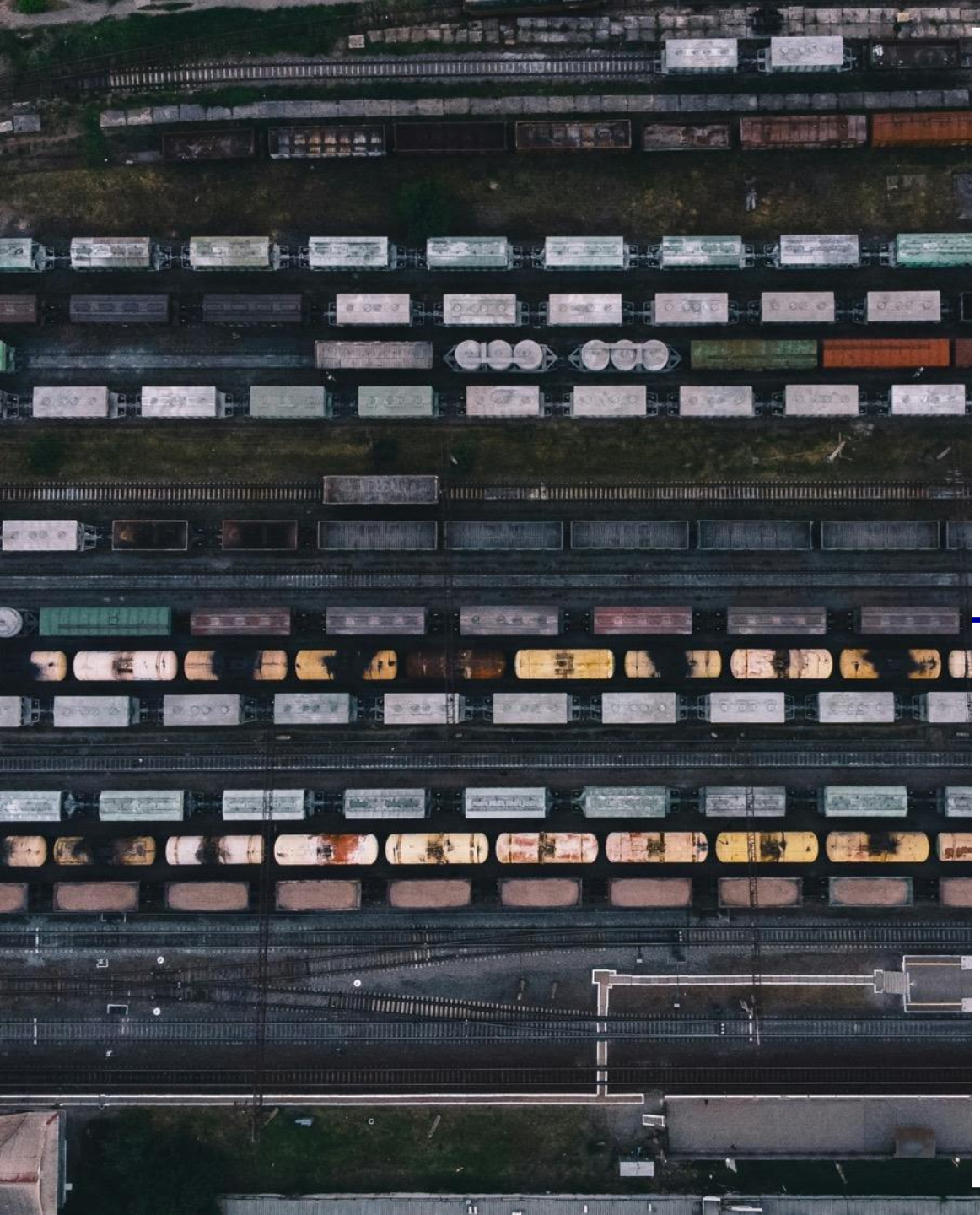


Supply Chain Security in Railway

Cybersecurity in railways

4th ENISA-ERA Conference

2nd October, Lille

2024

INTRODUCTION

Anna Prudnikova, MSc, CISSP, GICSP
Cyber security expert in OT
Secura, a Bureau Veritas company

Anis Bouaziz
Cyber security consultant OT/ICS
Secura, a Bureau Veritas company

EXAMPLES OF ATTACKS ON SUPPLY CHAIN

REUTERS World Business Legal Markets More

Nordex hit by cyber security incident, shuts IT systems

Reuters

April 2 (Reuters) - Germany's Nordex Group, which along with its develops, manufactures and distributes wind power systems, ha

Cyber attack on Deutsche Windtechnik

04/22/2022

Technology Deutsche Windtechnik internal

Cyber-attack on DNV's ShipManager software affects 1,000 ships

IT & SOFTWARE

January 17, 2023, by Jasmina Ovcina Mandra

Around 1,000 vessels were affected by the recent ransomware cyber-attack on DNV's ShipManager software, the classification society confirmed.

Ransomware Operators Leak Data Stolen From Wind Turbine Giant Vestas

on December 09, 2021

CYBER SECURITY NEWS · 4 MIN READ

Toyota's Supply Chain Cyber Attack Stopped Production, Cutting Down a Third of Its Global Output

ALICIA HOPE · MARCH 9, 2022

Vatican hit by suspected cyber attack days after Pope criticises Russia COMMENTS

By Euronews with Reuters & AFP • Updated: 01/12/2022

Uber suffers major cyber attack

Details are trickling out of an apparent 'near total' compromise of ride-sharin

Uber by an alleged teenage hacktivist

Hackers demand $50m from Mediamarkt, disrupt computer access: RTL

Business Tech & Media November 9, 2021

SECURITY / POLICY / TECH

LastPass reveals attackers stole password vault data by hacking an employee's home computer

LEGISLATIVE ACTIVITY IN EUROPE

2022

UNECE R155 & R156

New regulation for automotive sector - cars and supply chain

2023

CYBER SKILLS ACADEMY

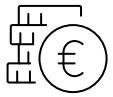
EU wide program for closing the cyber skills gap

2024

NIS 2

Essential & Important Entities **must reinforce cyber measures and supply chain**

2025



DORA

Traditional and non-traditional financial institutes must implement cyber measures

CRA

All connected products must demonstrate cyber conformity

2026 & BEYOND

MPR

Machinery must account for AI and Cybersecurity for safety

RED

Radio devices must reinforce cybersecurity

IMPACT OF CYBER SECURITY ON THE VALUE CHAIN

OWNERS OPERATOR

- Where are my risks?
- How can I prevent attacks?
- How can I prepare for attacks?

SYSTEM INTEGRATOR

- Am I aware of all the connected devices and systems?
- Am I sure the entire system is designed securely?

MANUFACTUERS

- Am I in compliance with the requirements of the market?
- Are the products I´m procuring secure?

SUPPLY CHAIN

- Am I producing secure products?
- How can I demonstrate my products are secure?

Rail Example

ALSTOM → KNORR-BREMSE → nexxiot

NIS2 DIRECTIVE – SUPPLY CHAIN REQUIREMENTS

SHOULD SUPPLIERS BE NIS2 READY?

(85) Addressing risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security service providers and software editors, is particularly important given the prevalence of incidents where entities have been the victim of cyberattacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers.

Directive Intro

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

Article 21

1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors.

2. The Commission, after consulting the Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated security risk assessment referred to in paragraph 1.

Article 22

ISO/IEC 27001 SUPPLY CHAIN REQUIREMENTS

SHOULD SUPPLIERS BE ISO/IEC 27001 READY?

A.15 Supplier relationships		
A.15.1 Information security in supplier relationships		
Objective: To ensure protection of the organization's assets that is accessible by suppliers.		
A.15.1.1	Information security policy for supplier relationships	*Control* Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
A.15.1.2	Addressing security within supplier agreements	*Control* All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.
A.15.1.3	Information and communication technology supply chain	*Control* Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
A.15.2 Supplier service delivery management		
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.		
A.15.2.1	Monitoring and review of supplier services	*Control* Organizations shall regularly monitor, review and audit supplier service delivery.
A.15.2.2	Managing changes to supplier services	*Control* Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

Domain A.15

SUPPLY CHAIN PROCESS

Qualification process

- High level checklist to be pre-filled by a supplier
- Qualification to be included in approved supplier list

Contracting

- High level commitment to Cybersecurity
- Agreement for third part audits once a year

Monitoring

- Review based (on site audits)
- Assessment based (detailed review of evidence)

SUPPLY CHAIN MANAGEMENT – EXAMPLE

Step 1. Creating Supply Chain Management procedures	Step 2. Preparing the list of requirements for suppliers	Step 3. Suppliers verification	Step 4. Monitoring of suppliers
Direct and in-direct purchasing	Defining criteria to split suppliers into different categories	Supplier reviews for low risks	Re-occuring review of suppliers
	Questtionairies for low and high risk suppliers	Supplier assessments for high risks	Follow up on reported suppliers changes, incidents etc
Timeline: 2 months	Timeline: 1 month	Timeline: 6-12 months	Timeline: Re-occuring

STEP 1

Supply chain management– ISMS
Focus IT

Supply chain management – SDLC
Focus components for products

Supply chain management - ISMS

Process for indirect purchasing: qualification, contracting, monitoring

Process for direct purchasing: qualification, contracting, monitoring

Information Security Requirements for Supplier Relationship Management

Cyber Security Requirements for third party components

Required templates: contract, supplier checklist, NDA etc

Required templates: contract, supplier checklist, NDA etc

STEPS 2 AND 3

SUPPLIER REVIEW
FOR LOW RISK SUPPLIERS

Quick check of suppliers based on prepared checklist

- Checklist based on the company requirements or best practise in cyber security (e.g. ISO27001)

SUPPLIER ASSESSMENT
FOR HIGH RISK SUPPLIERS

Detailed review of suppliers including risk assessments

- Requirements assessed including evidence review from each supplier

STEP 4

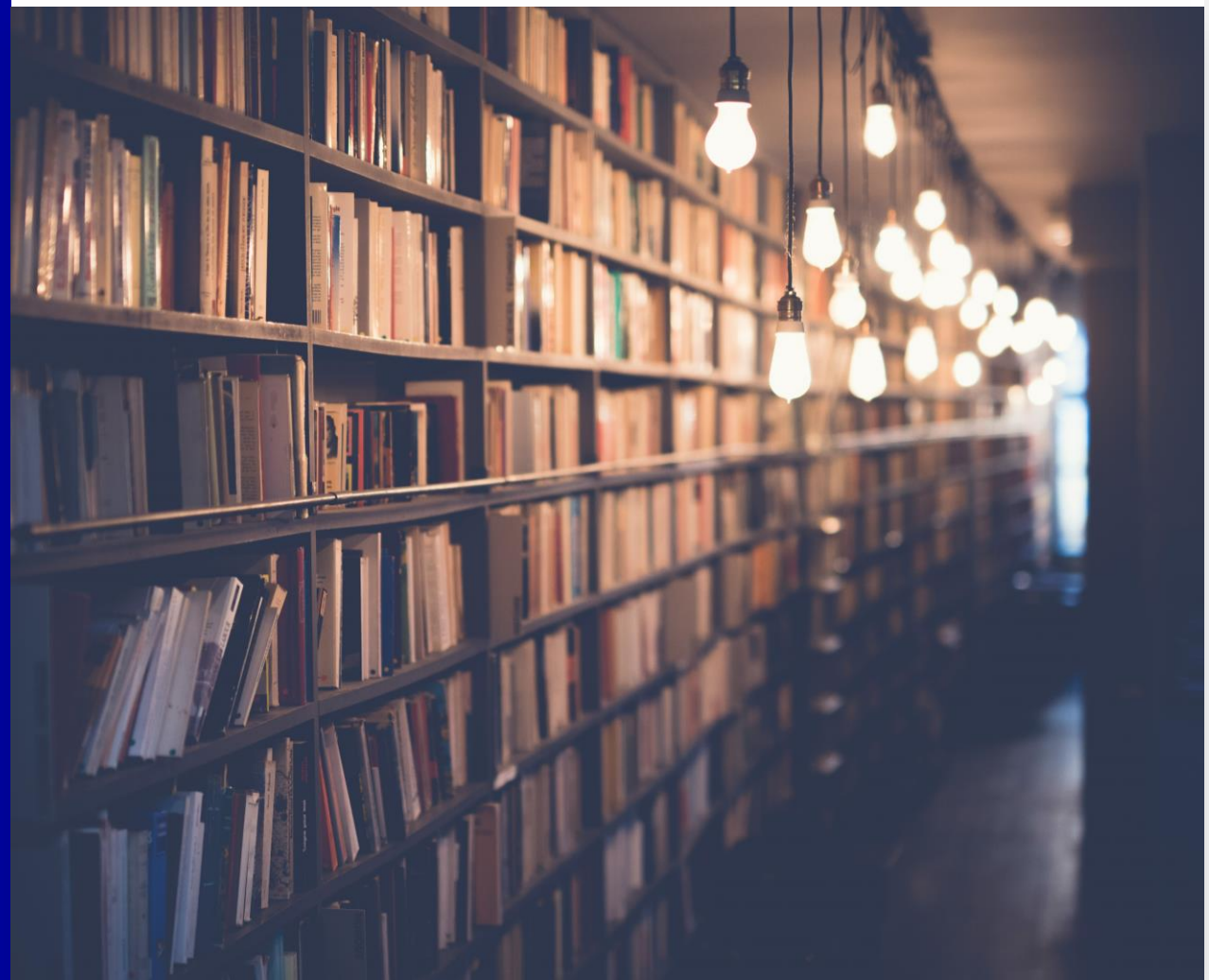
- Important to perform **regular review of existing suppliers** at least once a year (repetition of Step 3)
  - **Focus on potential changes** of suppliers details and specific risks
  - **Reaction to incidents** related to suppliers and intregration into general incident response process

SUPPLY CHAIN MANAGEMENT

This is a process rather than one-time activity.

Using a dedicated supply chain monitoring tool will simplify the process

BEST PRACTICES



01 The volume of supplies for a large organization can be in thousands; focus on critical and high risks first

02 Use requirements from excisting standards such as ISO27K and IEC62443, this will support consistency in the eco-system

03 Agree on the responsibilities for cyber security in supply chain early in the process, whether it is purchasing, IS team, product security team etc.

04 Select the optimal contracting way to include cyber security, negotiating will be a difficult process

05 Pay attention to specifics of direct and in-direct purchasing, in certain cases even products used direcrly in production might come under in-direct purchasing

QUESTIONS?
CONTACT US

ANNA PRUDNIKOVA
Head of International Cybersecurity services

Anna.prudnikova@bureauveritas.com

BUREAU VERITAS