Strengthening the UK's Supply Chains

Recommendations on Cybersecurity and Traceability

About the collaboration

This project highlights the necessity for the UK to develop supply chain tracking solutions tailored to its specific context. Addressing key challenges such as creating UK-specific guidelines, providing support for small businesses, ensuring robust data security, clarifying technical standards, and promoting international collaboration will be essential for the success of these initiatives.

By leveraging emerging technologies, such as blockchain and Artificial Intelligence (AI), the UK can significantly enhance supply chain management. These technologies offer improved transparency, security, and efficiency, which are critical in building a resilient supply chain. Proactively addressing these challenges and embracing innovation will help the UK establish a secure and trustworthy supply chain ecosystem, fostering economic growth in an increasingly interconnected world.

About the Centre for the South

This project was funded by the Centre for the South (CftS), a policy institute founded under the University of Southampton.

The CftS uses equitable approaches to stimulate cross-sector collaboration across the Central South, mobilising knowledge and using evidence to drive more informed place-based decision making, for mutual prosperity.

Find out more
www.centreforthesouth.co.uk

Thank you

This project was funded and supported by the University of Southampton New Things Fund Scheme.

References

Gokkaya, B., Karafili, E., Aniello, L. and Halak, B. (2024), "Global supply chains security: a comparative analysis of emerging threats and traceability solutions", Benchmarking: An International Journal. **https://doi.org/10.1108/BIJ-08-2023-0535**

National Institute of Standards and Technology (2024), "Supply Chain Traceability: Manufacturing Meta-Framework", NIST Internal Report 8536. U.S. Department of Commerce. **https://doi.org/10.6028/NIST.IR.8536.ipd**

National Institute of Standards and Technology (2023), "Supply Chain Traceability Recommendations", Draft version 5, May 14, 2023.

Researchers

Dr Erisa Karafili Associate Professor in Cybersecurity, School of Electronics and Computer Science, University of Southampton, UK. **e.karafili@soton.ac.uk**

Betul Gokkaya PhD Candidate, School of Electronics and Computer Science, University of Southampton, UK. **betul.gokkaya@soton.ac.uk**

Context

Supply chains play a key role in modern economies by ensuring goods and services are delivered reliably to the citizens. However, supply chains are vulnerable to cyber-attacks, disruptions, and inefficiencies, which have serious, far-reaching consequences. When supply chains fail, it is not just businesses that suffer, essential services can be delayed, consumer safety can be compromised, and economic stability is threatened. A single collapse in supply chains can lead to inflated prices and shortages and it has a vast economic impact, for example only the global supply chain management software market is expected to reach nearly $31 billion by 2026.

Cyber-attacks targeting supply chains have been on the rise, causing major disruptions to operations and sometimes also physical harm. These attacks can disrupt the tracking of goods, causing delays and a loss of consumer trust, and further consequences including improper allocation of resources and financial losses. Some other disruptions caused by cyber-attacks are as follows:

- **Operational shutdowns** In 2024 64% of manufacturing and production organizations reported experiencing cyber-attacks that disrupted operations, up from 56% in 2023 and 55% in 2022. This marks a 41% increase since 2020, signaling a *growing threat to supply chain stability*.
- **Seaport disruptions** Major global seaports have been crippled by cyber-attacks, halting cargo operations and causing widespread delays. For example, Maersk experienced a cyber-attack that took down IT systems across its global terminals. These disruptions rippled across global supply chains, delaying shipments and trade routes.
- **Equipment failures** Cyber-attacks have led to dangerous malfunctions in industrial machinery, where digital threats caused significant physical harm to industrial infrastructure.

SUPPLY CHAINS' TRACEABILITY

In the UK, there is ongoing progress toward enhancing product traceability, particularly in sectors like food and pharmaceuticals. However, there is no fully standardized or comprehensive system covering all industries. While advanced technologies such as blockchain and digital traceability platforms are increasingly adopted to improve transparency, gaps remain in achieving universal traceability across diverse supply chains. These challenges highlight the need for further alignment between government initiatives and industry standards to better protect supply chains from cyber-attacks and security breaches.

HIGHLIGHTS

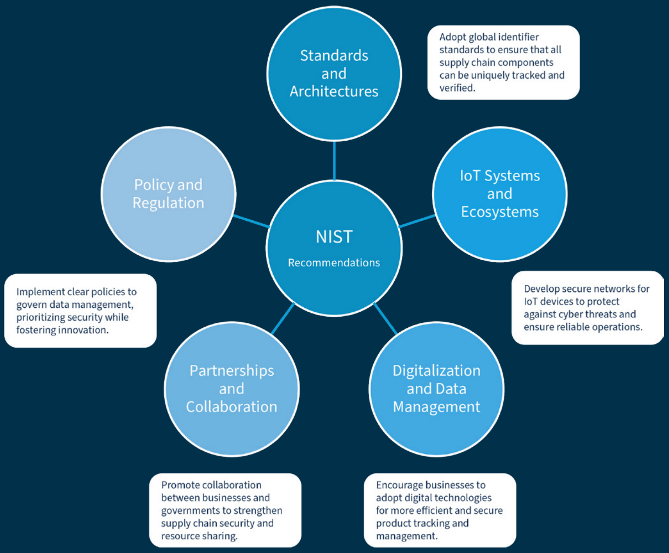
→ **Need for UK-Specific Standards:** There is a significant gap in UK-specific regulations and standards for product traceability, which are essential to promoting a *secure* and *transparent* supply chain environment.

→ **Challenges for Small Businesses:** Small and medium-sized enterprises (SMEs and MEs) in the UK face difficulties in adopting complex traceability systems without simplified solutions and targeted support.

→ **Data Privacy and Security Risks:** Insufficient attention to data privacy and security within existing frameworks leaves UK supply chains exposed to potential breaches and vulnerabilities.

→ **Limited International Collaboration:** There is a lack of clear strategies for international collaboration, which is crucial for UK businesses that rely on global supply chains.

Figure 1: An extraction of recommendations from NIST


Standards and Architectures
Policy and Regulation
NIST Recommendations
IoT Systems and Ecosystems
Partnerships and Collaboration
Digitalization and Data Management

Adopt global identifier standards to ensure that all supply chain components can be uniquely tracked and verified.

Implement clear policies to govern data management, prioritizing security while fostering innovation.

Develop secure networks for IoT devices to protect against cyber threats and ensure reliable operations.

Promote collaboration between businesses and governments to strengthen supply chain security and resource sharing.

Encourage businesses to adopt digital technologies for more efficient and secure product tracking and management.

CURRENT GUIDELINES FOR SUPPLY CHAINS SECURITY

Supply chain traceability is essential to ensuring both security and transparency across industries. While the National Institute of Standards and Technology (NIST) Act - Supply Chain Traceability Recommendations provides valuable guidance for developing tracking systems, it does not fully resolve all challenges. The NIST guidelines offer a foundational framework especially for improving supply chain visibility and security, but our analysis identified several gaps, particularly in UK-specific customization and the needs of small businesses.

Findings

We identified the following gaps and challenges that are not addressed by the current UK and NIST guidelines.

NEED FOR UK-SPECIFIC STANDARDS

There is a lack of UK-Specific Customization and Standards. While the NIST guidelines provide a strong foundation for supply chain traceability, they are not tailored to the unique needs of UK businesses. There is a need for UK-specific regulations and customized solutions that address the country's distinct challenges, offering clear guidelines and support for the implementation of appropriate technologies to ensure secure and transparent supply chains.

CHALLENGES FOR SMALL BUSINESSES

The NIST guidelines may not adequately support small businesses, which often face unique challenges in adopting complex traceability systems. Without specific guidance or resources, small firms may struggle with the implementation of these solutions.

INSUFFICIENT FOCUS ON DATA PRIVACY AND SECURITY

Data privacy and security concerns are not given enough attention in the guidelines, leaving sensitive supply chain information at risk. This creates vulnerabilities that could undermine the overall effectiveness of the traceability framework.

AMBIGUITY IN "TRUSTED ARCHITECTURES"

The guidelines provide an unclear definition of "trusted architectures," and the lack of detailed technical guidance hampers the practical implementation of secure systems.

LIMITED SUPPORT FOR INTERNATIONAL COLLABORATION AND LEGACY SYSTEMS

The guidelines offer only a preliminary approach to international collaboration and fail to provide strategies for integrating legacy systems. This further complicates the implementation of supply chain traceability measures in the UK.

CHALLENGES WITH IoT DEVICES

The NIST guidelines do not fully address the diversity and scalability of Internet of Things (IoT) devices, nor do they provide sufficient guidance on managing the lifecycle of these devices. This limitation obstructs the effective use of IoT technologies in supply chain traceability.

LACK OF INCENTIVES FOR IoT ECOSYSTEM ADOPTION

The absence of clear incentives for businesses to adopt trusted IoT ecosystems may slow down widespread adoption and affect the long-term sustainability of the proposed solutions.

Recommendations

We provide the following recommendations to address the identified gaps in supply chain traceability and promote UK business security by ensuring product authenticity and security. We believe that it is crucial for the UK to implement the following recommendations in order to establish a strong and resilient supply chain ecosystem that promotes trust, transparency, and security in an increasingly interconnected and technology- driven world.

1. Develop UK-specific guidelines and standards: Create clear and actionable guidelines tailored to the UK's unique regulatory environment and industry landscape. These guidelines should explicitly identify the technologies and methods required to track every movement of a product at each step of its journey, encompassing all suppliers involved in its production, from raw materials to the end customer.

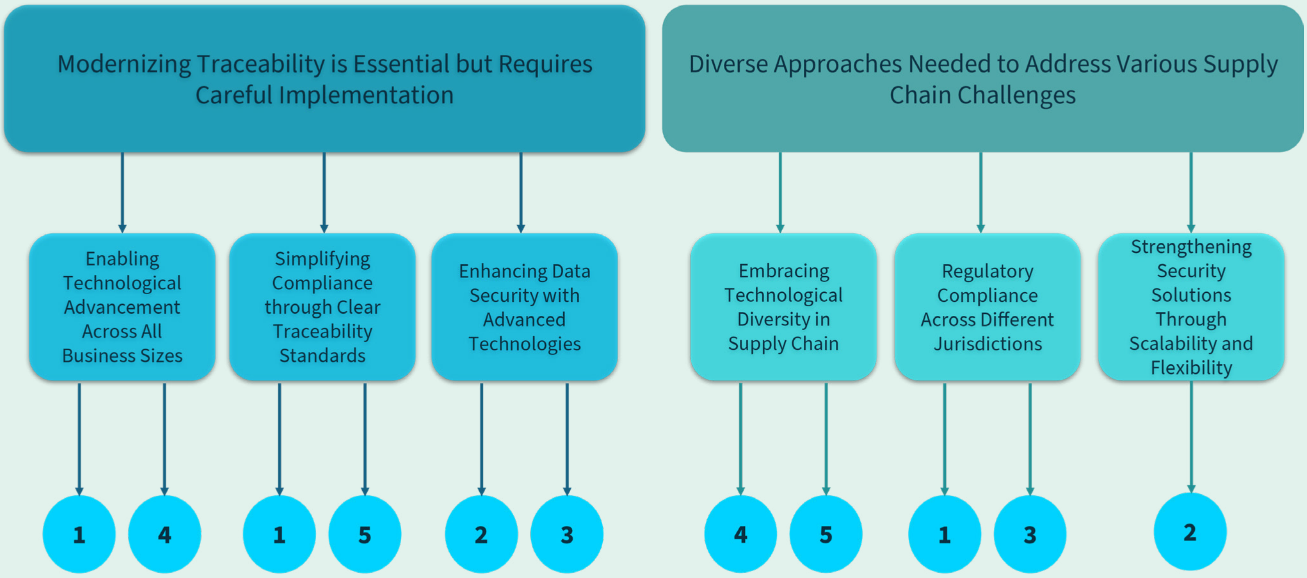
2. Use blockchain for transparency: Utilize blockchain technology to handle and track solution data, proving that it cannot be altered, providing visibility, and enhancing security across the supply chain.

3. Risk assessment and best practices: Implement robust risk assessment and security best practices to ensure the technologies used in tracking solutions, such as IoT devices for container tracking, are secured and protected against data tampering and unauthorized access. This should include regular vulnerability assessments, penetration testing, and the implementation of strong encryption and authentication protocols.

4. Support small businesses: Offer financial assistance, comprehensive training programs, and user- friendly, affordable technology solutions tailored to their needs and resources. This will empower small businesses to overcome the economic and technical barriers associated with adopting robust tracking systems, enabling them to participate fully in a secure and transparent supply chain ecosystem.

5. Using AI and machine learning: By using artificial intelligence and machine learning algorithms, businesses can analyze large volumes of supply chain data in real time. This helps SMEs and MEs gain valuable insights into their operations, identify potential risks, and make informed decisions, even with limited resources. For larger organizations, AI-driven analytics can optimize complex supply networks, allowing for proactive risk mitigation and efficient resource allocation across global operations.

Figure 2: Impactful Results of Proactive Supply Chain Strategies



Modernizing Traceability is Essential but Requires Careful Implementation
Diverse Approaches Needed to Address Various Supply Chain Challenges
Enabling Technological Advancement Across All Business Sizes
Simplifying Compliance through Clear Traceability Standards
Enhancing Data Security with Advanced Technologies
Embracing Technological Diversity in Supply Chain
Regulatory Compliance Across Different Jurisdictions
Strengthening Security Solutions Through Scalability and Flexibility
1
4
1
5
2
3
4
5
1
3
2

The numbers in the figure correspond to the specific recommendations outlined for modernizingtraceability and addressing supply chain challenges.

Find out more

Dr Erisa Karafili Associate Professor in Cybersecurity, School of Electronics and Computer Science, University of Southampton, UK. **e.karafili@soton.ac.uk**

Betul Gokkaya PhD Candidate, School of Electronics and Computer Science, University of Southampton, UK. **betul.gokkaya@soton.ac.uk**

DOI: 10.5258/SOTON/PP0086