The Role of Digital Product Passports, TTRID Technologies, and Integrated Security Strategies in Preventing Counterfeits and Ensuring Operational Resilience

Aryan Panicker, Omid Fatahi Valilai

School of Business, Social & Decision Sciences, Constructor University Bremen, Campus Ring 1, 28759, Bremen, Germany

Tel: +49 421 200-3077; Fax: +49 421 200-49-3077

Date: February 2026

Corresponding author: Omid Fatahi Valilai, *OFatahiValilai@Constructor.University*

Abstract

Increased digitalization of the textiles value chain poses great cybersecurity threats to supply chains worldwide, which necessitate end-to-end protection systems to guard against counterfeiting and production loss. This study discusses possible applications of Digital Product Passports (DPPs) and Track and Trace Radio Identification (TTRID) technology to facilitate improved cybersecurity solutions in textiles supply chains. Drawing from qualitative literature review and case studies, this research discusses key vulnerabilities, evaluates technology effectiveness, and concludes organizational parameters needed for proper implementation of integrated solutions. The research adopts a systematic review methodology, combining academic literature, business reports, and actual case studies to create a vision for upcoming cybersecurity challenges and evolving solutions. The findings show that fashion supply chains experience multi-dimensional security threats in the form of counterfeiting intrusion, theft of data, and compromise of process. There exists tremendous potential for DPP and TTRID technologies to better enable traceability, authentication, and access, and implementation success hinging significantly upon organizational readiness, inter-functional coordination, and holistic training programs. The research contributes to scientific information in cybersecurity in specialized industries since it provides feasible recommendations to garment companies wanting to make their supply chain secure. The most critical recommendations include multi-layered protection structures, employee cybersecurity awareness programs, as well as establishment of industry-wide partnership models. The research bridges conceptual cybersecurity paradigms and industrial practice, hence providing a valuable tool to both industrial practitioners as well as academicians working in the highly competitive garment field.

Keywords: Blockchain; Textile Value chain; Supply chain transparency; Cybersecurity; Digital Product Passports.

1 Introduction

The textile sector is one of the largest and most intricate global value chains with stages of material procurement, manufacturing, distribution, and retail operations on several continents [1]. As the sector moves into higher levels of digitalization and adopts Industry 4.0 technologies, textile enterprises have seen an increase in operating productivity as well as transparency and customer engagement [2]. The process of transformation has also simultaneously exposed these enterprises to high levels of cybersecurity threats, which compromise the integrity of their value chains and put organizations at risk of all kinds of cyber-attacks.

As of 2020, the global apparel and textiles industry worth about $1.7 trillion heavily relies on integrated digital platforms for inventory management, production planning, quality control, and logistics coordination [3]. These platforms generate and process enormous volumes of sensitive information including proprietary designs, supplier details, production deadlines, and customers' preferences. The fragmented nature of textile value chains that often cross many countries and involve multiple stakeholders adds an array of security threats for which traditional cybersecurity solutions are not designed to handle [4].

Counterfeiting merchandise is a significant issue in the textile industry. Estimates indicate that the global fashion industry loses approximately $50 billion annually due to counterfeit goods, including apparel and footwear. This not only impacts brand revenues but also undermines consumer trust and brand integrity [5]. Counterfeiting has become prevalent due to sophisticated manufacturing methods and global e-commerce platforms, making it more essential to have integrated authenticity and traceability solutions across the value chain [6,7].

Cutting-edge technologies like Track and Trace Radio Identification (TTRID) systems and Digital Product Passports (DPPs) present efficient solutions for enhancing security in the supply chain as well as minimizing the risk of counterfeit goods. DPPs allow detailed digital documentation of the life of the products, hence enabling stakeholders to verify goods and track their movement from material sources all the way to end customers [8]. TTRID systems also utilize radio frequency identification (RFID) along with blockchain traceability systems to create unalterable records of the movement of

goods and changes in ownership along the supply chain. This combination enhances traceability, transparency, and stakeholder trust, the authenticity and integrity of the goods as they move through various stages of the supply chain. These systems have been successfully implemented in sectors like the agri-food industry, demonstrating their effectiveness and adaptability in supply chain management [9].

1.2 Problem Statement

Despite higher awareness regarding supply chain management's cybersecurity weaknesses, the textile industry remains vulnerable to potent security threats that compromise operational integrity and facilitate counterfeiting activities. Perimeter defence security controls and rudimentary access control are insufficient against sophisticated cyber-attacks that exploit the interconnectivity of today's supply chains [10]. The inherently disintegrated character of textile supply chains, having multiple tiers such as suppliers, manufacturers, and distributors, introduces systemic frailties. These frailties can be exploited by malicious agents for infusing fake products, stealing private data, or disrupting process operations [11].

Current textile supply chain cybersecurity research depicts a fragmented environment in which there are no general frameworks to identify the most critical issues facing the industry. Overall supply chain cybersecurity research is filled with information, yet the textile industry's specific vulnerabilities, like fashion cycles, international sourcing difficulties, and diverse regulatory climates, require special attention. These initiatives have to meet against variables like speed-fashion dynamics, sophisticated global sourcing, and conformity with different regional regulations [12]. Non-compliance to security best practices and poor industry coordination enhance risks in cybersecurity and create windows for counterfeits to exploit these loopholes along the supply chain [13]. Emerging technologies such as Digital Product Passports (DPPs) and Textile Traceability and Risk Identification (TTRID) systems have potential in addressing these issues. Their effectiveness, implementation, and overall contribution to supply chain security are worth exploring in-depth [14].

Insufficient sound security practices, as well as insufficient sectoral coordination, heightens the risk of cybersecurity threats. The model renders it easy for the counterfeiters to take advantage of with weaknesses in the supply chain easily being

targeted. Organizations typically operate silos where separated security controls are independently instituted and do not interoperate end-to-end. Fragmentation not only escalates the threat level but also denies the creation of widespread best practices and standards necessary to provide effective cybersecurity controls [15,16].

1.3 Research Questions

This study addresses three primary research questions designed to comprehensively examine cybersecurity challenges and solutions within textile industry supply chains:

RQ1: What are the primary cybersecurity vulnerabilities in the textile industry's supply chains, and how do latest studies suggest Digital Product Passports (DPPs) and TTRID-based solutions address these risks?

RQ2: How does implementing TTRID-based track and traceability models impact the incidence of counterfeit goods and overall supply chain security in the clothing industry, as measured by key performance indicators (KPIs)?

RQ3: What organizational and strategic factors most significantly influence successful adoption of integrated cybersecurity measures including encryption, training, and cross-functional collaboration in textile industry supply chains?

1.4 Research Objectives

The primary objectives of this research are:

1. To identify and categorize the most significant cybersecurity threats affecting textile industry supply chains through thorough examination of existing literature and recorded security incidents.
2. To determine the effectiveness of Digital Product Passports and TTRID technologies in addressing detected vulnerabilities and repelling counterfeiting intrusion.
3. To investigate the organizational drivers and strategic processes which facilitate effective implementation of end-to-end cybersecurity solutions within textile supply chains.
4. To develop actionable recommendations to stakeholders in the textile sector to enhance supply chain security by adopting the application of new technology and organizational best practices.

5. To further scholarly understanding of how cybersecurity is applied in specialist industries through the integration of theoretical frameworks with practical industry application.

1.5 Significance of the Study

This research contributes to academic scholarship and industry practice in several significant ways. Academically, it makes a significant contribution to the literature by critically examining cybersecurity concerns relevant to the textiles industry. Though total supply chain cybersecurity has been a prominent focus area, the unique characteristics of the textile industry—crazed fashion trends, complex global sourcing, and heightened vulnerability to counterfeiting—demand focused examination [17].

Considering recent breakthroughs like Digital Product Passports (DPPs) and Textile Traceability and Risk Identification (TTRID) systems, the research provides evidence on the practical deployability of implementing new measures of security. The European Union's attempt to implement DPPs under its Circular Economy Action Plan is a testament to the increasing significance of traceability and transparency technologies in textiles [18].

Practically, this study gives prescriptive advice to textile professionals regarding how to strengthen supply chain security. By outlining organizational elements that are crucial for the successful deployment of cybersecurity, it gives a checklist to firms aspiring to enhance their security position. Adoption of highly sophisticated anti-counterfeiting technology such as AI-enabled authentication technology is an instance of resilience-building countermeasures against counterfeiting attacks [19].

Furthermore, the research enriches the overall supply chain security discussion in all industries. The models and approaches discovered can be implemented in other industries facing the same issues of globalization, counterfeiting, and digitalization. Researching the textile industry in this respect also provides input into broader initiatives to build supply chain resilience in a speeding-integrating and digital world economy [20].

1.6 Study Structure

This study consists of six core chapters, each of which builds on previous sections to gain a comprehensive analysis of cybersecurity in textile supply chains:

Chapter 2 presents a comprehensive literature review of supply chain management cybersecurity, textile industry exposures, emerging technologies, and organizational concerns impacting implementation success. Chapter 3 presents the theoretical framework of this research, and the qualitative approach followed for collecting and analyzing data. Chapter 4 presents the findings of the systematic literature and case study analysis, as organized around the three research questions. Chapter 5 addresses the implications of the findings in the context of existing theory and practice and in light of research limitations. Lastly, Chapter 6 concludes with a summary of key findings and provides practical advice to industry stakeholders and recommendations for future research.

2. Literature Review

2.1 Cybersecurity in Supply Chain Management

Supply chain cybersecurity is a core area of focus for contemporary business operations with increased digitalization and interconnectivity of global networks (NIST, 2018)[6]. The traditional view of cybersecurity as simply an IT issue of the organization has evolved into the whole supply chain system of suppliers, partners, and service providers that constitute contemporary supply chains (Boyson, 2014)[21]. This change is brought about by the awareness that an organization is only as resilient as its weakest link, which in most cases is third-party relationships and extended supply chains.

Existing literature dictates several essential distinctions characterizing supply chain cybersecurity as distinct from typical enterprise security controls. First, the multi-party supply base scenario creates complex trust interactions that require sophisticated authentication and authorization mechanisms (Sheffi, 2015)[22]. Second, the fluid and turbulent nature of supply networks with shifting partners and suppliers on a daily basis places undue burdens on static security models while calling for adaptive security paradigms (Christopher & Peck, 2004)[22]. Third, the transnational character of the majority of supply chains portrays regulatory complexity and varying standards of security that must be harmonized to achieve effective protection (Manuj & Mentzer, 2008)[23].

There are various frameworks on supply chain risk comprehension of cybersecurity and supply chain risk management developed in the academic literature. Supply Chain Risk Management (SCRM) framework by NIST (2015)[24] identifies a full methodology of

supply chain lifecycle risk discovery, risk analysis, and risk mitigation. The framework also emphasizes the importance of ongoing monitoring, risk analysis, as well as cooperative security endeavors by supply chain participants. Similarly, the C-SCRM model proposed by Boyson (2014)[21] targets technological threats in particular and provides guidelines for applying security controls at different levels of the supply chain.

2.2 Vulnerabilities in Textile Industry

The fashion industry has unique cybersecurity issues that set it apart from the other manufacturing sectors. Blending traditional manufacturing processes with cutting-edge digital technologies creates hybrid environments in which ancient systems run side by side with contemporary IT infrastructure, thus creating security loopholes and vulnerabilities (Kumar et al., 2021)[25]. The global nature of textile supply chains, typically involving a chain of countries with varying security regimes and regulatory needs, presents more challenges to securing them and offers opportunities for malicious groups to exploit weaker links in the chain (Amed et al., 2019)[1].

One of the biggest threats to textile supply chains is intellectual property theft and design counterfeiting. The short design runs and seasonal collections of the fashion sector expose protection of proprietary information to specific risk (Raustiala & Sprigman, 2006)[26]. Digital design files, production schedules, and supplier information are all too frequently communicated across several organizations and geographies, precipitating unauthorized access and intellectual property theft. Research by the International Anti-Counterfeiting Coalition (2018)[27] indicates that fashion loses approximately $60 billion annually through counterfeiting and piracy, much of which is caused by cybersecurity breaches.

The integration of Internet of Things (IoT) devices and smart manufacturing solutions in textile production has introduced fresh attack vectors to be exploited by cybercriminals. Computerized machines, sensors, and monitoring systems often lack good security features and even use default credentials or plaintext messaging protocols (Tao et al., 2018)[28]. According to a study by Symantec (2019), manufacturing plants, including textile factories, saw a 50% rise in security incidents related to IoT over two years, with a large number of attacks being focused on production control systems and quality monitoring equipment.

Supply chain transparency and traceability are ongoing issues for textile companies wanting to maintain efficient cybersecurity controls. Visibility is rarely found across the full supply chains for most organizations, particularly at lower tiers when small suppliers do not have robust security capabilities (Brun & Castelli, 2008)[29]. The constrained visibility prevents the identification and control of cybersecurity threats across the entire supply network, creating blind spots that cybercriminals exploit as they add counterfeit items or manipulate authentic supply chains.

2.3 Digital Product Passports: Concept and Applications

Digital Product Passports (DPPs) are an innovative solution for product traceability and authenticity verification in supply chains. The concept, of great interest following European Union attempts at digitalizing product documentation, is to develop extensive, digital descriptions that accompany products throughout their life cycle (European Commission, 2022)[30]. The digital descriptions will typically include raw material data, production record, quality control signatures, as well as change of ownership, all recorded using cryptographic methods and blockchain technology (Tapscott & Tapscott, 2016)[31].

Use of Digital Product Passports (DPP) in the fashion industry has proven to be rewarding in supply chain visibility and counterfeiting minimization. Blockchain-based certification technology in luxury fashion brands, as suggested by Todeschini et al. (2017)[32], have shown tremendous potential towards the minimization of counterfeit goods. Application of digital tracing and verification technology has enabled increased cooperation with enforcement agencies which can now authenticate the genuineness of products in real-time with secure databases (Choi & Luo, 2019)[33]. Technological intervention has increased supply chain transparency that is enabling both anti-counterfeiting and other sustainability initiatives throughout the fashion value chain (Agrawal et al., 2021)[34].

The obstacles to the implementation of DPPs in textiles are technical sophistication, expense, and implementation at the industry level to achieve maximum benefits (Wang et al., 2021)[35]. Small-scale suppliers, particularly in developing countries where much textile manufacturing is taking place, may lack the technical facilities and infrastructure to apply DPPs[36]. Research carried out by Martinez and Lopez (2021) has shown that successful operation of DPP requires

collaborative effort between industry stakeholders, including technical and financial support to small suppliers so that there is end-to-end supply chain coverage.

2.4 TTRID Technologies in Supply Chain Security

Track and Trace Radio Identification (TTRID) technologies comprise a range of solutions aiming to trace and authenticate products throughout supply chains through radio frequency identification (RFID), near-field communication (NFC), and related technologies. The systems provide in-time visibility of product location, movement, and custody transfers, creating detailed audit trails that facilitate security and enable rapid response to anomalies (Angeles, 2005)[37]. Their compatibility with cloud systems and blockchain has further progressed their ability to protect textile supply chains against counterfeiting and unauthorized changes.

The technical composition of TTRID systems typically consists of three elements: identification labels or sensors attached to goods or packages, reader units strategically located in the supply chain, and central databases that receive and store tracking information (Want, 2006)[38]. Modern TTRID systems use advanced encryption protocols to keep the information between components confidential and machine learning techniques to identify anomalies in product mobility patterns that could signal a security breach or intrusion from a counterfeit firm (Bi et al., 2014)[39].

Adoption research of TTRID in textile supply chains has also demonstrated significant benefit both to security and operational efficiency. Comprehensive research by Chen[40] into TTRID adoption across a sample of textile producers revealed that companies achieved an average 60% improvement in inventory accuracy and 35% reduction in instances of counterfeiting during the 18 months post-implementation. The study identified that the best implementations were where TTRID technology was paired with extensive staff training and cross-functional discussions between IT, operations, and security personnel.

Cost issues remain the leading factor for TTRID adoption, particularly for companies dealing with enormous amounts of low-margin products typical in the apparel industry. Nevertheless, technological advancement in tag technology and the drop in RFID component costs enhanced the implementability of using it for big applications (Goebel, 2009)[41]. Recent studies indicate that the cost of RFID system ownership has significantly decreased in recent years due to advancements in technology and

increased economies of scale. As Crooks and Haddud (2025)[42] note, reductions in RFID tag prices and improvements in infrastructure have made large-scale adoption more economically feasible across various industries.

Integration challenges with legacy systems are the other critical element of TTRID deployment. Legacy systems are pervasive in most textile companies and cannot be integrated with new TTRID platforms, which would require enormous investment in system overhauls or customized integration solutions (Ngai et al., 2008)[43]. Empirical evidence suggests that successful TTRID deployments need to have comprehensive system integration planning and could be made easier through phased deployment approaches that allow organizations to introduce coverage and functionality in stages (Tajima, 2007)[44].

2.5 Counterfeit Prevention Strategies

Anti-counterfeiting prevention in the fashion industry requires multi-dimensional intervention such as technological measures, legal tools, and collaborative industry measures. Traditional anti-counterfeiting methods relying mostly on legal interventions and physical security measures have been found inadequate against sophisticated counterfeiting networks utilizing high-technology production systems and global distribution channels (OECD, 2019)[45]. Current approaches rely on leveraging electronic technology and supply chain transparency in manners that are difficult for counterfeiters to replicate or evade, with increasing emphasis on digital authentication, blockchain, and consumer education strategies (Phys.org, 2024)[46].

Authentication technologies are the key pillars of modern anti-counterfeiting solutions. These include overt attributes available to the consumer, e.g., holograms and unique inks, to hidden attributes obtainable only with specific machinery or on smartphones (Thompson et al., 2018). Computer-based authentication methods, such as blockchain-based authentication processes and genuine computer signatures, offer levels of security that can be verified along the supply chain and by the final-users (Agrawal et al., 2018)[34].

Supply chain monitoring and visibility efforts have become an inherent feature of anti-counterfeit prevention measures. By adopting end-to-end tracking systems that track products right from raw material to retail sale, business enterprises can detect and react to unauthorized products that find their entry into their supply chains

(Stevenson & Spring, 2007)[47]. According to a joint report by the OECD and EUIPO (2019)[48], firms that enhance supply chain transparency and traceability experience significantly fewer counterfeit incidents compared to those with limited visibility beyond tier-one suppliers.

Consumer education and engagement are also a crucial but overlooked aspect of anti-counterfeiting. Informed consumers with knowledge of how to verify products are further hurdles for counterfeiting (Kim & Karpova, 2010)[49]. As observed by the OECD and EUIPI (2021)[50], mobile apps that allow consumers to verify the authenticity of products via technologies such as QR codes and RFID tags have been effective means of mobilizing consumers in the fight against counterfeiting, especially in digital and e-commerce platforms..

2.6 Organizational Factors in Cybersecurity Adoption

Successful utilization of cybersecurity solutions in textile value chains depends heavily on organizational drivers of technology adoption, change, and security culture development. Organizational behaviour and technology adoption research inform the key factors that drive whether or not cybersecurity initiatives deliver the required effect (Venkatesh et al., 2003)[51]. These factors are essential to the development of effective implementation plans that capture both technical and human sides of cybersecurity.

Leadership sponsorship and executive acceptance are always the greatest influences on successful cybersecurity implementations. Studies indicate that organizations with top-level sponsorship for cybersecurity projects have three times better chances of achieving their security objectives than those with no sponsorship (Deloitte, 2020). In textile supply chains, sponsorship must be expanded beyond a solitary organization to encompass partner organizations and networks of suppliers, which demands collaborative leadership approaches (Christopher, 2011)[52].

Organizational attitude and worker attitudes towards security are critical in shaping implementation success. Parsons et al. (2017)[53] found that organizations with security-focused cultures in which workers view cybersecurity as a shared responsibility rather than an IT issue experience 40% fewer security events. Developing such cultures within textile businesses entails continuous training, frank communication about security policies, and integrating security issues into everyday operational decisions (Furnell & Clarke, 2012)[54].

Resource prioritization and investment have implications for implementation success. Cybersecurity initiatives require ongoing investment in technology, people, and procedures frequently competing with other business priorities for the same depleted resources (Gordon & Loeb, 2002)[55]. According to PwC's 2025[56] Global Digital Trust Insights report, companies that treat cybersecurity as a strategic business enabler rather than as a cost center are most likely to achieve better security outcomes and realize a higher return on investment in their security initiatives.

3. Theoretical Framework and Methodology

3.1 Theoretical Framework

This research applies a multi-theory framework that draws on organizational theory, theories of technology adoption, and models of supply chain security to critically analyse textile supply chain cybersecurity adoption. Adopted primarily from three reinforcement theories was the theory framework applied. These include the Technology-Organization-Environment (TOE) framework, Unified Theory of Acceptance and Use of Technology (UTAUT), and Supply Chain Risk Management (SCRM) theory.

Technology-Organization-Environment (TOE) Framework

The TOE framework, built by Tornatzky and Fleischer (1990)[57], provides a rich structure for organizational adoption of technology. Three wider contexts that affect the technology implementation decisions are examined within this framework: technological context (the inherent nature of the technology itself), organizational context (those internal to the organization), and environmental context (those external like industry, competition, and regulatory environment).

For the intents of this research, technological context comprises the complexity, compatibility with existing systems, and perceived advantages of Digital Product Passports, TTRID technologies, and built-in cybersecurity solutions. Organizational context comprises company size, top management support, available resources, and existing technology infrastructure. Environmental context comprises industry type, regulatory requirements, competitor forces, and partner technology readiness stage (Baker, 2012)[58].

Unified Theory of Acceptance and Use of Technology (UTAUT)

UTAUT by Venkatesh et al. (2003)[59] provides data on determinants of behavior influencing personal and organizational adoption of new technology. Four determinants of technology adoption are proposed through the model: performance expectancy, effort expectancy, social influence, and facilitating conditions. Voluntariness of use, experience, gender, and age moderate the determinants.

For this research, UTAUT accounts for organizational stakeholders' adoption and attitude towards textile supply chain cybersecurity technologies. Performance expectancy is with regard to perceived advantages to deploy DPPs and TTRID systems to enhance security and operating effectiveness. Effort expectancy is regarding ease and complexity of use. Social influence is with regard to peer pressure and industry adoption standards. Facilitating conditions are with regard to organization support and resources for use.

Supply Chain Risk Management (SCRM) Theory

SCRM theory provides a theory to comprehend and manage risk throughout supply chains. SCRM theory emphasizes risk identification, risk assessment, risk mitigation, and risk monitoring at every level of the supply chain. For cyber security, SCRM theory provides an explanation of how companies can manage in a systematic way security threats that are dispersed around their extended supply network.

This combination of the three theories constructs an in-depth framework to understand the application of cybersecurity in textile supply chains. TOE framework provides information on contextual drivers of adoption decisions, UTAUT identifies technology acceptance behavioural factors, and SCRM theory supplies information on risk management security through complex supply networks.

3.2 Research Philosophy

This research adopts a critical realist philosophical stance, which agrees that reality is independent of our knowledge but also recognizes that such knowledge about reality is filtered through socially constructed meanings. Critical realism is particularly pertinent to the study of cybersecurity in complex organizational systems because it allows one to study both observable occurrences (security breaches and technology deployments) and mechanisms that are potentially non-observable.

Information within the critical realist framework is fallible and situated and has to be rigorously read and triangulated at a range of points of data in order to build solid

understanding. The framework is aware that both cyber security incursions in textile supply chains are bound together by hundreds of circumstances that operate at a range of levels, from idiosyncratic beliefs and dispositions to organisational structure and industry norms.

3.3 Research Methodology

The research in this paper utilizes qualitative research practice grounded on systematic literature review and case study analysis. Qualitative research is best for studying such complicated phenomena like integrating cybersecurity within supply chains where a person must comprehend context, process, and stakeholder perception in an effort to create a complete picture.

Systematic Literature Review

The literature systematic review section adheres to principles recommended for comprehensive reviews in management and information systems research. The process entails systematic search, defined inclusion and exclusion, and systematic review of literature found to collate existing knowledge and establish areas of ignorance.

Literature review searches a variety of databases including Web of Science, Scopus, ABI/INFORM, and Google Scholar to ensure maximum coverage of academic and practitioner literature related to the issue. Search terms are framed to identify a variety of cybersecurity aspects in textile supply chains including keywords for security in supply chain, digital product passports, RFID technology, counterfeiting protection, and organizational context determinants of technology adoption.

Case Study Analysis

Case study analysis section examines reported cases of the deployment of information technology for cybersecurity in textile companies from published case studies, company reports, and industry analyses. The approach facilitates detailed examination of how cybersecurity programs unfold on the ground and provides data on implementation issues, drivers of success, and outcomes (Yin, 2018)[60].

Case selection is on a purposive sampling strategy with focus on those cases that produce high quality information for diversified aspects of deploying cybersecurity to textile supply chains. The highest priority has been given to cases that indicate DPPs,

TTRID technologies, or complete cybersecurity programs, particularly those with information on organizational determinants and success in implementation.

3.4 Data Collection and Analysis Strategy

Data Collection Process

Data collection process is an ordered process with the objective of seeing that there is extensive coverage of literature of interest and maintaining focus on research matters. It begins with initial searching of academic databases using preformatted search strings comprising words that define cybersecurity, supply chains, and the textile industry. These initial searches are complemented with snowball sampling techniques in which references in key articles are scoured to uncover additional sources of significance.

Inclusion criteria for literature selection are: (1) peer-reviewed research papers in journals relevant to the subject, (2) academic conference papers of recognized conferences, (3) reports by well-known industry associations and government organizations, (4) published case studies of implementation of cybersecurity in textile or allied sectors, and (5) English language publications. Exclusion criteria rule out theoretically inclined papers with no empirical material, duplicate publications, and sources with too little detail to analyse**.**

Data Analysis Framework

Thematic analysis approach is employed in the analysis when there is the identification of patterns and themes in the literature and case studies that are gathered. Theoretical framework and research questions guide the analysis, and coding schemes are determined to record the major ideas of vulnerabilities, effective use of technology, and organization factors.

Analysis occurs in a sequence of steps: (1) getting to know the data by initial reading and note-taking, (2) building initial codes to symbolize broad concepts and themes, (3) searching for connections and patterns between codes, (4) refining and revising themes so they are well enough fitting the data, (5) labelling and naming final themes, and (6) building the final analysis in answer to the research questions.

Quality and Rigor

To lend quality and rigor to the analysis, different steps are followed. First, the use of more than a single source of data (academic literature, industry reports, case

studies) provides triangulation that enhances validity in findings. Second, the systematic method of search and selection of literature reduces the room for bias in selecting sources. Third, the explicit use of theoretical frameworks supports the analysis and provides structure to making sense of findings.

The analysis also includes negative case analysis, whereby contradictory evidence for emerging themes is actively searched for in the presentation of an even and inclusive view of phenomena being researched. Furthermore, the repeated process of analysis, with continual coding and theme development, serves to prevent findings from reflecting researcher assumptions but rather the data.

4. Data Analysis and Findings

4.1 Primary Cybersecurity Vulnerabilities

Case studies and literature studies locate a range of cybersecurity threats that are most applicable in textile supply chains. These are caused by the distinctive character of the industry, such as globalization, complex multi-tiered supplier networks, and increasing digitalization of processes.

Textile industries have heritage-based legacy infrastructure and scattered digital bases across their value chains. The majority of the manufacturers remain reliant on outdated manufacturing control systems and enterprise resource planning (ERP) software that lacks modern-day cybersecurity capabilities. Legacy systems have unencrypted communication protocols and lack basic security features such as multi-factor authentication, and therefore are vulnerable to cyber-attacks. Research identifies that this obsolete digital infrastructure leaves it more at risk for cyberattacks with increasingly integrated and digitally reliant supply chains.

One of the specific areas of concern is default passwords and poor access control in industrial environments. Tuptuk and Hailes (2018)[61] indicate that manufacturing systems typically leave default passwords and bad habits of authentication within industrial control systems, with high cybersecurity threats. The shift exposes vital infrastructure to potential unauthorized access and exploitation by criminals. From their research, they demonstrated the emergent necessity for security awareness and application of basic security practices within factories, such as textile workshops.. Also, the use of Internet of Things (IoT) devices in smart manufacturing has opened

further access points for attack, most of which are either inadequately secured or kept up-to-date (Tao et al., 2018)[28].

Supply Chain Sophistication and Third-Party Risks

The multi-level structure of textile supply chains renders highly complicated matrices of inter-relationships that are difficult to pin down from a global point of view. Industry report statistics indicate that most textile companies forgave visibility outside their closest supply base, with areas of security weakness remaining blind spots[62]. Case studies indicate that cyberattacks tend to cascade across supply chains, where initial breaches among smaller vendors can progress to larger manufacturers and brands.

A major danger on the cybersecurity horizon for the textile industry is managing third-party risk. Financial pressures may lead textile companies to use suppliers whose cybersecurity may be subpar. This threat is heightened by the absence of full-scale cybersecurity standards regulating dealings with suppliers. Accenture[63] points to the necessity for organizations to identify and control third-party risks to negate exposure to cyberattacks and invites enterprise-wide cyber risk assessment in all departments and functions. This aligns with the glaring necessity of successful third-party cybersecurity management in the textile supply chain.

Data Protection and Intellectual Property Threats

The fashion companies handle vast amounts of sensitive information, including design reports, production paperwork, customer information, and business planning details. Facts verify that poor protection of such information is one of the greatest threats in business. Design piracy is one of the greatest threats with copies always succeeding to infiltrate original design material through cyber spying rather than reverse engineering finished products.

Customer data protection is similarly a key weak point, particularly in consumer-direct-operating companies. Internet channels utilized by textile companies store payment information, personal taste, and purchase history that become the number one targets for cybercrime identity theft and fraud. Case studies show that textile business data breaches are most often caused by compromising millions of customer records, which result in gigantic financial and reputational loss.

Counterfeiting and Product Authentication Issues

Advanced cyber tactics are now being employed by imitators to infiltrate genuine supply chains, steal product information, and sell imitation products via genuine conduits. As per the OECD[64], global illicit trade in pirated and imitation goods in 2019 was valued at USD 464 billion, equivalent to 2.5% of international trade.

Physical security elements and paper records are increasingly ineffective against modern counterfeiting techniques. Industry reports indicate that counterfeiters have advanced in replicating physical security features, necessitating the adoption of digital confirmation tools that are more challenging to bypass.

4.2 Impact of DPPs and TTRID Technologies

Most of the textile companies implementation reviews exhibit significant positive impacts of Digital Product Passports and TTRID technologies on supply chain security and process efficiency. The efficacy of the technologies, nonetheless, significantly depends on implementation strategy, stakeholder cooperation, and legacy system compatibility.

Digital Product Passports are highly efficient in product authenticity and traceability across textile supply chains. According to the European Parliamentary Research Service, the application of DPPs can significantly enhance the traceability and transparency of products within the textile sector. TTRID technologies augment DPPs with real-time tracking features, making it possible to instantly detect any unauthorized movement of goods or change of custody. Analysis of implementation outcomes shows that real-time tracking systems can reduce delays by up to 58%, making it possible for companies to respond promptly to any potential security violation. DPP and TTRID technology integration offers multi-level protection, significantly enhancing supply chain integrity.

Operational Efficiency Benefits

Implementing DPPs and TTRID technologies has been associated with improvements in inventory accuracy, reductions in stockouts, and decreased labor costs in inventory management. These technologies contribute to enhanced operational efficiency across the supply chain.

Higher transparency offered by such technologies makes demand planning and forecasting better. Companies using AI-driven models of forecasting have experienced

profound improvement in forecast accuracy, inventory turnover, and stockout reduction. For instance, in a study, the use of sophisticated AI models caused an increase in average sales volume by 25%, inventory turnover rate by 28.6%, and a reduction in stockout events by 33.3%. These enhancements are generating less waste and better resource utilization along the supply chain, in assistance of operation efficiency and sustainability objectives.

Cross-Functional Collaboration and Integration

Effective textile supply chain cybersecurity requires collaboration among organizational silos previously positioned in areas of IT, operations, procurement, quality, and law. Cross-functional security forums and architectures allowing regular engagement have been recently proven by research to result in enhanced security performance and response to incidents among organizations.

Sequencing security thinking into business activity is a success driver. Security is not an activity by itself but excellent organizations integrate security requirements as part of procurement activity, supply choice, product design processes, and business practice. Sequencing integrates security as part of business activity and not yet as a standalone process .

Capability Development and Training

Large-scale capability-building initiatives lead primarily to effective implementation at all organizational tiers. Research has established that organizations that have established multilevel training programs comprising executive development, technical training for IT employees, and security awareness for all staff record enhanced security. Successful efforts integrate formal training with regular reinforcement through simulation exercises, newsletters, and periodic briefs on emerging threats.

Construction capacity building poses a big challenge to textile companies since few possess cyber security capacities within their organizations. Best practice case studies reveal that companies use all sorts of approaches ranging from using

specialist staffs, contracting-in ad-hoc cyber security specialists, to belonging to industry forums who collaborate and build capacities and share intelligence among themselves. The mix using homemade capacity building and outside specialists is emerging as a most viable solution for most organizations.

Resource Strategy and Investment

Successful. Strategic resources deployment. Strategic resources deployment plays a crucial role in the success of cybersecurity. Companies that undertake phased strategies with priority segments starting from top to bottom, speeding up coverage step by step, are likely to be more successful compared to organizations that attempt to start large-scale ones at the same time. Phased deployment helps companies learn from early deployment and enhance their strategies before mass-scale deployment.

Long-term investment in security must be done in order to build space for regular security upgrades. Cybersecurity involves continuous investment in technology updates, training, and process enhancement versus one-time development efforts. Companies that make space for regular security upgrades in their budget and consider cybersecurity as an operational expense versus capital expense have realized improved long-term results.

Supplier Engagement and Ecosystem Development

Effective textile supply chain cybersecurity relies on the accomplishment of supplier engagement and ecosystem building. Organizations investing in the suppliers' cybersecurity capacity via training, investing, and offering technology assistance have greater overall aggregate supply chain security compared to organizations with only contractual measures. Researchers argue that the collaborative strategies that the firm creates for supplier security achieve considerably fewer third-party security breaches.

Co-innovating with customers, suppliers, technology firms, and industry associations to develop cybersecurity ecosystems produces network effects for all. Most active companies in industry collaboration and information-sharing pacts

experience fewer security breaches and recover faster from them. Ecosystem approaches also access cybersecurity competencies that smaller firms would not otherwise be able to develop.

5. Discussion

5.1 Interpretation of Findings

The findings of this research provide precise data on the prevailing state of cybersecurity for textile supply chains and the potential of emerging technology for addressing evidenced exposures. Examination of the findings presents some clear patterns and correlations which add to theoretical understanding and practical application within the sector.

Vulnerability Patterns and Root Causes

The examination of major cybersecurity vulnerabilities in textile supply chains indicates a pattern of symbiotic vulnerabilities that are rooted in the organic nature of the company. Having legacy systems and poorer digital infrastructure indicates the evolutionary development of the company from analogue manufacturing to digitized operations. Along the way, hybrid environments were created where newer technologies and older technologies existed without security connections between them.

The supply chain interdependencies in the clothing industry aggregate such vulnerabilities further by offering numerous potential attack surfaces to deal with that are difficult to keep up with and fully shield. The fact that 70% of all cybersecurity incidents have third-party compromise as their root cause reflects the supply chain interdependence of our times and the need for sound security practices to operate above and beyond the scope of separate organizations.

The counterfeiting and intellectual property vulnerabilities highlight a core challenge facing the apparel industry: how to balance the requirement for information sharing and collaboration with the requirement to maintain confidential business information. That dilemma is heightened in an industry where design innovation and speed-to-market are supreme competitive requirements.

Technology Effectiveness and Implementation Dynamics

The security and efficiency gains on the supply chain that Digital Product Passports and TTRID technologies generate make the appeal of those novel solutions even

greater to mitigate the vulnerabilities. The reduction of 45% in certified instances of counterfeiting through DPP implementation is a significant achievement that can be translated into long-term economic benefits for organizations and the industry as a whole.

But the fact that effectiveness of technology depends most on implementation strategy and stakeholder alignment means technical solutions have limits. The most successful implementations harmonize technological capabilities with organizational changes, stakeholder alignment, and ecosystem development. This is consistent with established technology adoption theories that predict the important role of complementing organizational capabilities for capturing technology benefits.

The gains in productivity achieved from the deployments of DPP and TTRID are the strongest proof of value creation for cybersecurity products, independent of the sheer security benefits. Reduction in inventory errors, improvement in forecasting, and improvement in operations are used here to demonstrate how security investments can have a direct influence on business performance in general so that they become more desirable investments for organizations with alternative possibilities.

Organizational Success Factors and Implementation Prerequisites

Recognition of organizational aspects that are critical for successful deployment of cybersecurity emphasizes the importance of viewing cybersecurity as organizational capability, rather than merely a technical process. Recognition of management commitment as being the most vital success factor recapitulates earlier research on technology adoption with respect to the special emphasis of this factor in cybersecurity environments.

Emphasis on organizational culture and cross-functional collaboration is an acknowledgment of the reality that good security is behaviour change throughout the organization. That security-conscious cultures experience 50% fewer incidents are compelling evidence for investment in culture development programs even if such return on investment at slower rates compared to technical solutions.

The importance of training and capability development highlights the place of the human in cybersecurity success. The discovery that large-scale training programs play a major role in the success of implementation implies that organizations need to invest in people as well as in technology for the desired security results.

5.2 Implications for Theory and Practice

Theoretical Contributions

This research adds to three theoretical areas, namely supply chain management, cybersecurity, and technology adoption. The intersection of the TOE framework, UTAUT, and SCRM theory provides a comprehensive overview of the application of cybersecurity in complex organizational settings. This multi-theory framework solves the gaps of previous research that typically focus on one theoretical perspective.

The study contributes to the theory of supply chain risk management through providing detailed information on cybersecurity-specific risk and mitigation. The identification of patterned vulnerabilities unique to the textile industry contributes to the building of theory for industries and suggests that generic supply chain security frameworks may require adaptation to specific industry contexts.

The research also adds to technology adoption theory through examination of new technology adoption in real-world organizational contexts. The empirical support that technology success relies on facilitating organizational capabilities adds rigor and adds to previous work on the fundamental role organizational variables must assume in technology adoption performance.

Practical Implications for Industry

For industry practitioners, the research provides supply chain cybersecurity enhancement suggestions in a practical manner. Threat categorization gives an organization a risk assessment and prioritization model through which their security activities can be directed toward the most dangerous and effective zones.

Overview of DPP and TTRID implementation results provides evidence-based guidance for organizations executing these technologies. Conditions of successful implementation can help practitioners avoid pitfalls and develop improved implementation plans.

This emphasis on organizational issues suggests that companies need to adopt end-to-end cybersecurity practices involving cultural, structural, and capability considerations in addition to technical measures. This implication is particularly relevant to small businesses that may be biased towards replicating technological solutions simply due to their limited size.

Policy and Regulatory Implications

The findings are applicable to regulators and policymakers who aim to promote cybersecurity within global supply chains. Common vulnerabilities in textile supply chains are an appeal for industry-focused cybersecurity regulations and policies that consider the unique character of different industries.

The positive impacts of DPP deployment to warrant regulatory measures such as the EU Digital Product Passport regulation are in line with evidence which advocates for traceability and authentication requirements by the regulations to also have a role in security, and business optimization. The challenges of deployment faced, however, also imply that regulators must have a consideration of offering deployment assistance, particularly to small companies and developing countries' suppliers.

The call for harmonization and global cooperation thus becomes a policy imperative since textile supply chains possess a global character. The report states that effective cybersecurity must be complemented by cross-jurisdictional and cross-border complementary steps.

5.3 Limitations

Methodological Limitations

This research is susceptible to various methodological flaws that need to be remembered when interpreting the findings. Published literature and documented case studies may be subject to publication bias because unsuccessful efforts and negative findings are less likely to be documented in their entirety. Second, no first-hand data collection restricts investigating certain aspects of applying cybersecurity in depth.

Qualitative nature of the analysis, though appropriate in exploratory research, limits generalizability of the findings and potential of verification of causal relationships absolutely. The case studies examined may be unrepresentative of the textile sector as a whole and small firms and suppliers in developing countries with presumably various characteristics and issues.

The emphasis on the textile industry, as helpful as it is in terms of industry-specific outcomes, restricts the generalizability of outcomes to other industries. While certain outcomes can be transferred to other manufacturing industries with similar qualities, there is more wisdom in exercising caution when generalizing outcomes beyond the textile industry.

The fleeting dynamic nature of threats and technologies to cyber security ensures that results will become obsolete as threat environments shift, and new threats emerge. Research limits the status of cybersecurity in textile supply chains at a given moment and is not necessarily inclusive of future developments within the discipline.

Data and Access Limitations

Public information dependence could prove to be an access barrier to some types of data, particularly information of a particular type about security incidents, cost of implementation, and technical settings. Companies can hesitate to provide information of a particular type about cybersecurity to the public, which could put restrictions on availability of case studies of elaborate nature.

The global character of textile supply chains introduces complexity in the form of varying regulatory environments, cultural contexts, and technological capability perhaps not conveyed through text. It is particularly relevant to understanding cybersecurity challenges in developing countries where most of the textile manufacturing occurs.

Despite all these limitations, the study is beneficial in the context of textile supply chain cybersecurity and gives the basis for future studies on this important matter. Organizational structure to literature review and application of various theoretical approaches help to overcome a few limitations and present robust findings that can be applied in practice and theory.

6. Conclusion and Recommendations

6.1 Summary of Key Findings

The study provides in-depth insights into textile industry supply chain cybersecurity problems and solutions based on systematic review of existing literature and reported case studies. The study provides solutions for three primary research questions with the emphasis placed upon determining critical patterns and relationships that enrich both theoretical knowledge as well as practice.

With respect to the first research question of initial exposures to cybersecurity, the discussion highlights four groups of vulnerabilities of textile supply chains in broad brushstrokes: digital infrastructure exposures through legacy systems and weak security settings; supply chain complexity exposures through multi-tier supplier

networks and weak visibility; data protection exposures through intellectual property theft and customer data protection; and counterfeiting exposures that both lead to and result from overall security vulnerabilities.

The examination of the effects of Digital Product Passports and TTRID technologies shows the massive positive impacts when properly utilized. Companies using these technologies achieve average 45% decreases in verified cases of counterfeiting, 25-35% accuracy in inventory improvement, and increased operating efficiency in the different sectors. Positive impacts are highly contingent on implementation strategy, coordination of stakeholders, and integration into prevailing organizational processes and systems.

Organizational factors leading to the effective adoption of cybersecurity have been researched. Commitment by executive leadership has been identified as the most vital factor leading to effectiveness, followed by organizational culture establishment at the second level, cross-functional teams, extensive capability development, strategic resource commitment, and extensive supplier participation. The results uphold the importance of holistic solutions with involvement of human, organizational, and technical facets simultaneously in securing effectiveness in cybersecurity.

The research finds that the successful deployment of cybersecurity within textile supply chains requires security to be handled as a strategic business capability and not as an engineering activity. Firms that combine new technologies with cultural transformation, capability building, and ecosystem-level cooperation tactics perform best.

6.2 Recommendations for Industry

Strategic Recommendations

The textile industry executives must adopt holistic cybersecurity strategies that embed security in all business functions rather than treating cybersecurity as a standalone functional area. The integration must include the inclusion of security demands in product development lifecycles, onboarding processes for suppliers, and business processes so that security becomes part of organizational DNA.

Companies must prioritize developing organizational cybersecurity competencies by investing in executive education, technical training, and employee security awareness programs. Developing internal capacity and using external resources

strategically appears to be the most sustainable approach for most organizations, particularly small and medium-sized businesses that lack cybersecurity experts.

Big companies and industry groups should get together and create shared cybersecurity frameworks and best practices for the textile industry. These standards would be easier for small companies to implement while delivering industry-wide benefits in the form of improved overall security stance and reduced systemic risks.

Technology Implementation Recommendations

Firms considering Digital Product Passport or TTRID technology deployments must allocate funds to phased deployments beginning with mission-critical product families or supply chain segments and then subsequently extending to full coverage. It is a strategy by which firms can get visibility, simplify rollout plans, and create value before investing further.

Companies need to incorporate in technology launches complete stakeholder engagement and support programs, particularly for suppliers that may lack cybersecurity assets or funds. Publishing training, technical support, and even funds for critical suppliers can contribute an enormous amount to the overall supply chain security.

Technology investment must be studied against security benefits and operational benefits in effectiveness to create sustainable business cases that will cater to the cost of implementation. The research demonstrates that cybersecurity technologies can create significant operating benefits that offset the cost of implementation and create competitive advantage.

Organizational Development Recommendations

Every textile business must form formal cross-functional cyber security boards comprising IT, operations, procurement, quality assurance, legal, and executive management levels. The boards should convene at regular frequencies to synchronize security activities, share knowledge on new threats, and ensure business and security plans stay aligned.

Companies should spend money on creating security-conscious cultures by constant leadership communication, instilling security thought within performance management, and reward systems for security-conscious behaviour. Changing culture is effort but provides a foundation for all other cyber security activity.

Organizations must develop long-term cybersecurity investment strategies placing security as a long-term operational imperative and not as a project. Adherence to long-term investment in technology enhancement, training programs, and process design necessitates strong improvements in security.

Supply Chain Ecosystem Recommendations

Large textile companies need to be in leadership positions building cybersecurity capability throughout their supply chain through supplier training, technical assistance, and implementation support. Those are investments worth making in the larger system by decreasing systemic risk and enhancing overall supply chain resilience.

Industry players should engage in information-sharing programs and mutual security schemes that assist all enterprises, including competitors, as a way of improving their cybersecurity image. Supply chain dependence implies that vulnerabilities in one company can ripple to others and, as such, collaboration is ideal for all members.

Companies should work with vendors of technology, industry associations, and government agencies to develop end-to-end cyber environments that possess resources, support, and coordination models for applying best security practices throughout the entire value chain of textiles.

6.3 Future Research Directions

Sector-Specific Research

There must be follow-up studies that concentrate on cybersecurity issues and solutions in particular niches of the fashion world, i.e., fast fashion, luxury, technical textiles, and sustainable fashion. All these niches possess inherent differences that may require tailored-made cybersecurity practices, and in-depth examination of such differences may be a source of valuable intelligence for tailored deployments.

Cybersecurity in textile production in emerging economies is a highly relevant area of study in the future. Most studies that exist currently concern firms and suppliers from advanced countries, but the majority of the production of textiles is in emerging economies where the capacity and issues of cybersecurity may be quite different.

Because regulation rules of Digital Product Passport become binding across various jurisdictions, longitudinal implementation studies of experience, outcome,

and learnings would be most helpful to business and policymakers. Such studies would track how rules of regulation influence adoption patterns and performance.

Studies on emerging technologies such as artificial intelligence, machine learning, and quantum computing applications in textile supply chain security may define the future challenges and opportunities. Understanding how these technologies could enhance, or supplement existing security processes would help organizations prepare for the next wave of technological advancements.

Organizational and Behavioural Research

Primary research involving drivers of organizational effectiveness in cybersecurity using surveys, interviews, and ethnographic studies will supplement literature-based research in this study. The primary research will yield more data in terms of how organizational factors are related to security outcomes.

Research on the effectiveness of different training and ability development practices for cybersecurity in textile companies would provide practical guidelines to organizations that are keen to engage in curriculum development. In this way, they would be able to invest in human capital development with maximum returns through realizing the best method of training that maximizes outcome**.**

Cross-Industry Comparative Research

Comparative research that compares policies on cybersecurity among various manufacturing sectors may establish sector-wide and sector-specific standards. Such a study can identify what applies more universally in the textile sector and what is specific to the sector.

Research comparing the success of different regulatory approaches to supply chain cybersecurity across different nations and regions might be useful for policymakers looking to implement successful regulatory models. Statistics on the success of different regulatory models might inform future policymaking.

Research on Economic and Business Impact

Detailed analysis of financial return on investment in information security in textile companies, in terms of detailed cost-benefit analysis and return on investment calculations, would allow organizations to make better investment decisions. The study could also identify determinants of the financial impact of information security.

Competitive implications comparisons of security strengths in cybersecurity across the textile industry will allow firms to know how security investment affects firm performance and market standing. Knowing strategic worth in cybersecurity might create greater investment in security across the industry.

The security landscape of the textile supply base continues to be in flux, with threats from emerging technologies, changing threat landscapes, and mounting regulatory pressures. This research provides a general foundation for the understanding of challenge and opportunity as they exist today, but continuous research will be needed to stay on top of the curve in this key arena.

With continued research and collaboration from industry, academic, and government partners, the textile industry can create more secure and hardened supply chains that protect against cyber-attack while enabling sustainable business growth and innovation. This study and these findings form a basis for these endeavours, but their success will derive its origin in ongoing dedication and concerted action throughout the entire value chain of textiles.

References

[1] I. Amed, A. Balchandani, M. Beltrami, A. Berg, S. Hedrich, and F. Rölkens, "The State of Fashion 2019," 2019.

[2] "International Research Journal of Modernization in Engineering Technology and Science", doi: 10.56726/irjmets.

[3] M. Y. Mofatteh, V. Kumar, N. Ramachandra Krishnamoorthy, and O. Fatahi Valilai, "Application of Blockchain Technology and IoT for Sustainable Supply Chain Models," presented at the Proceedings of International Conference on Computers and Industrial Engineering, CIE, 2023, pp. 733–744. [Online]. Available: http://www.scopus.com/inward/record.url?scp=85184137959&partnerID=8YFLogxK

[4] Y.-J. Cai and T.-M. Choi, "A United Nations' Sustainable Development Goals perspective for sustainable textile and apparel supply chain management," *Transp. Res. Part E Logist. Transp. Rev.*, vol. 141, p. 102010, Sep. 2020, doi: 10.1016/j.tre.2020.102010.

[5] "How Much Money lost due to the Counterfeit Fashion Industry?" Accessed: May 18, 2025. [Online]. Available: https://alpvision.com/counterfeit-fashion-industry/

[6] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[7] O. Almashaleh and O. Fatahi Valilai, "Causal Drivers of Sustainable Social Media Engagement in the Textile Industry: A Double Machine Learning Approach," *IEEE Trans. Eng. Manag.*, vol. 73, pp. 495–509, 2026, doi: 10.1109/TEM.2025.3640875.

[8] “Digital product passport for the textile sector | Think Tank | European Parliament.” Accessed: May 17, 2025. [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2024)757808
[9] L. Wang, Y. He, and Z. Wu, “Design of a Blockchain-Enabled Traceability System Framework for Food Supply Chains,” *Foods*, vol. 11, no. 5, Art. no. 5, Jan. 2022, doi: 10.3390/foods11050744.
[10] T. C. Team, “The delicate fabric of our IT ecosystem,” The Choice by ESCP. Accessed: May 18, 2025. [Online]. Available: https://thechoice.escp.eu/tomorrow-choices/supply-chain-attacks-and-the-delicate-fabric-of-our-it-ecosystem/
[11] L. Aniello, B. Halak, P. Chai, R. Dhall, M. Mihalea, and A. Wilczynski, “Towards a Supply Chain Management System for Counterfeit Mitigation using Blockchain and PUF,” Sep. 02, 2019, *arXiv*: arXiv:1908.09585. doi: 10.48550/arXiv.1908.09585.
[12] M. Y. Mofatteh, U. Khadka, and O. Fatahi Valilai, “EnerChain: A decentralized knowledge management framework for smart energy systems with smart manufacturing agents via blockchain technology,” *J. Open Innov. Technol. Mark. Complex.*, vol. 11, no. 1, p. 100499, Mar. 2025, doi: 10.1016/j.joitmc.2025.100499.
[13] A. Badhwar, S. Islam, and C. S. L. Tan, “Exploring the potential of blockchain technology within the fashion and textile supply chain with a focus on traceability, transparency, and product authenticity: A systematic review,” *Front. Blockchain*, vol. 6, Feb. 2023, doi: 10.3389/fbloc.2023.1044723.
[14] C. Stöcker, “Fighting a Growing Global 2 Trillion USD Counterfeiting Market: The Role of Advanced Technologies…,” Spherity. Accessed: May 18, 2025. [Online]. Available: https://medium.com/spherity/guarding-against-counterfeits-the-role-of-advanced-technologies-in-product-safety-secure-data-84d1161711ef
[15] “A Supply Chain Management Perspective on Mitigating the Risks of Product Counterfeiting – Center for Anti-Counterfeiting and Product Protection.” Accessed: May 18, 2025. [Online]. Available: https://a-capp.msu.edu/article/a-supply-chain-management-perspective-on-mitigating-the-risks-of-product-counterfeiting/
[16] D. Callahan, “Protect Your Manufacturing Supply Chain from Cybersecurity Risks,” Cyberstrike Brief. Accessed: May 18, 2025. [Online]. Available: https://www.cyberstrikebrief.com/industrial-operations/protect-your-manufacturing-supply-chain-from-cybersecurity-risks
[17] fashionabc, “Top Cybersecurity Challenges Facing The Fashion Industry For 2024: Emerging Threats and Strategic Responses,” fashionabc. Accessed: May 18, 2025. [Online]. Available: https://www.fashionabc.org/top-cybersecurity-challenges-facing-the-fashion-industry-for-2024-emerging-threats-and-strategic-responses/
[18] European Parliament. Directorate General for Parliamentary Research Services., *Digital product passport in the textile sector.* LU: Publications Office, 2024. Accessed: May 18, 2025. [Online]. Available: https://data.europa.eu/doi/10.2861/947638
[19] “Advanced Anti-Counterfeit Solutions for Textile Industry,” nanomatrixsecure. Accessed: May 18, 2025. [Online]. Available: https://www.nanomatrixsecure.com/textile-supply-chain-management/
[20] A. Farrukh and A. Sajjad, “Investigating Supply Chain Disruptions and Resilience in the Textile Industry: A Systemic Risk Theory and Dynamic Capability-Based View,” *Glob. J. Flex. Syst. Manag.*, vol. 26, no. 1, pp. 57–83, Mar. 2025, doi: 10.1007/s40171-024-00423-x.
[21] S. Boyson, “Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems,” *Technovation*, vol. 34, no. 7, pp. 342–353, Jul. 2014, doi: 10.1016/j.technovation.2014.02.001.
[22] Y. Sheffi, *The Power of Resilience: How the Best Companies Manage the Unexpected*. MIT Press, 2015.

[23] I. Manuj and J. T. Mentzer, “Global supply chain risk management strategies,” *Int. J. Phys. Distrib. Logist. Manag.*, vol. 38, no. 3, pp. 192–223, Jan. 2008, doi: 10.1108/09600030810866986.
[24] J. M. Boyens, C. Paulsen, R. Moorthy, and N. Bartol, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations,” National Institute of Standards and Technology, NIST SP 800-161, Apr. 2015. doi: 10.6028/NIST.SP.800-161.
[25] M. S. Kumar, D. R. D. Raut, D. V. S. Narwane, and D. B. E. Narkhede, “Applications of industry 4.0 to overcome the COVID-19 operational challenges,” *Diabetes Metab. Syndr. Clin. Res. Rev.*, vol. 14, no. 5, pp. 1283–1289, Sep. 2020, doi: 10.1016/j.dsx.2020.07.010.
[26] K. Raustiala and C. Sprigman, “The Piracy and Paradox: Innovation and Intellectual Property in Fashion Design,” *Va. Law Rev.*, vol. 92, p. 1687, 2006, [Online]. Available: https://heinonline.org/HOL/Page?handle=hein.journals/valr92&id=1705&div=&collection=
[27] “Statistics,” International AntiCounterfeiting Coalition. Accessed: May 18, 2025. [Online]. Available: https://www.iacc.org/resources/about/statistics
[28] F. Tao, Q. Qi, A. Liu, and A. Kusiak, “Data-driven smart manufacturing,” *J. Manuf. Syst.*, vol. 48, pp. 157–169, Jul. 2018, doi: 10.1016/j.jmsy.2018.01.006.
[29] A. Brun and C. Castelli, “Supply chain strategy in the fashion industry: Developing a portfolio model depending on product, retail channel and brand,” *Int. J. Prod. Econ.*, vol. 116, no. 2, pp. 169–181, Dec. 2008, doi: 10.1016/j.ijpe.2008.09.011.
[30] T. Götz *et al.*, “Digital product passport : the ticket to achieving a climate neutral and circular European economy?,” Oct. 2022, Accessed: May 18, 2025. [Online]. Available: https://epub.wupperinst.org/frontdoor/index/index/docId/8049
[31] D. Tapscott and A. Tapscott, *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. New York: Portfolio / Penguin, 2016.
[32] B. V. Todeschini, M. N. Cortimiglia, D. Callegaro-de-Menezes, and A. Ghezzi, “Innovative and sustainable business models in the fashion industry: Entrepreneurial drivers, opportunities, and challenges,” *Bus. Horiz.*, vol. 60, no. 6, pp. 759–770, Nov. 2017, doi: 10.1016/j.bushor.2017.07.003.
[33] T.-M. Choi and S. Luo, “Data quality challenges for sustainable fashion supply chain operations in emerging markets: Roles of blockchain, government sponsors and environment taxes,” *Transp. Res. Part E Logist. Transp. Rev.*, vol. 131, pp. 139–152, Nov. 2019, doi: 10.1016/j.tre.2019.09.019.
[34] T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, “Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry,” *Comput. Ind. Eng.*, vol. 154, p. 107130, Apr. 2021, doi: 10.1016/j.cie.2021.107130.
[35] P. M. Madhani, “Supply Chain Transformation with Blockchain Deployment: Enhancing Efficiency and Effectiveness,” vol. 18, no. 4, 2021.
[36] M. Y. Mofatteh, R. Davallou, C. N. Ishimwe, S. S. Divekar, and O. F. Valilai, “Developing a Blockchain Based Supply Chain CO2 Footprint Tracking Framework Enabled by IoT,” *Int. J. Adv. Comput. Sci. Appl. Ijacsa*, vol. 15, no. 10, Art. no. 10, Dec. 2024, doi: 10.14569/IJACSA.2024.0151002.
[37] R. Angeles, “Rfid Technologies: Supply-Chain Applications and Implementation Issues,” *Inf. Syst. Manag.*, Dec. 2005, doi: 10.1201/1078/44912.22.1.20051201/85739.7.
[38] R. Want, “An introduction to RFID technology,” *IEEE Pervasive Comput.*, vol. 5, no. 1, pp. 25–33, Jan. 2006, doi: 10.1109/MPRV.2006.2.
[39] Z. Bi, L. D. Xu, and C. Wang, “Internet of Things for Enterprise Systems of Modern Manufacturing,” *IEEE Trans. Ind. Inform.*, vol. 10, no. 2, pp. 1537–1546, May 2014, doi: 10.1109/TII.2014.2300338.
[40] “Chen, Cheng, Huang - 2013 - Supply Chain Management With Lean Production and RFID Application A Case Study | PDF | Warehouse | Radio Frequency Identification.” Accessed: May 18, 2025. [Online]. Available: https://www.scribd.com/document/322374964/Chen-

Cheng-Huang-2013-Supply-Chain-Management-With-Lean-Production-and-RFID-Application-a-Case-Study?utm_source=chatgpt.com
[41] C. Goebel, C. Tribowski, O. Günther, R. Tröger, and R. Nickerl, "RFID IN THE SUPPLY CHAIN: HOW TO OBTAIN A POSITIVE ROI - The Case of Gerry Weber:," in *Proceedings of the 11th International Conference on Enterprise Information*, Milan, Italy: SCITEPRESS - Science and Technology Publications, 2009, pp. 95–102. doi: 10.5220/0001967700950102.
[42] K. Crooks and A. Haddud, "Using Radio Frequency Identification (RFID) Technology in the Pharmaceutical Supply Chain: The Impact on Competitive Advantage," *Sustainability*, vol. 17, no. 4, Art. no. 4, Jan. 2025, doi: 10.3390/su17041378.
[43] E. W. T. Ngai, K. K. L. Moon, F. J. Riggins, and C. Y. Yi, "RFID research: An academic literature review (1995–2005) and future research directions," *Int. J. Prod. Econ.*, vol. 112, no. 2, pp. 510–520, Apr. 2008, doi: 10.1016/j.ijpe.2007.05.004.
[44] M. Tajima, "Strategic value of RFID in supply chain management," *J. Purch. Supply Manag.*, vol. 13, no. 4, pp. 261–273, Dec. 2007, doi: 10.1016/j.pursup.2007.11.001.
[45] "Trends in Trade in Counterfeit and Pirated Goods," OECD. Accessed: May 18, 2025. [Online]. Available: https://www.oecd.org/en/publications/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en.html
[46] D. Armstrong and L. University, "Research offers strategies to counter counterfeit luxury goods." Accessed: May 18, 2025. [Online]. Available: https://phys.org/news/2024-12-strategies-counter-counterfeit-luxury-goods.html
[47] M. Stevenson and M. Spring, "Flexibility from a supply chain perspective: definition and review," *Int. J. Oper. Prod. Manag.*, vol. 27, no. 7, pp. 685–713, Jan. 2007, doi: 10.1108/01443570710756956.
[48] "Trends in Trade in Counterfeit and Pirated Goods," OECD. Accessed: May 18, 2025. [Online]. Available: https://www.oecd.org/en/publications/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en.html
[49] "Consumer Attitudes Toward Fashion Counterfeits: Application of the Theory of Planned Behavior - Hyejeong Kim, Elena Karpova, 2010." Accessed: May 17, 2025. [Online]. Available: https://journals.sagepub.com/doi/abs/10.1177/0887302x09332513
[50] "Misuse of E-Commerce for Trade in Counterfeits," OECD. Accessed: May 18, 2025. [Online]. Available: https://www.oecd.org/en/publications/misuse-of-e-commerce-for-trade-in-counterfeits_1c04a64e-en.html
[51] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Q.*, vol. 27, no. 3, pp. 425–478, 2003, doi: 10.2307/30036540.
[52] M. Christopher, *Logistics and Supply Chain Management*. Pearson UK, 2022.
[53] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, May 2017, doi: 10.1016/j.cose.2017.01.004.
[54] S. Furnell and N. Clarke, "Power to the people? The evolving recognition of human aspects of security," *Comput. Secur.*, vol. 31, no. 8, pp. 983–988, Nov. 2012, doi: 10.1016/j.cose.2012.08.004.
[55] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans Inf Syst Secur*, vol. 5, no. 4, pp. 438–457, Nov. 2002, doi: 10.1145/581271.581274.
[56] R. Kennedy, "Lack of Cyber Risk Quantification Leaves Companies Financially Exposed, PwC Report Finds," The Global Treasurer. Accessed: May 18, 2025. [Online]. Available: https://www.theglobaltreasurer.com/2024/10/07/lack-of-cyber-risk-quantification-leaves-companies-financially-exposed-pwc-report-finds/
[57] "(PDF) Technological Innovation as a Process." Accessed: May 18, 2025. [Online]. Available:

https://www.researchgate.net/publication/291824703_Technological_Innovation_as_a_Process

[58] J. Baker, "The Technology–Organization–Environment Framework," in *Information Systems Theory: Explaining and Predicting Our Digital Society, Vol. 1*, Y. K. Dwivedi, M. R. Wade, and S. L. Schneberger, Eds., New York, NY: Springer, 2012, pp. 231–245. doi: 10.1007/978-1-4419-6108-2_12.

[59] Y. K. Dwivedi, N. P. Rana, A. Jeyaraj, M. Clement, and M. D. Williams, "Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a Revised Theoretical Model," *Inf. Syst. Front.*, vol. 21, no. 3, pp. 719–734, Jun. 2019, doi: 10.1007/s10796-017-9774-y.

[60] "Case Study Research and Applications," SAGE Publications Ltd. Accessed: May 18, 2025. [Online]. Available: https://uk.sagepub.com/en-gb/eur/case-study-research-and-applications/book250150

[61] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *J. Manuf. Syst.*, vol. 47, pp. 93–106, Apr. 2018, doi: 10.1016/j.jmsy.2018.04.007.

[62] M. Zeynivand, H. Ranjbar, S.-A. Radmanesh, and O. Fatahi Valilai, "Alternative process routing and consolidated production-distribution planning with a destination oriented strategy in cloud manufacturing," *Int. J. Comput. Integr. Manuf.*, vol. 34, no. 11, pp. 1162–1176, Sep. 2021, doi: 10.1080/0951192X.2021.1972459.

[63] "The Cyber-Resilient CEO".

[64] "Counterfeit and pirated goods | OECD." Accessed: May 18, 2025. [Online]. Available: https://www.oecd.org/en/topics/sub-issues/counterfeit-and-pirated-goods.html