Proposal No. 830929 Project start: 1 February 2019

Call H2020-SU-ICT-03-2018 Project duration: 42 months

Cyber Security for Europe

D9.12

Supply Chain Security Recommendations 1

Document Identification	
Due date	31 January 2021
Submission date	26th May 2021
Revision	1.0

Related WP	WP9	Dissemination Level	PU
Lead Participant	NTNU	Lead Author	Sunil Chaudhary (NTNU)
Contributing Beneficiaries	NTNU, TDL, ATOS, UM, JAMK	Related Deliverables	D9.26

Abstract: This report is the first deliverable in the sequence of two deliverables that make security recommendations to the supply chain. The recommendations are made specifically focusing on small and medium-sized enterprises so to protect against cyber challenges that could arise due to the integration of emerging technologies into the supply chain.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929. This document and its content are the property of the CyberSec4Europe Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CyberSec4Europe Consortium and are not to be disclosed externally without prior written consent from the CyberSec4Europe Partners. Each CyberSec4Europe Partner may use this document in conformity with the CyberSec4Europe Consortium Grant Agreement provisions and the Consortium Agreement.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Executive Summary

The digital transformation of the supply chain has significantly improved its performance but at the same time, this has opened it to cyber attacks. Cybercriminals are exploiting the weak components in supply chain activities and partners to infiltrate the target organisation's systems and data. In these circumstances, cybersecurity is an imperative necessity all across the supply chain network.

In this report, we have made cybersecurity recommendations that can be helpful to mitigate different cyber risks and threats that may arise from the integration of different emerging technologies. In order to do so, we obtained two cyber threat scenarios to the supply chain from our industry partner, which are:

1. On the use of permissioned blockchain in a supply chain
2. On the use of smart contract in a supply chain

In addition to a description of each scenario, it also includes potential weaknesses and their exploitation, impacts on SMEs if the weaknesses are exploited, lessons learned by organisations, and roadmap solutions in accordance with the CyberSec4Europe project's deliverables D4.3 and D4.4.

Finally, we make recommendations in terms of both technical and non-technical measures to mitigate cyber challenges discussed in the scenarios. The recommendations have been arranged in the following categories:

- General IT security recommendations
- Legal and standards recommendations
- Security recommendations specifically derived from CyberSec4Europe
- Tools recommendations
- Recommendations for the EU

Document information

Contributors

Name	Partner
Sunil Chaudhary	NTNU
Vasileios Gkioulos	NTNU
Marko Kompara	UM
David Goodman	TDL
Pasic Aljosa	ATOS
Jani Päijänen	JAMK

Reviewers

Name	Partner
Antonio Lioy	POLITO
Ricarda Weber	SIEMENS
Martin Wimmer	SIEMENS

History

Version	Date	Authors	Comment
0.01	2020-08-28	Sunil Chaudhary	1st Draft
0.02	2021-02-05	Sunil Chaudhary	2nd Draft
0.03	2021-03-21	Sunil Chaudhary	3rd Draft
0.04	2021-04-05	Sunil Chaudhary	4th Draft
0.05	2021-04-14	Sunil Chaudhary	5th Draft
0.06	2021-05-21	Sunil Chaudhary	6th Draft
0.07	2021-05-25	Sunil Chaudhary	7th Draft
1.00	2021-05-26	Ahad Niknia	Final check, preparation and submission process

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**AI**	Artificial Intelligence
B	**BCM**	Business Continuity Management
	BPM	Business Process Management
C	**COTS**	Commercial Off-The-Shelf
	CPS	Cyber-Physical System
	CSIRT	Computer Security Incident Response Team
D	**DAO**	Decentralised Autonomous Organisation
	DSC	Dispute Smart Contract
	DLT	Distributed Ledger Technology
E	**EAD**	Electronic Advance Data
	EEA	European Economic Area
	ENISA	European Union Agency for Cybersecurity
	EPC	Engineering, Procurement, and Construction
	ERP	Enterprise Resource Planning
	EU	European Union
F	**FG DLT**	Focus Group on Application of Distributed Ledger Technology
G	**GDPR**	General Data Protection Regulation
I	**ICT**	Information and Communication Technology
	IEC	International Electrotechnical Commission
	IoT	Internet of Things
	IP	Intellectual Property
	ISMS	Information Security Management System
	ISO	International Organisation for Standardisation
	IT	Information Technology
	ITU-T	International Telecommunication Union Telecommunication Standardisation Sector

M	**M2M**	Machine to Machine
	ML	Machine Learning
	MSP	Managed Service Provider
N	**NIS**	Network and Information Security
O	**OT**	Operational Technology
	OTTF	Open Trusted Technology Forum
	O-TTPS	Open Trusted Technology Provider Standard
S	**SBS**	Small Business Standards
	SCC	Supply Chain Cybersecurity
	SCM	Supply Chain Management
	SME	Small and Medium Sized Enterprise

Glossary of Terms

R **Risk**

A combination of cyber threat probability and the potential loss or harm related to technical infrastructure or the use of technology within an organisation.

T **Threat**

A cybersecurity circumstance or incident or act with the potential to cause harm by a way of its outcome.

V **Vulnerability**

Weaknesses in a cyber system that can be exploited by hackers or malicious programmes.

1 Supply Chain Cybersecurity

A supply chain in the context of this report is understood as a globally distributed and interconnected network of stakeholders, processes, functions, information, and resources, regardless of phase (creation or distribution of a product) and sector (information technology (IT) supply chain, logistics, manufacturing etc.)

The product and services in the supply chain can be physical, digital, or a combination of both, and is the result of the interaction between multiple stakeholders that can be *transnational* (in the global supply chain), including non-European Union (EU) countries. In the case of physical products, their interactions involve various processes, including the transport of all components and goods, the tracing of their location, guaranteeing the quality and integrity, certification, accreditation, etc. In contrast, the delivery of software systems and services to customers generally does not require logistics, however, resellers, distributors, service providers, and consultants play a major role in ensuring the end-user (or company) has the right set of systems and services to meet its business needs [1].

The active management of supply chain activities is called supply chain management (SCM)**.** Through SCM, enterprises seek to achieve sustainable and defensible competitive advantage by maximising customer value and at the same time lowering operating costs and improving profitability [2]. The globalisation of supply chains has highly increased the concern for risks including threats against availability among organisations [3] [4].

With digital transformation, organisations in a supply chain are heavily dependent on the Internet and information and communication technology (ICT) infrastructures. Certainly, digitally-enhanced supply chain activities contribute to improving the overall efficiency of the supply chain; however, at the same time, they expose organisations to a multitude of cyber attacks which increased by 78% in 2018 [5].

In order to address these cyber attacks, organisations in the supply chain must have cybersecurity strategies and measures in place to protect the entire value chain actively and pre-emptively. Supply chain cybersecurity (SCC) focuses on the prevention of both machine-based cyber threats and vulnerabilities, and those caused by human error, negligence, and vulnerabilities. It is imperative that SCS extends throughout the supply chain because it is nearly impossible to determine where risks will evolve from.

2 Report Objective, Scope, and Methodology

The main objective of this report is to make cybersecurity recommendations to the supply chain specifically focusing on small and medium-sized enterprises (SMEs). SMEs represent 99% of the enterprises in the European Union [6] and play important roles in supply chains.

Supply chains are continuously evolving with large organisations adopting emerging technologies. In order to do business with these large organisations and remain competitive in the market, SMEs will eventually be forced to adopt such emerging technologies. As a matter of fact, to make the most of the opportunities and gain competitive advantage and remain a reliable part of the supply chain, many SMEs are already making technology transformations. However, a major problem with this is that most SMEs suffer resource constraints and have a limited capacity to invest in up-to-date cybersecurity measures. Further, cybersecurity is not directly tied to revenue generation or cost-cutting and so is often considered to be a low priority investment by SMEs. It is a well-known fact that cybersecurity remains as strong as the weakest link in the chain. So if not acted upon with appropriate and effective cybersecurity measures, SMEs can become the weakest link in the supply chain cybersecurity and can pose a danger also to major corporations that they do business with.

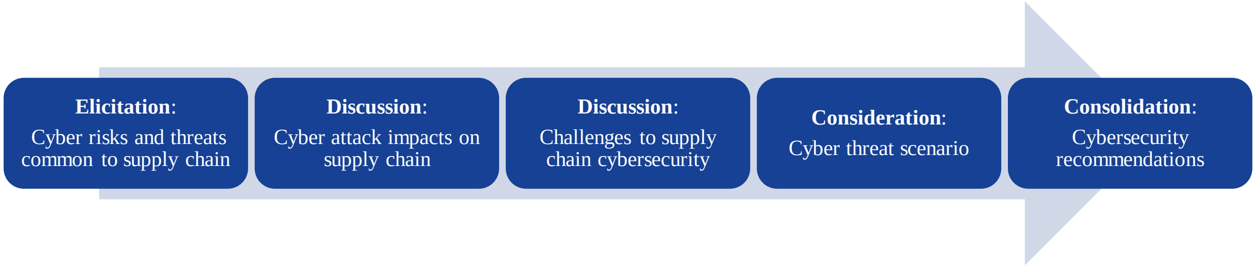
Elicitation:
Cyber risks and threats common to supply chain
Discussion:
Cyber attack impacts on supply chain
Discussion:
Challenges to supply chain cybersecurity
Consideration:
Cyber threat scenario
Consolidation:
Cybersecurity recommendations

Figure 1: Steps followed for the study

In this report, we followed the steps indicated in Figure 1. Before we delved into the actual objective, we discussed three essential aspects relevant and helpful to understand the importance of our recommendations and also raise the cybersecurity awareness of supply chain stakeholders. Initially, we elicited (via a brainstorming session in which all partners participated) and briefly explained some common cyber risks and threats to the supply chain. These threats and risks are as follows:

- Cyber-physical attack
- Data breaches and General Data Protection Regulation (GDPR) non-compliance
- Supply chain impersonation attack
- Business identity theft

This is followed by a discussion on the impacts of cyber attacks on the supply chain, which are derived from CyberSec4Europe deliverable D4.3 [7]. The impacts are categorised into:

- harm to operations,
- harm to assets,
- harm to individuals,
- harm to other organisations, and
- harm to the nation.

Then, we discussed the challenges to supply chain cybersecurity. We primarily discussed:

- potential challenges that may arise due to size, type and location of organisation, and
- potential cyber risks and threats that will be inherited to the supply chain by the integration of emerging technologies like industry 4.0 and CPS, cloud computing, IoT, AI and ML, big data, and augmented and virtual reality.

In order to achieve the objective of this report, we considered two cyber threat scenarios relevant to the supply chain (provided by our industry partner). These two scenarios are based on CyberSec4Europe deliverable D5.2 [8] and do not cover the overall supply chain. However, this narrowing of focus was important in order to align our work with CyberSec4Europe and at the same time make more concrete and specific recommendations.

- Scenario 1: On the use of permissioned blockchain in a supply chain
- Scenario 2: On the use of smart contracts in a supply chain

Along with the threat scenario description, each of them also contains the following:

- Potential weaknesses and their exploitation
- The impact on SMEs
- Lessons learned

- Roadmap solutions

Finally, necessary technical and non-technical recommendations are consolidated and made to the supply chain so as to remove/manage the elicited threats and risks. These recommendations are arranged as follows:

- General IT security recommendations
- Legal and standards recommendations
- Security recommendations specifically derived from CyberSec4Europe
- Tool Recommendations, and
- Recommendations to the EU.

3 Cyber Risks and Threats Common to Supply Chain

The following cyber threats and risks are identified:

- Cyber-physical attack
- Data breach and GDPR non-compliance
- Supply chain impersonation attack and identity theft
- Threats and risks originating by the implementation of, for example, artificial intelligence (AI), big data, Internet of Things (IoT) (refer to Section 5)

3.1 Cyber-Physical Attack

A cyber-physical attack is defined as "*a security breach in cyberspace that adversely affects physical space*." [9] In this attack, the malicious user exploits the vulnerabilities to take control of the computing or communication components with the intention to cause damage to property or put lives at risk.

The supply chain increasing dependency on computerised and networked environments is making it vulnerable to cyber-physical attacks. For example, IoT-based temperature monitoring systems (used to control, regulate, and track the temperature of a particular environment) are used to actively monitor the temperature in warehouse storing, or refrigerated trucks transporting temperature-sensitive products, such as medicines, vaccines and different food items. Attackers can take control of this IoT system and set the temperature of the environment so as to damage the goods. Similarly, autonomous vehicles will be adopted by the logistics industry in the near future [10]. Attackers can hack these vehicles to steer them into a crowd putting lives at risk.

3.2 Data Breaches and GDPR Non-Compliance

A data breach is any exposure to enterprise confidential, sensitive or protected data to unauthorised entities. It can occur due to technology vulnerabilities or human behaviours, although in most cases human behaviours are found to be responsible.

Data sharing among suppliers, manufacturers, distributors, retailers, customers, subcontractors, and beyond is an important component of cooperation and coordination in SCM. For example, data on sale and demand forecasting flow from downstream enterprises to their upstream partners whereas order state data flows from upstream enterprises to their downstream partners. These data flows in SCM while helping to achieve a common objective and improve performance, also lead to exposing multiple cybersecurity threats due to the involvement of a multitude of diverse actors at many levels. For instance, a data controller in the supply chain can appoint a processor on its behalf to process the data, which can sub-contract some or all of the processing to another entity and so forth. On average, an enterprise shares its sensitive data with approximately 583 third parties in the supply chain [11], which makes it very challenging for an enterprise to control the security measures taken by partners with access to sensitive data. These are all reasons why data breaches due to third parties is a prevalent problem in the supply chain [11].

From receiving an order to meeting a customer request, along the supply chain there may be points, such as logistics and distribution, marketing and customer service, that may require collecting and managing data which will need protection in compliance with the GDPR. But a vast majority of businesses and organisations in the European Economic Area (EEA) still fail to fully comply with the GDPR despite their interest and readiness to make appropriate investments [12] [13]. This partial compliance or non-compliance with the GDPR occurs for various reasons, for example, a difficulty in understanding various technical aspects of data security, a misconception among some SMEs that they are not of much interest for the regulators [12], employees with insufficient GDPR training who could not align personal data protection with the regulations [14] and intentions to exploit the vague technical specifications of the GDPR for benefit [13].

3.3 Supply Chain Impersonation Attack

An impersonation attack is defined as " *an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol*." [15]

Supply chain impersonation attacks have become a major threat to every organisation. In this, cybercriminals impersonate business owners and executives using phishing emails to steal money, data or other sensitive information [16]. In a more sophisticated variant of an impersonation attack, the attackers impersonate a legitimate vendor or supplier, which does business with the targeted company, to intercept a bank transaction or wire instruction to get hold of funds or sensitive information. For example, the attacker impersonates a legitimate supplier and sends a phishing email with a legitimate unpaid invoice to the targeted organisation's payment department asking to clear the dues. The targeted organisation makes the payment thinking that it has paid a legitimate invoice when in reality the transaction is made to the attacker's account.

3.4 Business Identity Theft

Business (or corporate) identity theft is a type of fraud that involves criminals stealing a company's identity and using it to commit fraud. In the supply chain, business identity theft is connected to cargo theft and fictitious pick-ups [17].

For example, cybercriminals use phishing and malware attacks to steal pick-up, delivery, and other sensitive information from a legitimate trucking company. They use the stolen information to pick up freight but once driven away the goods are never seen again.

4 Impacts of Cyber Attacks on Supply Chain

Cyber attacks can come from anywhere, at any time, and to any business partner in the supply chain. Their impact can lead to operational, financial, and reputational damages that may not be completely recoverable or repairable. It is important to make proper impact assessments of a cyber attack that can vary depending on the context and cascading effects. CyberSec4Europe deliverable D4.3 (p.52-53) has very comprehensively presented the potential impacts to our society resulting from a supply chain failure.

Impacts on society due to a supply chain failure

- **Harm to Operations**
  - *Inability to perform current missions/business functions*: attacks through the supply chain become commonplace, and organisations are always vulnerable.
  - *Inability, or limited ability, to perform missions/ business functions in the future*: as organisations are always vulnerable, it becomes impossible to fully recover from continuous attacks.
  - *Harms (e.g. financial costs, sanctions) due to noncompliance*: complex regulations cannot be implemented.
  - *Relational harms*: trust relationships between organisations are lost because managing the supply chain threats has become an impossible task.
- **Harm to Assets**
  - *Damage to or loss of physical facilities*: terrorist attacks take advantage of supply chain vulnerabilities to damage physical facilities, also causing human casualties.
  - *Damage to or loss of information systems or networks*: traditional cyber-attacks, such as ransomware, relentlessly disable the underlying IT infrastructure that supports the supply chain ecosystem.
  - *Damage to or loss of component parts or supplies*: it becomes impossible to manage the threats against digital assets when the supply chain is transformed into a chaotic supply web.
  - *Damage to or of loss of information assets*: various information assets are tampered with by malicious adversaries rendering the knowhow and intellectual property of companies useless.
  - *Loss of intellectual property (IP)*: IP routinely gets stolen from corporations and governments.
- **Harm to Individuals**
  - *Injury or loss of life*: counterfeited or altered products affect people either directly or indirectly.
  - *Physical or psychological mistreatment*: the public cannot trust the safety of the products they use in their daily lives.
- **Harm to Other Organisations**
  - *Relational harms*: the interconnected nature of supply chains causes damage to all actors involved in this vertical if the ecosystem can no longer be trusted.
- **Harm to the Nation**
  - *Relational harms*: loss of trust relationships with other nations, loss of national reputation, loss of national security due to the impact on the critical infrastructure.

5 Challenges to Supply Chain Cybersecurity

There are several factors that pose challenges to the implementation of SCC. The participating organisations in the supply chain can be of different in terms of size, type and location, which will impact their cybersecurity. For example,

- SMEs and micro-SMEs usually have limited resources for cybersecurity so they may require prioritising cyber assets and risks to deploy the available resources effectively;
- business sector and activity determine an organisation’s critical cyber assets that need to be protected using its finite resources; and

- global supply chains may consist of organisations located in different countries with disparate national legislations on cybersecurity, data protection, and privacy.

In addition, there exist multi-tiers of subcontracting making it challenging to conduct and keep records of third-party risk management which involves checking and ensuring that third parties, such as manufacturer, suppliers, distributors, and other business partners maintain an acceptable level of cybersecurity.

Amidst stiff business competition, organisations are under constant pressure to innovate and evolve so that they can offer their products and services at a lower cost maintaining high quality and on time delivery. Businesses are continuously transforming their supply chains to meet modern customer demands. Emerging technologies, such as cyber-physical systems (CPS), AI and machine learning (ML), IoT, big data, cloud computing, and augmented and virtual reality are being integrated into digital supply chains. Along with common threats like malware attacks, data breaches, information distortion, un(intentional) vulnerabilities, and malicious updates/maintenance, these organisations also inherit new threats particular to these emerging technologies. Some risks and threats that the supply chain may inherit by the integration of the emerging technologies, mentioned in CyberSec4Europe deliverable D4.4 (p.64) [18] are explained here.

- ***Industry 4.0 and CPS***: The smart manufacturing in Industry 4.0 (enabling technologies like industrial IoT, machine to machine (M2M) communication, big data analytics, advanced robotics, cloud computing, AI, machine learning (ML), and augmented reality) [19] and the integration of CPS have slimmed down the distance between IT and operational technology (OT) in manufacturing. By this IT/OT convergence, the industrial control system ceases to be isolated. It gets exposed to different IT attack vectors that are even capable of causing breakdown and disrupting the operation of a company's manufacturing plants [20].
- ***Cloud computing:*** Cloud computing introduces several security challenges; for example, data breaches (via hacking, insider threat, and credential theft) [21]. Moreover, the quality and availability of service are dependent on the Internet connection. By shifting the workload to the cloud, the supply chain also inherits these security challenges.
- ***IoT***: Industrial IoT in smart manufacturing and IoT-based warehouse and logistic monitoring system connects the supply chain ecosystem to the Internet and exposes it to various cyber-attacks. Moreover, IoT security is interconnected to a number of disciplines like IT security, OT security, and physical safety [19]. For example, malicious or malfunctioning sensors can provide wrong information about the state of a supply chain process.
- ***AI and ML***: The inherent limitations in the underlying AI algorithms and models are exploited to manipulate AI systems and alter their behaviour to serve malicious intents. Examples of AI-attacks are input attacks (i.e., cause an AI system to malfunction by modifying the input that is fed into the system) and poisoning attacks (i.e., damage AI model so that, once deployed, it is intrinsically faulty and easy to manage by the attacker) [22] [23]. Supply chain using AI algorithms and models for purposes like demand prediction for inventory management, smart manufacturing to boost operational efficiencies, and real-time tracking mechanisms to optimise fleet management processes [24] accordingly inherit their limitations. For example, the attackers can craft an input attack or a poisoning attack if get access to the AI model used for demand prediction or its training data set.
- ***Big data:*** Big data analytics is increasingly being used in supply chain management for purposes such as analysing consumer behaviour and usage patterns, enhance inventory management, and streamline e-commerce [25]. But the data analytics involve processing countless sensitive records, the consequences of which, if they end up in the wrong hands, could be potentially disastrous. The main challenges related to the secure use of big data are access control and authentication, secure data management and source validation and filtering [26].
- ***Augmented and virtual reality:*** Augmented and virtual reality have the potential to impact supply chains in areas like product and process design, data and process visualisation, employee collaboration, and experienced-based learning [27]. However, utilising this technology in

organisations implies incorporating OT privacy and security into IT considerations. Further, if digital reality does not match physical reality, this may cause incorrect and invalid decisions and inappropriate actions.

As pointed out in the same deliverable D4.4 (p.92), organisations can analyse and utilise cyber threat landscape or trend reports periodically published by governmental agencies like ENISA [28] [29], and companies like Accenture [30] and Symantec [5] during the development of their risk and threat strategies in order to get an overview of cyber threats, together with current and emerging trends, that are prevalent in the supply chain. Further, Kaspersky [31] publishes a cyber threat landscape report specific to a technology or a business sector. Most of these threat landscape reports are available for free so even resource constrained SMEs can utilise them.

6 Scenarios for Supply Chain Security

In order to make an initial identification of supply chain cyber threats, we are going to look at two scenarios which are based on the supply chain demonstrator use cases from deliverable D5.2 as well as the deliverables D4.3 and D4.4.

In addition to its description, each scenario also contains:

- **Potential weaknesses and their exploitation**: Explains vulnerabilities to the supply chain by implementing the technologies and processes mentioned in the scenarios.
- **The impact on SMEs**: Explains potential impacts on SMEs if the vulnerabilities are exploited (since SMEs represent 99% of enterprises in the EU and provide two-thirds of private-sector employment [6])
- **Lessons learned**: Explains lessons learned by organisations from the incidents that can be helpful in resolving the security issues.
- **Roadmap solutions**: Provides roadmap solutions in accordance with deliverables D4.3 and D4.4, for industrial challenges in the supply chain, i.e., deliverable D5.2 to manage the vulnerabilities.

6.1 Scenario 1: On the Use of Permissioned Blockchain in a Supply Chain

The supply chain system for industrial products includes many challenges that spread through the value chain, such as compliance assurance and accountability related to distributed manufacturing. Very often there is the main contractor, a large organisation that relies on the increasing number of global SMEs, that manufacture locally and sell globally. More recently digital technologies brought changes in business models with significant benefits not only for the main contractor but also for SMEs; for example by improving logistics and customer services such as by having on-demand products. SMEs, however, have more difficulties adopting new technologies that are aligned with those employed by large companies.

The main contractor generally uses complex processes to track and monitor not only the location, movements, and availability of parts but also their quality and compliance. Automation in monitoring the state of a complex interconnected supply chain introduces new threats, for example, related to the collection of data, or the use of artificial intelligence and big data.

In machinery manufacturing, many SME subcontractors might use 3D printers, for which there is specific EU product harmonisation legislation in place. They fall under the definition of machinery under the Machinery Directive 2006/42/EC [32] ,and manufacturers must ensure compliance with the applicable essential health and safety requirements.

In addition, there are other compliance requirements, often stemming from the main contractor's policies or guidelines, or from standards such as, "*Best Practices in Cyber Supply Chain Risk Management*" [33] and "*Cybersecurity Framework Manufacturing Profile*" [34]. The latter clearly establishes the need to: "*define, implement, and enforce policy and regulations*" (PR.IP-5) and "*conduct detection activities in accordance with applicable federal and state laws, industry regulations and standards, policies, and other applicable requirements*" (DE.DP-2).

As the main contractor increases control over its suppliers, it tries to implement measures to track risks and incidents down to their originating points. For this reason, SME suppliers are required to collect design, manufacturing and test data, as well as to share them to prove compliance.

This scenario considers a large company that designs, installs and delivers custom-built complete electrical stations or substations, for instance, with the purpose of enabling a high-voltage electrical current transmission with minimum losses.

Concerning cybersecurity, they must be built applying secure development processes, making sure that state-of-the-art security mechanisms (e.g., concerning authentication, authorisation) are implemented and that they do not contain any malware or logic bombs (which could be implanted as part of complex cyber-attacks).

A large company monitors not only the location, movements, and availability of parts, components, and products but also the quality and compliance of the goods with a specified manufacturing and quality assurance process. The determination of the exact fault in the production and the supplier responsible for this step requires triggering of a particular procedure that is implemented, monitored, and controlled through a particular workflow that used to be implemented in a business process management tool. The workflow starts at the point in time where the large organisation publishes the design and starts creating an associated feasibility study.

The main difference in relation to traditional business process management (BPM) tools is that relevant information about the workflow states and completion of steps is provided by means of tokens, which can be stored locally by the subcontracted entities or in a distributed ledger i.e., blockchain.

When a subcontractor SME completes a step of the workflow it has to provide proof about its activities. Technically, this is achieved by obtaining or creating a signed token that certifies the event. This token can be consumed - i.e., evaluated and processed - in subsequent steps of the workflow for ascertaining the preconditions for those next steps. Tokens do not only keep a history about the execution of the workflow: as in more conventional systems like OAuth, they may also provide evidence about attributes of parts or machines or trust assertions, etc.

In summary, a distributed ledger represents the workflow's audit trail and any attack on it would prevent having proof of compliance, resulting in monetary fines.

6.1.1 Potential Weaknesses and their Exploitation

The main contractor is likely to use a permissioned blockchain, which relies on some trusted and centralised services that could be exploited by malicious parties and could lead to attacks. But beyond these attacks, there are other threats, such as attacks on deterministic consensus protocols (sabotage, intentional fork, block size or withholding, batch time attack, or transaction reordering). There are also threats such as malicious validating nodes or external attacks, related to vulnerabilities introduced by the main contractor that need to have a certain amount of centralisation to provide a generalised platform for the subcontractors.

6.1.2 Impact on SMEs

Failure to comply with any requirement will usually result in the contractor incurring monetary liabilities. While the main contractor coordinates all design, procurement, and construction work and ensures that the whole project is completed as required and in time, subcontracted SMEs also face similar monetary liability. The risk of non-compliance has become a pressing concern for SMEs in recent years, particularly for manufacturers with operations in multiple countries and jurisdictions. Attacks on permissioned blockchain that serves as a support for compliance, audits, system validations, audit trails etc. would result in a failure to produce verifiable certifications which can be used to demonstrate compliance to regulation.

It might have an impact on limited ability to perform missions/business functions in the future, besides financial costs or sanctions due to non-compliance. Finally, there are also relational damages since trust between organisations is lost.

6.1.3 Lessons Learned

The introduction of new technologies in the supply chain, such as workflows linked to a permissioned blockchain, is also introduces new threats, for which an SME might not have carried out a risk assessment or has no know-how needed to deal with risk mitigation.

6.1.4 Roadmap Solutions

Managing the input and output of a manufacturing engineering, procurement and construction (EPC) organisation is very complex, and the security of the system controlling it is crucial. The current CyberSec4Europe roadmap for supply chain mentions different developments that would help protect the supply chain in the given scenario. While there are already many solutions for the provision of security and privacy for IT and OT infrastructures, networks and data storage, communications, solutions for real-time detection, penetration testing, software analysis tools, physical unclonable functions, etc., it is important for them to be appropriately combined to provide an adequate level of protection.

One of the most prominent solutions for the main problems associated with the present scenario is blockchain technology. The blockchain would serve to contain and exchange information of the supply chain-related events between involved parties. At the same time, it also provides traceability, accountability, and trust (especially when third-party certification is involved) between parties. A possibility of accountability mechanisms that would allow trusted third parties to review the workflow and resolve conflicts between entities in the supply chain is discussed.

For the proactive response to threats, lightweight distributed attack detection mechanisms and risk management play a key role. The automation of the latter or at least parts of it are a significant point in the supply chain roadmap. Emphasis is given to the automation of searching for the weakest points in the supply chain and the continuous vulnerability analysis processes that monitor the compliance and potential and/or existing security and privacy issues of supply chain processes. Here, because of the automated processing, compliance with regulations is explicitly voiced.

The roadmap identifies three long term solutions that are relevant to the given supply chain scenario. The first are the digitals twins and the self-healing mechanisms that would bring a continuous adaptation of different security aspects to the changing circumstances. The second goal is the communication between different blockchains and the execution of automated tasks (outside or inside various blockchains) to automatically monitor the state of a complex interconnected supply chain. The third major future step in securing the supply chain is the use of artificial intelligence and big data. This could be used to improve the threat intelligence gathering, and the consequent decision-making processes and response, as well as help automatically harden supply chain IT-OT infrastructures.

6.2 Scenario 2: On the Use of Smart Contract in a Supply Chain

Paperless trading is a promising means of dealing with the logistical challenges of cross-border trade and small shipments across borders. Another benefit is that it can help governments address growing physical security concerns about potential threats hidden in commercial packages. However, the current paperless trade policy frameworks introduce several cybersecurity risks, for example, in data authentication and security as well as data protection, retention, archiving, and sharing.

On the other hand, blockchain technology offers immutable records and it improves levels of trust and transparency in the trade ecosystem. It seems like a perfect solution for scenarios where parties have different views, and for providing support for conflict or dispute resolution.

In relation to cross-border trade and retail supply chain, we should also mention that on 1 January 2021 it became mandatory for all cross-border deliveries of commercial items to be digitally preregistered (electronic advance data – EAD) [35] [36] with the postal service in the destination country, prior to export of the commercial item from its country of origin.

Digitising goods deliveries also introduces new cybersecurity risks. EAD includes the name and address of the sender, recipient, their telephone number or email address, the number of items in the consignment, the total weight, the type of transaction (traded good, gift, etc.), postal fees, etc, which is also risk for data protection and privacy.

The pharmaceutical industry and in particular pharmacies, many of which are SMEs, are especially at risk. Fake and substandard medicines, as well as other medical products are a threat, but so is paperless trading for those ill-prepared or unprepared SMEs [37].

CyberSec4Europe deliverable D5.2 with a use case in the retail sector describes three examples of supply chain disputes, that can also apply to SME pharmacies. This use case presents a blockchain-based solution to solve disputes of any kind and deploys a smart contract designed to streamline the dispute process (so-called dispute smart contract (DSC)).

In existing supply chains, the retailer has limited visibility into the supply chain because

i) the enterprise resource planning (ERP) systems of the different stakeholders are siloed and incompatible with each other, and

ii) stakeholders are concerned about confidentiality, thus sharing little information. If there is a delay or error in the shipment, the retailer raises a dispute and a significant amount of time is spent on review, evidence gathering, negotiation and settlement.

A single view of documents is therefore a key requirement for improving trust and transparency in the cross-border trade process. It is important that any participant logging into the trading platform will get the same view (version, updates, and history) of the document as any other member of the network. We should note that this functionality can be achieved without using blockchain, but using a trust-minimised blockchain infrastructure, in which the nodes of the various participants are synchronised in real-time.

As all participants have the same view of the status of deliveries and transactions, participants can recognise delays faster and take remedial action without raising a dispute. If there is a dispute, then the process of review, evidence gathering, negotiation and settlement is also much faster.

However, the current regulative framework does not recognise smart contracts and blockchain transactions as legally binding, so there are also all kinds of solutions that might help in the transition to paperless trading by allowing the coexistence of traditional trading contracts and corresponding smart contracts running on the blockchain. Coexistence is achieved by automatically translating relevant trade terms and conditions specified in trading contracts to the corresponding logic implemented in smart contracts, and afterwards installing the resulting code on the peers of the blockchain network.

6.2.1 Potential Weaknesses and their Exploitation

Attacks such as the decentralised autonomous organisation (DAO) attack and the parity wallet are consequences of bugs in the smart contract code. The idea of generating (semi) automatic code generation from trading contracts reduces the cost of implementing smart contracts, but automatic translation might increase the chance of occurrence of unintended mistakes, bugs or security vulnerabilities. In essence, these types of incidents are similar to application security incidents, with vulnerabilities such as overflow, underflow, re-entrancy or dependence on timestamping or transaction ordering.

6.2.2 Impact on SME

A retail supply chain is very complex because it requires the participation of different stakeholders such as manufacturers, wholesalers, distributors, customers, information service providers, and in the case of some specific retail sectors, such as pharmacy, also regulatory agencies.

Processes that are under threat are inventory management, logistics and quality management, among others. Incidents related to paperless trading or established mechanisms for dispute resolution can also result in monetary loss, due to lengthy and costly legal actions. In the case of specific retail sectors, for example, pharmaceutical SMEs, they can also suffer reputation damage or inability to forecast accurately, which cab eventually cost human lives.

6.2.3 Lessons Learned

Many retail companies are well aware of supply chain risks, whether these are related to physical or to cyber incidents.

Most large pharmaceutical companies, for example, hold significant stocks to ensure their patients are protected from any type of unpredictable event, but for small pharmacies this is not the case. Many companies producing generic drugs may be dependent on a single provider. In addition, SME pharmacies do not have tools to understand and map global supply chain risk dependencies and exposures and are more vulnerable to any kind of disruption.

Paperless trade could be a potential bottleneck in supply chain management for SMEs and regulatory documentation can be particularly difficult for smaller businesses with less experience and resources. In contrast, solutions such as distributed ledger technology (DLT) and the introduction of smart contracts bring significant benefits for cross-border trade. A proper risk assessment should be done before the adoption of new technologies and when needed, preventive measures should apply. In addition, impersonation attacks, or other attacks on advanced electronic data, its integrity or accuracy, should trigger effective and efficient risk mitigation.

6.2.4 Roadmap Solutions

This retail case scenario combines the problems of trust between involved parties (i.e. stores, shipping companies, logistics and transport operators, insurers, and end customer) and securing information that is shared amongst them. The current CyberSec4Europe roadmap for supply chain discusses solutions that will or should be developed to protect the supply chain in the given scenario. As was the case for the previous scenario, there are already many solutions in the market that can provide a suitable security level for IT infrastructures and networks when combined appropriately.

The same as in the case of the first scenario, in this retail scenario, the integration of a blockchain solution into the supply chain to store and track the data of the shipped goods is an excellent solution to provide

- digitalisation, together with smart contracts recording, payment, (import) taxes, creating and signing a legal contract between parties, etc., can be done very quickly,
- the security of information – blockchain is a very secure and resilient technology also offering integrity and legitimacy of its content,
- trust without the need for a trusted central organization and
- a means of preventing counterfeiting – by recording a unique identifier of the shipped product, it becomes very difficult to replace it with a counterfeit during transport.

One of the goals for this environment is also to make different blockchains able to exchange data; for example, a blockchain that is used to track the materials among different manufacturers from the first scenario could communicate with the retail blockchain in this scenario, reducing possible vulnerabilities while the data is not secured by either of the blockchains. Again, accountability protocols build on top of blockchains could provide the means for a determinative and quick solution when a party in the process is in breach of the established rules/contract.

In a retail scenario, when dealing with consumers, there is a higher chance of processing personal data, which require special attention for the business to comply with various new regulations. As was the case in the first scenario, a self-healing system can help harden the security of the supply chain on many levels, from the privacy policies used to hardware configuration; for example, in case of a security incident (or any other difficulties) at one of the shipping companies the system automatically redistributes the goods to different distributors. Another big obstacle to overcome is implementing integrity and trust in the transition between the digital and physical worlds and the inherent problems when securing IoT. Finally, artificial intelligence and big data can also impact security in the circumstances of the scenario. With the strength of intelligence-gathering, these two technologies make automation and better decision making for the system's security (and other parts) much easier and more accurate.

7 Cybersecurity Recommendations

This section makes cybersecurity recommendations to the supply chain, which include both technical and non-technical measures. General recommendations are made in terms of IT security guidelines, relevant cybersecurity regulations/directives and standards, and cybersecurity tools. While CyberSec4Europe recommendations are derived from deliverables D4.1 and D4.3. Although the recommendations are made focusing on the potential risks and threats that may arise in the two scenarios from section 5, they are also applicable to supply chain security in general.

7.1 General IT Security Recommendations

- Cyber attacks are inevitable so be proactive by developing your defences on the premise that your systems will be breached [38]. Do not only focus on how to prevent a breach but also on how to mitigate an attacker's ability to exploit the successful attack and the consequent recovery from the breach. This includes having appropriate risk management and incident management strategies, monitoring to detect and quickly report and respond to incidents, abilities to collect information on a breach and assessing its impact, streamlined recovery processes from cyber attacks fast while keeping financial and reputational impact and damage to a minimum, etc.
- All data and systems are not equally vital to an organisation. With burgeoning vulnerabilities and finite resources for cybersecurity, protecting everything is not an option [39]. Identify and categorise cyber assets (infrastructures assets and data) that are critical and need protection. Define privileged access to the assets and assign permissions and rights depending on the user's (human

users as well as non-human users such as applications and machine identities) roles/tasks/attributes when it comes to accessing them; ensure everything works with the least privileges possible.

- Supply chains require suppliers and vendors to share communication channels for the exchange of the necessary information required to make the supply chain work. Unfortunately, this also causes an enlarged attack surface whereby attackers can use these connections to spread their poison across the supply chain. It is, therefore, a good idea to have specific service-level agreements on security with other entities in the supply chain and/or require continuous certification from them. Where possible, provide them with relevant guidelines on how to protect their connections to your organisation and their systems in general, and audit their compliance to ensure they are acting accordingly and are not a liability.
- It is often said that people are the weakest link in the protection of any system. It is important to remember that and continue to prevent such exploitation from happening. IT security systems will not secure an organisation's assets unless employees throughout the supply chain use secure cybersecurity practices [38]. The simplest and most basic recommendation is to make sure users/employees use unique, strong credentials, preferably together with multifactor authentication. Create written policies and frequently train and educate employees on security and on the most common attack strategies that target them (e.g. social engineering) and how to respond in such situations.
- Promote and incorporate privacy and security by design for a secure development process for both network and systems. Practice good software design principles to reduce inherent vulnerabilities in the code that can be leveraged by attackers to launch security attacks. This has also been recommended by deliverable D4.1 (p. 36).
- If you have not already done so, check out recommendations and guidelines by other organisations. A good start would be ENISA's recommendations and guidelines for emerging technologies and supply chains in ICT [40] [41], IoT [19] [42] [43], big data [26], cloud computing [44] and Industry 4.0 [45]. There are also other organisations that provide security guidelines and recommendations for emerging technologies, such as AI [22] [24], CPS [46] and Industry 4.0 [47]. Certainly, every guideline and recommendation may not be applicable to an organisation, or feasible for it to implement particularly for SMEs. But referencing them can provide an idea (free of cost) on the course of action the organisation has to take and accordingly align people, process and technology to improve its overall cybersecurity.
- Perform regular independent reviews and audits. These can be used to flush out vulnerabilities and weaknesses as well as bolster the consumers' trust in the organisation's supply chain and end products.

Cybersecurity defence can be expensive to implement, especially for SMEs. In such a situation, an organisation has to work on an effective strategy that can help it to achieve an acceptable level of protection against cyber attacks but at an affordable cost or at least within budget. These basic IT protection concept can potentially contribute to reducing cybersecurity cost.

- All data and systems in an organisation are not equally critical. This also implies that applying the same level of security control everywhere and equally in an organisation is a waste of resources, not forgetting that resources are finite and to have them allocated for cybersecurity, they have to compete with the aspects that are directly connected to the organisation's revenue generation [39]. More importantly, there is a risk that the most valuable digital assets that demand high-level protection will be left vulnerable while very necessary resources are allocated for the protection of less critical digital assets. Thus, there is a need for security threat and risk assessment to identify the most critical digital assets in the organisation, prioritise the remaining digital assets and accordingly set cybersecurity controls for them.

- An organisation could be subscribing to redundant or out-of-context data in the name of security, for example, a log source feed or threat intelligence feed. It should assess whether the collected data enables a better investigation or not and decide whether to collect it.
- Cybersecurity is not all about technology, but equally important elements are people and processes. This also means that organisations should not heavily invest only in technology solutions but also focus on educating and training employees and process improvement. In addition, increasing the number of technology solutions will make the cybersecurity complex requiring employees to spend more time on training. Further, if the technology solutions are from different vendors, they may create interoperability challenges. So, focusing on people and process improvement, eliminating duplicate tools and investing only in necessary technology solutions and considering single vendor solutions (if possible) may contribute to reducing cybersecurity costs.
- An organisation does not always have to depend on proprietary and expensive cybersecurity solutions. Many cybersecurity tools are open source, and available for free or at a nominal cost (some examples of such tools and things to consider when choosing them are in section 7.4). Similarly, organisations can utilise training and awareness resources that are available for free (several such resources have been elicited in the CyberSec4Europe deliverable report D9.11 [48]) to educate and train their employees.

7.2 Legal and Standards Recommendations

7.2.1 Legal Recommendations

In December 2020, the European Commission unveiled its new Cybersecurity Strategy to strengthen Europe's readiness against cyber threats, along with regulatory proposals to address cyber and physical resilience of critical entities and networks, which since 2018 has been the operational domain of the first directive on the security of network and information systems (NIS Directive)[1], published in 2015.

Despite the achievements of the NIS Directive, as a key driver to a new institutional and regulatory approach to cybersecurity in the Member States, it was generally recognised that, due to the rapid changes in the progress of the digital transformation of society and businesses as well as the greatly expanded threat of cyber attacks introducing new challenges, a revision was required – the so-called NIS 2.0, which is currently being negotiated.

This new directive is based on a risk-management approach, providing a list of basic security requirements and incident reporting obligations that must be applied by entities in the sectors to which they apply across the EU. The proposal introduces more precise provisions on the process for incident reporting, including the content of reports and timelines.

Among the significant changes being made are widening the scope of the law's application to additional industry sectors, strengthening the existing rules on security requirements and incident reporting, while also increasing the maximum fines that can be applied.

One of the significant aspects of the new cyber landscape is that any disruption in one entity or one sector can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative

[1] The NIS Cooperation Group was established by Article 11 of the 2016 NIS Directive to ensure strategic cooperation and the exchange of information among Member States in cybersecurity. Operationally, the Cooperation Group is supported by the CSIRTs.

impacts in the delivery of services across the whole internal market. As the *SolarWinds* incident has shown, a vulnerability in a small part of a global supply chain can stay under the radar for a long time, until it has endangered the whole chain. Risk management in the supply chain has therefore become a defining issue for the ICT industry and other sectors that are the top targets for cyber attacks, including healthcare, energy, banking, education and government. Although the scope of the revision to the NIS Directive is capped at medium and large enterprises, leaving Member States to identify and address SMEs with a high security risk profile, a cyber attack like *SolarWinds* takes no prisoners: it is totally indiscriminate in the damage it wreaks.

Amongst the proposed changes, the key sections impacting supply chains are under Chapter IV 'Cybersecurity risk management and reporting obligations' and Articles 18 and 19 in particular.

- **Article 18,** Cybersecurity risk management measures, asserts that

  > *Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.*

  The article goes on to identify a number of the measures referred to above, all of which are relevant in the context of supply chains, but specifically (d):

  > *supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services*

- **Article 19**, EU coordinated risk assessments of critical supply chains, states that the Cooperation Group together with the Commission and ENISA.

  > *… may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.*
  >
  > *The Commission, after consulting with the Cooperation Group and ENISA, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to.*

Hence, NIS 2.0 will require individual companies to address cybersecurity risks in supply chains and supplier relationships, emphasising supply chain risk management, demanding that the regulated entities assess the quality and the cybersecurity practices of their suppliers and service providers, especially big data companies and managed service providers, during their continued business relationship.

At the level of EU, the proposal will seek to strengthen supply chain cybersecurity for key ICT sectors. The Member States, in cooperation with the Commission and ENISA will carry out coordinated risk assessments of critical supply chains to track the threats of key services, systems and products used in each sector. European Computer Security Incident Response Teams (CSIRTs) are expected to facilitate coordinated vulnerability disclosure procedures, to improve information sharing between reporting entities and ICT vendors.

To what extent enterprises in the EU will comply with the NIS Directive could be a major concern. Infringement of EU directives and regulations occurs occasionally [49] and some common reasons found to be associated with their non-compliance are administrative shortcomings, interpretation problems and issue linkage [50]. SMEs are recommended to comply with the NIS directive by implementing a sector-specific cyber resilience programme. After all, this is necessary to access a market in other EU member states. In addition, EU legislation has been found to have positive effects on a wide range of SMEs except for its compliance costs which again tend to diminish as SMEs become more familiar with requirements [51] .

7.2.2 Standards Recommendations

Many standards have been developed in response to a changing landscape and the increased sophistication of cyber attacks in the supply chain. Some relevant International Organisation for Standardisation (ISO)/ International Electrotechnical Commission (IEC) standards that target supply chain security are listed in Table 1.

Standards	Target Group
Open Trusted Technology Provider Standard (O-TTPS), now known as ISO/IEC 20243-1:2018 [52]	The standard consists of a set of guidelines, requirements, and recommendations that address specific threats to the integrity of hardware and software commercial off-the-shelf (COTS) ICT products throughout the product life cycle. It focuses more on the physical supply chain, for example, mitigating the risk of counterfeit and tainted components.
ISO 28000 series [53]	The standard series specifies the requirements for a security management system particularly dealing with security assurance in the supply chain. The standard is applicable to all sizes of organisations and at any stage of the supply chain.
ISO/IEC 27036-1:2014 [54]	The standard provides guidance on information security within the context of third-party/supplier relationships. Supply chain attacks through third-party software or data storer have become an alarming issue so organisations must have visibility over their third-party software providers and data storers.
IEC 62443 [55]	The standard provides effective solutions (both technical and process-related) for industrial supply chains. This also incorporates security technologies for industrial automation and control systems.
ISO/TS 22318:2015 [56]	The standard gives guidelines for business continuity management (BCM) specifically focusing on the issues faced by an organisation in its supply chain continuity.
ISO/IEC 27001 [57]	The standard provides requirements for an information security management system (ISMS). The people part of ISO/IEC 27001 also covers information security awareness, education, and training. An ISMS includes and contributes to the examination and management of information security risks, including threats, vulnerabilities, as well as impact and likelihood of attacks and their mitigations. Most organisations can defend themselves by implementing an ISMS and other best practices, as described in ISO/IEC 27001.

Table 1: ISO/IEC standards for supply chain security

Obtaining standards certification can be initially expensive (though this cost is influenced by the size and complexity of the organisations), but in the long run, it brings many benefits to organisations, including to SMEs. In general, it will help organisations to reduce costs, increase productivity, and access to new markets [58]. To SMEs, it helps to, for example, build customer confidence, meet regulation requirements, reduce costs, gain market access [58], improve innovative capacity, and enhance competitiveness [59].

In terms of cybersecurity, for example, ISO/IEC 27001 will enable organisations comply with business, legal, contractual and regulatory requirements, and thus avoid costly penalties associated with non-compliance with laws and regulations, financial losses and reputational damages resulting from cyber attacks, and to reduce the need for frequent audits. For example, it is recommended to perform an ISO/IEC 27001 internal audit annually [60].

Organisations like Small Business Standards (SBS) and the European DIGITAL SME Alliance help with the standardisation efforts of the European SMEs. The SBS represents the interests of SMEs in the standardisation processes, raises SME awareness about standardisation, facilitates their uptake of standards and motivates them to engage in the standardisation processes [61]. Similarly, the European DIGITAL SME Alliance develops and promotes guides for the implementation of standards, for example, it developed the SME guide for the implementation of ISO/IEC 27001 on information security management [62].

Organisations can make use of standards like those described in Table 1 to build robust supply chains and protect them from harm. If possible, it is suggested to consider using open, non-proprietary (i.e., de jure standards develop in the absence of underlying technology, dominant or proprietary, needed for implementation) standards and certification programs such as those produced by the Open Trusted Technology Forum (OTTF) [63], which includes O-TTPS [64]. When appropriate, support and/or collaborate with standardisation bodies to develop standards for analysing, managing, and mitigating supply chain cybersecurity risks.

7.3 Security Recommendations Specifically Derived from CyberSec4Europe

CyberSec4Europe deliverable D4.1 (p.16-17) has pointed out two critical issues in the supply chain. First, there is a special need to adapt the emerging technologies (IT-OT) for the supply chain as well as mitigate the risks and threats they introduce. Second, threats are increasing significantly in number and severity. To address the potential challenges that may arise due to these critical issues, the deliverable recommends the following mitigations:

- To establish a dynamic risk assessment on the supplier side so that the supplier selection decision can be based on a systematic evaluation (both risk-based and business-driven).
- To add protection at all levels (at hardware, software, communication, and storage levels) and authentication using hardware security, cloud, and cryptography-based authentication methods.
- To propose reliable and dynamic event management mechanisms, prevention, and detection. A supply chain must be able to dynamically and accurately manage events and detect and prevent anomalous states in optimal times.
- To include assurance measures through verification and compliance with regulatory frameworks. A supply chain should comply with all the processes and regulations required for its good performance and security.
- To establish standardisation and certification measures, however, not enough standardisation and certification mechanisms are available for the emerging technologies.

- To make sure trustworthiness and resilience of operations and services are in acceptable states and at all times. This is possible if all elements are permanently connected and safe to preserve the integrity of the products or the service, and confidentiality and integrity of industrial data.
- To keep operational performance and establish measures that help control the complexity of the system to incorporate security measures and ensure the availability of processes, resources and data streams when they are demanded.
- To extend the technological and security culture within the supply chain operations specifically security specialists with knowledge and understanding of both the available technologies and the current policies are needed.
- To establish trust between suppliers and customers. Suppliers should be properly audited and protected by applying diverse control measures.

The same deliverable (p. 27-28) also recommends the supply chain to have the capabilities listed in Table 2.

Capability	Description
Traceability, procurement, and accountability	Transparency mechanisms in all operational processes.
Notification and multi-language management	Multi-language notification capacities to adequately inform about anomalous events or status.
Governance and assurance	Self-adaptive implementation of effective, harmonised, and lightweight security metrics, formal methods, and controls. Policies application according to security requirements, and design guidelines. Proofs of penetration testing, and interchangeable format support for methods and tools.
Standardisation and certification	Enforcement of standardisation, certification, and homologation tools and methods.
Resilience	Recovery measures 24/7 and working at optimal times.
Cyber crisis management	Readiness (24/7 monitoring), response (limit damage and losses), and recovery (returning to normal operation, assessing the causes, and disseminating lessons learned) [65].
Suitable hardware update	Hardware update to accommodate future software components.
Post-quantum cryptography	Preparation with cryptography for the quantum computing era.
Defensive tools	Tools to manage availability, integrity, and confidentiality of operations, services, and data; secure access; and unforeseen events or anomalous states.

Table 2: Capability required for the supply chain security

As non-technical measures, the deliverable makes the following recommendations:

- to define applicable policies and standards, and also explore those that are currently in use
- to implement standardisation and certification for new technologies that are being adopted (refer section 7.2.2)
- to embed redundant mechanism in integrated safety systems
- to utilise and implement freely available tools, for example, open source tools (refer section 7.4)
- to promote security awareness through reliable education and training programmes.

The deliverable (p. 28) recommends implementing and benefitting from the following technologies that will contribute to achieving the capabilities mentioned in Table 2:

- DLT for auditing and accountability mechanism allowing to establish responsibilities and transparency in the entire value chain,
- homomorphic cryptography for the option to perform computations on encrypted data (i.e., privacy-preserving during outsourced storage and computation) and help to set trust with providers,
- strong authentication using cryptographic-based advanced methods and authorisation systems using the principle of least privilege,
- Big data, ML and AI to extract pattern and identify abnormal behaviours,
- IoT applied to the area where standards and certification are not fully developed, e.g., to authenticate and track goods, and monitor storage, and
- lightweight formal techniques to ensure or prove a software obtained from other developers is secure against potential attacks.

The aforementioned recommendations may become valuable for large organisations, but they do not seem to consider the resource-constrained situation of SMEs. For example, expecting SMEs that may not have access to many current technologies to use post-quantum cryptography is an unrealistic recommendation. There are several other recommendations like using formal methods, homomorphic cryptography, and multi-language notification that may be infeasible (due to lack of expertise) or unaffordable for SMEs to apply.

The recommendation to use DLT (in D4.1) has been followed by the CyberSec4Europe deliverables D5.1 [66], D5.2 and D.5.3 [67]. These reports have demonstrated how a permissioned blockchain can be sought to streamline the supply chain processes and stakeholder activities and address security and privacy challenges that may arise in the supply chain due to the implementation of emerging technologies and IT/OT convergence. In order to do so, these reports have considered two use cases, which are: (1) supply chain for retail, and (2) compliance and accountability in distributed manufacturing.

Deliverable D5.1 has elicited the security and privacy requirements together with functional and non-functional requirements. Further, the same report has also analysed how using a blockchain could address the elicited privacy and security concerns. Similarly, deliverable D5.2 has presented the specifications for the two use cases essentially through a blockchain-based solution that deploys a smart contract to streamline the dispute processes in the supply chain. Finally, deliverable D5.3 has validated the requirements elicited and analysed in D5.1. It has particularly focused on those requirements that the fundamental properties of the underlying blockchain platform (i.e., Hyperledger Fabric) satisfy by design. In the supply chain for retail use case, the following requirements are validated: identity management and authentication, integrity, confidentiality and access control, fault tolerance and performance. Likewise, in compliance and accountability in distributed manufacturing use case, the following requirements are validated: identity management and authentication, integrity, anonymisation, non-repudiation, accountability, performance and fault tolerance.

A blockchain could provide several benefits like:

- digital audit trails,
- a platform to share, record, and track supply chain information,
- a distributed trust architecture for the supply chain, and
- reducing cost and time needed to handle disputes in the supply chain.

However, blockchain technology is not an optimal solution and has a number of **features that can create challenges** for supply chain organisations if it is implemented. Some prominent concerns are presented here.

- It is virtually impossible to change or delete data/information registered on a blockchain, i.e., the transaction is irreversible, though, in a private blockchain, the authorised organisation can delete or rewrite nodes. It means an organisation has to be exceptionally cautious to ensure that entered data is correct. Moreover, this contradicts the GDPR, mainly articles 16 and 17. Article 16 grants an individual with the *right to rectification*, i.e., the data subject has the right to ask the data controller for the rectification of inaccurate personal data concerning him or her. Likewise, article 17 empowers the data subject with the *right to erasure or be forgotten*, i.e., the data subject has the right to demand the data controller erase personal data concerning him or her under different stated circumstances.
- Once the data controller has shared data/information on a blockchain, it loses control over who processes the personal data and how. This may violate GDPR articles 6 (i.e., *lawfulness of processing*) and 7 (i.e., *conditions for consent*).
- A blockchain does not guarantee data protection outside its architecture. This also means the data still remains vulnerable to *endpoint security risks;* for example, due to unsafe user behaviour attackers may get access to the blockchain keys.
- There are several other challenges in the adoption of blockchain technology in supply chain management. S. Bag et al. [68] examined 15 selected barriers using data from SMEs in India. Their study found mostly non-technical reasons, for example, in overall "lack of management vision" and "cultural differences among supply chain partners" and for green supply chain management, "collaboration challenges" and "hesitation and workforce obsolescence" to be the most influential barriers in the adoption of blockchain technology. Another similar study is by S. Jabbar et al. [69], which investigated the challenges on the uptake of blockchain for supply chain management. This study found non-technical challenges like "lack of industry-wide standards and practices in the adoption of blockchain" and "lack of support for various ERP solutions by blockchain" to be the critical barriers. Similarly, "lack of interoperability standards between different vendors' blockchain" to be a major impediment to its wider adoption.

Therefore, to address the aforementioned problems related to blockchain technology, organisations can do the followings:

- First and foremost, organisations must need to know and separate the blockchain hope from the hype. Blockchain technology presents a number of complex challenges like interoperability and scalability issues that must be overcome before it can truly deliver on its promises [70]. So, organisations must establish that using blockchain will improve their supply chain management. In addition, they possess the needful resources to implement this technology correctly and efficiently for their purposes.
- Organisations should perform a risk assessment of the data/information and accordingly classify it. It should share only that data/information about which they are confident that sharing will not infringe any directives, regulations and laws. If there exists even the slightest doubt, it is suggested avoiding sharing that data/information.

- Organisations must ensure that proper mechanisms are in place to prevent incorrect data from being written onto the blockchain.
- Organisations must address endpoint security risks, primarily to safeguard against human errors, negligence, and vulnerabilities so that attackers could not steal or get access to blockchain keys. Some potential measures include not writing the blockchain keys in files or sharing via email, regularly updating anti-virus software and performing device scan, and raising cybersecurity awareness of employees.
- Adopting the below mentioned standards could potentially mitigate challenges like a lack of industry-wide standards and practices and interoperability:
    - The standardisation sector of International Telecommunication Union Telecommunication Standardisation Sector (ITU-T) Focus Group on Application of Distributed Ledger Technology (FG DLT) [71] has published guidelines outlining specifications, use-cases (include several use cases of supply chain), regulations, and standards for DLT. These guidelines provide a clear view on how DLT and blockchain could best be applied.
    - ISO/TC 307 [72] is a standard for blockchain and DLT that is in development. The standard will cover security and privacy specifications in the operation of different applications of blockchain and DLT that include supply chain and smart contract.
- Regarding other non-technical challenges, they are related to management and could be mitigated presumably by raising the awareness of managers and decision-makers on the benefits of blockchain technology and how they can contribute to its efficient adoption.

The aforementioned challenges to the supply chain are equally applicable to SMEs' supply chains. In addition, there are also other challenges to the diffusion of blockchain technology among SMEs, for example, low awareness of salient features of blockchain, and lack of access to digital infrastructures [73]. Unless these challenges are addressed, a border adoption of blockchain technology by SMEs will remain uncertain.

7.4 Tools Recommendations

Technology is an important pillar of supply chain cybersecurity. But acquiring up-to-date cybersecurity tools and technologies can be expensive. Therefore, organisations are suggested, particularly SMEs, to benefit from those tools and technologies that are open source and available free to use or for a nominal cost, if possible. A similar recommendation had also been made by CyberSec4Europe deliverable D4.1 (p. 20).

A simple web search can provide lists of various cybersecurity software that are available free to use. A few examples of such tools resulted from our search are [74]:

- *Networking and operating system hardening*: OpenVPN (VPN solutions), ModSecurity (Firewall application), and SafePad (Encrypted text editor).
- *Internet security*: AdBlocker (filters annoying ads), CheckShortURL (checks where shortened URLs are taking), and NoScript (prevents from falling for cross-site scripting and other types of script web attacks).
- *Email security:* SPAMfighter (spam filtering), Spamihilator (spam filtering), and SpamBully (spam filtering).
- *Password management, recovery, and attack tools*: LastPass (password manager), KeePass (password manager), and Ophcrack (password cracker).
- *Vulnerability scanning tools*: Burp Suite (vulnerability scanner), Nessus (vulnerability scanner), and Malwarebytes (Anti-malware software).

- *Networking and security auditing tools*: NMAP (network scanner), ZENMAP (network scanner), and HPing (TCP/IP packet assembler/analyser)
- *Cybersecurity framework and operating systems:* Kali Linux (offer a variety of free cybersecurity and penetration testing utilities), Qubes (security-focused desktop operating system), and Metasploit Framework (penetrating testing framework).

Tools for Internet security, email security, system hardening, and password management can be useful for protecting IT/OT infrastructures and networks, and employees against common attacks like phishing, malware attacks, and data breaches. Then, scanning, auditing, and testing tools can be used for penetrating testing and software analysis. As a matter of fact, deliverable D4.3 (p.65) has presented in its 12-month plan to apply or adapt such security tools for supply chain security.

Similarly, there are various EU projects that offer cybersecurity tools for free. A few examples are mentioned in Table 3. They are mainly cybersecurity self-assessment tools for organisations, particularly focusing on SMEs. Such tools are helpful to identify and learn about cyber risks, exploits and vulnerabilities in an organisation. This information is valuable in the development of any organisation's cybersecurity strategy, policies and procedures.

EU Projects	Tools Offered
Cyberwatching.eu [75]	It offers the following cybersecurity self-assessment tools for organisations, particularly focusing on SMEs: • GDPR Temperature Tool • Cybersecurity Self Assessment for SMEs • Cyberwatching Information Notice Tool • Cyberwatching Cyber Risk Temperature Tool
SMESEC [76]	It offers Cybersecurity Self Assessment tool for SMEs.
GEIGER [77]	It plans to offer GEIGER cybersecurity counter, a solution that can be used on the web or smartphone to dynamically show the level of current risks for a company and is targeted at SMEs.
CyberSec4Europe [78]	Work package (Deliverable D3.4) plans to offer tools to support elicitation and representation of assets, security requirements and threats. Work package 7 (Deliverable D7.2) offers Cyber Sandbox Creator, a tool for creating open-source and lightweight virtual labs for cybersecurity education, testing and certification and is aimed at individuals and SMEs.

Table 3: Cybersecurity tools from EU Projects

However, when selecting and deciding on an appropriate free and open-source tool, along with its usefulness (i.e. how much it meets the need) organisations must also examine aspects like the quality of documentation it has, the complexity and expertise needed to implement and use it, at what phase in the open-source life cycle it sits and others. It is advisable to choose mature tools with proper documentation and support, better usability, and an active feedback community.

7.5 Recommendations to the EU

The sections on methods, mechanisms and tools in the research and development roadmap (latest in D4.3; Section 7 in each of the verticals e.g. Section 4.7 for Supply Chain) contain different solutions (including those being developed in CyberSec4Europe) relevant to solving some of the important challenges discussed in different verticals. Those presented in the supply chain vertical are the most directly connected with the two scenarios described in section 5, although solutions from the other verticals could also be applied to securing supply chains. The most important approaches and measures for the two scenarios are provided in Table 4. The recommendations are targeted to EU-funded research projects investigating cybersecurity for supply chain and their SMEs participants.

Approaches	Measures
Risk management methodologies and frameworks	Identifying, assessing, and mitigating specific risks during the entire life cycle of a system. This section includes GDPR considerations.
Distributed detection, continuous monitoring and incident management	Provide measures that allow the underlying system to detect and respond before major disruptions arise within the system.
Traceability, shared data spaces	Traceability of goods in a supply chain is of great importance for multiple reasons (e.g. scheduling production, theft/counterfeiting prevention, logistics, etc.). With Industry 4.0, shared data space is a necessity for efficient operation between organisations; however, this brings the problems of confidentiality and unauthorised usage. The main proposed solution here is the use of blockchain.
Privacy preservation in blockchain	Associated research would allow integration and interaction of new partners in a complex supply chain.
Password-less authentication	Advanced authentication mechanisms are necessary to prevent impersonation attack/identity theft (which could lead to leaked trade secrets, slowed production if the attacker escalates the attack on the system or if they disrupt the supply chain, etc.).
Identity management solutions for the IoT	Supply chains include (or have the potential to include) a lot of IoT devices, protection of which has always been challenging. This section tackles the problems of authentication in such an environment.
Security tools	Similar to some previous solutions, it contains strong and privacy-preserving authentication mechanisms
Privacy-preserving assets	When sharing data between different organisations in a supply chain, sometimes depending on the data, anonymisation of the data could be important to preserve competitive advantage or customer information.

Unlinkability and minimal disclosure	This is especially important when personal data is involved (e.g. retail) because its security and user's privacy is an essential responsibility (especially with the new regulations).

Table 4: Recommendations from roadmap deliverable D4.3

8 Next Steps

For the next deliverable (D9.25), we plan to investigate real-world cyber-attacks on a number of supply chains spanning different vertical sectors and countries as well as comparing and contrasting with the recommendations made in this report.

9 References

[1] C. Hopping, "What is the supply chain?," ITPro, https://www.itpro.co.uk/strategy/28710/what-is-the-supply-chain-1

[2] M. Christopher, Logistics and Supply Chain Management: Strategies for Reducing Cost and Improving Service, London, UK: Pearson Education, 1998.

[3] J. Hintsa et al., "Supply chain security management: An overview," *Internationa Journal of Logistics System and Management*, Bd. 5, Nr. 3-4, p. 344–355, 2009.

[4] E. McGarrell & D. Closs, "Enhancing security through the supply chain," IBM Center for the Business of Government, April 2004.

[5] Symantec, "Internet Security Threat Report Volume 24," https://docs.broadcom.com/doc/istr-24-2019-en

[6] D. Clark, "Number of small and medium-sized enterprises (SMEs) the European Union in 2018," https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/#:~:text=Number%20of%20small%20and%20medium,the%20European%20Union%20in%202018&text=There%20were%20estimated%20to%20be,employed%20fewer%20than%20nine%20people

[7] E. Markatos et al., "D4.3 Research and development roadmap 1," Cyber Security for Europe, https://cybersec4europe.eu/wp-content/uploads/2020/09/D4.3-Roadmap-v5-NEW.pdf

[8] A. Sforzin et al. "D5.2 Specification and Set-up Demonstration case Phase 1," Cyber Security for Europe, https://cybersec4europe.eu/wp-content/uploads/2020/05/D5.2-Specification-and-Set-up-of-Demonstration-Case-Phase-1-v1.0_Submitted.pdf

[9] G. Loukas, Cyber-Physical Attacks: A Growing Invisible Threat, Oxford, UK: Butterworth-Heinemann, 2015.

[10] DHL, "Self-Driving Vehicles," https://www.dhl.com/global-en/home/insights-and-innovation/thought-leadership/trend-reports/self-driving-vehicles.html

[11] D. Alickaj & P. Bowhay, "Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risks," Businesswire, San Francisco, CA, USA, 15 November 2018.

[12] GDPR.EU, "GDPR small business survey: Insight from Euopean small business leaders one year into the General Data Protection Regulation," GDPR.EU, https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf

[13] J Mohan et al., "Analyzing GDPR compliance through the lens of privacy policy," in *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*, Springer, Cham, October 2019, p. 82–95.

[14] KPMG, "The GDPR: Are you ready for the road ahead?," KPMG, Ireland, 25 May 2018.

[15] C. Adams, "Impersonation Attack," in *H. C. A. van Tilborg (ed.) Encyclopedia of Cryptography and Security*, Boston, MA, https://doi.org/10.1007/0-387-23483-7_196, Springer, 2005.

[16] D. Young et al., "Supply Chain Impersonation: Just Another Tool in a Threat Actor's Bag," FireEye, https://www.fireeye.com/blog/products-and-services/2019/10/supply-chain-impersonation-another-tool-in-threat-actor-bag.html#:~:text=Supply%20Chain%20Impersonation%3A%20Just%20Another%20Tool%20in%20a%20Threat%20Actor's%20Bag,-October%2021%2C%20201

[17] BlueGrace Logistics, "Identity theft is on the rise, and cargo theft might not be far behind," https://blog.mybluegrace.com/bluegrace-logistics/identity-theft-is-on-the-rise-and-cargo-theft-might-not-be-far-behind/

[18] E. Markatos et al., "D4.4 Research and development roadmap 2," Cyber Security for Europe, https://cybersec4europe.eu/wp-content/uploads/2021/02/D4.4-Research-and-Development-Roadmap-2-v3.0-submitted.pdf.

[19] ENISA, "Good Practices for Security of Internet of Things: In the context of Smart Manufacturing," https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

[20] Kaspersky, "Threat landscape for industrial automation systems," https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf

[21] ENISA, "Cloud Security Guide for SMEs: Cloud computing security risks and opportunities for SMEs," https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

[22] M. Comiter, "Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It," Harvard Kennedy School, Belfer Center for Science and International Affairs, https://www.belfercenter.org/publication/AttackingAI

[23] S. Herpig, "Securing Artificial Intelligence-Part 1: The attack surface of machine learning and its implications," https://www.stiftung-nv.de/sites/default/files/securing_artificial_intelligence.pdf.

[24] T. Jacobs, "Artificial Intelligence (AI) in Supply Chain & Logistics Supply," Throughput Inc., https://throughput.world/blog/topic/ai-in-supply-chain-and-logistics/#:~:text=AI%20in%20Supply%20Chain%20can%20help%20in%20Optimization&text=Today%2C%20AI%20can%20seed%20in,manual%20tasks%20can%20be%20automated

[25] ERP Solutions oodles, "Benefits of Using Big Data in Supply Chain Management," https://erpsolutionsoodles.medium.com/benefits-of-using-big-data-in-supply-chain-management-1bcc1f6c915f#:~:text=Big%20data%20analytics%20is%20playing,in%20improving%20supply%20chain%20management.&text=Analytics%20reports%20enable%20decision%2Dmakers,cost

[26] ENISA, "Big Data Security: Good Practices and Recommendations on the Security of Big Data Systems," https://www.enisa.europa.eu/publications/big-data-security

[27] Deloitte, "Utilizing virtual reality to drive supply chain innovation," https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-cons-utilizing-virtual-reality-to-drive-supply-chain-innovation.pdf

[28] ENISA, "ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected," https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

[29] ENISA, "Looking into the crystal ball: A report on emerging technologies and security challenges," https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball.

[30] Accenture, "2020 Cyber Threatscape Report," https://www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf

[31] Kaspersky, "Threat landscape for industrial automation systems," https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf

[32] European Union, "Directive 2006/42 of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/ec (recast)," *Official Journal of the European Union,* Bd. 9.6.2006, pp. 24-86, 2006.

[33] E. Conway, N. Luu and E. Shaffer, "Best Practices in Cyber Supply Chain Risk Management: Managing supply chain risks end-to-end," NIST, 2015,

https://www.nist.gov/system/files/documents/itl/csd/NIST_USRP-Cisco-Cyber-SCRM-Case-Study.pdf

[34] K. Stouffer et al., "Cybersecurity Framework Manufacturing Profile 8183," NIST, https://csrc.nist.gov/publications/detail/nistir/8183/rev-1/final

[35] Universal Postal Union, "WCO–UPU Guidelines on the Exchange of Electronic Advance Data (EAD) between Designated Operators and Customs Administrations," http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/up

[36] International Air Transport Association, "IATA Guidance Material on EU-ICS2: MAIL Electronic Advance Data (EAD) Filing," https://www.iata.org/contentassets/15ee3a255dc447b886d9a7e91fa65dbe/position-paper-on-mail-ead-filing-eu-ic

[37] A. Moosivand , A. Rajabzadeh Ghatari, and H.R. Rasekh, "*Supply Chain Challenges in Pharmaceutical Manufacturing Companies: Using Qualitative System Dynamics Methodology*," Iranian Journal of Pharmaceutical Research, 01 Jan 2019, 18(2):1103-1116.

[38] NIST, "Best Practices in Cyber Supply Chain Risk Management," https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

[39] P. Kaminski et al., "Protecting your critical digital assets: Not all systems and data are created equal," McKinsey & Company, https://www.mckinsey.com/business-functions/risk/our-insights/protecting-your-critical-digital-assets-not-all-systems-and-data-are-created-equal

[40] C. Karsberg & M. Dekker, "*Secure ICT Procurement in Electronic Communications*," https://www.enisa.europa.eu/publications/secure-ict-procurement-in-electronic-communications

[41] S S. Cadzow et al., "Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward (2015)," https://www.enisa.europa.eu/publications/sci-2015

[42] ENISA, "Baseline Security Recommendations for IoT: In the context of Critical Information Infrastructures," https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[43] C. Skouloudi et al., "Guidelines for Securing the Internet of Things: Secure supply chain for IoT," ENISA, https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things.

[44] M.A.C. Dekker & D. Liveri, "Cloud Security Guide for SMEs: Cloud computing security risks and opportunities for SMEs," ENISA, https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

[45] ENISA, "Industry 4.0 - Cybersecurity Challenges and Recommendations," https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations/.

[46] J.A. Yaacoub et al. "Cyber-physical systems security: Limitations, issues and future trends," *Microprocessor Microsyst,* Bd. 77, Nr. 103201, Sep 2020 .

[47] S. Livingston et al. " Managing cyber risks in the electric power sector: Emerging threats to supply chain and industrial control systems," https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cybe

[48] S. Chaudhary et al. " SME cybersecurity awareness program 2,“ CyberSec4Europe, https://cybersec4europe.eu/wp-content/uploads/2021/05/D9.11-SME-cybersecurity-awareness-program-2-FINAL-submitted-1.pdf.

[49] European Commission, "Infringement decisions," https://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/index.cfm?lang_code=EN&typeOfSearch=false&active_only=0&noncom=0&r_dossier=&decision_date_from=&decision_date_to=&EM=MT&title=&submit=Sear“.

[50] G. Falkner et al., "Non-Compliance with EU Directives in the Member States: Opposition through the Backdoor?," *West European Politics,* Bd. 27, Nr. 3, pp. 452-473, 2004.

[51] European Commission, "Cost of the Cumulative Effects of Compliance with EU Law for SMEs," file:///C:/Users/sunilc/Downloads/final-report_en.pdf.

[52] ISO/IEC, "ISO/IEC 20243-1:2018 -Information technology - Open Trusted Technology ProviderTM Standard (O-TTPS)- Mitigating maliciously tainted and counterfeit products- Part 1: Requirements and recommendations," https://www.iso.org/standard/74399.html

[53] ISO, "ISO 28000 series- Specification for security management systems for the supply chain," https://www.iso.org/standard/44641.html

[54] ISO/IEC, "ISO/IEC 27036-1:2014- Information technology - Security techniques- Information security for supplier relationships - Part 1: Overview and concepts," https://www.iso.org/standard/59648.html

[55] IEC, "IEC 62443- Industrial communication networks – Network and system security –Part 2-1: Establishing an industrial automation and control system security program," https://webstore.iec.ch/preview/info_iec62443-2-1%7Bed1.0%7Den.pdf

[56] ISO/TS, "ISO/TS 22318:2015- Societal security- Business continuity management systems - Guidelines for supply chain continuity," https://www.iso.org/standard/65336.html#:~:text=ISO%2FTS%2022318%3A2015%20gives,the%20management%20of%20supplier%20relationships

[57] ISO/IEC, "ISO/IEC 27001- Information Security Management," https://www.iso.org/isoiec-27001-information-security.html

[58] ISO, "ISO and Small and Medium Enterprises," https://www.iso.org/iso-and-smes.html#:~:text=ISO%20International%20Standards%20help%20businesses,requirements%2C%20at%20a%20lower%20cost

[59] European Commission, "Standardisation and SMEs," https://ec.europa.eu/growth/smes/sme-strategy/access-to-markets/standardisation_en#:~:text=Standardisation%20brings%20many%20benefits%20to,capacity%2C%20and%20enhance%20their%20competitiveness

[60] L. Irwin, "How to conduct an ISO 27001 internal audit," IT Governance, https://www.itgovernance.co.uk/blog/how-to-conduct-an-iso-27001-internal-audit#:~:text=Experts%20recommend%20carrying%20out%20an,least%20once%20every%20three%20years..

[61] Small Business Standards, "The Voice of European SMEs in Standardisation," https://www.sbs-sme.eu/standards/what-standard.

[62] J. Bieliauskaite, "New SME Guide on Information Security Management: the standard ISO27001 made easy for SMEs," European Digital SME Alliance, https://www.digitalsme.eu/new-sbs-guide-information-security-management-standard-iso27001-made-easy-smes/

[63] The Open Group, "The Open Trusted Technology Forum (OTTF)," https://www.opengroup.org/forum/trusted-technology-forum

[64] The Open Group, "Developing Open Standards and Certification Programs to Help Assure Product Integrity and Global Supply Chain Security," https://www.opengroup.org/membership/forums/trusted-technology-forum/trusted

[65] Deloitte, "Cyber Crisis Management," https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/cyber-crisis-management.html

[66] A. Sforzin et al., "D5.1 Requirements Analysis of Demonstration Cases Phase1," CyberSec4Europe, https://cybersec4europe.eu/wp-content/uploads/2020/06/D5.1-Requirements-Analysis-of-Demonstration-Cases-Phase-1-v3.0.pdf

[67] A. Sforzin et al. "D5.3 – Validation of Demonstration Case Phase 1," CyberSec4Europe, https://cybersec4europe.eu/wp-content/uploads/2021/02/D5.3-Validation-Demonstration-Case-Phase-1-v1.0-submitted.pdf

[68] S. Bag et al., "Barriers to adoption of blockchain technology in green supply chain management," *Journal of Global Operations and Strategic Sourcing,* Bd. 14, Nr. 1, pp. 104-133, 2021..

[69] S. Jabbar et al., "Blockchain-enabled supply chain: analysis, challenges, and future directions," *Multimedia Systems*, Bd. Special Issues, 2020.

[70] G. Volpicelli, "Does blockchain offer hype or hope?," The Guardian, https://www.theguardian.com/technology/2018/mar/10/blockchain-music-imogen-heap-provenance-finance-voting-amir-taaki

[71] ITU-T, " Focus Group on Application of Distributed Ledger Technology," https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx

[72] ISO, "Strategic Business Plan ISO/TC 307," https://isotc.iso.org/livelink/livelink/fetch/2000/2122/687806/ISO_TC_307__Blockchain_and_distributed_ledger_technologies_.pdf?nodeid=19772644&vernum=-2

[73] OECD Library, "How can Blockchain ecosystems serve SMEs?," https://www.oecd-ilibrary.org/sites/18ac5acb-en/index.html?itemId=/content/component/18ac5acb-en#:~:text=Blockchain%20technologies%20present%20distinct%20opportunities%20for%20SMEs%20and%20start%2Dups.&text=SMEs%20and%20new%20firms%20can,driven%20innovati

[74] B. Subramanian, "An Overview List of Free Cybersecurity Tools," DataScience Foundation, https://datascience.foundation/sciencewhitepaper/an-overview-list-of-free-cybersecurity-tools, 01 December 2019.

[75] Cyberwatching.eu, https://cyberwatching.eu/.

[76] SMESEC, https://www.smesec.eu/index.html.

[77] GEIGER, https://project.cyber-geiger.eu/.

[78] CyberSec4Europe, https://cybersec4europe.eu/.