Three Essential Actions to Manage Supplier Risk under NIS2 Directive

Dr. Sander Zeijlemaker, is Managing Director of Disem Institute, a Research Affiliate Cybersecurity at MIT CAMS, agenda contributor to the World Economic Forum, member of the ENISA Ad-hoc security operation center working group, president of the Security, Stability and Resilience special interest group of the System Dynamics Society.

Dr. Laura Georg Schaffner is group head of strategy and security awareness at for AXA , associate professor at EM Strasbourg Business school, expert to the Horizon Europe group part of European Commission, and non-resident research fellow at the Center for Long-term Cybersecurity at UC Berkeley.

Abstract

In an interconnected digital society managing cyber risks becomes a precondition for driving an organizational strategy. In this space managing suppliers is essential to remain resilient to cyber threats. As the updated Network and Information Security Directive (NIS2) pushed cyber risk management to the board room, this article provides three essential actions management boards need to take to manage supplier risks under NIS2.

Today's modern and interconnected society is increasingly dependent on the internet and computer technology. Advanced technological innovations like cloud computing, artificial intelligence, machine learning, the Internet of Things, robotic process automation, and digital twin technology are being increasingly integrated into businesses and organizations. Concepts like smart cities, Industry 5.0, e-health, smart grids, and the Fourth and Fifth Industrial Revolutions play increasingly predominant roles in our day-to-day lives and society.

However, this societal digital transformation also has downsides: persons, organizations, and society are becoming increasingly susceptible to cyber threats. Unfortunately, the inevitability of human behavioral limitations, imperfections in security-boosting technology, increasing multi-supplier dependencies, and adversarial evolution guarantee that organizations will regularly face cyber threats.

Currently, large organizations have a 25% probability of experiencing a cyberattack,[1] with an average remediation cost of 4.8 million dollars. Defense failures account for 53% of these attacks, while unintended control lapses cause 47%.[2] Yet, the larger societal impact of these cyberattacks is of even greater concern. Such impact, through supply chains, can be 19 to 400 times higher than the cost suffered by the individual organization.[3] Unfortunately, only 27% of supply chains are regularly monitored and evaluated by their customers.[4]

Overall, this underscores the importance of governing and overseeing a cyber risk management strategy, especially from a supply chain perspective, a very significant precondition for any successful digital business or organizational strategy. [5] [6] [7]

Cyber risk management enters the boardroom through NIS2

This significance of cyber risk has prompted governments to push cyber risk governance to the boardroom. Consequently, the European Union has issued the new Network and Information Security Directive (NIS2). NIS2 focuses on protecting critical infrastructures and adopts a supply chain perspective. Organizations are categorized as critical or essential infrastructures and hence are obligated to ensure the security of their operations. Through a supply chain focus in NIS2, their suppliers can be subjects as well. Non-compliance with NIS2 can result in significant consequences for organizations, comprising fines up to 10 million or 2% of global revenue, personal liability for board

---

[1] Cynthia Institute (2021). Information Risk Insights Study: A Clearer Vision for Assessing the Risk of Cyber Incidents. https://www.cyentia.com/wp-content/uploads/IRIS2020_cyentia.pdf.
[2] IBM Security (2022). Cost of a Data Breach Report 2022. https://www.ibm.com/reports/data-breach.
[3] Welburn, J. W., & Strong, A. M. (2022). Systemic cyber risk and aggregate impacts. Risk Analysis, 42(8), 1606–1622.
[4] BlyeVoyant (2024). The State of Supply Chain Defense: Annual Global Insights Report 2023, BlueVoyant.com. https://www.bluevoyant.com/resources/the-state-of-supply-chain-defense-2023.
[5] Zeijlemaker, S., Siegel, M., Khan, S., Goldsmith, S. (2022, August 4). How to align cyber risk management with business needs. World Economic Forum, Cyber Security Working Group.
[6] Pearlson, K., & Hetner, C. (2022, November 11). Is Your Board Prepared for New Cybersecurity Regulations? IT Security Management, Harvard Business Review. http://bit.ly/40Jql8v.
[7] Hepher, M. & Powell, C.T. (2020). Make Cybersecurity a Strategic Asset, special collection "reboot your strategy," MIT sloan management review, Fall 2020, MITSMR-Cloudera-Reboot-Your-Strategy-0920.pdf (sodipress.com).

members, or temporary management bans.[8] Under NIS2, security is no longer an option but a necessity.

The core principles of NIS2 are:

- *Duty of care:* This is a risk-based approach to secure critical processes and systems, coupled with established plans and procedures to mitigate the effects of materialized cyber threats. Such plans include incident response, disaster recovery, business continuity planning, and crisis management.
- *Incident reporting:* This is mandatory reporting within 24 and/or 72 hours if cyber events disrupt critical or essential product or service delivery to national CERTs, e.g., CERT-FR[9].
- *Supervision:* Critical organizations can be audited for NIS2 compliance before and after a cyber threat materializes, while essential organizations can be audited after such a breach.

The issuance of NIS2 is timely. Supply chain attacks are expected to triple by 2025 compared to 2021, with associated global annual damages expected to shoot up to 138 billion dollars by 2031[10].

NIS2 implementation poses challenges to the organization

NIS2 implementation is easier said than done as managing cyber risk is very challenging. It involves prioritizing, budgeting, and resourcing cyber risk efforts in a constantly changing environment with, for instance, evolving adversary tactics and skills, shifting organizational priorities, changing organizations – in terms of people, processes, technology, and suppliers –, emerging security events, etc[11]. This makes governing and overseeing cyber risks very difficult, requiring sufficient board attention,[12] especially as governance and oversight are critical preconditions for securing organizations[13].

Simultaneously, implementing NIS2 will require organizations to put in more effort to enhance their defensive capabilities. However, they will also face challenges due to a shortage of qualified security resources. For example, the USA currently has approximately 750,000 job openings in this field[14]. Europe likely faces a similar situation. Therefore, achieving effective ongoing workload reduction becomes essential. Automation and the realization of economies of scale are critical to establishing a security architecture that is prepared for the future.

Overall, the implementation of, NIS2 poses challenges for organizations. This raises the question: what steps can organizations take to address these challenges?

Three essential steps for managing your suppliers under NIS2

To overcome these challenges, organizations need to take the following actions:

1. *Have a business, operational, and financial understanding of materialized (supplier-induced) cyber threats that impact your service and product delivery.* This requires a clear understanding of how your business strategy relies on technological solutions today and in the future, a clear understanding of your sourcing strategy (what solutions are supplier-dependent and which are internally managed), and a clear understanding of the susceptibility of these technologies to the ever-evolving cyber threats. As organizations struggle with limited budgets and resources, it is crucial to translate the impacts of these cyber threats into consequences for business, operations, and finance. Cyber risk quantification tools can help by making threat mitigation efforts comparable to other strategic business investment options.

---

[8] European Union (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022. https://eur-lex.europa.eu/eli/dir/2022/2555.

[9] Centre gouvernemental de veille, d'alerte et de réponse aux attaquees informatiques www.cert-ssi-gouv.fr

[10] Glosserman, B. (2024, April 4). The world narrowly escapes a supply chain doomsday scenario, The Japanese Times, https://www.japantimes.co.jp/commentary/2024/04/09/world/worrying-about-cybersecurity/#:~:text=CyberSecurity%20Ventures%2C%20another%20security%20firm,to%20%24138%20billion%20by%202031.

[11] Zeijlemaker, S., and Siegel, M. 2023. "Capturing the Dynamic Nature of Cyber Risk: Evidence from an Explorative Case Study," in Hawaii International Conference on System Sciences (HICSS) – 56, 2023 January 3rd – January 6th, Hawaii. https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/e9fbf734-b80c-45a4-ad7e-3ceb9768c07d/content

[12] Zeijlemaker, S., Hetner, C., and Siegel, M., (2023, June, 2). 4 Areas of Cyber Risk That Boards Need to Address, Harvard Business Review. https://hbr.org/2023/06/4-areas-of-cyber-risk-that-boards-need-to-address?ab=hero-subleft-1.

[13] Zeijlemaker, S. & Siegel, M. (2023). Six governance principles for cyber resilience: What the Board Needs to Know about Cyber Risk, One Conference, 2023, October 3 - 4, The Hague, The Netherlands. https://emagazine.one-conference.nl/2023/six-governance-principles-for-cyber-resilience/

[14] Cyber Seek US. Cybersecurity supply-demand heat map accessed on 2023, January 20 by https://www.cyberseek.org/heatmap.html.

2. *Mature the capability to evaluate and monitor your supplier landscape.* A common approach to evaluating and monitoring suppliers involves using supplier-oriented questionnaires to assess their state of security and compare it to the defenders' own security policies and strategies. This is supported by monthly service management meetings between the defender and its supplier to address security gaps and monitor cyber risk through (semi) annual assurance statements (e.g., ISAE 3402 or SAS 70). Unfortunately, this approach is labor-intensive and reactive, failing to address the challenges mentioned earlier.
However, technological evolution currently enables organizations to scan the internet for supplier presence and provide near-real-time[15] insight into their security state[16] through software-as-a-service solutions. This view is limited by and outside in view but also reduces the labor intensity of supplier management processes. This evolution continuous because in the age of artificial intelligence and machine learning, futuristic approaches may use simulation-aided techniques to change this near-real-time insight into forward-looking predictive analyses, providing insights into the future security state of suppliers[17]. These new technologies to monitor the supplier landscape reduce effort, provide clear transparency, and enable more timely interventions.
3. *Embed resilience in the ecosystem.*
Embedding resilience in the ecosystem helps organizations minimize the impact of cyber events and maintain the delivery of products and services even under difficult circumstances. However, this requires a system-of-system approach and collaboration at both operational/tactical and strategic levels between organizations.[18] [19] At a strategic level, organizations should participate in public-private partnerships that foster resilience, create a strong network of organizations that can help one another (during cyber threats, competitors can become colleagues), and share best practices in cyber risk governance and supplier management. National and international initiatives like Campus Cyber in France create such a forum for formal and informal exchange.[20] At the operational/tactical level, organizations should share information, such as threat intelligence, incident updates, and post-mortem reports. They should also provide timely support and cooperation, harmonize response procedures and communication through joint exercises and red-team tests, and explore alternative ways to deliver services and products. Embedding resilience also entails reimagining the supplier-customer relationship across the value chain.

Conclusion for the Board of Directors

On board level, this needs to be monitored and supported through structured questions on the strategic and operational advancement of the directive's implementation. Ideally, tools should help boards to be updated in real-time on the risk situation and in turn adjust any changes to the organization's risk appetite. This requires a holistic assessment of the information values that exist inside the organization that require protection and guide the selection of risk management and security measures. The value of intellectual property, for example, lies in its confidentiality. Any risks to core IP should be either avoided or mitigated. An appropriate mechanism for ensuring confidentiality of data may be strong encryption, aligned with the overall company architecture. The board must be informed about the value at risk, financial consequences, hence impact on the business in case of failure, and the maturity of matching mitigation measures. In particular, looking at 3rd party risks, these are not always obvious and therefore should be assessed in a category of its own. Besides contractual measures,

---

[15] https://www.greatamericaninsurancegroup.com/docs/default-source/cyber-risk/securityscorecard-instantly-monitor-the-security-health-of-any-organization.pdf?sfvrsn=b3ff43b1_8

[16] https://www.bsigroup.com/globalassets/localfiles/en-ie/csir/resources/exchange/bitsight---bsi-cyber-resilience-presentation.pdf

[17] Zeijlemaker, S. & Von Kutzschenbach, M. (2022). Threat actors' perspective on organizations: Why shouldn't we do the same to manage cyber risk in the supply chain? 40th International System Dynamics Conference in Frankfurt and virtually July 18-22, 2022.

[18] Falco, G. J., & Rosenbach, E. (2022). Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford University Press.

[19] World Economic Forum and Partners (2021, March 23). Principles for Board Governance of Cyber Risk, https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk/

[20] Launched in February 2022, Campus Cyber is a network of 160+ organizations in France to set actions federating the cyber security community www. Campuscyber.fr

companies possess the possibility to audit as well as insure against such risks, again depending on their ability to quantify the losses a business disruption or loss of data would mean to the organization. When looking at risks, organization's should also perceive the opportunity. The intention for NIS2 is to create resilience for the economies in Europe. The objective of the reporting to coexert responses to attacks cross industry and beyond national boundaries creates a platform for improving the trust of all market stakeholders and hence supports the further digitalization and efficiency of the business.