"The implementation of the NIS 2 Directive: challenges and solutions"

By Jan Martin Lemnitzer, Department of Digitalization, Copenhagen Business School

September 2022

Executive summary

This report is based on a series of three hybrid workshops in November and December 2021 at Copenhagen Business School inviting practitioners to discuss issues relating to the introduction of new or extended cyber security regulatory duties as the NIS 2 Directive as passed and implemented. Our experts quickly identified the rules regarding **cyber risk supply chain monitoring** as the biggest problem with the implementation of NIS 2 as they will require the biggest step up from what is currently practiced by most companies. The discussions revealed that there is no clear consensus on how exactly companies should monitor their supply chains for cyber risks. What emerged is a picture whereby each company improvises their own approach, if they are conducting a cyber risk analysis of their supply chains at all. There are detailed and expensive audit procedures that are used for a small number of high-risk suppliers. But these are not scalable due to their cost, which is why most companies have no reliable information about the cyber risk posed by most companies they do business with. We cannot leave this problem to 27 national regulators and need clear guidance from Brussels to answer (at least) the following questions:

How should companies distinguish between high and low risk suppliers?

What measures are required for each of these groups, both during the onboarding process and afterwards?

To what extent can cyber risk rating agency scores be a part of this process?

Risk rating agencies have seen huge growth in recent years, and their scores are increasingly used to support important business decisions. If regulators take the view that a cyber risk supply chain monitoring system that relies on the scores provided by a rating agency fulfills the requirements of NIS 2, we will see a huge expansion of these agencies' customer base, and several serious issues with rating agencies that are not widely understood by EU policy makers will become critical problems for cybersecurity in the EU if left unattended.

NIS 2 also poses serious difficulties to SMEs. First, while the Directive excludes companies with fewer than 50 employees, that leaves a huge number of companies above that threshold are far away from having a mature IT security setup in place. Second, the supply chain management requirements in NIS 2 will mean that many companies that are not covered by NIS but deliver to companies that are in scope will soon experience the need to document their cyber security practices in ways they will seriously struggle to comply with. They need to step up fast or risk being dropped out of the supply chain by important customers. Therefore, we need a basic cybersecurity standard especially designed for SMEs in the EU. Ideally, we should also set up standardized auditing systems building on this standard to ensure that SMEs know a certification will be respected by all of their business partners.

In the Solutions section at the end, this report makes five recommendations:

1) Issue clear guidelines how the supply chain management requirements in NIS 2 should be interpreted

2) Ensure that regulators in all member states are properly staffed

3) Create a new IT security standard specifically for SMEs

4) Create a simple but effective cyber risk auditing system at EU or member state level

5) Establish rules for cyber risk rating agencies to ensure transparency and accountability

1. The workshop series

Impressed by the draft for the new NIS 2 Directive to ensure a high common level of cybersecurity in the EU we wanted to find out what these new rules will mean in practice for the companies and organizations that will have to implement them. We organized a series of three hybrid workshops in November and December 2021 at Copenhagen Business School inviting practitioners to discuss issues relating to the introduction of new or extended cyber security regulatory duties once NIS 2 is passed by EU authorities and implemented by the member states. Our experts came from the financial industry, software companies, rating agencies, consultancies, tech companies and the energy sector, and all were dealing with the implementation of cybersecurity legislation as part of their daily work. Some attended two or all workshops, others were invited to one of the events for their specific expertise. To ensure free-flowing and open discussions, the meetings were held under the Chatham House rule which specifies that 'participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed'. We are grateful to Microsoft for providing the funding that enabled the workshops. It is important to note that Microsoft did not influence the content of this report or the recommendations it makes.

2. Cyber risk supply chain monitoring emerges as the most critical issue

Early in the first workshop when discussing where practitioners foresee problems with the new rules and how companies should prepare for the new reality of tighter cybersecurity practices and risk management, a consensus emerged that our experts perceived the rules regarding cyber risk supply chain monitoring as the biggest issue with the implementation of NIS 2 as they will require the biggest step up from what is currently practiced by most companies. It is also the one rule that will indirectly affect many companies that are not in scope of NIS 2, and it is where our experts felt the regulation is the least clear about what level of supply chain scrutiny it would like companies to conduct.

In academic and policy discussions and reports on cyber risk in supply chains there is a strong focus on ICT supply chain issues whereby vulnerabilities are introduced through the acquisition of faulty or manipulated software and hardware. However, while ICT supply chains risks for software and hardware are real and have moved up many governments' agendas following the Huawei/5G debate, for individual companies many of the solutions discussed here have little practical relevance. The experts pointed out that very few companies have the skills and capacity to conduct a meaningful analysis of the source code of software they are considering buying and thereby identify hidden security issues. One participant from an antivirus software company described how they once attempted to hire an external company to verify the security of its endpoint security solution but found that no company was willing to take on this responsibility. In short, the solutions offered to ICT supply chain issues such as trust centres allowing potential customers to inspect source code or hardware are beyond all but the largest and most sophisticated companies. A company facing the mundane but important task of selecting a provider for an online shopping solution, a payment processor or a cloud provider cannot afford to hire experts to sift through the code line by line.

Rather, the due diligence they should (and once NIS 2 is implemented in many cases must) conduct is a cybersecurity adaption of classic supply chain risk management techniques. However, there is universal agreement that many of these techniques such as sending detailed questionnaires to

existing or potential business partners do not work very well in cyber security. Crucially, while there are standards and recommendations, there is no clear consensus in business how the cyber risks in supply chains should be managed.

This is why the experts assembled in the first workshop were surprised and confused that the NIS 2 draft existing at the time compelled critical infrastructure companies to conduct 'state of the art' cyber risk supply chain monitoring. They pointed out that first, the 'state of the art' in any field involving digital technology is constantly changing and thus not a stable framework of reference. The latest compromise draft following discussions between the European Parliament and the European Council has removed the 'state of the art' phrase from the text and inserted a reference to international and European standards, but that does not solve the problem. International standards like ISO 270001 were developed for large companies with huge IT security, risk management and compliance units, and the NIST recommendations on cyber risk and supply chain monitoring are 326 pages long. The discussions revealed that there is no clear consensus on how exactly companies should monitor their supply chains for cyber risks, and what emerged is a picture whereby each company improvises their own approach, if they are conducting a cyber risk analysis of their supply chains at all.

3. How to monitor supply chains for cyber risk

The problem begins with the questionnaires that are sent out as part of classic supply chain risk management. For cyber security, they can easily involve a hundred or more questions, which may or may not be relevant or even intelligible for each supplier. Providing reliable and detailed answers requires a serious commitment of staff time on the side of the company having to fill them out, and full honesty and insight regarding the maturity of their cyber security measures. Therefore, there is an inbuilt incentive to provide superficial or even misleading answers, which means companies do not trust the filled-out questionnaires they receive back at face value. Usually, they schedule a long phone conversation or online meeting with the IT security staff of the company to clarify some of the answers or probe deeper. If doubts remain or the supplier will get particularly deep access to a company's network, it can send in a team of IT Security experts for a site visit or arrange for an external auditor. Both options are expensive, both in terms of the financial costs as well as the working hours of scarce expert staff.

In short, there is a known and detailed way to assess a vendor's cyber security that all experts agree they are confident in. However, it is so time consuming and expensive that it is reserved for those companies seen as posing the highest risk. Companies seen as lower risk receive minimal or no attention at all regarding their cyber security from supply chain risk managers.

That makes the process through which suppliers are selected as posing a high risk a particularly critical one for the cybersecurity of a company. Still, the experts painted a picture of each large company using their own approach, sometimes using tools they created themselves. Common criteria that were referred to are:

1. the extent to which the new vendor or service provider would get access to the company's networks.
2. The extent to which the new vendor or service provider would get access to the company's physical sites.
3. The criticality of the products or services provided from a business continuity point of view (how important is what they are delivering to keep business going, how difficult is it to replace them?).

All experts describe a risk management process that is focusing heavily on the onboarding part or is triggered by an extension of an existing supplier's activities, e.g. if they take on a new task giving them deeper access to company networks. Companies face re-assessment after one and a half to three years, but there is very little oversight once a company is in a supply chain. It is rare for a company to be pushed out of an existing supplier relationship if they supply reliably.

In summary, the experts agreed that the status quo of cyber risk supply chain management is unsatisfactory, with three main problems:

1. There is a strong focus on the onboarding process, and little visibility of what happens at a company afterwards regarding their cyber security.
2. Most companies are assessed through their answers on improvised excel sheets that they fill out and send back. There is limited confidence in the process, and both customers and vendors must go through it again for every new business relationship.
3. We have a process that is thorough and trusted but it is not scalable and therefore reserved for a small number of high-risk suppliers. This neglect of lower risk companies means that most companies have no reliable information about the cyber risk posed by most companies they do business with.

4. The role of cyber risk rating agencies

This lack of cyber risk information and the difficulty of scaling up established ways to acquire it is a gap in the market that cyber risk rating agencies have stepped up to exploit. So-called "outside-in" ratings agencies promise to provide an accurate and reliable "cyber risk score" for any company without the need to inspect their premises or even talk to their IT team. The basic idea is to run a vulnerability scanner that searches for unpatched potential entry routes into a company's IT system and to combine the result with a number of other data points to generate a score that is usually modelled on US credit ratings (i.e. between 250 and 900). Companies like Bitsight, Security Scorecard or RiskRecon use different combinations of data – from monitoring online hacker chats to company size – as a proxy for exposure risk and then run bespoke algorithms to create their scores. While each "cyber risk score" is created in a different way, all of these companies claim to provide an accurate assessment of any company's IT security with a simple click.

Having found their first clients in the cyber insurance industry, they are now making big inroads in supply chain management as they offer a very easy way to assess any company's cyber risk quickly and cheaply and thus solve the scalability problem we identified above. Moreover, since the software solution is automatized it can offer continuous monitoring and detect changes in a company's IT security posture as they happen. The big question is whether and to what extent a cyber risk supply chain monitoring system that relies on the scores provided by a rating agency fulfills the requirements of NIS 2. If regulators take this view, we will see a huge expansion of these agencies' customer base, and several serious issues with rating agencies that are not widely understood by EU policy makers will become critical problems for cybersecurity in the EU if left unattended.

5. How reliable are risk rating scores?

As one of our experts put it, the main problem with risk rating scores is that while a bad score means a company most likely has very bad cyber security in place, a very good score does not inspire equal confidence that a company's cyber security is indeed very good. There is an inherent problem in the methodology of the rating agencies that they know nothing about what happens inside a company, both regarding the network configuration and the cyber security processes the company has in place.

Moreover, there is already an emerging cottage industry of service providers offering to optimize a company's BitSight or RiskRecon score. In some of the largest companies, there are already staff members in IT departments that have this task on their job description. One of our experts pointed out that the detailed reports provided to customers by the rating agencies are *de facto* a manual on how to raise the company's scores without necessarily making big investments in or significant improvements to company cyber security. For example, an IT security department running its own honeypot for threat research purposes would receive a significantly lower score because the rating software would only detect a company computer that was completely exposed without establishing that the exposure was deliberate. Just by switching off the honeypot, the company could increase its cyber risk score.

A further issue we discussed with the representatives of the rating agencies is the way they deal with known breaches, which lead to an automatic reduction of the score that is then reduced over time. This is done regardless of whether the breach was the result of a newly exploited zero-day vulnerability at a software supplier or whether it was caused by a vulnerability in the company's servers that should have been patched years ago. While companies should be encouraged to be open about the cyber attacks they are dealing with and share information publicly, this automatic punishment is a strong deterrent to disclose any breaches.

Finally, there is a question over the way IP addresses are assigned to individual companies. Bitsight gives its accuracy rate as 96%, which still means that 4% of the hundreds of thousands of companies they score are judged on the configuration of websites they do not own. Some industry experts assume the real accuracy rate is much lower than 96%. Moreover, very few companies regularly check whether the IP addresses assigned to them by the various risk rating agencies are correct and ask for their reports to be modified. In many cases, mistakes will go unnoticed and determine the final score.

6. What if we all relied on risk rating agencies?

Two years ago, BitSight changed its branding materials and shifted from describing itself as an exciting tech startup towards pronouncing itself as the standard in cyber security risk rating. Their confidence grew along with their sector, as more and more companies bought their services and started relying on their scores for business decisions. One sales manager of a rating agency mentioned that he had already seen supplier contracts that include a clause meaning the business relationship is terminated automatically if the supplier's rating at the agency falls below a certain specified score. As the importance of their ratings grows, companies will increasingly focus on doing what they can to ensure they receive good scores, which means focusing cyber security spending on areas that the rating agencies can measure. Everything that does not influence the score is bound to see less attention and ultimately investment, creating a lopsided view of business cyber security.

Moreover, the companies that establish themselves as market leaders today are highly likely to dominate cyber risk scores for many years to come. Thus, the situation today is comparable to that just prior to the rise of the big bond rating agencies in the United States in the 1960s, when Moody's, S&P and Fitch realized that players in the growing corporate bond market needed easy ways to determine the risk associated with each new issue. Together, they formed an oligopoly, ultimately dominating credit rating globally, as no comparable companies arose in Europe or elsewhere. The 2010 financial crisis brought the painful realization that these ratings companies had immense power over European companies' and even states' financial viability but little accountability regarding how they created their scores.

Foreseeing serious issues with this emerging sector, the US Chamber of Commerce persuaded the leading players in the new industry to sign a voluntary pledge in 2017 promising every company the right to see its own rating report and make appeals at no cost. Moreover, the companies promised transparency surrounding the models, data and algorithms they use to create the scores. However, industry sources complain that agencies have become less and less transparent about how their models work, treating them as commercial secrets. Especially if NIS 2 regulators accept cyber risk scores as part of a cyber risk supply chain monitoring regime that is compliant with the Directive, EU authorities should take a closer look at this industry and ensure its business practices are transparent and responsible. Ultimately, the EU might even want to consider creating its own cyber risk rating agency.

7. SMEs and cyber risk management

The second workshop focused on SMEs and cyber risk: while the threat environment is getting ever more dangerous, SMEs remain underprepared for the cyber risks they are facing. Moreover, they will soon have to demonstrate their credentials in cyber risk management to a much-increased number of potential customers who will be required to conduct risk monitoring. In this way, the new rules for companies in scope of NIS 2 will have a direct effect on huge numbers of companies that are not in scope but will now be asked to document their cyber security practices whenever they try to sell their wares or services to a company regulated by NIS 2.

The problem is that these companies will face a real struggle with the new requirements: as the participants explained, small companies and startups tend not to have much written documentation or policies, and rarely employ people who have experience in or knowledge of compliance procedures. If they have a bespoke IT department, they will rarely have more than one person with special skills in IT security. Therefore, the usual approaches relying on questionnaires tend not to produce satisfactory results since SMEs are unwilling or unable to dedicate staff time to filling them out properly, and often lack the expertise to answer cogently to detailed follow-up questions.

Interestingly, both investors who ran specialized funds for investment into SMEs and insurers selling cyber insurance told us that they essentially ignored the precise cyber risk posed by SMEs. The investors felt they could safely ignore the risk of a breach as it would not necessarily have a huge negative impact on a company's financial performance. The insurers in turn collectively underestimated the cyber risks posed to SMEs by ransomware, which led to the huge market correction in terms of prices and access to cyber insurance that is still ongoing now. In short, there is a huge problem with measuring SME cyber security risk, and the market has not been able to solve it.

As the representatives of SMEs in the Fintech sector pointed out to us, even smaller companies willing to spend money on sound cyber security advice do not find it easy to obtain. Small FinTech's need to have cyber security risk management practices in place since they are regulated as financial institutions but find it a struggle to hire IT security consultants since most of the good ones try to acquire more lucrative work for larger companies. Therefore, they are forced to hire tiny companies where it is impossible for them to ascertain whether they have the necessary competence or follow best industry practices. In one recent case in Austria, a small IT security provider servicing SMEs in the local area was breached, which meant that more than a dozen small companies in the same area were hacked at once. Since SMEs are highly likely to increasingly move towards cloud-based IT security providers, they need clear guidance on how to choose, onboard, monitor and manage their cloud-based IT security providers in order to maintain a sense of control over their own IT security.

The drafters of the NIS 2 Directive tried to solve the problems with SMEs and cyber security by excluding companies beneath 50 employees from the scope of the new rules, but that still leaves a huge group of small and medium sized companies that are larger but are far away from having a mature IT security setup in place. This group will seriously struggle with the implementation of NIS 2 and needs the clearest possible guidelines and support from regulators. Moreover, as explained above, the supply chain management requirements in NIS 2 will mean that many companies that are not covered by NIS but deliver to companies that are will soon experience the need to document their cyber security practices in ways they did not have to before.

All experts agreed that we need a new IT security standard specifically created for SMEs in the EU, comparable to what the UK is trying to achieve with CyberEssentials and CyberEssentials Plus. The solutions section will outline how this standard could look like.

8. Relations with regulators

The third workshop assembled insights and experiences from practitioners working on cyber security and regulatory affairs in industries such as financial services that have been implementing tight cybersecurity regulation for years. All participants felt surprisingly positive towards cyber security regulation and argued that in general it tends to improve the ways in which cyber security is discussed and practiced in companies. Regulators are seen as being good at guiding companies towards a basic cyber security setup that is appropriate and responsible given the cyber risks they face. They were also seen as determined to ensure that the cyber security awareness training for staff member is meaningful and ideally role-based, although the absence of clear standards and much research into the effectiveness of such training means they have a difficult job at hand in trying to both set and ensure good practices.

The experts considered regulators to be less effective in helping companies transition from a decent to a mature and sophisticated cyber security setup. A typical pattern here is that companies spend heavily on software and service providers as they expand their cybersecurity and then cut back once they find out what really works for them. There was a lively debate to what extent helping companies in this position should be a key task for regulators or not.

One thing all experts agreed on was that the implementation of NIS 2 would require not just companies but crucially also regulators in all 27 member states to hire vast numbers of experts in business cyber security. If there are not enough regulators and auditors to actually follow up on what is happening in companies we will have a situation where many companies (and especially smaller ones) will be formally regulated but de facto unsupervised. However, the market for business cyber security experts with skills in compliance and regulatory standards is empty, with large companies that can afford to pay substantial salaries struggling to recruit. For national authorities seeking to hire the necessary staff for the estimated tenfold increase in companies they will oversee it will be impossible to complete with industry and consultancies for the best talent. What this means is that regulators will have to hire junior staff and train them up themselves, and given how soon NIS 2 will be implemented they should start doing this immediately, in all member states. As for the companies coming into the sphere of cybersecurity regulation for the first time, experts from the consulting industry are already preparing for what they see as the ‘next GDPR’ where panicked companies will pay any price to get consultants into the house in a mad rush just before the implementation deadline. However, this approach will be even less effective for NIS 2 than it was for data protection rules: as one expert put it, ‘proper cyber security needs to become part of the company culture, and it’s hard to outsource culture change’.

9. Solutions

1) Issue clear guidelines how the supply chain management requirements in NIS 2 should be interpreted

While the 'state of the art' phrase has been removed from the draft, the reference to international and European standards does not solve the problem. Most industry standards like ISO 270001 were developed for large companies, and instructing companies with just over 50 employees to implement 'industry standards' is simply not the guidance they need right now. Instead, we need clear answers to (at least) the following questions:

How should companies distinguish between high and low risk suppliers?

What measures are required for each of these groups, both during the onboarding process and afterwards?

To what extent can cyber risk rating agency scores be a part of this process?

Moreover, these guidelines must come from Brussels since we simply cannot leave this for individual regulators to figure out. Supply chains frequently cross national boundaries, and companies operating in all EU countries cannot set up 27 slightly different supply chain monitoring systems.

2) Ensure that regulators in all member states are properly staffed

NIS 1 failed because there was no coherent enforcement by national regulators. To ensure they can and will fulfil their tasks with NIS 2, they not only need guidelines on how the NIS 2 requirements are to be interpreted but also need the right number of staff members with the required expertise. Since they will not be able to meet their needs through recruitment alone, a coordinated hiring and training process (ideally supported by the EU Commission) should begin immediately.

3) Create a new IT security standard specifically for SMEs

While we are not short of IT security standards, very few of them have been designed with the realities in smaller companies in mind. For smaller companies, investing time and effort into complying with one of them only makes sense if it is universally recognized by their business partners. Therefore, a basic standard like this that has the approval of the EU, or a system whereby member states approved their own standards but grant mutual recognition would be a game changer for cybersecurity in small companies.

The measures required by this new standard must be feasible to implement without extensive specialist IT knowledge, and they must come a cost point that is manageable for smaller companies. At the same time, they must be carefully chosen to achieve the highest security gain at the lowest price. The UK's National Cyber Security Centre attempted to provide such a universal minimum standard with its Cyber Essentials certification programme for small businesses. It has just been updated and will now demand multi-factor authorization, password management and tighter security regarding the use of cloud services. Combined with least privilege principles, network segmentation, breach response and mandatory staff training it could serve as a good starting point for any country considering a minimum standard for SMEs.

4) Create a simple but effective cyber risk auditing system at EU or member state level

In Austria, both the government and private industry realized the size of the challenge of implementing NIS and decided to take a proactive stance. Under the guidance of the Ministry of the Interior, the country's NIS authority, a leading credit rating agency acquired a small cyber security company to create a package combing a recognized standard, a nationwide auditing system and network as well as their own vulnerability scanner. The CyberTrust Austria scheme launched in 2021 has a basic standard for smaller companies and a gold standard for larger companies with includes more sophisticated elements like SIEM network monitoring. The standard questionnaire is deliberately limited to 25 questions, and companies face follow-up questions for basic standard and a full audit for gold standard. The presence of the Ministry of the Interior on CyberTrust Austria's board ensures that the ratings are valid for the NIS audit, and the costs are borne by the critical infrastructure companies that need to secure their supply chains. Member states should consider whether having a comparable system in place might make it easier for their critical infrastructure companies to comply with the new NIS 2 Directive. A centralized system at EU level would offer the best efficiency but would require member states to entrust it with a ley aspect of the protection of their national critical infrastructure.

5) Establish rules for cyber risk rating agencies

Next to clarifying how cyber risk rating agencies can be used as part of a company's supply chain risk management according to NIS 2, it is also time to create some rules for this new and growing industry. The principles identified by the US Chamber of Commerce in 2017 that many companies pledged to respect as a part of a voluntary arrangement are a good starting point. They demand transparency on how the scores are generated, and accountability towards the companies whose scores they sell, giving them a guaranteed complaints mechanism and a right to see their own reports for free. Ultimately, the EU might consider setting up its own ratings agency or system to preempt a situation where ratings that are critical for business decisions are set by a handful of US companies wielding enormous market power.