; Edelman. 2021. Edelman Trust Barometer 2021. https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021%20Edelman%20Trust%20Barometer.pdf

[4] World Economic Forum. 2021. Principles for Board Governance of Cyber Risk. https://www.weforum.org/reports/136f100d-381a-4b09-a891-de2299144992

[5] World Economic Forum. 2020. Cybersecurity Leadership Principles: Lessons learnt during the COVID-19 pandemic to prepare for the new normal. https://www.weforum.org/reports/cybersecurity-leadership-principles-lessons-learnt-during-the-covid-19-pandemic-to-prepare-for-the-new-normal

[6] Dobrygowski, Daniel & William Hoffman. 2019. We need to build up 'digital trust' in tech. Wired. https://www.wired.com/story/we-need-to-build-up-digital-trust-in-tech/

[7] Bettinger, Kimmy. 2021. 12 ways a human-centric approach to data can improve the world. World Economic Forum Agenda. https://www.weforum.org/agenda/2021/08/12-ways-a-human-centric-approach-to-data-can-improve-the-world/

[8] World Economic Forum. 2020. Partnership against cybercrime. https://www.weforum.org/reports/partnership-against-cybercrime

[9] World Economic Forum. 2021. Trustworthy IoT coalition. https://www.weforum.org/projects/trustworthy-iot-coalition