The NIS 2 Directive – Where Cyber Risk meets Supply Chain Management

Jan Martin Lemnitzer, jl.digi@cbs.dk and Günter Prockl, gp.digi@cbs.dk

Many will have already heard about the new NIS 2 Directive which the EU passed to improve the cyber defenses of critical infrastructure. The new Network and Information Systems (NIS) 2 Directive, coming into force on 17 October 2024, not only replaces the NIS 1 Directive from 2016 but marks a quantum leap in cybersecurity regulation in the European economy.

What is new in Cyber risk regulation?

The most important change is that where NIS 1 relied on recommendations, the key provisions in NIS 2 are compulsory: companies ignoring them face hefty fines, similar to GDPR. Further, managers responsible for cybersecurity negligence can even be removed from their positions by the regulator. Secondly, the NIS 2 Directive is part of a general EU embrace of *risk-based regulation*, where companies must assess the risks facing them and take security measures accordingly. The regulator will then review the documentation and inform the company whether they consider their cybersecurity measures appropriate to their cyber risk level, or whether they need to do more. Companies therefore need to be able to understand cyber risk management and act on their assessments or face permanent conflict with the authorities. Thirdly, the scope of what counts as critical infrastructure has been expanded enormously – experts expect that ten times more companies will fall under the NIS 2 regime compared to its predecessor.

In Denmark alone, more than a thousand companies will be directly affected by NIS 2. Therefore, it was natural that companies' first instinct was to check whether they were in scope of the directive. A quick look into the 14-page annex of the NIS 2 Directive will tell a company whether it is active in a sector of the economy that is listed as 'essential' or 'important'. If one's sector is included, the need to act is obvious. But what if your sector is not listed there? The main purpose of this short note is to show that this does not mean you will *not* be affected by the new Directive. This is because NIS 2 introduces new requirements for how companies in scope need to manage the cybersecurity standards of their suppliers. So even if you are not in scope but supply a company that is in scope, you are still highly likely to face requests for new forms of documentation to prove that your cybersecurity standards and practices make you a trustworthy business partner.

The complexity of modern supply chains

In Supply Chain Management, we try to manage and align beyond the company's boundaries. We want to integrate our company's suppliers and possibly their suppliers to realize a so-called holistic view that is promising better performance than the limited view of a single actor. Still, even when taking a holistic view, a managed supply chain is never a uniform entity but rather an actively woven, complex network made up of many involved companies. They must all position themselves with their own business model and need to remain attractive for the customers and partners in the chain. Supply Chain Management thus rests on a collaboration of more or less autonomous actors that are linked together via more or less tight relationships.

The development of such relationships takes time and requires investments, for example in more closely interconnected communication technology, but also in trust and long-term supplier development. This links to cost and gain sharing, to control and supply chain leadership but also to new risks and dependencies. As such, supply networks may quickly become complex, and the development of tight relationships consumes time and money. Therefore, not all relationships are typically treated the same way. In supply chain theory we often use supply risk and profit impact to separate strategic suppliers from non-strategic suppliers.

Additionally, we often segment supply chains into a hierarchy of first tier, second tier and third tier suppliers. Each actor on one level is absorbing the complexity of the levels situated vertically below in the chain. This comes however also at a price of risk. For example, we have had high-profile scandals involving leading brand manufacturers whose products were produced using child labor by their subcontractors in low-cost countries. The brand manufacturers were heavily blamed for lacking control over their upstream suppliers. Companies at the end of the chain thus bear consequences for the behavior of companies upstream and try to establish a strict control regime accordingly. In addition, in modern supply chains, the physical product is becoming increasingly less important. Rather, it serves just as a platform for services that offer the customer a combined solution instead of ownership of a product. Value is not resulting from product sales but from comprehensive provision of such solutions. This implies the increased integration of additional service providers and more heterogeneous cross industry collaboration with an increased number of interfaces. This multiplies the challenges of complexity and control in the supply chain.

Cybersecurity in supply chains

What is happening now is that this kind of supply chain thinking is being absorbed into how cybersecurity is handled. Companies realize that they may have strong cyber-defenses themselves but once they have given a supplier some form of access to their network, their security is only as strong as the defenses of that supplier against cyber-attacks such as ransomware. Therefore, when defining supplier attractiveness, it's no longer only about prices, reliability, or other classic relationship properties but increasingly about compliance with cybersecurity standards and the ability to demonstrate such compliance. In other words, focal companies downstream will have to take a much closer look at the cybersecurity standards and capabilities of their suppliers upstream to increase their own attractiveness and to demonstrate their own reliability. The relative importance of that new selection criteria may depend on many other factors such as whether a focal company is in scope of the NIS 2 Direc-

tive, or how critical a supplier's position is in their supply chain. With the pending publication of the Danish implementation law only expected for spring 2024, the precise details are still unclear, especially regarding the regulatory setup. Nevertheless, we are confident enough to predict that the importance of cybersecurity in related business decisions will increase significantly. The focal companies will introduce new requirements both for cybersecurity standards and the documentation of the cybersecurity practices of their suppliers. Unfortunately, since best practice standards for how to evaluate supplier's cybersecurity standards are still unsettled, companies that supply different larger companies within the scope of NIS 2 might likely face different requests to demonstrate their trustworthiness regarding cybersecurity risk from different customers in different supply chains.

Cybersecurity in small and medium-sized enterprises (SME)
Many SME's will find dealing with cybersecurity compliance a struggle, for at least three reasons:

First, many large companies push the challenge upstream relying on data collection based on questionnaires that are difficult and time-consuming to complete. Large companies use them to get an overview of both the technical measures and the organizational processes that are in place to defend a company's networks. That implies that upstream companies need either a highly skilled employee having a comprehensive view across the company or the capability to communicate the task and coordinate the answers between different business units. Moreover, while standardized solutions are available, most large customers create their own as they believe the standardized questionnaires don't meet their specific needs. In consequence, this means that small companies supplying several large customers will receive multiple large questionnaires with 100 or 150 questions each. As one tech expert in a Danish SME told us, having nine large customers sending nine different questionnaires means that he must devote a month every year just to fill out questionnaires. Obviously, it is tempting for some companies to adopt a box-ticking approach and simply answer 'yes' to everything, but a follow-up call by the large companies' compliance department might result in a difficult conversation and a worsening of the relationship to an important customer.

Second, companies might well be asked to create policies, plans and documentation that are unfamiliar to them, such as a company cybersecurity policy, an incident response plan, or an analysis of their cyber risk. Many companies without the necessary expertise in-house will turn towards consultants to help them create such documents, but for many smaller SMEs this will severely stretch their budgets. It is precisely this problem that our new project 'Cybersecurity of Supply Chains: Creating actionable guidance for SMEs' (kindly funded by Industriens Fond) wants to help solving. We will create templates and guidance materials that break down the language of business cybersecurity and standards into plain language and questions that anybody running a business would understand. Once companies have a clearer picture of their cybersecurity needs and requirements they might still opt for external support. However, now they will know precisely what they need from a consultant or IT security company. This will make this process both more efficient and much cheaper.

Third, an increased focus on cybersecurity will most likely uncover the need for more investments. Fortunately, some key technologies such as 2-factor authentication for company accounts are relatively cheap and standard business software for SMEs often come with free security features (such as Microsoft Defender). However, once a business has grown slightly it will most likely need more advanced security features such as network segmentation or the services of a cloud-based IT security provider. SMEs would be well advised to hire an external expert to help them with the initial audit of what hardware and software they are running in their company – the percentage of companies that can give a ready answer to this question is surprisingly low. Inevitably, this will cost money.

But it is money well spent, as it not only improves potential defenses against cyber-attacks such as ransomware that can have a catastrophic impact on a company's business. As shown above it will also put SMEs in a better position in the new world of cybersecurity supply chain risk management. When larger clients can see that partners take cybersecurity seriously, produce relevant documentation and make smart investments, they will continue to trust and want to do business with them. This is unlikely to be the case for those of competitors who keep ignoring the cyber risks they are facing.

Forfatter: Jan Martin Lemnitzer

Jan Martin Lemnitzer is Assistant Professor at the Department of Digitalization, Copenhagen Business School. His research focuses on cyber aspects of international conflict, business cybersecurity, cyber insurance, and cybersecurity regulation (especially its implementation). In 2021, Jan ran a multi-stakeholder workshop series on challenges regarding the implementation of the EU's NIS 2 directive on the protection of critical infrastructure (kindly sponsored by Microsoft). In the same year, he was a member of working groups 4 (cyber norms) and 6 (ICT supply chain security) of the Paris Call for Trust and Security in Cyberspace. Since 2023, Jan is PI of the research project 'Cybersecurity of Supply chains: Creating Actionable Guidance for Danish SMEs' funded by Industriens Fond. Jan is also participating in the 2023 session of the Geneva Dialogue on responsible behaviour in cyberspace which this year focuses on supply chain cybersecurity.

Forfatter: Günter Prockl

Günter Prockl is Associate Professor for Supply Chain Management at the Department of Digitalization, Copenhagen Business School, and affiliated and guest lecturer at different European Universities. Years of work in client oriented, science-based consulting, and before that on shop floors in production planning and control, has inspired his research on theoretical and practical key challenges regarding management, services and operations in supply chains and logistics. Also, academic experience as doctorand, habilitand, associate professor, adjunct and professor at different university chairs, has been an inspiration. Specific topics of interest relate to business models of key supply chain actors, processes, and network structures, (human) resources in logistics, sustainability, and the application of related digital technologies. Consequently, Günter's research approaches are often interdisciplinary but specifically targeted on the management aspects.