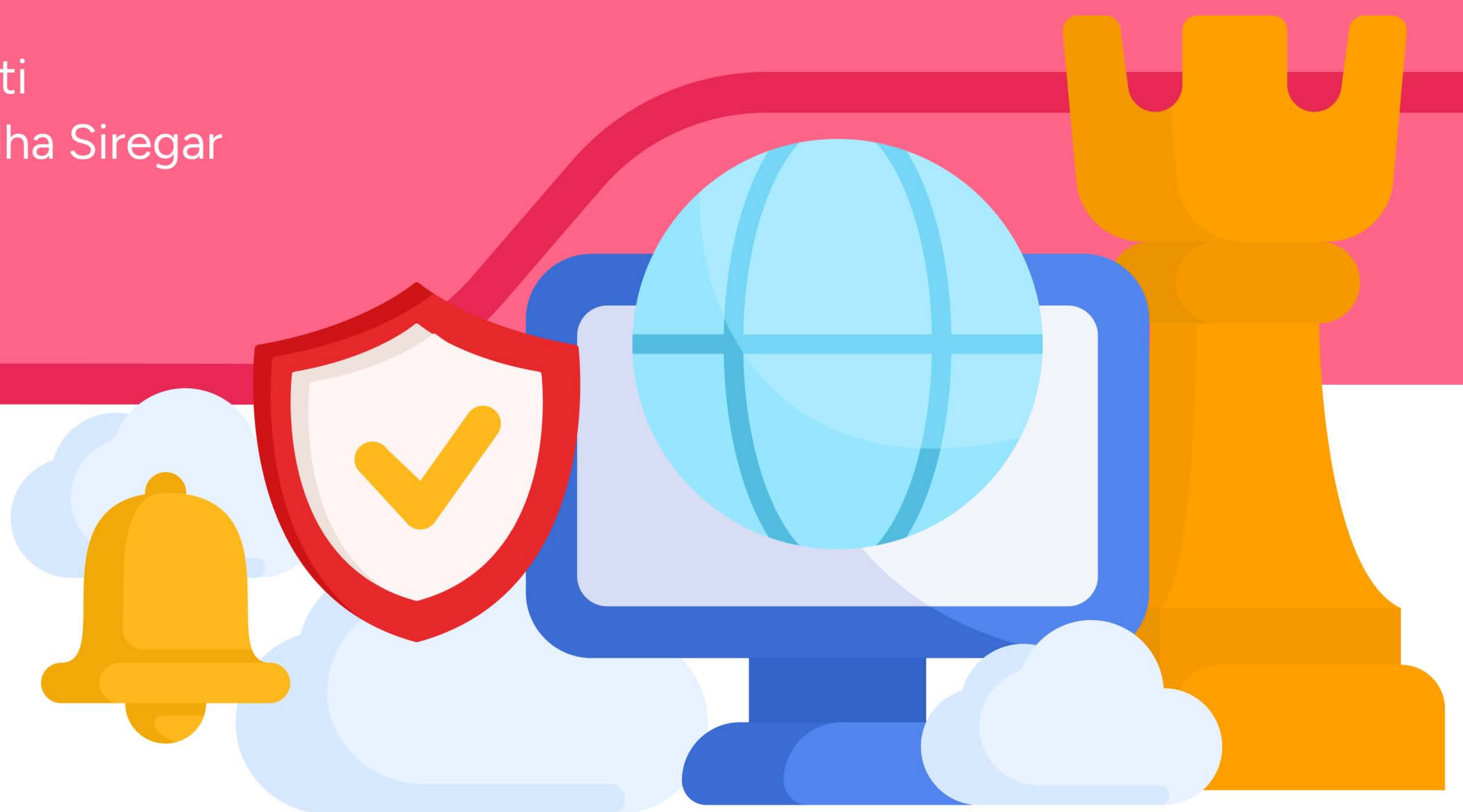


Complexity in Cyberspace: A Call for Security-Minded Leaders

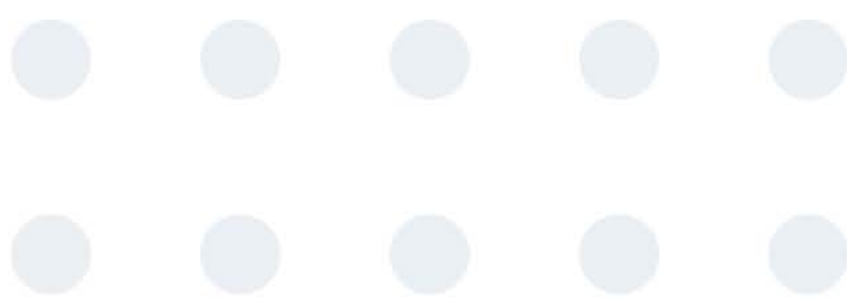
Author : Tjok Istri Sintawati
Editor : Achmed Faiz Yudha Siregar



Introduction

In this intelligent age, security-minded leaders need to develop comprehensive cyber strategies and reach cyber resilience within their organization and the ecosystem. With the duality of growing digital transformation in business—on the one hand giving extensive benefits to the business, but on the other hand giving rise to cyberthreats—leaders need to navigate the complexity of cyberspace. A call-to-action to global leaders stated in the report of Global Cybersecurity Outlook 2025, published by the World Economic Forum (WEF). This report tries to decode the growing complexity of cyberspace nowadays and explain the strategic role that leaders should take on.

Cyber risk, as mentioned by 72% of respondents in the Global Cybersecurity Outlook (GCO) 2025—consisting of 321 leaders from 57 countries—is reported to be increasing. Previously, in the Chief Risk Officers Outlook published in October 2024, cyber risk was also considered by leaders as the 3rd biggest threat that could threaten an organization. The evolution of cybercrime, which is increasing in terms of modus operandi and frequency, is a serious threat to organizational leaders.



Cyber Risks	How Can It Become More Sophisticated
Ransomware attack	Ransomware, which could prevent us from accessing our own system, data, or files, is significantly more innovative. The commoditization of ransomware models is getting stronger, coupled with the continued growth of RaaS (Ransomware-as-a-Service (RaaS) models.
Cyber-enabled fraud (such as phishing, business email compromise, vishing)	GenAI technology impacts more well-developed phishing at a lower cost. There is also a rapidly growing cybercrime-as-a-service (CaaS) that allows individuals/ groups without technical expertise to engage in illicit online activities by purchasing tools and support.
Identity theft	Deepfakes, supported by GenAI technology, can create convincing impersonations of the voice, video, images, and writing styles of organization senior leaders.

Mitigating the Underlying Risks of More Interconnected Supply Chains

Cyber experts and large organizations recognized that the greatest challenges of cyberspace complexity are vulnerabilities that come within interconnected supply chains. Among several issues of interconnected supply chains, the most concerning issue stated by organizations is centered on third-party management. There are several risks associated with third parties that are sometimes overlooked.

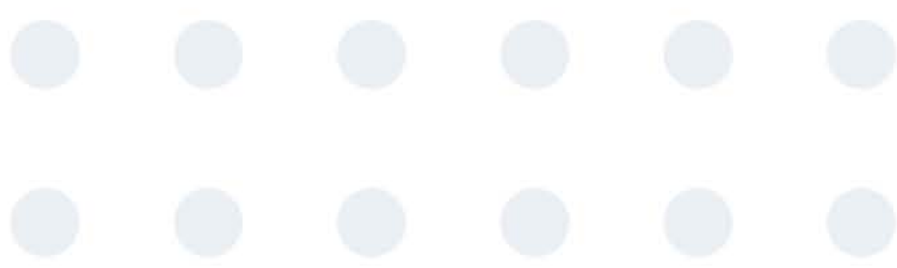
Inevitable Risk in Relation to the Third Party	Undesirable Bigger Impact that Might Happen
Software vulnerabilities might come from third parties or vendors.	Exploit weakness in the supply chain, such as malware distribution.



Inevitable Risk in Relation to the Third Party	Undesirable Bigger Impact that Might Happen
Lack of visibility through the security standard of the third parties might lead to different degree of security maturity.	Harder to implement cyber regulations and gain cyber resilience.
Dependency on the limited number of critical providers might become a systemic point of failure.	Any vulnerability that happens to the providers will have knock-on effects through the extensive client base and maybe a ripple effect throughout the ecosystem.

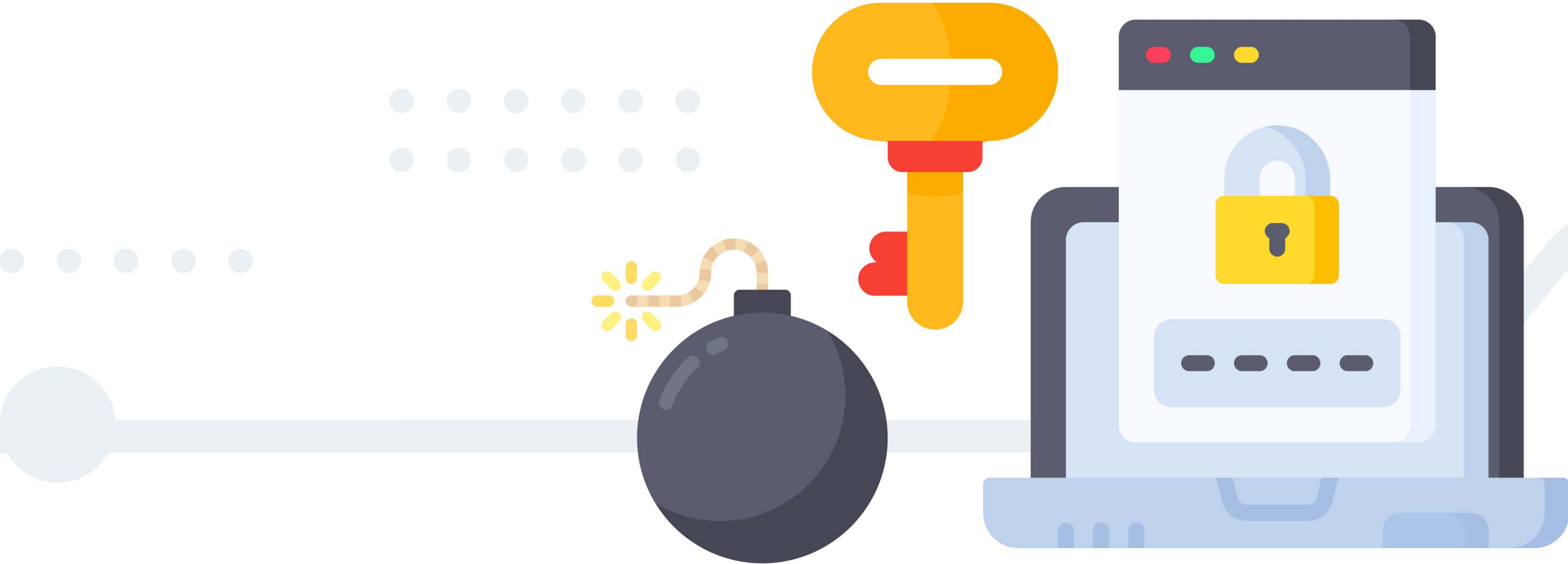
The risks of more interconnected supply chains are intensified by the growing exacerbating inequity in cyberspace. The inequity throughout the cyber ecosystem—between those who have resources to adapt and those who do not—will affect the resilience of the ecosystem as a whole because any incident affecting the less mature organizations will impact the entire supply chain.

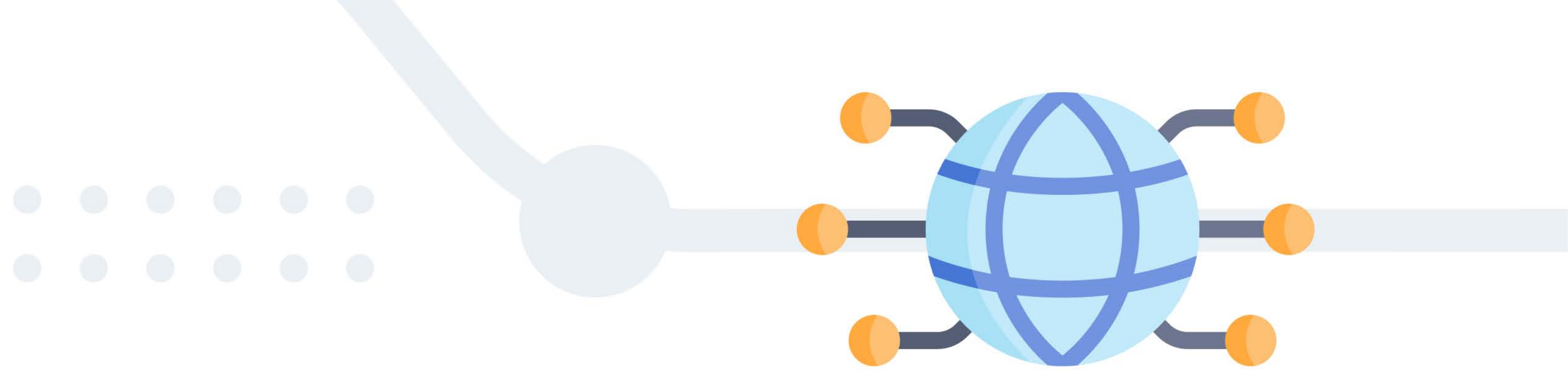
Actor	How Can It Become More Sophisticated
Large vs small organization	- Small organizations are nearly close to the critical tipping point where they can no longer effectively secure themselves against the increasing complexity of cyber risks. On the other hand, cyber resilience in large organizations is reported to be sufficient. - The fact that global demand for cybersecurity professionals exceeds supply also makes large organizations more vulnerable in this case. - Cyber insurance is becoming more mature in recent years, but larger organizations seem to get more benefit because they are better able to afford it than small organizations.



Actor	How Can It Become More Sophisticated
Developed vs emerging countries	Organizations in the Global South, such as those in Africa and Latin America, tend to be less confident in declaring cyber resilience than organizations in the Global North, such as Europe and North America.
Multi sectoral	- Organizations in the financial sector are more advanced in cybersecurity compared to the manufacturing sector, which is still in the early stages of building cyber resilience. - Organizations in the public sector also expressed that they are not yet adequate enough to achieve cyber resilience compared to organizations in the private sector.

Cyber resilience is a mandate for the entire ecosystem, whether large or small organizations, in the more interconnected supply chains. This condition requires a leadership strategy to handle cybersecurity, such as through oversight, which board members receive regular updates on cyber incidents, trends, vulnerabilities, and risk predictions both from internal and external third parties, which has been proven to increase cyber resilience. Reflecting also on the inequity conditions that occur, collective action is also needed to achieve cyber resilience because in an interconnected ecosystem, overall resilience depends on its weakest links. Large organizations may be able to provide incentives that help smaller organizations to achieve cyber resilience which will have an impact on the resilience of the entire ecosystem. International collaboration is also important as a collective effort to deal with increasingly sophisticated and borderless cybercrime.





Dealing with Geopolitical Dynamics in the Intelligent Age

The evolution of cyberthreats and escalating geopolitical tensions pose significant risks of disruptions to vital infrastructure that jeopardize human safety. Based on interviews with leaders for this report, one CISO stated that state-sponsored attackers are increasingly not targeting governments only but trying to disrupt economies and critical infrastructures, consequently creating chaos in the global system. In this case, cyberthreats could attack the control system and compromise data of the critical infrastructure, i.e., water facilities and communications infrastructure, which guarantees the lives of wider communities. Several cyberthreat cases related to geopolitical tension that have ever happened and endanger human lives can be a reflection for leaders in enhancing cyber resilience.

High-risk Area	Emerging Threats
Water facilities	A cyberattack on the largest water utility in the United States happened in 2024, causing disruptions in the operations. It also raises awareness about the security of critical infrastructure, such as the OT system (remote access points and outdated software).
Biosecurity	In 2024, two laboratories in South Africa and the United Kingdom became targets of cyberattacks. There is rising concern about cyberattack capability to incapacitate essential laboratory systems, interrupting operations and causing loss of data integrity, which can lead to endangering safety protocols.
Communications infrastructure	Critical communications infrastructure, such as telecommunications infrastructure, satellites, and undersea cables, is often being target of cyberattacks. The cyberattack on the communications infrastructure e.g., ViaSat satellite network in Europe; 124 cyber operations in the space sector relating to the Ukraine-Russia conflict; and an undersea cables incident in the Baltic Sea.
Climate and energy	The emerging renewable energy systems—which are important for powering modern technology—need to be designed with security as one of the foundational priorities. This is an urgent need because the energy system has become a highly attractive target for cybercriminals.

As also consequence of the more interconnected world, a risk of becoming collateral damage. In this situation, understanding the geopolitical dynamics itself has become crucial for effective long-term risk management. It is not limited only to advanced skills in cybersecurity but also to the implementation of old-fashioned risk management. This management requires to analyze the problem from a business-impact perspective first before managing and accepting any residual risk.

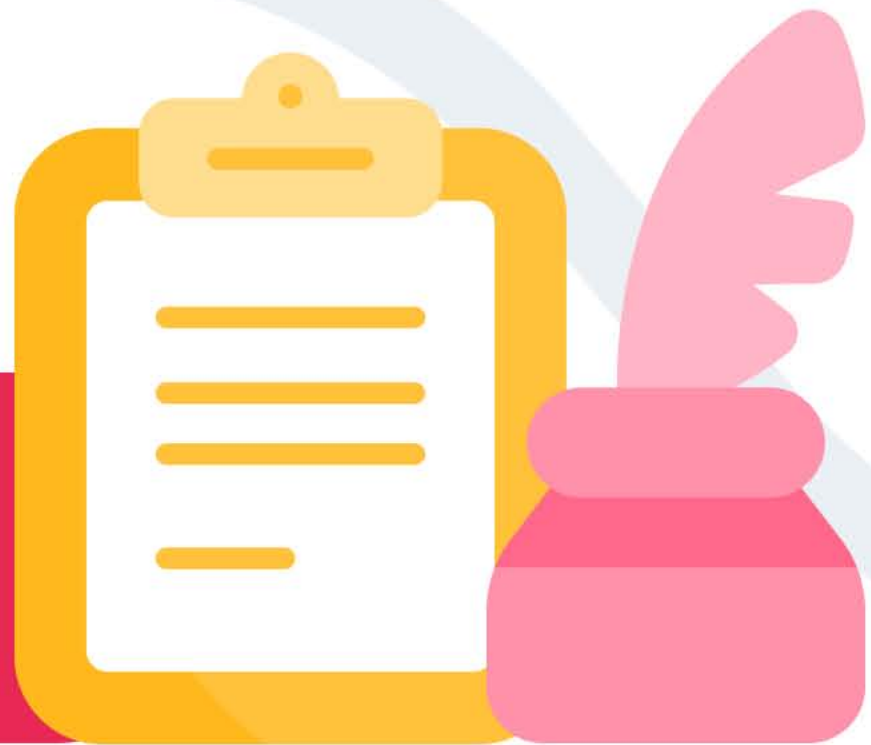
Striving for Better Regulation to Ensure Global Cybersecurity



Regulation is considered as one of the most important drivers to gain cyber resilience by 78% of CISOs and 87% of CEOs surveyed in this report. Although cyber regulation is important as a legal framework to mandate cybersecurity practice, in reality there is also a challenge in the overlapping regulations worldwide which adds complexity to the cybersecurity strategies.

Region	Regulations
America	Cyber Incident Reporting for Critical Infrastructure Act (CIRCA), Brazil’s General Data Protection Law (LGPD)
Africa	Nigeria’s Data Protection Regulation (NDPR)
Asia-Pacific	Japan’s Act on the Protection of Personal Information (APPI), Singapore’s Cybersecurity Act
Europe	The Network and Information System Directive 2 (NIS2), the EU’s General Data Protection Regulation (GDPR), Digital Operations Resilience Act (DORA)

In a situation where regulations are complex and numerous, which causes fatigue among companies and reduces the effectiveness of their objectives—public-private cooperation is important to achieve global regulatory harmonization. This effort can create cybersecurity standards that can be applied across regions more consistently and effectively. Organizations can also be more flexible to adapt to emerging threats and technologies.



Strengths and Weaknesses of the Report

Strength



Richness & Broad Scope of Data

The data in this study were obtained using a mixed method that makes the data rich. The scope of data in this study is also broad because the participants involved came from 57 countries and included multi-stakeholders such as executives, industry leaders, government, academics, and civil society.



Strategic Insights for Leaders

This study unravels the complexity of cyberspace and the concerns of various leaders regarding the increasing cyber risk. This can be useful for global leaders to take the first step in realizing cyber resilience.

Weakness



Lack of Analysis in Each Issue

The abundance of data in this study, on the other hand, also resulted in the analysis conducted on each issue being discussed less comprehensive.



Overemphasizing Executives' Perceptions

The data in this study were obtained mostly from executive-level participants, so it minimally included perspectives from individuals in the lower hierarchy, such as those related to obstacles in the field that they might experience.

Reference

World Economic Forum. (2024, October). Chief risk officers outlook: October 2024. <https://www.weforum.org/publications/chief-risk-officers-outlook-october-2024/#:~:text=Chief%20risk%20officers%20are%20most,anticipating%20volatile%20conditions%20has%20increased>.