# The Illusion of Control and the Challenge of an Adaptable Digital Enterprise

**Também disponível em português**
***www.isaca.org/currentissue***

The instability of society in general, the increase in the interconnection of devices and the continuous customer demand for new experiences underpin the operating scenario of modern organizations. Due to the increased flow of personal and organizational information, organizations are creating and developing new value propositions that change the way they do things and enable the development of new products and services in digital business ecosystems, leveraging the key capabilities of their strategic allies.[1]

This new normal of today's enterprises and society in general, with greater interconnection between the physical, the logical and the biological, presents a paradigm change that goes beyond cause-and-effect understanding. It opens possibilities of recognizing global dynamics based on relationships between elements that define the behaviors of systems—whether political, economic, social, technological, legal or environmental. Therefore, to understand the inherent properties of a system and explore the emerging properties that manifest due to the dynamics of the system itself, it is necessary to develop a systemic way of thinking that considers the flow of visible and invisible interconnections.[2]

Protecting the value proposition of organizations in the current environment is not an exercise in mitigating or preventing adverse events, but rather in reducing the impact of what is not understood or cannot be foreseen. That distinction is necessary to overcome the illusion of control and the false sense of security derived from the often futile and desperate attempts by organizations to predict social and economic instabilities, which may, in the end, affect the organization's own dynamics.[3]

Enterprise risk management should be positioned to address uncertainties by shifting attention from avoiding failure, which is inevitable, to understanding control as a dynamic balance between decreasing uncertainties (i.e., known risk, application of known controls) and amplifying novel emerging behaviors (i.e., latent and emerging risk, design and execution of scenarios and simulations). The goal should be to fully reimagine what else could go wrong, create a vigilant posture and determine how best to respond to all types of threats.[4]

In addition, it is helpful to analyze the illusion of control of cyberrisk management in organizations, how to overcome it in light of the dynamic nature of risk and, thus, recognize the flaws of executives in understanding and managing cyberrisk. Making sense of the digital strategies that are configured and deployed in the current environment of innovation and technological disruption demands assuming risk within the framework of thresholds defined, agreed on and simulated by the organization.

## Why Is Control an Illusion?

Perhaps the scenario most desired by humans is the feeling of having things within a known and validated spectrum of variation. It is natural to want the peace of mind that comes with knowing an equivalent action can be repeated in the future with results similar to those initially experienced. People have a need to forecast outcomes based on past experiences and to see expected behaviors materialize so they can maintain their agendas and set plans to achieve specific goals.[5]

However, when top management is committed to this type of perspective, based on some recognized successes of its proposals and strategies, it tends to fall into an arrogant posture and overvalue

**JEIMY J. CANO M.** | PH.D., ED.D., CFE, CICA

Has more than 25 years of experience as an executive, academic and professional in information security, cybersecurity, forensic computing, digital crime and IT auditing. In 2016, he was named Cybersecurity Educator of the Year for Latin America. He has published more than 250 articles in various journals and presented papers at industry events at the international level.

experience, which can lead to choosing investments based on efficiency rather than the organization's capacity for adaptation and flexibility if things do not go as planned. This situation usually creates tension with risk teams, which must accept the executive dispositions without major objections based on an exercise of command rather than an exercise of reflection, challenge, and orientation that considers the environment's potential volatility, instability and uncertainty.

In particular, executive teams try to simplify their perspectives on risk by having a defined risk framework, benchmark reports from other organizations in their business sector, and an overview of how others have dealt with such risk. This may lead to influence bias,[6] which comes from equating the experience of others with the particular dynamics of the organization, generating a false sense of security. This position can lead to blind spots in the organization and enable new spaces for adversaries to create situations that are possibly off the radar of the exercises carried out by the BoD and the organization's risk team.

In general, control is understood in organizations as an exercise of limiting uncertainties by restricting concrete conditions to allow for a known framework of actions with expected and manageable results. The better the uncertainties are known, the better the organization's mobilization and projection capabilities will be. To the extent that past data and those available from peers offer greater and better perspectives, the risk appetite will grow. Therefore, greater challenges will be taken on by the organization without evaluating current capabilities and implementing necessary updates to address what does not go according to plan.[7]

Making decisions based only on the criteria of limiting uncertainty and with data from past events creates a gap that makes organizations more susceptible to unpleasant surprises. The result is little or no margin for action, which leads to loss of reputation with clients due to lack of preparedness and response capacity. When an unfortunate event occurs, a control dilemma is created, which limits the discretion and autonomy of the business areas (who know the terrain firsthand) to act. Instead, the highest-ranking executives are the ones who devise a solution that returns control to the organization and gives peace of mind to both the board of directors (BoD) and its stakeholders.[8]

However, control does not lie strictly in following the established plan or strategy (in a specific time, manner and place). Instead, it is about staying the course and adjusting to the conditions of the environment, creating different scenarios that allow rethinking of actions and amplification of options to deal with instabilities that arise. In this way, the organization can not only achieve what it wants, but also build a base of key learnings that will help update its capabilities to face new uncertainties.[9]

Making decisions based only on the criteria of limiting uncertainty and with data from past events creates a gap that makes organizations more susceptible to unpleasant surprises.

## The Illusion of Control of Systemic Risk

Cyberrisk resides in the interconnections and interactions of different components configured by people, processes, technology and regulations. These interconnections and interactions are a dynamic ecosystem that maintains a flow of information that is used to define the state of protection and operation of the initiatives that arise in a digital context. It is not the regulatory compliance foreseen for known risk factors,

but the recognition of their instability and changeability that enables the capabilities necessary to align and coexist with the breaches that will occur.[10]

Because cyberrisk is systemic, its materialization requires a contagion analysis of such risk (i.e., an analysis of the cascade effect derived from the level of coupling and interactions observed). Such an analysis determines the organization's sensitivity and response capacity in the face of uncertain or unstable events that compromise its functioning and the level of impact on the organization's strategic objectives. The materialization of cyberrisk is a challenge to the organization's cybersecurity maturity model in the face of the internal and external changes that the organization encounters and reveals blind spots in its security and control model.[11]

If cyberrisk management is understood as an exercise to limit the exploitation of vulnerabilities, prevent attacks and mitigate the materialization of risk, then organizations will work in their comfort zone of complying with the application of norms and standards, understanding uncertainty and instability as their enemies and, therefore, taking part in a crusade in which certainties will be scarce and surprises will be constant news for the BoD. By adopting this perspective, organizations will always maintain a victim posture that offers no margin for recovery and learning, which gives the adversary the advantage of having uncertainty as a fundamental factor in carrying out its actions.[12]

When cyberrisk is understood as part of the dynamics of the organization and its relationships inside the digital business ecosystem, it is then understood that it is necessary not only to reduce uncertainty and instability, but also to increase the organization's capacity to learn from and overcome successful attacks. In this sense, it is important to focus on risk evolution and updating cybersecurity capabilities, which causes the intelligence capacity of the adversary to deteriorate, generating greater uncertainty in the adversary's risk model. It is also necessary to study the cascading effects of the materialization of this risk, with resilience as a fundamental factor to account for the instability and chaos generated by a successful adverse event.[13]

## The Seven Flaws of Executives

Today's executives find cyberrisk an important topic because many high-visibility cyberattacks, usually on critical infrastructures, have resulted in consequences for the managers of organizations, particularly with respect to their responsibilities for monitoring and assuring the risk required not only by audit committees, but also by the supervisors of each of the organization's business sectors.[14]

It is important to focus on risk evolution and updating cybersecurity capabilities, which causes the intelligence capacity of the adversary to deteriorate, generating greater uncertainty in the adversary's risk model.

In dealing with this risk, managers accustomed to the inertia of traditional risk management end up treating cyberrisk as one more risk to the organization, particularly associated with technology issues, which means treating it as a known risk with controls that are clearly verifiable. This is like betting on the outcome of a scenario that is by definition uncertain, which demonstrates a lack of knowledge, is possibly reckless, and shows a lack of upholding the primary duty of executives, the duty of care. This, ultimately, compromises the organization's initiatives and its ability to respond.[15]

In this regard, C-level executives must be vigilant in recognizing and overcoming the seven transgressions that are often committed when confronting the challenge of adequate and relevant cyberrisk management for the organization:

1. **Thinking they can predict extreme events**—It is more effective to focus on the consequences and assess the impact of extreme events.
2. **Studying the past to manage current and future risk**—Today's world does not resemble the past; both interdependencies and nonlinearities have increased.
3. **Ignoring advice on what not to do**—An organization can succeed by avoiding losses while its rivals try to win.
4. **Assuming that risk can be measured by standard deviations**—There is no such thing as tamed randomness. Changes do not move within certain limits.

5. **Failing to realize that what is mathematically equivalent is not psychologically equivalent**—It is possible to be fooled by the risk presentation framework or mathematics.
6. **Believing that efficiency and shareholder value maximization do not tolerate redundancy**—Most executives do not realize that optimization makes organizations vulnerable to changes in the environment because it often involves not having duplicated capacities, replacement parts or alternate plans in the face of unforeseen events.
7. **Thinking that uncertain events have linear and known causes and effects**—Critical and systems thinking are required to see emerging effects and threats.[16]

These transgressions and key related observations reveal executive biases and blind spots. Acknowledging these weaknesses may be uncomfortable, but it is necessary to deepen the critical thinking required to understand the uncertainties, instabilities and tensions that generate cyberrisk in the digital ecosystem in which an organization operates.

This understanding equips executives to implement a more mature treatment of cyberrisk that goes from the comfort of standards to the generation and practice of scenario exercises and playbooks. The goal is to enable an organization to maintain a vigilant posture in the face of the inevitability of failure and to exhibit due care and diligence in cyberrisk monitoring and assurance.[17]

## How to Overcome the Illusion of Control

To find concrete ways to overcome the illusion of control, it is necessary to think of control as the harmony between the limitation of instabilities and the amplification of uncertainties. The aim is to find the right level of vigilant navigation in which the organization can learn and constantly reconfigure its capabilities to respond to cyberrisk, maintaining operations with the minimum of adverse effects to deliver on its value proposition for its customers.

To accomplish this, it is necessary to visualize cybersecurity management from a systemic-cybernetic viewpoint that implies maintaining an assurance cycle for known risk. Known practices and standards enable an organization to keep operations in compliance with basic requirements. An adaptive cycle that encourages challenging assumptions, generating scenarios of uncertainties and emerging threats, and simulating unexpected events helps create a capacity for resilience, allowing an organization to learn and unlearn, and, thus, surprise its adversary on its own familiar ground—uncertainty.[18]

The crossroad of these two cycles is in the scenarios, which create opportunities for the organization to learn. In these scenarios, the organization declares what it does not know and that it is willing to advance all the necessary intelligence to learn from its adversary and its capabilities. It can then return to its assurance cycle to identify its blind spots and seek a flexible and dynamic configuration infrastructure capable of adjusting to the changing conditions of the environment.

An organization will have control of cyberrisk when it has embraced uncertainty and understands it is a natural part of operation and recognizes and incorporates resilience as part of its daily practice.

This continuous interaction keeps the organization on its feet and aware that it is exposed to both known and unknown vulnerabilities. Understanding that the management of enterprise cybersecurity consists of reducing its attractiveness to attackers by reducing vulnerabilities, learning from attackers' methods and resolving security incidents within the limits of the organization's capacity are essential.[19] Consequently, the organization reaches an understanding that the exercises of security and control do not result in the absence of failures, vulnerabilities or breaches, but in harmony and balance when the inevitability of failure is realized. It creates an opportunity for learning that challenges the knowledge and the innovation capacity of both the adversary and the organization.

Thus, an organization will have control of cyberrisk when it has embraced uncertainty and understands it is a natural part of operation and recognizes and incorporates resilience as part of its daily practice.

**LOOKING FOR MORE?**

- Read *Incorporating Risk Management into Agile Projects*. *www.isaca.org/incorporating-risk-management-into-agile-projects*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Control exists when enterprise cybersecurity translates into an exercise of locating thresholds and operating within the risk appetite declared by the organization. This type of control can trigger absorption and containment mechanisms in the face of uncertain events to maintain operations despite a successful adverse event.[20]

## Next Steps

Once BoDs are aware that their organizations operate and evolve in digital ecosystems crossed by cyberrisk, they should take actions to address the seven transgressions of the executive teams in the management of this risk, including:[21]

- Identifying responsible parties and cybersecurity stakeholders in each area
- Identifying the particular circumstances that increase cyberrisk in each area
- Creating a cyberrisk council composed of those responsible for cybersecurity in each area, including the chief information security officer (CISO) and at least one member of the BoD, to carry out functions such as:
  - Analyzing the circumstances that increase cyberrisk in the area and determine the risk appetite
  - Proposing an action plan to manage cyberrisk
  - Presenting the plan to the executive team and BoD
  - Reporting progress of the plan to stakeholders
  - Evaluating the results of the plan on a quarterly basis for reports to the executive team and BoD

## Conclusion

Managing cyberrisk in modern organizations is a constant challenge of learning and unlearning. It requires overcoming one's own biases about traditional risk management and thinking of uncertainty as an ally to create new opportunities and fine-tune the organization's operating thresholds when things do not go according to plan.[22] It is an exercise that aims not to protect or reduce risk, but rather to ensure the value proposition and strengthen business capabilities in the face of the inevitability of failure.

Control is not only limiting, mitigating, and reducing attacks, vulnerabilities, and failures that are generally known. This approach translates into both a regulation cycle and an adaptation cycle, which implies amplifying uncertainties and instabilities from the design and simulation of scenarios based on latent and emerging risk, which creates new learning opportunities.[23] When this is understood, it is possible to overcome the illusion of traditional control based on the inertia and myopia associated with the few certainties that can be had, thanks to the application of best practices and the installation and operation of the most advanced technological tools available.

Cyberrisk management is dynamic because conditions always change, and the flow of information is both constant and often unexpected.

Control is an exercise based on two cycles: regulation and adaptation. Regulation helps to limit, mitigate and reduce attacks, vulnerabilities and failures, while adaptation helps in amplifying uncertainties and instabilities from the design and simulation scenarios based on latent and emerging risk to create new learning opportunities.[24] With this understanding, it is possible to overcome the illusion of traditional control based on the inertia and myopia associated with the few certainties that can be had, thanks to the application of best practices and the installation and operation of the most advanced technological tools available.

Cyberrisk management is dynamic because conditions always change, and the flow of information is both constant and often unexpected. Therefore, it demands a change of thinking that establishes a new paradigm for security and control professionals.[25] It implies recognizing the organization as part of a digital ecosystem in which it is necessary to know how it can be affected by others and how others can be affected by it. Consequently, it is not only about ensuring what happens inside, but also taking advantage of opportunities with other strategic partners in the ecosystem.

Cyberrisk management entails the configuration of an adaptable digital enterprise to enable flexibility, autonomy, orchestration and discovery of new opportunities in the foundations of its enterprise architecture (i.e., the business model, business operations, strategy). This enables the organization to take advantage of the instability and uncertainty changes produce, to be resilient, and to deliver new value propositions to its customers.[26]

## Endnotes


1 Subramaniam, M.; *The Future of Competitive Strategy: Unleashing the Power of Data and Digital Ecosystems*, MIT Press, USA, 2022

2 Capra, F.; *The Web of Life. A New Scientific Understanding of Living Systems*, Anchor, USA, 1997

3 Taleb, N.; D. Goldstein; M. Spitznagel; "The Six Mistakes Executives Make in Risk Management," *HBR's 10 Must Reads on Managing Risk*, Harvard Business School Publishing, USA, 2020

4 Zeijlemaker, S.; M. Siegel; "Capturing the Dynamic Nature of Cyber Risk: Evidence From an Explorative Case Study," *Proceedings of the 56th Hawaii International Conference on System Sciences*, 27 December 2022, *https://hdl.handle.net/10125/103372*

5 André, C.; "Uncertainty Invites Wisdom," *Mind and Brain*, May/June 2021, *https://www.investigacionyciencia.es/revistas/mente-y-cerebro/la-presin-del-tiempo-833/la-incertidumbre-invita-a-la-sabidura-19848*

6 Meyer, R.; H. Kunreuther; *The Ostrich Paradox: Why We Underprapare for Disasters*, Wharton Digital Press, USA, 2017

7 Buheji, M.; D. Ahmed; H. Jahrami; "Living Uncertainty in the New Normal," *International Journal of Applied Psychology*, 13 August 2020, *http://article.sapub.org/10.5923.j.ijap.20201002.01.html*

8 Beer, S.; *Decision and Control: The Meaning of Operational Research and Management Cybernetics*, John Wiley and Sons, United Kingdom, 1994

9 Martinez-Moyano, I.; R. Oliva; D. Morrison; D. Sallach; "Modeling Adversarial Dynamics," *Institute of Electrical and Electronics Engineers 2015 Winter Simulation Conference (WSC)*, December 2015, *https://ieeexplore.ieee.org/document/7408352*

10 World Economic Forum, "Understanding Systemic Cyber Risk," Global Agenda Council on Risk and Resilience, October 2016, *https://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf*

11 European Systemic Risk Board, *Systemic Cyber Risk*, Germany, February 2020, *https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf*

12 Cano, J.; "Security Risk Management and Cybersecurity: From the Victim or From the Adversary?" *Cybersecurity in the Age of Smart Societies. Advanced Sciences and Technologies for Security Applications*, 3 January 2023, *https://link.springer.com/chapter/10.1007/978-3-031-20160-8_1*

13 *Op cit* Zeijlemaker and Siegel

14 Deloach, J.; "The Top Risks for 2023: A Global View," NACD BoardTalk, 4 January 2023, *https://blog.nacdonline.org/posts/top-risks-2023-global*

15 Lam, J.; *Implementing Enterprise Risk Management. From Methods to Applications*, John Wiley and Sons, USA, 2017

16 *Op cit* Taleb *et al.*

17 Day, G.; P. Schoemaker; *See Soon, Act Faster: How Vigilant Leaders Thrive in an Era of Digital Turbulence*, MIT Press, USA, 2019

18 Cano, J.; "Rethinking the Practice of Security and Cybersecurity in Organizations: A Systemic-Cybernetic Review," Global Strategy, Report No.58, 2020, *https://global-strategy.org/repensando-la-practica-de-la-seguridad-y-la-ciberseguridad-en-las-organizaciones-una-revision-sistemico-cibernetica/*

19 Zeijlemaker, S.; *Managing the Dynamic Nature of Cyber Security: A Future-Proof Strategy, This Is How It Works*, Disem Institute, Netherlands, 2022

20 Coden, M.; M. Reeves; K. Pearlson; S. Madnick; C. Berriman; "An Action Plan for Cyber Resilience," *Sloan Management Review*, 4 January 2023, *https://sloanreview.mit.edu/article/an-action-plan-for-cyber-resilience/*

21 Falco, G. *et al.*; "Cyber Crossroads: A Global Research Collaborative on Cyber Risk Governance", Cyber Crossroads, 2021, *https://arxiv.org/abs/2107.14065*

22 *Op cit* André

23 *Op cit* Cano, 2020

24 *Ibid.*

25 Medoh, C.; A. Telukdarie; "The Future of Cybersecurity: A System Dynamics Approach," *Procedia Computer Science, 3rd International Conference on Industry 4.0 and Smart Manufacturing*, 8 March 2022, *https://doi.org/10.1016/j.procs.2022.01.230*

26 Woerner, S., P. Weill; I. Sebastian; *Future Ready, The Four Pathways to Capturing Digital Value,* Harvard Business Review Press, USA, 2022