УДК 342.951:004.056.5
DOI 10.47367/0021-3497_2025_2_416

GLOBAL PERSPECTIVES ON CYBERSECURITY LAWS AND DATA PROTECTION IN THE TEXTILE INDUSTRY

ГЛОБАЛЬНЫЕ ПЕРСПЕКТИВЫ ЗАКОНОВ О КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЕ ДАННЫХ В ТЕКСТИЛЬНОЙ ПРОМЫШЛЕННОСТИ

N.A. IBRAHIM[1], I.O. JASIM[2], D. SHOOKUMOVA[3], H.N. AL-BAYATI[4], K. SALMAN[5]

Н.А. ИБРАГИМ[1], И.О. ДЖАСИМ[2], Д. ШУКУМОВА[3], Х.Н. АЛЬ-БАЯТИ[4], К. САЛМАН[5]

**([1]Al-Turath University, Baghdad, Iraq,
[2]Al-Mansour University College, Baghdad, Iraq,
[3]Osh State University, Osh, Kyrgyzstan,
[4]Al-Rafidain University College, Baghdad, Iraq,
[5]Madenat Alelem University College, Baghdad, Iraq)**

**([1]Университет Аль-Турат, Багдад, Ирак,
[2]Университетский колледж Аль-Мансура, Багдад, Ирак,
[3]Ошский государственный университет, Ош, Кыргызстан,
[4]Университетский колледж Аль-Рафидаин, Багдад, Ирак,
[5]Университетский колледж Маденат Алелем, Багдад, Ирак)**

Email: dr.khdier.salman@mauc.edu.iq

In the context of the increasing digitalization of the textile industry, increasing its vulnerability to cybersecurity threats, this study assesses the data protection mechanisms and legal frameworks in organizations of different sizes. The paper focuses on cybersecurity practices, security risks, investment efficiency, and policy effectiveness in five categories of enterprises: small, medium, and large manufacturers, international suppliers, and distributors.

The study uses a systems approach, including stratified sampling, probabilistic risk modeling, systems maturity assessment, and compliance testing. Using multivariate analysis, we examine the key relationships between incident frequency, financial losses per incident, level of investment in cybersecurity, and actual system performance.

The results show that international suppliers and large manufacturers have significantly higher financial liability despite a relatively low incident frequency. In contrast, small enterprises experience a much higher rate of breaches, due to their low investment and immaturity in cybersecurity solutions. For small and medium-sized enterprises, the cost-benefit analysis shows that the most effective interventions are employee training (two-thirds of respondents expect a positive effect from implementing training programs) and specialized software (more than 80% of respondents noted a return on the use of targeted software products compared to general-purpose ones).

The presence of formal cybersecurity policies is also associated with a reduction in both the frequency and severity of incidents across all types of organizations. An assessment of technical performance revealed significant differences in latency and throughput metrics, with larger companies generally demonstrating better optimization of technical solutions and higher cybersecurity index scores.

The findings highlight the critical need to develop scalable and affordable protections, as well as to ensure alignment between cybersecurity standards and applicable legal regulations. The article highlights the need for differentiated policies and investment models that take into account the size and complexity of organizations to improve the resilience of the industry to the growing cyber threat.

В условиях нарастающей цифровизации текстильной промышленности, повышающей ее уязвимость к угрозам кибербезопасности, настоящее исследование дает оценку механизмов защиты данных и правовых рамок в организациях различного масштаба. Основное внимание в работе уделяется практике обеспечения кибербезопасности, рискам нарушения безопасности, эффективности инвестиций и результативности политики в пяти категориях предприятий: малые, средние и крупные производители, международные поставщики и дистрибьюторы.

В исследовании применен системный подход, включающий стратифицированную выборку, вероятностное моделирование рисков, оценку зрелости систем и проверку соблюдения нормативных требований. С помощью многовариантного анализа изучены ключевые взаимосвязи между частотой инцидентов, финансовыми потерями на один случай, уровнем инвестиций в кибербезопасность и реальной производительностью систем.

Результаты показывают, что международные поставщики и крупные производители несут значительно большую финансовую ответственность при сравнительно низкой частоте инцидентов. Напротив, малые предприятия сталкиваются с нарушениями гораздо чаще, что обусловлено низким уровнем инвестиций и незрелостью применяемых решений в области кибербезопасности.

Для малых и средних предприятий анализ соотношения затрат и выгод демонстрирует, что наибольшую эффективность дает обучение сотрудников (две трети респондентов ожидают положительный эффект от внедрения программ обучения) и внедрение специализированного программного обеспечения (более 80% респондентов отметили отдачу от применения целевых программных продуктов по сравнению с универсальными).

Наличие формализованных политик в области кибербезопасности также связано со снижением как частоты, так и серьезности инцидентов во всех типах организаций. Оценка технической производительности выявила значительные различия в показателях задержек и пропускной способности: более крупные компании, как правило, демонстрируют лучшую оптимизацию технических решений и более высокие показатели индекса кибербезопасности.

Полученные выводы подчеркивают критическую необходимость разработки масштабируемых и доступных мер защиты, а также обеспечения соответствия между стандартами кибербезопасности и действующими правовыми нормами. В статье акцентируется внимание на потребности в дифференцированных политических мерах и инвестиционных моделях, учитывающих размер и сложность организаций, для повышения устойчивости отрасли к увеличивающейся киберугрозе.

Keywords: cybersecurity, textile industry, breach risk, data protection, investment efficiency, maturity modeling.

Ключевые слова: кибербезопасность, текстильная промышленность, риск проникновения, защита данных, эффективность инвестиций, моделирование зрелости.

Introduction

The international textile industry is diverse and multifaceted global enterprise interconnected within itself and also occupies a prominent position in the global economy. With vast supply chains stretching from raw materials purchases to the delivery of finished products, it has increasingly been turning to digital systems to increase its efficiency, enhance its quality and drive profits. While time this digital transformation delivered enormous positives, including productive production processes, in efficient logistics and improved consumer experiences, it also introduced a myriad of new exposures [1].

The adoption of smart technology has generated a massive increase in the amount of sensitive data that is created and shared via the Internet of Things (IoT), big data analytics and cloud computing. Trade secrets and intellectual property, along with confidential data and customer information, now reside in digital architectures that are an ever more frequent target for cyberattack. The supply chain's interlinkages exacerbate the predicament: one at-risk cog can devastate the operations of several parties, with consequent financial and reputational damage. In addition, because the industry is inherently global, the threats are borderless, putting these companies at even greater cyber risk, which requires robust, joint responses [2].

One of the frequent worries alluded to is protecting supply chains that are typically made up of many different entities spanning multiple locations. These supply chains are examples of the processes that rely on digital technologies to carry out elements like communication with suppliers, inventory management and logistics but are logistic IT systems, are points of vulnerability to be exploited by attackers [7].

Compounding the problem is the lack of uniform regulatory standards for cybersecurity and data protection in the textile sector. This lack of agreement makes it difficult for multinational corporations striving to maintain compliance and consistency across several jurisdictions with varying legal interpretations, standards, and enforcement modalities. The absence of standard guidance also makes it more difficult for smaller businesses, and particularly those in developing markets, to deploy effective cybersecurity protections. leading to a growing risk of data breaches, the theft of intellectual property and industry supply chain disruption [3].

The textile sector is often devoid of the institutional knowledge and the resources needed to set up strong cyber defenses. Many firms, especially smaller manufacturers and suppliers operate on narrow margins and may be more concerned with short-term operational problems than with long-term security spending. Even large, multinationals organizations with significant resources available to them struggle to achieve consistent security across disparate geographic regions and third-party partners [4]. Research suggests that regulatory frameworks have an important role in defining baseline security standards. This includes a range of industries, but all that's still a diverse split-territory between regions, with rules differing significantly. The lack of uniformity complicates compliance, particularly for multinational corporations. The literature [8] shows that there is a gap in design of industry specific guidelines.

As the threat landscape continues to change, traditional solutions such as firewalls or antivirus programs are no longer enough. Cybercriminals are using sophisticated cyberattacks on vulnerable links in the textile industry's digital ecosystem: ransom locks, phishing scams and supply chain attacks. Such threats can disrupt operations and undermine consumer trust. But with increasing consumer awareness of data privacy, and how their data is used, many are becoming less willing to remain in the dark about how their data is being handled. Even a single breach can have a crushing reputational impact, lost loyalty, and a market value blow [5].

Employees in every role, from shop floor worker to C-suite executive to the C-suite, need to be trained to identify threats and react accordingly. Additionally, working together through sharing of knowledge concerning best practices and principles to devise common guidelines that align security across security standards would help alleviate the risks associated with breaches

and establish a more solid foundation for a resilient industry framework [6].

Research [9] quantified the financial loss from data breaches and cyberattacks, further underscoring the business case for taking action to prevent them. In this respect, researchers have advocated greater industry specific inquiry to identify cost efficient mechanisms that ensure security outlays do not compromise operational necessity. Though the textile industry is often not cited itself, casual observation indicates that companies dominating more studied industries should take notes from the textile industry [10].

Protection practices in place will be vital to remaining competitive, safeguarding stakeholder interests and upholding consumer trust.

This article aims to contribute to the ongoing discussion on the right way that we could provide the necessary baselines to harmonize effective cybersecurity policies in ways that do not compromise the security of vital information but rather promote exercise and contingency within the entire textile value chain.

Methodology

The methodological framework for this study integrates data-centric risk quantification, cybersecurity maturity modeling, investment-performance analytics, and policy evaluation design. To ensure empirical rigor, the framework adopts multivariate modeling, structured sampling, and equation-based metric derivations—aligned with international standards in industrial cybersecurity evaluation [2, 3, 6, 11, 12].

Structured Data Collection and Sampling Design

Data collection employed a stratified random sampling method to ensure statistical representation across multiple tiers of textile industry actors, including small-scale manufacturers, medium-scale producers, large integrated enterprises, global suppliers, and regional distributors. The strata were based on firm size, operational complexity, and global market exposure.

Primary data were obtained using:

- Digital cybersecurity audit surveys
- Structured breach and protocol implementation reports
- Enterprise-level compliance checklists

Each firm was evaluated based on the following dimensions:

- Number of confirmed cybersecurity breaches (per annum)
- Financial loss per breach (in USD)
- Percentage of firms with basic cybersecurity protocols (BCP)
- Percentage of firms with advanced cybersecurity frameworks (ACP)

Table 1

Firm Type	Sample Size (N)	Reported Breaches (RB)	Avg. Financial Loss per Breach (AFLB, USD)	BCP Implementation (%)	ACP Implementation (%)
Small-Scale Manufacturers	50	10	5,000	60	20
Medium Manufacturers	75	15	15,000	70	30
Large Enterprises	25	20	50,000	80	50
International Suppliers	30	25	100,000	85	70
Distributors	20	5	10,000	50	15

This dataset serves as the foundational input for the risk assessment, maturity evaluation, and subsequent modeling procedures [11, 13, 14].

Multivariate Cyber-Risk Probability Function

Cyber-risk exposure is quantified using an augmented breach probability function, extending classical risk modeling with dynamic financial scaling. The base equation for breach probability P_i for firm i is:

$$P_i = \frac{\lambda_i \alpha_i}{\phi_i + \epsilon}, \quad (1)$$

where $\lambda_i \in \mathbb{N}$ number of breaches (RB); $\alpha_i \in \mathbb{R}^+$ average financial loss per breach (AFLB), $\phi_i \in [0,1]$ cybersecurity investment index

(CII) normalized, $\epsilon \to 0$ infinitesimal constant to avoid division by zero.

This continuous probability metric accounts for firm-specific financial exposure, breach intensity, and mitigation investments. The index ϕ_i is derived through normalization of per-firm investment metrics:

$$\phi_i = \frac{I_i}{\max(I)} \quad , \qquad (2)$$

where I_i is the reported cybersecurity investment of firm i and max (I) is the maximum investment across the sample [12, 14, 15].

Weighted Cybersecurity Maturity Model (WCMM)

Maturity levels are classified using a weighted additive model that aggregates three core cybersecurity functions: Employee Training Programs (ETP), Encryption Implementation (ENC), and Incident Response Infrastructure (IRI). The model follows:

$$Maturity\ Score_i = w_1\ ETP_i + w_2\ ENC_i + w_3\ IRI_i \qquad (3)$$

Subject to constraints:

$$\sum_{j=1}^{3} w_j = 1, \qquad w_j \in \mathbb{R}^+, \quad ETP_i, ENC_i, IRI_i \in [1,5]$$

where w_1=0.3, w_2=0.35, w_3 =0.35 based on expert calibration. Each component is scored based on compliance levels with ISO/IEC 27001 standards.

T a b l e 2

Firm Type	Employee Training (ETP)	Encryption Adoption (ENC)	Incident Response (IRI)
Small Manufacturers	1	1	1
Medium Manufacturers	2	2	2
Large Manufacturers	3	3	3
International Suppliers	4	4	4
Distributors	1	1	1

This scoring is later mapped to categorical maturity levels (Basic → Integrated) using a 5-interval classification.

Security Investment Efficiency Modeling

To model investment efficiency across cybersecurity programs, a dynamic return function $\mathcal{R}_i$ is defined as:

$$\mathcal{R}_i = \frac{B_i - (C_i + M_i)}{C_i + M_i}, \qquad (4)$$

where B_i benefit in USD (theoretical reduction in expected loss), C_i capital expenditure on cybersecurity systems, M_i operational maintenance costs over one fiscal year.

This formulation is consistent with return-on-security-investment (ROSI) modeling frameworks in enterprise cyber-economics [16, 17]. Additionally, projected financial losses avoided are simulated using stochastic estimators of breach reduction impact rates from controlled firm environments.

The benefit component B_i is parameterized as the product of breach mitigation rate and estimated average loss per breach per firm category.

Policy Effectiveness Evaluation Schema

To assess the institutional effect of formal cybersecurity policies, a pre-post delta model is used. The relative effectiveness ΔE_i for each firm is expressed as:

$$\Delta E_i = \frac{RB_i^{pre} - RB_i^{post}}{RB_i^{pre}} \quad . \qquad (5)$$

And the severity reduction function ΔS_i Delt is given by:

$$\Delta S_i = \frac{SI_i^{pre} - SI_i^{post}}{SI_i^{pre}} \quad , \qquad (6)$$

where RB_i^{pre}, RB_i^{post} breach frequency before and after policy enforcement, and S_i severity Index scored based on impact and recovery time (1–100 scale).

This dual-function model supports inference on whether implemented data protection laws, governance frameworks, or ISO-compliant policies have a statistically significant impact on firm security behavior [5, 8, 18].

Legal and Ethical Framework Alignment

The entire methodology is framed within international data protection and privacy statutes, including the General Data Protection Regulation (GDPR), EU Cybersecurity Act, and ISO/IEC 27001, contextualized for textile supply chains. Ethical compliance, reporting transparency, and human-centric data privacy were observed through the Sustainable Cyber Governance Model [3, 6, 19].

Results

The frequency of cybersecurity breaches and the associated financial losses were analyzed across five categories of firms in the textile sector (fig. 1). These included small and medium manufacturers, large enterprises, international suppliers, and distributors. Breach data were taken from annual security filings by companies, which mirror actual operational weaknesses. This was also assessed with regard to the severity of the financial loss, so that both the economic consequences of these breaches could be ascertained.

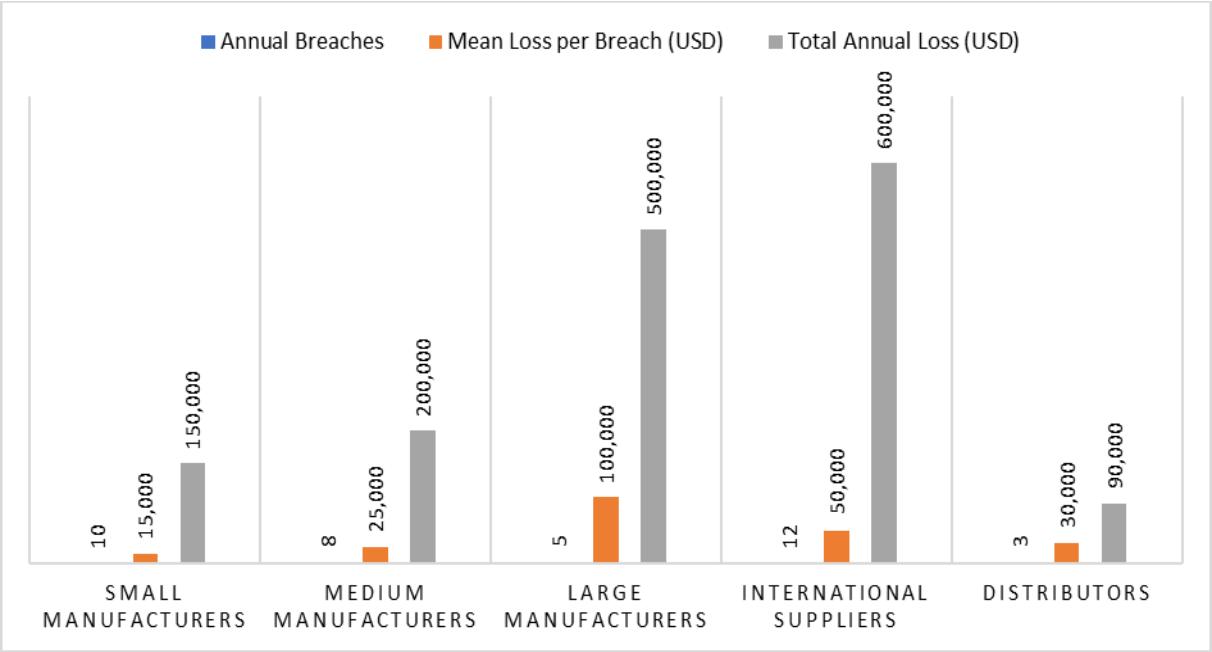

Fig. 1

The data shown in Figure 1 clearly shows that there is a stratification of the effect of cybersecurity breaches conditioned on firm type. Small manufacturers did see more fragmentation here though (10 a year) but were not costless at $15,000 per breach, meaning their modest annual loss, overall, was $150,000. Medium-sized companies had fewer breaches but the cost per breach was higher, tallying an average annual loss of $200,000. Large manufacturers, on the other hand, who reported fewer incidents (5) had a disproportionate loss at $100,000 per breach, for a total loss of $500,000. The vast majority of losses, $600,000, resulted from international suppliers. Distributors had the least number of breaches and moderate losses. These figures illustrate the reality that the larger and more complex the operation, the greater the financial exposure.

Table 1 evaluates the susceptibility of firms to a cyber threat using a risk probability model. The calculation was made on the reported number of breaches, average financial loss per incident, and each firm's cybersecurity investment index.

Table 3

Firm Type	Breaches (λ)	Loss per Breach (USD)	Investment Index (0–1)	Breach Probability Score
Small Manufacturers	10	5,000	0.2	250,000
Medium Manufacturers	15	15,000	0.5	450,000
Large Manufacturers	20	50,000	0.8	1,250,000
International Suppliers	25	100,000	0.7	3,571,429
Distributors	5	10,000	0.4	125,000

Table 3 represent that international suppliers appear to have the highest risk probability scores for severe breaches according to the data, driven by the high frequency of incidents and the significant financial exposure in the investment indices. Similarly, large manufacturers appeared particularly vulnerable, but largely due to the number of dollars lost in each breach. Medium manufacturers balanced their breach count and spend, resulting in a mid-tier risk score. Interestingly, the distributors scored the lowest for minimal exposure. Small manufacturers continued to be vulnerable from inadequate spending on security, too. These findings demonstrate that breach frequency and the investment have primary first-order influences on the cybersecurity risk across firm types.

A cybersecurity maturity assessment was performed to analyze how well enterprises have embedded effective cybersecurity practices. Its review assessed employee training, the deployment of encryption and the establishment of incident response protocols. Each of these aspects was rated on a 1 to 5 scale and merged to form a weighted maturity score. This information allowed firms to be classified into standard maturity levels from Level 1 (basic) to Level 4 (advanced). In fig. 2 we validate the firm's readiness within textiles to defense against Cyber Threats due to procedural health from inside.

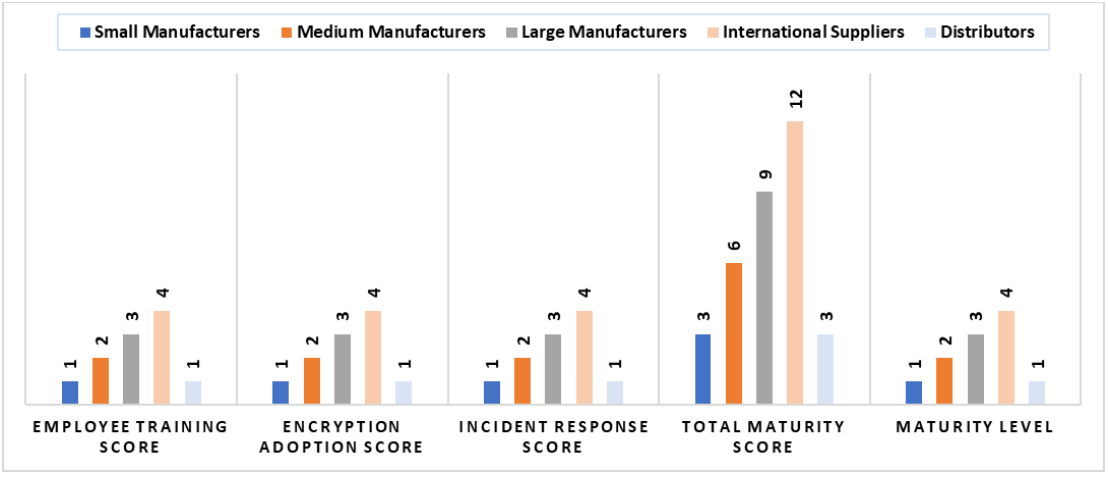

Fig. 2

The results shown in Figure 2 a linear relationship between organizational size and maturity in cybersecurity. International suppliers displayed their highest maturity level (Level 4), showing that they had a mature cybersecurity posture, including strong encryption, active training programs, and advanced incident response capabilities. Level 3 was attained by large manufacturers that demonstrated seemingly steady, but not necessarily optimal development. Medium manufacturers were placed in Level 2, indicating a transitional phase of development. Small manufacturers and distributors faired poorly (Level 1) with little security infrastructure in place and a clear need for significant investment in both technology and personnel training. The data highlight the disparity in cybersecurity adoption between big enterprises and smaller entities.

Fig. 3 reflects upon the financial return that firms received from adopting specific cybersecurity measures. They included every-

thing from antivirus and firewalls to employee training, enterprise-level security systems and cloud-based defense platforms. Return on Investment (ROI) was calculated against the total cost of each measure (upfront and ongoing costs) relative to the financial loss avoided as a result of reduced breaches in terms of volume or severity.

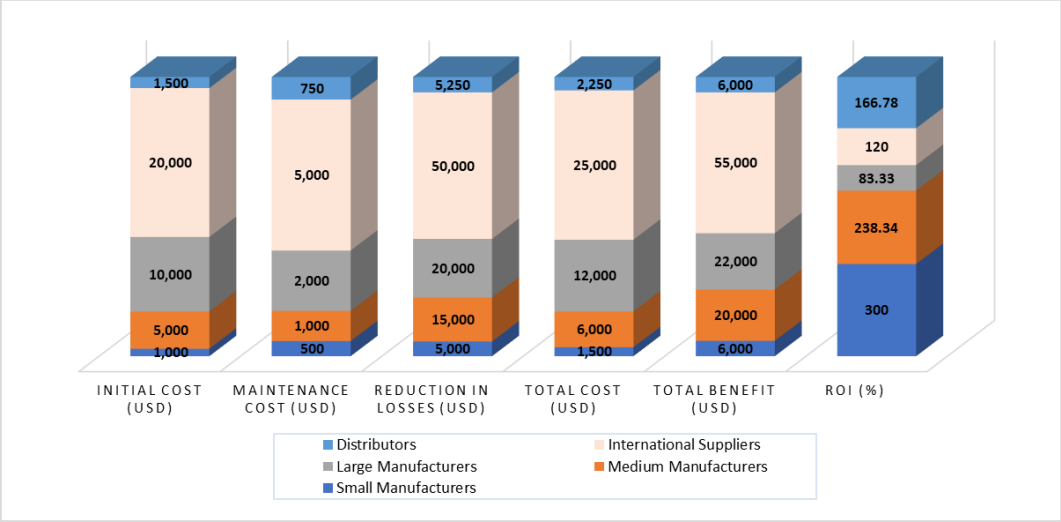

Fig. 3

Small manufacturers achieved the highest ROI (300%), primarily due to the relatively low costs of their implemented solutions and the noticeable reduction in losses. Medium manufacturers also demonstrated strong returns (238.34%), confirming the value of employee training and endpoint security systems. Large manufacturers and international suppliers experienced moderate returns, as their higher investment levels produced proportionate benefits, but at reduced efficiency. Distributors, with minimal expenditures, yielded a respectable 166.78% ROI. The data suggest that while high-end systems are essential for larger firms, smaller organizations can achieve substantial protection gains through low-cost interventions if applied strategically.

The influence of cybersecurity policies was examined by comparing breach data before and after policy adoption (table 4). This included evaluating breach frequency, financial losses mitigated, and changes in a firm's Security Index score a composite indicator of overall threat management improvement. The objective was to assess whether formalized policy adoption, such as ISO/IEC 27001-based protocols, GDPR-aligned processes, leads to measurable improvements in cybersecurity outcomes across various categories of textile firms.

Table 4

Firm Type	Breaches Before Policy	Breaches After Policy	Mean Reduction Rate (%)	Financial Savings (USD)	Improved Security Index
Small Manufacturers	15	10	33	10,000	0.30
Medium Manufacturers	20	12	40	30,000	0.40
Large Manufacturers	25	15	40	50,000	0.50
International Suppliers	30	20	33	100,000	0.60
Distributors	10	6	40	5,000	0.20

Policy implementation had a positive effect on all firm types (Table 4). The highest breach rate reduction rate of 40% and the most significant average cost savings of $30,000 (medium manufacturers) and $50,000 (large manufacturers), were recorded. International

suppliers had the highest absolute savings, $100,000, although the reduction rate was a bit lower. The Security Index scores increased steadily with firm maturity levels from 0.20 for distributors to 0.60 for international suppliers. The results reinforce that standardized cybersecurity policies improve security outcomes and provide measurable risk reduction benefits, particularly in organizations with existing technical infrastructure and governance capability.

Two critical performance metrics in cybersecurity are latency (the time it takes to detect a threat) and throughput (the number of threats that can be handled per second). In fig. 4 we analyze these indicators to assess system responsiveness across firm types. The efficiency ratio was used to measure how efficiently each firm processes incoming threats. The higher the throughput and lower the latency, the better the overall performance, which is key in automated or digital integration textile processing for tackling advanced persistent threats.

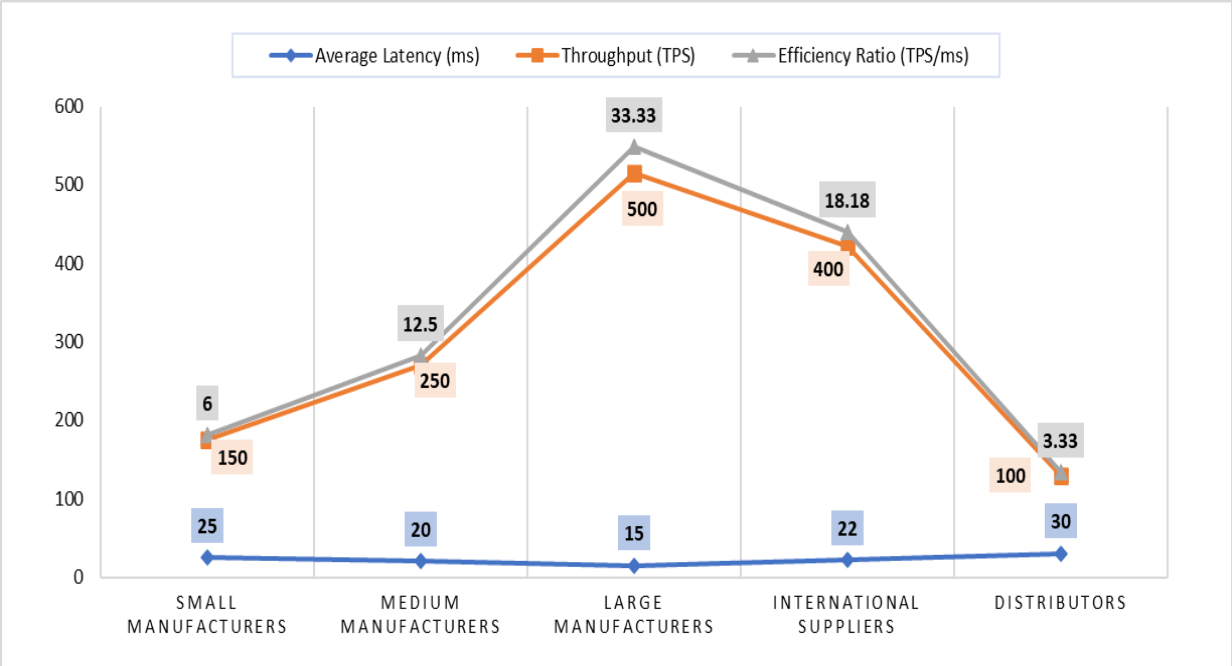

Fig. 4

As demonstrated in Figure 4, significant manufacturers had the best performance when it comes to their system showing the most throughput (500 TPS) and the lowest latency (15 ms) leading to an efficiency ratio of 33.33 TPS/ms. International suppliers also performed strongly (response time) likely reflecting proper firewall architecture and extensive automated monitoring systems. The medium manufacturers produced balanced metrics with satisfactory latency and a noteworthy throughput that earned a robust efficiency score. In contrast, small manufacturers and distributors fell behind, underscoring a need to upgrade detection and processing systems. These disparities highlight infrastructure investment's contribution to facilitating real-time cyber defense capabilities that are important for firms processing high throughput across a multitude of movable data goods.

A composite Cybersecurity Performance Index (CPI) derived from the latency and throughput measures we analyze in fig. 5. This index shows how well a firm's security systems do against the maximum possible latency (30 ms) and throughput (500 TPS). The CPI is between 0 and 1 and enables easy benchmarking across both firm sizes and infrastructure levels. A higher score on the CPI indicates that the cybersecurity environment is proportioned and well-versed and optimized.

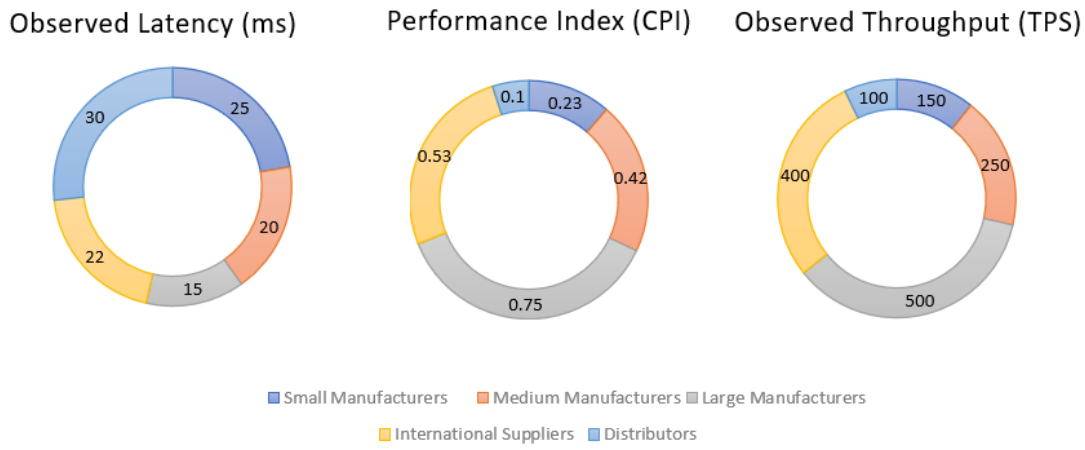

Fig. 5

Compared to all firm types, large manufacturers reached 0.75 CPI, showing a good merger between low latency and high processing power. International suppliers had a score of 0.53, signifying their advanced maturity level combined with a strong infrastructure. Medium manufacturers scored fair, while small firms and distributors scored below 0.30, indicating acute underdevelopment of real-time response capabilities. Specifically, the CPI reveals systemic discrepancies in cybersecurity deployment and emphasizes the need for investment and policy attention among firms with lower indices. It acts as a marker for regulators and industry stakeholders seeking to kick up cyber security preparedness in the textile industry.

Discussion

The findings of this study present an interesting picture of the issues facing cybersecurity and data protection within the global textile industry. The results suggest that companies have unique vulnerabilities depending on their size and operational scope, and smaller manufacturers and distributors are the most likely to fall prey to breaches. The frequency of breaches and financial losses reported here emphasize both the real costs of cybersecurity defects, as well as highlight the broader systemic threat in the industry's growing interconnected supply chains [15].

A major insight is the extent to which targeted investments in cybersecurity drive down both the frequency and severity of breaches. By virtue of their superior resources, larger manufacturers enjoy a distinct advantage in deploying advanced cybersecurity controls that lead to the lower breach frequencies, and certainly higher overall performance index. In contrast, many smaller firms find themselves unable to budget adequately for strong security frameworks. This gap demonstrates an industry-wide demand for more accessible, affordable, and scalable cybersecurity options across companies of all levels [12].

What is also noteworthy about this study is the quantification of the impact of standardized security policies. Companies that use consistent, well-defined security policies experience significant decreases in the number of breaches as well as the severity of incidents. Fostering regional and international regulatory harmonization will be a godsend for mitigating the cybersecurity risk facing the textile industry. The fragmented regulatory landscape creates compliance hurdles for global firms, but the positive outcomes for companies with stringent policies illustrate the advantages of a consolidated approach [20].

When comparing these findings to previous studies, it is clear that the cybersecurity profile of the textile industry differs starkly from other sectors. While research in areas such as finance or healthcare often highlights the rapid embrace of security technologies, the textile sector seems relatively sluggish on this front. This gap is due to a variety of factors: tighter working margins, less investment in IT as a whole, and a legacy focus on physical infrastructure rather than into digital systems [21, 22]. However, as digital transformation becomes more and more prominent, sophisticated cybersecurity solutions must be introduced as well [17].

It is the fact that textile supply chain is so interconnected that makes it a man attraction for the criminals of the internet. With more manufacturers and suppliers using IoT devices, cloud platforms and big data analytics, the attack surface is growing. This poses a risk and increases the demand for proactive threat management strategies that move beyond traditional perimeter defenses [23].

Cybersecurity systems which work optimally ensure breaches are avoided altogether, and that operational disruptions created through incident responses are as minimal as possible. Companies that push fewer products over time at lower latency without compromising security have proven that cybersecurity and controlled production processes are not inherently at odds. This is consistent with industry trends emphasizing the importance of operational resilience as being equal to that of security; succeeding in integrating these two will likely result in significant competitive advantages [24].

In this larger context, these results mean that the textile sector is at an inflection point. Some firms especially the larger ones are progressing to full cybersecurity solutions approach, other still falls behind. Industry-wide initiatives and standards may be needed to level the playing field between small and large companies, as small and big firms experience stark differences in breach rate, financial loss, and performance metric vulnerabilities. In addition to regulatory changes, initiatives may also include industry attempts to create common best practices, provide training programs, and set standards for cybersecurity certification [19].

The discussion reflects both progresses made and the challenges that remain in securing the global textile industry's digital infrastructure. By highlighting such vulnerability areas, quantifying targeted investment benefits in these areas, and examining the role of an appropriately consistent regulatory environment, this study adds to a body of work dedicated to policy and practice in an area deserving of greater attention. The results highlight that clear policies and standardization, technological adoption, and cross-sector collaboration will be crucial in creating a more resilient and secure textile industry going forward.

Conclusion

The article has delved into the changing landscape of cybersecurity laws and data protection in the industry, identifying key takeaways that can inform more effective strategies and policies moving forward.

One of the key findings of the study is a clear link between targeted cybersecurity investments and better security outcomes. The results also underscore the need for standardized security policies. A third key finding is that the specific characteristics and complexity of the textile supply chain require tailored solutions; Ensuring that the typology and scale of solutions developed are appropriate to particular what are known as 'systems of routing' within the supply chain.

The study also highlights the need for proactive threat management. As the digital transformation of the industry accelerates, older patterns of cooperation are increasingly challenged and a new understanding is needed, an understanding that the findings from experiences across multiple organizations will contribute to.

The global textile industry has a brief window of opportunity to reshape cyber measures and data protections. By making data-driven investments in secure infrastructure, facilitating standardized policies, and launching collaborative initiatives, it can help create a more secure digital landscape that will not only reduce risks but help foster innovation and resilience.

REFERENCES

1. *Giannopoulos M., Tsagkatakis G., Tsakalides P.* Higher-Order Convolutional Neural Networks for Essential Climate Variables Forecasting. Remote Sensing, 2024. **16**, DOI: 10.3390/rs16112020.

2. *Das S., Panda P.* Use of Artificial Intelligence on Cyber Security and the New-generation Cyber-attacks. International Journal For Multidisciplinary Research, 2024. **6**(2). https://doi.org/10.36948/ijfmr.2024.v06i02.14521

3. *Morales-Sáenz F.I., Medina-Quintero J.M., Reyna-Castillo M.* Beyond Data Protection: Exploring the Convergence between Cybersecurity and Sustainable Development in Business. Sustainability, 2024. 16(14), 5884; https://doi.org/10.3390/su16145884

4. *Layode O., Naiho H., Labake T. et al.* Addressing Cybersecurity Challenges in Sustainable Supply Chain Management: A Review of Current

Practices and Future Directions. International Journal of Management & Entrepreneurship Research, 2024. **6**(6). p. 1193…1214

5. *Obasi S.C. et al.* Cybersecurity's Role in Environmental Protection and Sustainable Development: Bridging Technology and Sustainability Goals. Computer Science & IT Research Journal, 2024. 5(5): p, 1145…1177 DOI: 10.51594/csitrj.v5i5.1140

6. *Lande O., Layode O., Naiho H. et al.* Circular economy and cybersecurity: Safeguarding information and resources in sustainable business models. Finance & Accounting Research Journal, 2024. **6**(6). p. 953…977, DOI: 10.51594/farj.v6i6.1214

7. *Alqudhaibi A. et al.* Towards a sustainable future: developing a cybersecurity framework for manufacturing. Technological Sustainability, 2023. **2**(4): p. 372…387.

8. *Oleksiewicz I., Civelek M.* Where Are the Changes in EU Cybersecurity Legislation Leading? Humanities and Social Sciences quarterly 2023. **30**(4). https://doi.org/10.7862/RZ.2023.HSS.50

9. *Sharma A.* The Impact of Cybersecurity Breaches on Big Businesses. International Journal of Advanced Research, 2024: p. 10…25.

10. *Amosu O., Kumar P., Ogunsuji Y. et al.* Enhanced cybersecurity measures: Protect customer data in e-commerce and retail industry. World Journal of Advanced Research and Reviews, 2024. **23**(02): p. 890…900.

11. *Vance D. et al.* Smart manufacturing maturity models and their applicability: a review. Journal of Manufacturing Technology Management, 2023. **34**(5): p. 735…770.

12. *Corallo A. et al.* Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level. IEEE Transactions on Engineering Management, 2023. **70**(11): p. 3745…3765.

13. *He C.Z. et al.* The Impact of Customer-Reported Cybersecurity Breaches on Key Supplier Innovations and Relationship Disruption. Journal of Information Systems, 2023. **37**(2): p. 21…49.

14. *Saeed S. et al.* A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors, 2023. **23**, DOI: 10.3390/s23167273.

15. *Saeed S. et al.* Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors, 2023. **23**, DOI: 10.3390/s23156666.

16. *Song J. and Park M.J.* A system dynamics approach for cost-benefit simulation in designing policies to enhance the cybersecurity resilience of small and medium-sized enterprises. Information Development, 2024: p. 02666669241252996.

17. *Kumar S. and Mallipeddi R.R.* Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. Production and Operations Management, 2022. **31**(12): p. 4488…4500.

18. *Zhu J.J. et al.* A Preemptive and Curative Solution to Mitigate Data Breaches: Corporate Social Responsibility as a Double Layer of Protection. Journal of Marketing Research, 2024. **61**(4): p. 778…801.

19. *Mahmood S., Chadhar M., Firmin S.* Cybersecurity Challenges in Blockchain Technology: A Scoping Review. Human Behavior and Emerging Technologies, 2022. **2022**(1): p. 7384000.

20. *Ahouanmenou S., Amy V.L., Poels G.* Information security and privacy in hospitals: a literature mapping and review of research gaps. Informatics for Health and Social Care, 2023. 48(1): p. 30…46.

21. *Zorin L.B., Zorina N.V., Kholopov V.A.* Industry 4.0: Approaches and Prospects for Use in Light Industry. Izvestiya Vysshikh Uchebnykh Zavedenii, Seriya Teknologiya Tekstil'noi Promyshlennosti, 2023. 1(403), p. 40…44.

22. *Polzunova N.N.* Digital Technologies in the Activities of the Textile Enterprises and the Efficiency of their Application. Izvestiya Vysshikh Uchebnykh Zavedenii, Seriya Teknologiya Tekstil'noi Promyshlennosti, 2022. 2(398), p. 21…30.

23. *Osman R. and El-Gendy S.* Interconnected and resilient: A CGE analysis of AI-driven cyberattacks in global trade. Risk Analysis, 2024. 45(4): p. 846…862 DOI: 10.1111/risa.14321

24. *Manivannan R., Senthil Kumar T.* Improved restricted Boltzmann machine-based optimization model for the network security system in cloud environment. Engineering Research Express, 2024. **6**(2): p. 025313. DOI: 10.1088/2631-8695/ad3f77

Рекомендована 4th International Conference of New trends and Smart technology. Baghdad, Iraq. Поступила 07.04.2025.