CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

THE NIS 2 DIRECTIVE AND THE VEXED PROBLEM OF SUPPLY CHAIN CYBERSECURITY RISK MANAGEMENT

Jan Lemnitzer, Department of Digitalization

Copenhagen Business School

October 2022

What is Supply chain cybersecurity?

- Supply chain cybersecurity Involves three elements:
- **(1) Hardware**
- Where exactly did that cheap Chinese IoT device come from, who can access it (Huawei debate) and will the supplier patch the software if vulnerabilities are found?
- **(2) Software**
- Did that cool Danish startup that wrote software for me check for vulnerabilities?
- If they used plenty of open source code elements and one of them is found to be problematic, will they alert me about it and fix the problem?
- **(3) monitoring the cybersecurity standards of suppliers**
- What do I know about the cybersecurity maturity and practices of my suppliers, especially those to whom I have granted access to my network?

What does NIS 2 have to do with that?

- NIS 2 requires that all companies in scope demonstrate an appropriate and effective supply chain cybersecurity risk management, at least of their direct suppliers.
- **So how do you do that?**
- While early drafts referred to ‘state of the art’ cyber risk supply chain monitoring, this has now been replaced by a reference to ‘international and European standards’.
- This was in response to criticism that a recognized ‘state of the art’ or ‘best practice’ approach does not exist.
- **Problem**: telling companies to ‘follow European and international standards’ isn’t any more helpful.

Current approaches are: 1) Too expensive

- Diligent companies send out questionnaires on cybersecurity practices that are often more than a hundred questions long and closely study the answers.
- They then schedule a long phone conversation with the IT security staff of their most important suppliers 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.
- So we have a process that is thorough and trusted but it is not scalable.
- In practice, it is reserved for a small number of high-risk suppliers.
- In other words, most companies have no reliable information about the cyber risk posed by most companies they do business with.

Current approaches are: 2) too unreliable

- Companies like Bitsight, Secure Scorecard or RiskRecon use ‘outside-in’ vulnerability scans and 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 without the need to visit or talk to a company.
- While a bad score means a company most likely has very bad cyber security in place, a very good score does not necessarily mean that a company’s cyber security is very good.
  - They tell us nothing about what is happening inside a company or its networks.
  - There are known ways to ‘optimize’ risk rating scores.
  - The IP addresses used to establish a company’s score might not belong to that company
- Still, they are increasingly being used as a single data point when deciding whether to onbard a company as a supplier or grant them a cyber insurance policy.
- 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.

Current approaches are: 3) very bureaucratic box-ticking exercises

- The reliance on questionnaires sent to suppliers was simply copied from classic supply chain management but it never worked particularly well for cybersecurity.
- Most questionnaires are very long and include a mix of technical and organizational questions – they rely on one person in the supplier company knowing all the answers or organizing internal expertise to fill it out.
- In practice, they encourage a ‘say yes to everything’ box-ticking mentality.
- This means they need active follow-up to have any effect as a cybersecurity tool.
- Barring that, all they do is shifting the compliance workload from the larger to the smaller company – but they do that very well.

So what will NIS 2 actually change in supply chain cybersecurity?

- So unless regulators step in the new NIS 2 rules will encourage companies in scope to send even longer questionnaires to an even larger proportion of their suppliers, and demand more supplementary documentation.
- Since larger companies usually create their own questionnaires, the workload for an SME supplying 8 or 10 NIS 2 companies will be substantial, and achieve no measurable cybersecurity gains.
- Instead, the result might be that SMEs unable to cope with the documentation demands will be dropped from supply chains.

CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

CYBERSECURITY OF SUPPLY CHAINS: PROVIDING ACTIONABLE GUIDANCE FOR SME'S

Jan Lemnitzer, Department of Digitalization

Copenhagen Business School

5 October 2023
CBS

EQUIS ACCREDITED · AACSB ACCREDITED · ASSOCIATION AMBA ACCREDITED · CEMS · PIM

The team: Researchers, Partner organizations and Advisory Board

- **Jan Lemnitzer** (Assistant Professor in Cybersecurity, Department of Digitalization, CBS)
  Business Cybersecurity, Critical infrastructure and Regulation, Cyber insurance and rating agencies, supply chains
- **Günter Prockl** (Associate professor, Department of Digitalization, CBS)
  Digital Supply Chains
- **Attila Marton** (Associate Professor, Department of Digitalization, CBS)
  Digital Ecosystems
- **Andrej Savin** (Professor, former Dean of CBS Law)
- EU Digital Regulation
- **Olivia Benfeldt (Assistant Professor, Department of Digitalization, CBS)**
- Digital Transformation, Corporate Cloud Computing
- **Michael Herburger** (Lecturer, FH Steyr, Austria)
  Cybersecurity of Supply Chains
- **Johann Ole Willers** (Postdoc, Department of Organization, CBS)
  Cybersecurity Maturity Assessment, Cyber insurance
- **Alisa Ananjeva** (Postdoc, currently Aalborg University)
- **Partner organizations: Dansk Erhverv** and **Dansk Industri**
- **Advisory Board: Madeline Carr** (Professor of Global Politics and Cybersecurity, UCL, UK), **Deborah Housen-Couriel** (Tel Aviv), **Jacob Herbst** (CEO Dubex)

The target group

- One target group are Danish companies seeking to protect their supply chains from cyber threats or to comply with upcoming regulation, in particular the SMEs among the 1079 companies which will be in scope of NIS 2.
- But the main ambition is to help Danish SMEs not covered by NIS 2 to establish and document the cybersecurity standards and policies they will need to avoid being dropped from supply chains by larger organizations – an important secondary effect of the NIS 2 regulation.

Our research

- We will study the supply chain cyber risk management practices of **25 case companies** using a site visit and in-depth interviews to establish what their practices are, who is charged with running them and what structural capabilities exist for introducing improvements.
- We will analyze the entire supply chain by interviewing stakeholders ranging from the company's IT security team, their supply chain managers and their executives to those companies that form part of the supply chain either as suppliers or customers.
- These case studies will be complemented by **closed workshops with industry experts** both from the supply chain and the IT/cyber security side.
- We will analyze the **available standards for supply chain cybersecurity** (NIST/BSI/ISO270001).
- We will explore how **cybersecurity labels** such as D-Seal, CyberEssentials or CyberTrust Austria should be part of the solution.
- We will investigate whether **new technologies** such as the software tools offered by **cybersecurity rating agencies** like BitSight or Security Scorecard can be part of the solution.

Our project goals

- This project will help Danish SMEs by creating actionable guides on how to assess and manage their supply chain risk and how to implement the most important cybersecurity measures necessary for their own security and to pass the onboarding process as suppliers for larger companies. The guides will be more actionable than comparable materials since they will be based on the implementation experience of our case companies.
- Moreover, we will develop toolboxes that help SMEs with creating the kind of policies and documentation that are most commonly required by their larger customers to demonstrate their cybersecurity standards, as well as a tool helping companies to distinguish between high, medium and low risk suppliers.
- We will focus on industries that are either already regulated (such as energy and finance) as they should offer the best practices for others to learn from, or industries that will be covered by NIS 2 but face no existing cybersecurity regulation (e.g. food production or transport) since these companies should face the biggest implementation challenges.
- We will work with D-Seal, the Cyber Risk Simulator project, industry networks and regulators to try and create a nationwide ecosystem providing supply chain cybersecurity through trust and verification.

OK, but what will you actually *change*?

- At a minimum, we want to provide a large number of Danish SMEs with free tools that will help them to assess their cyber maturity, introduce basic cybersecurity measures and produce the documentation of cybersecurity practices that will be necessaru to ensure that they are not dropped by their customers for compliance reasons.
- The ultimate ambition is to help create an ecosystem of trust that rests on common standards and procedures to ensure appropriate cybersecurity across supply chains without wasteful bureaucracy (such as every large company sending their own questionnaires to suppliers).
- We assume that this ecosystem of trust will have D-Seal at its heart, but it can only work if large companies and regulators are closely involved in the design of processes and standards.

Right, so we can leave that one to you then?

1) **You wish. This will require a huge effort by pretty much every Danish company.**
2) **But if it works Denmark could be a model for a nationwide ecosystem of trust in supply chain cyber security management.**
3) **Could your company be one of our case companies?**
4) **What is dearly needed from the EU are clear answers and guidelines 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?*
- 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.