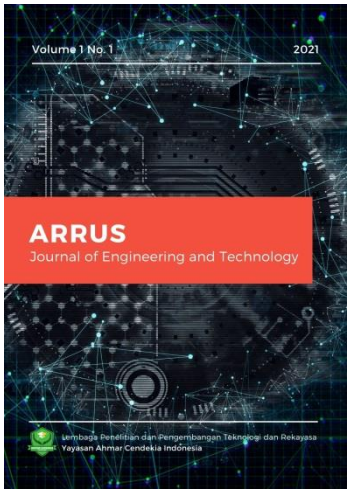
https://doi.org/10.35877/jetech3434

OPEN ACCESS

ISSN [Print]: 2776-7914



REVIEW ARTICLE

A Review of Cybersecurity Framework Implementation for Retail Industry: Challenges and Recommendations

Eleonora Anggi Ardhaninggar, Kallamulah Ramli *

*Department of Electrical Engineering, Faculty of Engineering, University of Indonesia, Depok, West Java.

*Corresponding author: Kallamulah Ramli, Department of Electrical Engineering, Faculty of Engineering, University of Indonesia, Depok, Indonesia

E-mail: k.ramli@eng.ui.ac.id

Abstract: Efforts to improve services by opening online data access to customers have become straightforward targets for cybercrime. Unfortunately, the researchers' findings reveal that there is presently no cybersecurity framework that completely aligns with the fundamental principles of the retail industry. This paper then analyzes the deployment of cybersecurity frameworks across various industrial sectors to determine which framework—or combination of frameworks—best aligns with the fundamental values of the retail industry. We compare the essential points of each cybersecurity framework with the TWOS Matrix, which represents the core values of the retail industry. We suggest NIST CSF, ISO/IEC 27001:2022, and Essential Eight as the best combination of cybersecurity frameworks for the retail industry. Therefore, the comparative analysis results recommend RCF as a novel framework suitable for implementation in the retail industry.

Keywords: Cybersecurity Framework, Retail Industry, Cybersecurity Framework Implementation, NIST, ISO 27001

1. INTRODUCTION

Today's technology and digitalization trends are rapidly expanding, impacting many people across all industry sectors. For example, we are familiar with the use of mobile phones, tablets, computers, and others as our tools to connect with the world online. The ease of use of today's technological devices also makes it easier for us to access various kinds of desired information, such as news from distant families across the island, information about the latest clothing trends on other continents, information about today's global economy, and so on. All industry sectors face the challenge of adapting to this rapid and significant growth. This includes leveraging technological devices to digitize data, enabling employees to access it anytime and anywhere, and enhancing the quality of services provided to customers. Organizations are also adapting to the rapid and large technological growth by implementing Internet-of-Things solutions to streamline production processes and enhance consumer shopping satisfaction, ensuring their brand remains relevant to their market and consumers. However, the efforts to improve services by opening access to large amounts of data online and to many people have become an effortless target for cybercrime. According to the Palo Alto Network's white paper, cybercrime poses a risk to all industry sectors, as evidenced by the growing number of cyberattacks, which have reached 1,636 attacks per organization per week, indicating a 30% increase year-over-year from 2021 to Q2 of 2024, as reported by Check Point. Therefore, the organization's technology division should prioritize strengthening industrial policy and implementing standardization in the application of technology within the industry.

https://doi.org/10.35877/jetech3434

ISSN [Print]: 2776-7914

However, many organizations are still not fully aware of this risk; they often view it as less urgent than the importance of the transactions required to achieve the daily, weekly, monthly, or annual sales goals they set annually. One example is the retail industry, where sales rely on online applications that connect transaction data from branches to headquarters. With so many consumers shopping both *offline* and *online*, customer data is a tempting prize for hackers who can benefit by selling or misusing the data. Regrettably, there is a lack of prioritization in enhancing systems and technology to address cybersecurity requirements, and the retail industry faces significant challenges in managing the risk of customer data ownership due to the preserved high investment prices at the outset. Besides that, the efforts of integration between the implemented technology and existing business models, as well as the efforts to manage all employees' participation in the change plan, starting with the initial briefing, training, and implementation that must be well scheduled and communicated, were the most challenging things for the retail industry in compensating for the rapid and large technology growth adaptation. Moreover, it could be argued that the rate of cyberattacks contributes to the relatively low data, which hovers around 9% compared to other industry sectors.

For the sake of increasing the security maturity level, there is still another way to be done by the retail industry, such as implementing the cybersecurity framework from the smallest and simplest things within the organization, because not a few boards of management later abandoned the idea of upgrading the security maturity level after seeing the high price of the initial investment. We can define the implementation of a cybersecurity framework as the optimal approach, as it aids in managing cybersecurity risks, creating a shared language for internal and external use, standardizing service delivery, and enhancing efficiency. Many cybersecurity frameworks, such as HECVAT for educational security, NIST for business purposes, ISO/IEC 27001:2022 for compliance with other cybersecurity regulations, and Essential Eight, which outlines eight crucial technical controls for organizations, are available globally. This paper aims to identify which cybersecurity framework that best suits retail organizations, considering both external regulations and the core values of the retail industry. We conduct a thorough review of numerous journals to determine the prevalent and industry-appropriate frameworks, and then we analyze the aspects of each framework that align with the TWOS Matrix of retail organizations, representing the core values of the retail industry.

The rest of the paper has a literature review of each chosen framework, a summary review of some picked journals, then explanation of the research method follows by the findings and analysis. Last, the conclusion provides a summary of the main points discussed before, then the references follow.

2. Literature Review

2.1. The Cybersecurity Framework Implementation

The researchers have analyzed research findings presented in journals addressing the implementation of cybersecurity frameworks across diverse industries. This search served as a reference and guideline in conducting this study. Based on the obtained results, it appears that there is currently no discussion surrounding the implementation of a cybersecurity framework for the retail sector. The researchers then looked at previous research about commonly used frameworks. They also examined the core values and strategies of the retail industry to ensure their framework aligns with industry needs and doesn't overburden retail companies. We have listed some of the research journals below.

2.1.1. Review of Cyber Security in Oil and Gas Industry in United Arab Emirates: Analysis of the Effectiveness of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework

The oil and gas sector in the UAE is especially susceptible to cyberattacks. This research shows that the NIST cybersecurity framework provides an effective strategy for combating cybercrime because of its flexibility, which encourages continuous improvement. This

https://doi.org/10.35877/jetech3434

ISSN [Print]: 2776-7914

research aims to enhance the framework's effectiveness by identifying its weaknesses, thereby increasing its resilience to cyberattacks. Furthermore, the results of this research can assist industry stakeholders in various oil-exporting nations, including the UAE, in reconfiguring the framework's structure by enhancing its elements, thereby fortifying and reinforcing information security. This research scrutinized cyber risk management publications, which encompass frameworks, standards, guidelines, and best practices put forth by government bodies, industry, and ten standardization organizations.

2.1.2. A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations

Research on cybersecurity for small and medium enterprises (SMEs) is still very limited and tends to focus on preventive aspects, such as security policies and procedures. Meanwhile, the detection, response, and recovery aspects of cyberattacks, which are increasingly common in SMEs, still receive less attention in research. This paper examines recent studies on the cybersecurity of small and medium-sized businesses (SMBs), emphasizing the correlation of this research with the widely recognized NIST Cyber Security Framework (CSF). Then summarize the primary challenges that small and medium-sized businesses encounter in establishing effective cybersecurity and conclude with essential recommendations for its implementation. Qualitative analysis dominates SMB cybersecurity research, focusing primarily on the Identify and Protect functions of the NIST Cybersecurity Framework, while the other existing functions receive less attention. Small and medium-sized businesses must possess the capability to detect, respond to, and recover from cyberattacks; insufficient research in these domains may leave them with minimal guidance on appropriate actions.

2.2. ISO/IEC 27001:2022

Global standardization in information security management enables organizations to systematically safeguard information and implement an Information Security Management System (ISMS) in a cost-effective manner. ISO/IEC 27001:2022 delineates policies and procedures for the implementation, maintenance, and enhancement of an organization's Information Security Management System (ISMS) applicable to enterprises of all sizes. The fundamental principles of ISO/IEC 27001:2022 include a holistic approach, technical controls, corporate culture, and continuous improvement to remain pertinent to evolving changes and challenges.

ISO/IEC 27001:2022 perceives information security as an integrated and interdependent system. Every facet of the organization, encompassing board management, entry-level personnel, business processes, and utilized information technology, contributes to the preservation of information security.

2.3. NIST CSF 2.0

The American National Institute of Standards and Technology (NIST) created the NIST Cybersecurity Framework (CSF) 2.0 to aid organizations in identifying, managing, and mitigating security risks. Composed of three elements: CSF Core, CSF Organizational Profiles, and CSF Tiers. CSF Core is the principal component of CSF, encompassing high-level cybersecurity taxonomy results that assist the organization in managing its security risks. CSF Organizational Profiles delineate the organization's present or aspirational cybersecurity posture. CSF Tiers delineate the framework through which an organization assesses and mitigates its security risks, as illustrated in the figure below.

https://doi.org/10.35877/jetech3434

ISSN [Print]: 2776-7914

(a) (b)

Figure 1: NIST CSF 2.0 elements: (a) NIST CSF Core Function and Organizational Profiles, (b) NIST CSF Tiers

NIST CSF 2.0 is distinctive due to its flexibility, allowing organizations with limited initial investment to enhance their security maturity. We achieve this by deconstructing the CSF Core to identify adoptable components, defining CSF Organizational Profiles, and evaluating their current or target profiles through the CSF Tiers. This is applicable to organizations of all sizes. NIST CSF 2.0 facilitates adoption across organizations of all sizes, and while certification is not required for implementation, the framework can serve as a baseline for security audits.

2.4. Essential Eight

The Australian Cyber Security Center (ACSC) has established a series of cybersecurity mitigation procedures comprising eight fundamental guidelines for organizations to safeguard systems and data against cyberattacks. The Essential Eight emphasizes the most effective, yet straightforward measures outlined in Table 1.

These frameworks necessitate minimal requirements, rendering them highly cost-effective for the organization. Organizations must determine and strategize the maturity level appropriate for their environment by evaluating the Essential Eight mitigation strategy, which comprises four maturity levels: level zero (commonly accepted), level one, level two, and level three. They subsequently identify the desired maturity levels for enhancing their cybersecurity system.

Table 1: The Essential Eight's Mitigation Strategy

Application Control	Restrict Administrative Privileged
Patch Application	Patch Operating Systems
Configure Microsoft Office Macro Settings	Multi-factor Authentication
User Application Hardening	Regular Backups

3. Research Method

In the absence of a cybersecurity framework specific to the retail industry, the author initiates this research with a literature review of prior journals concerning cybersecurity framework implementation across various sectors to identify a suitable framework for adoption. Then conducts interviews with the management of retail businesses to understand their fundamental core values and perspectives on the retail industry and uses the TOWS matrix to evaluate the strategic planning in place. After figuring out what the strategic plan is and why it's important, the author conducts a qualitative comparative analysis of each selected cybersecurity framework, examining each component and subsequently connecting them to retail's core values. We put the strategic plan next to the cybersecurity framework that was previously used to look at all the theoretical parts and choose the right category for each core value. Additionally, the strategic plan is also used to assess how optimistic the retail industry is regarding efforts to enhance cybersecurity, so that the framework plan created is relevant and its implementation can be carried out continuously in the future.

https://doi.org/10.35877/jetech3434

ISSN [Print]: 2776-7914

4. Results and Discussion

4.1. Retail's Industry Core Values and TOWS Strategic

The initial phase involves recognizing the strengths, weaknesses, opportunities, and challenges encountered by the company, along with the essential values within the retail sector, which are derived from discussions with business stakeholders on the board management. We will perform a strategic examination using the TOWS Matrix approach. A TOWS matrix assists in synthesizing information and developing a strategic plan for progression. TOWS provides a foundational framework for developing a strategy that highlights necessary changes and offers several benefits, such as it provides a transparent visual representation of the core components of the strategy, also its evaluates both internal factors and external influences (see Appendix 1).

The interview results also yielded several perspectives on various aspects of retail business, such as the products/services offered, pricing, location, promotion, service quality, supply chain, and business mode. These aspects led to the identification of core values in retail business, which act as fundamental principles for companies in their operations and interactions with customers, employees, and other stakeholders. These values shape the company culture and differentiate one company from another, among other things:

1. The company is customer-centric, prioritizing the needs and satisfaction of customers by providing personalized shopping experiences and promptly addressing consumer complaints.
2. We consistently seek new innovations that meet or exceed market needs, utilize technology to create enjoyable shopping experiences, and implement creative and effective marketing methods.
3. Integrity encompasses being truthful and transparent with consumers, guaranteeing the excellence of products marketed, and maintaining ethical business practices.
4. Efficiency is the ability to manage costs optimally without compromising customer service.

4.2. The Comparison of Cybersecurity Framework

Next, we will execute a mapping of cybersecurity framework operations using data sources from popular information security and cyber frameworks used by numerous organizations, including ISO/IEC 27001:2022, NIST CSF 2.0, and Essential Eight. We will conduct the evaluation of cybersecurity frameworks using comparative analytical methodologies that consider definitions, focus, structure, scope, objectives, details, implementation, and the number of subcategories and levels, as outlined in the subsequent table.

Table 2: The Comparative Analysis Components of Common Cybersecurity Framework

Components	ISO/IEC 27001:2022	NIST CSF 2.0	Essential Eight
Definition	International standard that offers a framework for the establishment and management of Information Security Management Systems (ISMS).	The framework established by NIST (National Institute of Standards and Technology) in the United States to assist enterprises in identifying, managing, and mitigating cyber threats.	The framework established by the Australian Cyber Security Centre (ACSC) serves as a fundamental reference for safeguarding systems and data against cyber threats.
Focus	Comprehensive, covering all aspects of information security, from management to technology.	Increased flexibility, enabling enterprises to tailor solutions to their individual requirements.	Specifically, concentrating on the eight most efficacious fundamental controls to safeguard systems and data.
Structure	Process-oriented, utilizing a Plan-Do-Check-Act cycle.	Function-oriented, comprising five fundamental functions: Identify, Protect, Detect, Respond, and Recover.	Control-oriented, featuring eight requisite controls for implementation.

https://doi.org/10.35877/jetech3434

ISSN [Print]: 2776-7914

Scope	Universal, relevant to all categories of organizations.	Primarily utilized in the United States, however gaining popularity worldwide.	Particularly for companies in Australia, however applicable to others as well.
Objective	Providing a comprehensive framework for building and managing an Information Security Management System (ISMS). The goal is to protect the organization's information assets from various threats.	Helping organizations identify, manage, and mitigate cyber risks. The focus is on flexibility and adaptability to diverse types and sizes of organizations.	Providing basic guidelines to protect systems and data from cyber-attacks. The focus is on the most effective controls to reduce common cyber risks.
Details	Very detailed, featuring numerous controls and sub-controls that require implementation.	More flexible, allowing organizations to choose the most relevant controls.	Simpler, with eight clear and specific controls.
Implementation	Requires strong management commitment and sufficient resources.	Easier to accommodate many sizes and categories of businesses.	Relatively easy to implement, even for organizations with limited resources.
Sub-categories Quantity	93	106	8
Level Quantity	-	Tier 1 – Tier 4	Level 0 – Level 3

4.3. The Retail's Cybersecurity Framework (RFC) Mapping

Implementing a cybersecurity framework in retail businesses entails more than merely installing security software; it necessitates fundamental changes in organizational operations and requires commitment from the whole organization. Through a systematic and sustainable approach, retail companies can protect valuable assets, build customer trust, and ensure business continuity. We conducted a mapping of core values based on these three frameworks, as presented in table 5, which serves as a cybersecurity framework for retail organizations.

Table 3: Cybersecurity Framework and Retail's Core Values Mapping

CORE VALUES	ISO/IEC 27001:2022	NIST CSF	Essential Eight
Consumer Satisfaction	A.7.5, A.8.29	PR.AA-03, PR.AA-04, PR.DS-10, PR.DS-11, DE.AE-04, DE.AE-06, RS.CO-03, RC.RP-03, RC.RP-04	Multi-factor Authentication, Patch Operating System, Restrict Administrative Privileges.
Innovation	A.5.36,	PR.PS-01, PR.PS-02, DE.CM-03, DE.CM-09, RS.AN-03, RS.AN-06	
Integrity	A.5.1, A.5.15, A.5.26, A.6.3, A.7.13, A.8.11, A8.13	ID.AM-05, ID.AM-07, ID.RA-5, ID.RA-06, PR.AA-01, PR.AA-02, PR.AT-01, PR.DS-10, PR.DS-11, DE.CM-06, DE.CM-09, DE.AE-02, DE.AE-03, RS.MI-01, RS.MI-02, RC.RP-01, RC.RP-02	Application Whitelisting, Patch Application, Configure Microsoft Office Macros, Restrict Administrative Privileges, User Application Hardening
Efficiency	A.7.5, A.8.7	PR.IR-01, PR.IR-02, PR.IR-03, DE.CM-01, DE.CM-02, DE.CM-06, RS.MA-02, RS.MA-03, RC.CO-03	

The mapping process has identified several similar categories among the core values in the retail industry. It is also broken down into five groups of NIST CSF 2.0 functions and sub-groups of ISO/IEC 27001:2022. The Essential Eight from NIST CSF 2.0 is mapped into each of these groups of functions. The image below illustrates our proposed framework for the retail industry.

https://doi.org/10.35877/jetech3434

OPEN ACCESS

ISSN [Print]: 2776-7914

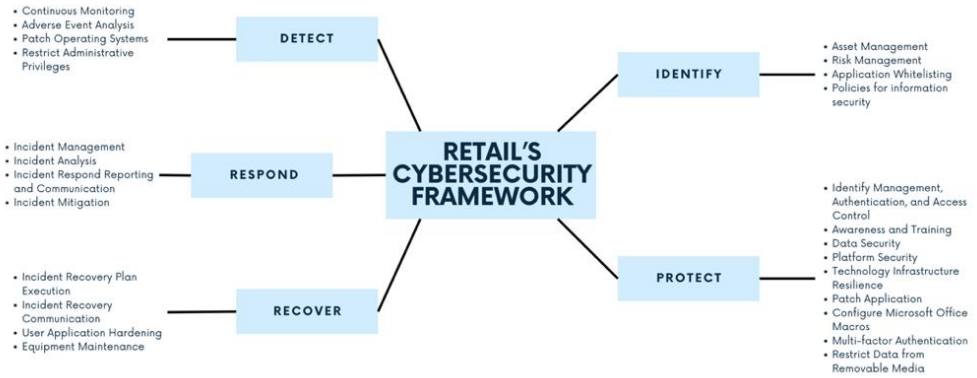


Figure 2: Retail's Cybersecurity Framework (RCF)

5. Conclusion

Connected to its strategic analysis, the retail sector possesses significant potential for growth and development. To attain these objectives, the retail sector must aggressively rectify existing deficiencies and capitalize on emerging opportunities. Through the implementation of appropriate policies, the retail sector may enhance its resilience and competitiveness in the digital age. Moreover, strategic analysis suggests that the retail sector remains optimistic about adopting cybersecurity measures that don't necessarily require substantial initial expenditures. One such measure is the incremental implementation of a cybersecurity framework for the retail industry, as depicted in Figure 4. This foundation aligns with the study's objectives, which include aligning the cybersecurity framework with core values and strategic analysis. This alignment enables retail companies to customize their security framework to their operational requirements, identify potential security vulnerabilities, and prioritize remediation efforts based on risk and business impact through precise mapping. In addition, by understanding the relationship between business values and security requirements, retail companies can protect their valuable assets and build customer trust. To provide a more comprehensive picture of the current state of cybersecurity implementation, further research can deeply examine the development of the framework through the weighting and level determination stages. Additionally, this study can refine the framework through comparisons with other aspects of the retail industry, thereby offering company leaders comprehensive improvement recommendations on the necessary steps and follow-up actions to ensure the protection of data/information held by each organization in general and the retail industry in particular.

References

Symantec. (2024). Cyber Security for Retail Services: Strategies that Empower your Business, Drive Innovation and Build Customer Trust. https://docs.broadcom.com/doc/cybersecurity-retail-en

Upguard. (2024). A Complete Guide to Cybersecurity. https://images.g2crowd.com/uploads/attachment/file/1300374/A-Complete-Guide-to-Cybersecurity.pdf

Donegan, P. (2022). Preparing for New Incident Reporting Requirements. HardenStance, PaloAlto Networks, November 2022

Australian Signals Directorate. (2022). Essential Eight Maturity Model. Australian Government, November 2022 , cyber.gov.au

Yigit Ozkan, B., Spruit, M. (2022). Adaptable Security Maturity Assessment and Standardization for Digital SMEs. *JOURNAL OF COMPUTER INFORMATION SYSTEMS*, https://doi.org/10.1080/08874417.2022.2119442

https://doi.org/10.35877/jetech3434

ISSN [Print]: 2776-7914

Chidukwani, A., Zander, S., Koutsakis P. (2022). A Survey on the Cyber Security of Small-to-Medium

Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*, Open Access Journal, Digital Object Identifier 10.1109/ACCESS.2022.3197899 Volume 10 2022

Patrizia Carello, M., Marchetti Spaccamela, A., Querzoni, L., Angelini, M. (2023). A Systematization

of Cybersecurity Regulations, Standards and Guidelines for the Healthcare Sector. Systematization of Cybersecurity doc. for the Health Sector, arXiv:2304.14955v1 [cs.CR] 28 Apr 2023

JumahALDhanhani, M., Mat Jizat, J. E. (2021). Review of Cyber Security on Oil and Gas Industry in

United Arab Emirates: Analysis on the Effectiveness of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework. Turkish Journal of Computer and Mathematics Education, Vol.12 No.11(2021), 714-720

AlBenJasim, S., Takruri, H., Al-Zaidi, R., Dargahi, T. (2024). Development of cybersecurity

framework for FinTech innovations: Bahrain as a case study. International Cybersecurity Law Review (2024) 5:501–532, https://doi.org/10.1365/s43439-024-00130-4

Petar Radanliev, P., Dave De Roure, D., Nurse, J. R.C., Nicolescu, R., Huth, M., Cannady, S., Mon

talvo, R. M. (2019). Cyber Security Framework for the Internet-of-Things in Industry 4.0. Munich Personal RePEc Archive, MPRA Paper No. 92565, https://mpra.ub.uni-muenchen.de/92565/

Alqudhaibi, A., Deshpande, S., Jagtap, S. and Salonitis, K. (2023), "Towards a sustainable future:

developing a cybersecurity framework for manufacturing", *Technological Sustainability*, Vol. 2 No. 4, pp. 372-387. https://doi.org/10.1108/TECHS-05-2023-0022

Imran, H., Salama, Dr. M., Turner, Dr. C., Fattah, Dr. S. (2022). Cybersecurity Risk Management

Frameworks in the Oil and Gas Sector A Systematic Literature Review. Advances in Information and Communication (pp.871-894), DOI:10.1007/978-3-030-98015-3_59

Roy, P. P. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the

ISO 27001 Information Security Standard. Natl. Conf. Emerg. Trends Sustain. Technol. Eng. Appl. NCETSTEA 2020, vol. 53, pp. 27001–27003, 2020, doi: 10.1109/NCETSTEA48365.2020.9119914

Merchan-Lima, J., Salinas, F. A., Oquendo, L. T., Sanchez, F., Fonseca, G. L., Quiroz, D. (2020).

Information security management frameworks and strategies in higher education institutions: a systematic review. Ann. des Telecommun. Telecommun., pp. 2019–2021, 2020, doi: 10.1007/s12243-020-00783-2

Yaqoob, T., Abbas, H., Shafqat, N. (2020). Integrated Security, Safety, and Privacy Risk Assessment

Framework for Medical Devices. IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 6, pp. 1752–1761, Jun. 2020, doi: 10.1109/JBHI.2019.2952906.

Prajanti, A. D., Ramli, K. (2019). A Proposed Framework for Ranking Critical Information Assets in

Information Security Risk Assessment Using the OCTAVE Allegro Method with Decision Support System Methods. https://www.researchgate.net/publication/335140807

Meszaros, J.,Buchalcevova, A. (2017). Introducing OSSF: A framework for online service

cybersecurity risk management. Computers and Security, vol. 65, pp. 300–313, Mar. 2017, doi: 10.1016/j.cose.2016.12.008

https://doi.org/10.35877/jetech3434

OPEN ACCESS

ISSN [Print]: 2776-7914

Appendix 1: TOWS Matrix of Retail Industry Representation Strategic

	Strength	Weakness
TOWS Matrix	1. Solid relationships with suppliers 2. Extensive branch network 3. Loyal customer base 4. Commitment to responsible business ethics	1. Delay in adopting technology. 2. Constraints in product customization. 3. Enhancing human resource skills requires considerable time. 4. The initial investment cost for technology is regarded as comparatively high.
Opportunity	**Strength – Opportunity**	**Weakness - Opportunity**
1. Sales through marketplaces 2. Social Media 3. AI Technology	- Leveraging a wide branch network for the implementation of new security standards. - Using product innovation to develop new security features. - Utilizing social media to enhance Security Awareness Among Employees and Customers.	- Forming partnerships with Cybersecurity Companies to strengthen infrastructure. - Keeping up with AI Technology trends to enhance threat detection.
Threats	**Strength – Threats**	**Weakness - Threats**
1. Changes in consumer behavior 2. Competition with new players 3. Global economic conditions that are not conducive 4. Increase in raw material prices	- Utilizing supplier relationships to acquire optimal security products. - Strengthening business ethics to avert internal data breaches.	- Implementing Cyber Insurance to alleviate financial loss risk. - Executing cyberattacks simulations or pen test to assess readiness