Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. 2025.0007, Cite as: https://doi.org/10.69709/COConnect.2025.178512

SCIFINITI

Research Article

OPEN ACCESS

Dynamic Information Security Systems through Adaptive Architecture

Rachel John Robinson✉,[1]

[1]IT Faculty, IU University of Applied Sciences, Frankfurter Allee 73A, 10247 Berlin, Germany

Article History
Submitted: January 2, 2025 Accepted: May 22, 2025 Published: June 26, 2025

Abstract
The manufacturing industry is at the forefront of a digital transformation that promises significant enhancements in product and service quality. However, this technological shift also raises concerns about data security and information protection. In response to these challenges, a research study was conducted to investigate cybersecurity incidents in the manufacturers and assess the effectiveness of the Zero-Trust Architecture (ZTA) as a solution. The primary objectives of this research were to examine the growing concern about cybersecurity breaches in manufacturing, analyze the vulnerabilities of manufacturing institutions and their impact on security, and evaluate the potential of ZTA as a solution to mitigate these risks. To achieve these objectives, a mixed-methods approach was employed. Interviews and surveys were used to gather data from key stakeholders, including manufacturer executives and employees. The results revealed several significant insights into cyber threats in the manufacturing sector. These included the prevalence of various types of cybersecurity incidents, the risk posed by employee practices and human error, and the preparedness of manufacturers in managing and recovering from breaches. Notably, the study highlighted specific attacks associated with manufacturers, such as financial operations via ATM skimming and email phishing attacks. Key takeaways from this research include the following: Zero Trust Architecture (ZTA) provides a robust solution for mitigating cybersecurity risks in the manufacturing industry. Additionally, financial threats such as ATM skimming and the prevalence of phishing attacks pose significant risks to manufacturers and their customers. Overall, this study provides valuable insights into the challenges facing manufacturers in protecting themselves against cyber threats and highlights the potential of ZTA as a critical component in their security posture.

Keywords:
zero-trust architecture; vulnerabilities; quantitative research; phishing attacks; cybersecurity; security models

1. Introduction

Cybersecurity is the discipline of protecting computer systems, networks, devices, and data from unauthorized access, cyberattacks, and loss or damage of information [1]. It covers a spectrum of technologies, techniques, and approaches used to ensure the integrity, availability, and privacy of digital assets. Confidentiality, Integrity, and Availability—collectively referred to as the CIA triad and shown in Figure 1—constitute a fundamental concept in cybersecurity.

Cybersecurity is now a key concern for people, companies, and governments worldwide, as digital technology is widely used and reliance on networked systems increases. A major component of cybersecurity is the mitigation of threats [1]. To lower the possibility of cyberattacks, one must find, assess, and minimize possible risks and vulnerabilities. Among the most often occurring cyberthreats of today are malware (including viruses, ransomware, and spyware), phishing efforts, distributed denial-of-service (DDoS) attacks, insider threats, and social engineering attacks. Cybersecurity initiatives seek to find, halt, and neutralize these threats by means of tools such as firewalls, intrusion detection systems, antivirus software, access restrictions, and security awareness training.

Application security is another facet of cybersecurity that focuses on protecting software applications and

* **Corresponding Author:**
Rachel John Robinson, IT Faculty, IU University of Applied Sciences, Frankfurter Allee 73A, 10247 Berlin, Germany, info@rachel-johnrobinson.com

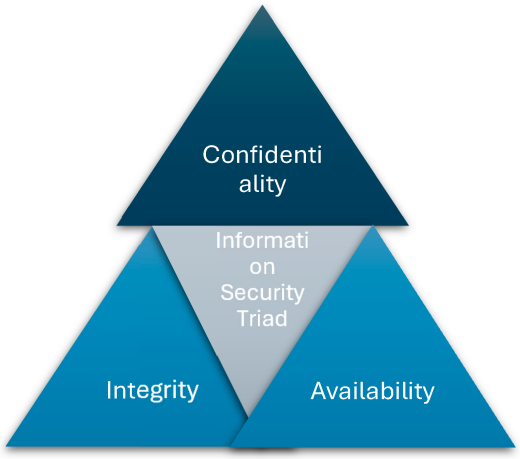

Figure 1: The CIA Information Security Triad.

online services from attacks and vulnerabilities [2]. Web application firewalls (WAFs), penetration testing, vulnerability assessments, and safe coding practices can all help to identify and close security flaws in software programs. Furthermore, cloud security protects platforms, infrastructure, and cloud-based services against security breaches and cyberattacks [2]. Identity and Access Management (IAM), data encryption, access restrictions, and security monitoring are among cloud security solutions meant to protect data and programs housed in cloud settings. Cybersecurity is essential to safeguard digital assets, defend data privacy, maintain corporate processes running smoothly, and inspire confidence in digital systems and services.

1.1. Security and Issues in the Manufacturing Industry

From common malware and phishing attempts to more complex cyberthreats like ransomware, distributed denial-of-service (DDoS) assaults, and insider threats, the manufacturing industry is vulnerable to a wide range of cybersecurity risks. These dangers are increasingly exposing manufacturers' digital assets, consumer data, and financial transactions, leading to monetary losses, reputational damage, and regulatory fines [3].

Several factors contribute to cybersecurity vulnerabilities in the manufacturing industry. Among the most crucial ones are the obsolete IT systems, the lack of investment in cybersecurity infrastructure and resources, the evolving nature of cyberthreats, and the insufficient cybersecurity awareness and training given to manufacturer staff and clients [3]. Cybercriminals also exploit new attack vectors and vulnerabilities introduced by the integration of digital financial systems and manufacturing services. Given the essential importance of the manufacturing sector in the financial system and the growing use of digital technology to improve manufacturing services, cybersecurity in the sector is of major consequence.

1.2. Past Cybersecurity Incidents in the Manufacturing Industry

Manufacturers began experiencing cybersecurity issues after they started using digital technologies. Since then, there has been a noticeable rise in cybersecurity incidents, which pose serious dangers to consumers, manufacturing institutions, and the integrity of the financial system. The following are noteworthy instances of cybersecurity mishaps that have previously affected the sector.

- Malware assault: The WannaCry ransomware assault, which affected manufacturers and other institutions globally, was the subject of a 2017 warning from the Manufacturers of Ghana. The goal of the attack was to encrypt data on compromised systems and demand ransom payments to release the decryption keys [4].
- Data Breach: Unauthorized access to data, including financial records, personal identification numbers, and account information for customers, is known as a data breach. For instance, a data breach at Commercial Manufacturer, Agricultural Development Manufacturer (ADM), in 2018 resulted in the compromise of its clients' personal information. Customers began to worry about the security of their personal information as a result of this data breach in 2018, which resulted in monetary losses and reputational harm [5].
- Phishing Scam: This type of scam tricks manufacturer personnel or customers into disclosing private information, like account numbers or login credentials, by sending them false emails, texts, or webpages. Phishing attacks on clients of several manufacturers, banks, including Eco Manufacturer and SC Bank, were also reported in 2019. The objective of these assaults was to pilfer money and personal data from gullible targets [6].

1.3. Statement of Problem

The manufacturing industry is currently experiencing a significant digital revolution, with a growing dependence on technology to provide financial resources effectively and adapt to the changing needs of customers. However, this advancement has brought about growing concerns over cybersecurity breaches in manufacturing institutions. As manufacturing institutions adopt digitalization, they not only benefit from technological developments but also

2025, Vol. 2, Article ID. 2025.0007
https://doi.org/10.69709/COConnect.2025.178512

become primary targets that aim to exploit weaknesses in the digital ecosystem.

The primary objectives of this study are as follows.

- To analyze the state of cybersecurity incidents in manufacturers,
- To identify vulnerabilities and the impact of cybersecurity incidents on manufacturers,
- To explore the theoretical foundations and applications of Zero-Trust Architecture (ZTA). and.
- To examine the potential of Zero Trust Architecture (ZTA) in mitigating cybersecurity risks in Manufacturers.

1.4. Significance of Study

This study holds academic importance by contributing to the burgeoning field of cybersecurity research, particularly within the context of the manufacturing sector in developing economies. The exploration of cybersecurity incidents in manufacturing, along with the evaluation of Zero Trust Architecture (ZTA), contributes valuable insights to the existing body of knowledge. It provides a nuanced understanding of the challenges faced by manufacturing institutions and advances the discourse on innovative cybersecurity frameworks [7]. This research will help protect financial assets and maintain customer trust in the context of the growing concern over cybersecurity incidents, especially in the manufacturing sector. Through vulnerability identification, evaluation of existing cybersecurity protocols, and recommendation of ZTA implementation, the study seeks to help manufacturers strengthen their defenses. Thus, the confidentiality of sensitive customer data will be preserved, financial transactions will be secure, and the trust that underpins manufacturer-client relationships will be upheld [7].

2. Methods

2.1. Traditional Security Models and Their Limitations

As the manufacturing sector grapples with the growing concern of cybersecurity incidents, it becomes imperative to scrutinize the traditional security models employed by manufacturing institutions. The following reviews examine the strengths and limitations of the Traditional Security Models, shedding light on the challenges they face in mitigating modern cyber threats.

Traditional Security Models in Manufacturing- Conventional security models, such as the perimeter-based approach, have long served as the mainstay of cybersecurity plans at global manufacturers. To stop unwanted access and safeguard the network perimeter, these models depend on building robust exterior defenses [8]. These approaches are often the primary means of protecting sensitive financial data in the manufacturing sector.

Perimeter-Based Security-Creating a safe perimeter around the network is the cornerstone of traditional security methods. Virtual private networks (VPNs), intrusion detection systems, and firewalls are frequently employed to fortify borders and keep bad actors out [8]. Even though perimeter protection can be useful in certain situations, it is not sufficient when dealing with advanced cyberthreats.

Limitations of Traditional Models- Traditional security approaches, however popular in the past, have a number of drawbacks that make them less effective in the modern threat environment. Their immobile nature is one of their main drawbacks. Conventional approaches are ill-suited to address the dynamic and ever-evolving nature of cyber threats because they presume a clear division between the internal and external networks [8]. The inadequacy of depending entirely on perimeter security increases as cyber attackers become more proficient.

Insider Threats and Traditional Models- Insider threats, in which people with authorized access abuse their privileges for malevolent ends, are a problem for traditional security frameworks. Employees in the manufacturing industry have access to sensitive client and financial data, making this vulnerability especially pertinent to the industry [9]. Those with malevolent intent within the network can take advantage of the trust that exists there.

2.2. Introduction to Zero-Trust Architecture (ZTA) and Alignment with Manufacturers' Challenges

There is a rising awareness that traditional security strategies might not be adequate in light of the growing concern over cybersecurity events in institutions. The idea of Zero-Trust Architecture (ZTA) as a cutting-edge, flexible cybersecurity paradigm is explored in this overview of the literature. ZTA presents a proactive approach to security that is in line with the ever-evolving nature of cyber threats by upending traditional trust frameworks. It is essential to comprehend ZTA's underlying principles and applications to assess how beneficial it might be for manufacturers. ZTA provides a more robust security posture by continuously verifying trust and reducing the attack surface through micro-segmentation and the enforcement of least privilege access. Conventional models, on the other hand, rely on perimeter defenses that are less effective against internal threats.

Evolution of Security Paradigms- Changes from perimeter-based security models to more dynamic and adaptable ones are necessary due to the growth of cyber threats. ZTA promotes a "never trust, always verify" stance, which is a break from the conventional "trust but verify" style of thinking [9]. This change is especially important for manufacturers since a more robust security architecture is required in light of the growing threat scenario.

Foundational Principles of ZTA- At the core of ZTA are several foundational principles that distinguish it from traditional security models. These principles include continuous verification, the least privilege access, micro- segmentation, and the assumption of compromise [9]. Each principle contributes to creating a security environment where trust is not automatic but continually validated based on real-time conditions.

Continuous Verification- The idea of continual verification is one of ZTA's main principles. ZTA continuously confirms the identity and security posture of users and devices during their interactions with the network, in contrast to existing models that give access based on static credentials [10]. This real-time validation improves the capacity to quickly identify and address possible security concerns.

Least Privilege Access-ZTA ensures that users and devices have the least amount of access necessary to do their tasks by upholding the principle of least privileged access. This lessens the potential repercussions of a security failure by restricting unauthorized access to vital resources [10]. In manufacturing, where insider threats are significant, least privilege access reduces potential damage from compromised credentials.

Micro-Segmentation- A key component of ZTA is micro-segmentation, which entails breaking the network up into smaller, more isolated sections. Communication between segments is restricted until explicitly approved, and each segment is viewed as a separate trust zone [11]. In the case of a compromise, this granular technique limits lateral movement within the network, strengthening the security posture of institutions.

2.3. Differentiating ZTA and Gaps Identified

Notable differentiations and gaps can be identified within the context of a manufacturer's cybersecurity domain, such as: Integration of Advanced Technologies: While the literature discusses traditional security models and Zero Trust Architecture (ZTA), there is a lack of comprehensive studies on the integration of advanced technologies such as artificial intelligence, machine learning, and blockchain in enhancing cybersecurity. Exploring how these technologies can be effectively implemented to prevent cyber threats and improve security protocols could fill this gap [12].

Human Factors in Cybersecurity: The primary focus is on technical aspects of cybersecurity, but there is limited understanding of the human factors involved. Research on employee training, awareness programs, and the role of human behavior in cybersecurity breaches is relatively scarce. Examining the impact of human factors on cybersecurity and developing strategies to mitigate risks associated with human errors could be beneficial.

Regulatory and Compliance Challenges: More research is needed on the regulatory and compliance challenges faced by institutions in implementing robust cybersecurity measures. Examining the effectiveness of existing regulations and identifying areas where improvements are needed could help in developing more comprehensive and effective cybersecurity policies and procedures.

Cost-Benefit Analysis of Cybersecurity Investments: While manufacturers invest in cybersecurity, there is limited research on the cost-benefit analysis of these investments. Understanding the financial implications of different cybersecurity measures and their impact on overall security could provide valuable insights for decision-makers in the banking sector [12].

Impact of Cybersecurity on Customer Trust and Adoption: Research on how cybersecurity measures influence customer trust and the adoption of digital services is limited. Investigating the relationship between cybersecurity practices and customer perceptions could help manufacturers to develop strategies to enhance trust and encourage the use of digital service areas [13].

Some of the above-noted areas are taken in such as the advanced technologies, awareness areas, data breach methodologies, etc., are explored for research orientation in this article.

2.4. Methodological Assumptions

According to Owusu and Antwi [14], information security in manufacturing involves a combination of technical and human elements; hence, a mixed approach of quantitative and qualitative methods will be employed in the conduct of this research. Quantitative methods through surveys using questionnaires will provide statistical evidence of trends and patterns in cyber threats, while qualitative methods through focused interviews will offer insights into the contextual factors influencing cybersecurity practices and the perceived effectiveness of zero-trust architecture [14]. Also, qualitative aspects are to be incorporated through focused discussion pointers and questions as

2025, Vol. 2, Article ID. 2025.0007
https://doi.org/10.69709/COConnect.2025.178512

part of data collection and analysis. By integrating these diverse perspectives and approaches, this research seeks to provide actionable insights that can form the basis for effective cybersecurity strategies. Figure 2 provides a pictorial view of the methodology that will govern the conduct of this research.

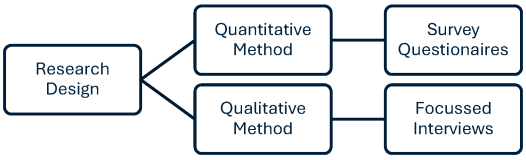

Figure 2: Research Methodology Framework.

Validity and reliability are critical aspects of research methodology that ensure the accuracy, consistency, and credibility of research findings. According to Rachel [15], validity and reliability are key concepts in research that contribute to the study's credibility and dependability. Internal and external validity techniques will be used collectively to ensure the validity of this study. To achieve internal validity, the research will ensure that chosen techniques are matched to the specific objectives of the research. The utilization of mixed procedures, encompassing surveys and interviews, is crucial in guaranteeing that the collected data is thoroughly investigated the research topic to accomplish the required objectives. The study selected its respondents using random sampling, as seen from the outside. As explained by [15], random sampling in surveys is essential to external validity as it ensures that the responses can be generalized to the entire population under study.

Reliability will be achieved through the proper structuring of data collection tools, efficient sampling techniques, and consultation with experts. Both the surveys and interviews will be structured in a manner that will solicit the required data. By carefully organizing the data gathering instruments, using effective sample strategies, and consulting with specialists, reliability can be attained. The design of the surveys and interviews will also ensure that the necessary information will be gathered.

2.5. Data Collection and Analysis

According to Postigo [16], effective data collection methods are essential for acquiring accurate and comprehensive information to address the objectives of the research. To achieve this goal, this study will use both quantitative and qualitative data collection methods. These methods will involve administering surveys and conducting interviews with selected manufacturers, cybersecurity experts, IT professionals, customers, policy makers, and other stakeholders within the manufacturing industry. To conclude, the study is to collect data from 100 participants within the industry.

Quantitative Data Collection Methods- Surveys will be distributed to a representative sample of employees across different roles within the selected manufacturers. The survey instrument will be designed to collect quantitative data on the awareness of cybersecurity incidents, current security measures, and the perceived efficacy of ZTA. The survey will employ a customized 5-point Likert scale, where respondents will provide their opinions against established scales such as strongly agree (SA), agree (A), neutral (N), disagree (D), and strongly disagree (SD), with corresponding weights of 5, 4, 3, 2, amongst other metrics. Other questions will involve multiple-choice questions (MCQs), which are essential in allowing the quantification of information security vulnerabilities and the prevalence of existing security measures. A stratified random sampling method was employed to ensure a diverse sample of at least 100 staff from a population of 1000 employees representing various departments and hierarchical levels within manufacturers. Participants will include staff from IT, risk management, operations, and other relevant departments. The surveys will be administered electronically, utilizing online survey platforms and direct email communication. The survey questionnaire will include a mix of Likert-scale questions, multiple-choice questions, and open-ended questions to capture both quantitative and qualitative responses.

Qualitative Data Collection Methods- Qualitative data will be collected through semi-structured interviews. This is to allow flexibility in exploring participants' experiences, perceptions, and insights regarding cybersecurity incidents and ZTA. The interview will cover topics such as cybersecurity threats faced, current security measures, challenges encountered, and potential attitudes towards the adoption of ZTA. These interviews will target key stakeholders within the manufacturing sector, such as cybersecurity experts, IT professionals, manufacturing staff, and representatives from these institutions. Participants in this interview will be selected through a purposive sampling technique, ensuring diversity and expertise in cybersecurity measures and challenges. The qualifications and role of participants for this interview will be a consideration for their selection. This is to ensure that the data gathered is a true representation of the targeted population and that the data can be generalized to the whole Manufacturing industry.

Data Analysis- Data analysis is a pivotal phase in research methodology, which offers the means to interpret and derive meaningful insights from the collected data. In order to carry it out in terms of organizing, analyzing, and drawing insights from data sources like interviews, reli-

able sources, and open-ended questions, tools like NVivo and ATLAS.ti were used. In cybersecurity, data analysis provides valuable insights into the nature, scope, and impact of cybersecurity threats. It also enables researchers to assess the effectiveness of potential mitigation strategies. According to [16], a researcher can assess the severity and frequency of cybersecurity incidents and anticipate future risks by analyzing historical data on cybersecurity incidents to identify trends, patterns, and emerging threats. To explain [17] further that by analyzing data to pinpoint vulnerabilities, researchers can prioritize security measures and allocate resources effectively to mitigate risks.

Descriptive analysis will be used to investigate the quantitative data collected from participants via the tools used. Dataset to include more clarity and provide insights into the different objectives of the research, and thereby link accordingly. According to Bank of Ghana [17], descriptive statistics help in simplifying and summarizing complex data sets, making them essential for initial data analysis in research contexts such as cybersecurity in manufacturing. This will involve summarizing and visualizing the collected data to gain insights into the frequency, distribution, and patterns of cybersecurity incidents within manufacturers. Generating summary statistics, such as mean, median, and standard deviation, combined with tables, charts, or graphs, will be used to illustrate the trends and correlations in the data collected [17]. Content and Thematic Analysis enables researchers to systematically explore and interpret complex qualitative data. This method provides deep insights into the patterns, themes, and meanings that emerge from the data [17]. Based on this, the Qualitative data generated from this research will be analyzed through content analysis, while thematic analysis will be used to identify patterns and themes in the qualitative data. The qualitative data will further be summarized through descriptive statistics to extract meaningful trends. This will include the use of mean value, standard deviation, and frequencies, summarized and presented through tables, graphs, and charts.

3. Results

This section describes the data findings about the study's objectives. Except the third objective, each is supported by both qualitative and quantitative analyses as presented below.

3.1. Objective 1: To Analyze the State of Cybersecurity Incidents in Manufacturers

The first objective sought to answer the question, "What is the landscape of cybersecurity incidents in Manufacturers?". To achieve this objective, respondents were asked a series of questions through surveys and interviews conducted with small-scale manufacturers from various sectors. First, respondents were asked about how concerned they are about the increasing frequency of cybersecurity incidents in manufacturing. As shown in Figure 3, using a 5-point Likert scale where 1 means "Not Concerned" and 5 means "Very Concerned", 38.6% of the respondents indicated that they were very concerned about the increasing rate of cybersecurity incidents within the manufacturing industry. This group was closely followed by 22.9% of respondents who believed that they were "Concerned" about this growing rate, while 10% expressed they were not concerned at all. This feedback indicates that a high percentage of the respondents expressed a worrying concern about the frequency of cybersecurity incidents within the industry, hence the need for an enhanced cybersecurity measure to mitigate cybersecurity risks remains. This finding aligns with the research conducted by [18], who suggested that while most developing countries are experiencing a surge in the adoption of digital technologies, the high incidences of cybersecurity cases call for better cybersecurity measures and practices. The external threat elements were also examined to identify patterns and determine best mitigation practices.

Based on the data provided, 38.46% of the participants expressed the concern that phishing attack was the most prevalent form of cybersecurity incidents encountered by manufacturers in the industry. 30.77% of the respondents also indicated that ATM Skimming Attack was a leading form of attack within the industry. As it is a study of small manufacturers, financial management via ATMs has been prevalent. Other threats like Ransomware, Insider Threat, and Data breaches were also identified, constituting 30.76% of the total. These findings reveal that Phishing and ATM Skimming Attacks were the prominent forms of attacks in the industry, hence the need for a more robust cybersecurity strategy. According to Dzomira [19], Phishing attacks in the manufacturing sector were highlighted as an ongoing prevalence threat, emphasizing the sophisticated techniques attackers use to deceive employees and customers of manufacturers in the industry. Again, a recent publication by [19] discusses some of the latest trends in ATM skimming and its associated impact on the manufacturing industry, which was becoming alarming. The Data Protection Commission (2024) discusses recent

2025, Vol. 2, Article ID. 2025.0007
https://doi.org/10.69709/COConnect.2025.178512

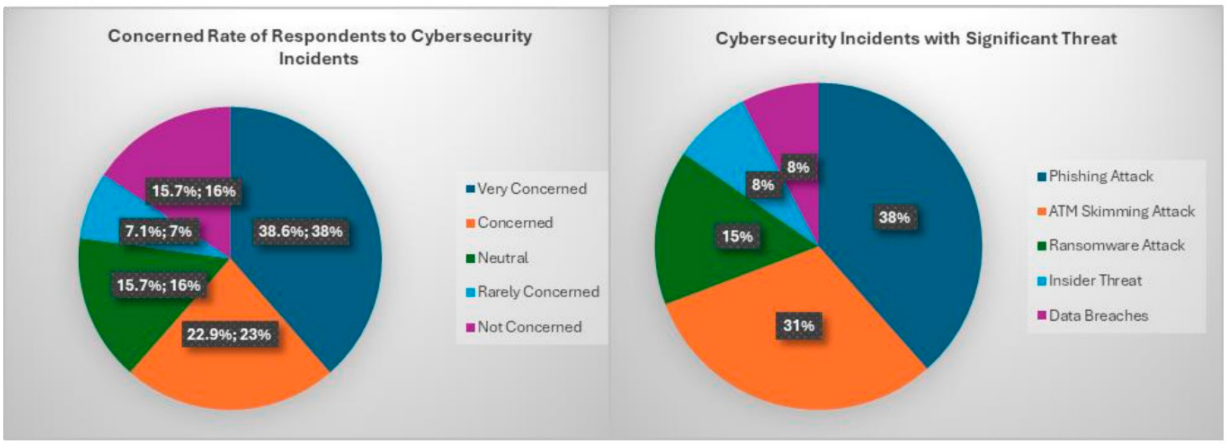

Figure 3: Chart showing Concerned Levels of Respondents and Cybersecurity Incidents in manufacturers.

data breaches in the manufacturing sector, highlighting their impact and the need for stronger data protection measures.

3.2. Objective 2: To Identify Vulnerabilities and the Impact of Cybersecurity Incidents on Manufacturers

This second objective sought to identify the vulnerabilities present in the cybersecurity infrastructure of manufacturers contributing to cybersecurity incidents within the industry. To do this, the research employed a questionnaire to collect the views of respondents on the technological, human, and organizational factors contributing to the rise of cybersecurity incidents within the industry. First, the respondents were asked about the type of vulnerabilities they believe in the internal realm that mostly contributed to cybersecurity incidents in their organizations.

Based on the provided data in Table 1, 26.15% of the participants expressed the concern that "Outdated Software and Systems" was the major vulnerability contributing to cybersecurity incidents in their manufacturers. 24.62% of the respondents also indicated "Insufficient Employee Training" as a leading vulnerability within the industry. Other vulnerabilities identified included "Weak Access Controls", "Inadequate Data Protection" and "Poor Incident Management", which accounted for 21.54%, 15.38% and 12.31% respectively of the total vulnerabilities. These survey results call for a multifaceted approach by manufacturers to effectively mitigate cybersecurity risks. This multifaceted approach falls in tandem with research identifying the importance of this approach to cybersecurity incidents, including [20]:

- Regular updates and patches for systems and software to mitigate risks from outdated technologies.
- Comprehensive employee training programs to ensure awareness of cybersecurity threats and best practices.
- Stronger access controls, such as multi-factor authentication and strict password policies, to prevent unauthorized access.
- Enhanced data protection strategies, including encryption and secure storage solutions, to safeguard sensitive information.
- Improved incident management capabilities, including the development of robust incident response plans and conducting regular simulation exercises.

The study went further to investigate "The confidence of employees in the technological measures implemented by their manufacturers to mitigate cybersecurity risks", "The extent to which employee practices contribute to cybersecurity risks," and "The confidence of employees in the preparedness of their manufacturer to handle and recover from cybersecurity risks". The feedback on this investigation is provided in Table 2.

3.3. Objective 3: To Explore the Theoretical Foundations and Practical Applications of Zero Trust Architecture (ZTA)

The next objective sought to explore the theoretical foundations and practical applications of Zero Trust Architecture (ZTA) in manufacturing. To do this, the researcher undertook a review of academic materials, journals, and reports on the principles underpinning ZTA, such as continuous verification and least privilege access, and explored how these principles can be applied in the specific context of manufacturers [21]. These theoretical foundations

Table 1: Type of Vulnerabilities contributing to Cybersecurity Incident(s).

No.	Type of Vulnerabilities	Frequency	Percentage (%)
1	Outdated Software and Systems	17	26.15
2	Insufficient Employee Training	16	24.62
3	Weak Access Controls	14	21.54
4	Inadequate Data Protection	10	15.38
5	Poor Incident Management	8	12.31
	Total	65	100

Table 2: Perception of Vulnerabilities Contributing to Cybersecurity Incidents in Manufacturers.

Likert 5-Point Scale / Survey Questions	Strongly Disagree (SD)	Disagree (D)	Neutral (N)	Agree (A)	Strongly Agree (SA)
(a) To what extent do you agree that the technological measures implemented by your manufacturer are effectively mitigating cybersecurity risks?	30.0	17.1	21.4	20.0	11.4
(b) To what extent do you believe employee practices contribute to cybersecurity risks in your manufacturing organization?	11.4	14.3	17.1	41.4	15.7
(c) Do you agree with the statement "Your manufacturer is well prepared to handle and recover from cybersecurity incidents"?	25.7	37.1	14.3	8.6	14.3

A 5-Point Likert Scale was used to represent the view of the respondents. A Likert scale of 1 represented "Strongly Disagree (SD)", 2 represented "Disagree (D)", 3 represented "Neutral (N)", 4 represented "Agree (A)", and 5 represented "Strongly Agree (SA)".

were extensively examined in the literature review. In the sections that follow, the researcher will highlight examples of real-world cases illustrating how manufacturers have adopted ZTA principles in mitigating cybersecurity risks [21].

Case Study: JPMorgan Chase & Co.- JPMorgan Chase has been at the forefront of adopting Zero Trust principles to secure its vast digital infrastructure. The manufacturer's approach focuses on validating every user and device that attempts to access its network [22]. JPMorgan Chase's Zero Trust Architecture is a robust security framework designed to protect its vast digital infrastructure from threats and unauthorized access. This comprehensive strategy focuses on validating every user and device that attempts to access the network, leveraging concrete technical implementations like identity-based segmentation, trust scores, and real-world use cases.

Key Implementations:

- Network Access Control (NAC): JPMorgan Chase utilizes NAC to authenticate and authorize devices before they can connect to the network. This ensures compliance with security policies.
- Privileged Access Management (PAM): The manufacturer implemented PAM solutions to control and monitor privileged accounts, reducing the risk of misuse of administrative credentials.
- Continuous Monitoring: All network traffic is continuously monitored and logged to detect and respond to anomalies in real-time.

Outcomes:

- Significant reduction in the attack surface.
- Enhanced ability to detect and mitigate threats quickly.
- Strengthened overall security posture through continuous validation.

3.4. Objectives 4: To Examine the Potential of Zero Trust Architecture (ZTA) on Mitigating Cybersecurity Incidents

This last objective aimed to provide actionable recommendations on how the adoption of ZTA can impact the mitigation of cybersecurity incidents in manufacturers. Considering the scope of this objective, the research used survey questionnaires and interviews to solicit the views of respondents on the following questions on ZTA.

2025, Vol. 2, Article ID. 2025.0007
https://doi.org/10.69709/COConnect.2025.178512

Firstly, respondents were asked about their awareness of Zero-Trust Architecture (ZTA) before the commencement of this survey. To define the acceptable or unacceptable range for this survey question (Table 3), a threshold was defined with a grouping criterion as established:

High Awareness: Responses indicating respondents who fall into higher categories of awareness ("Highly Aware" or "Aware"). Combined percentage calculated as 15.5% + 24.5% = 40.0%. Low Awareness: Responses indicating respondents who fall into lower categories of awareness ("Neutral", "Limited Awareness", or "No Awareness"). Combined percentage: 10.0% + 45.0% + 5.0% = 60.0%

Based on the combined percentages, the Acceptable Range and Unacceptable Range were defined as: Acceptable Range: If more than 50% of respondents indicate high awareness (Highly Aware and Aware), this would imply a good level of awareness among respondents. Unacceptable Range: If more than 50% of respondents indicate Limited Awareness ("Neutral", "Limited Awareness", and "No Awareness"), this would mean a poor level of awareness among employees.

From the survey results, 60.0% of respondents indicate a low level of awareness of Zero-Trust Architecture, which is significantly more than the 50% threshold. This suggests that awareness among manufacturers' employees regarding Zero-Trust Architecture is limited, suggesting the need for more awareness to improve the situation. This feedback from the survey tallies with some of the views of the respondents on the level of awareness of ZTA. For example, respondent R1, a Systems Administrator during the interview, expressed that "while I am aware of other cybersecurity models such as Defense-in-Depth and its associated benefits, ZTA is completely new to me." Similarly, respondent R3, a Chief Information Security Officer, highlighted that "I am aware of Zero-Trust-Architecture and some of the benefits it provides, but I do not have any prior experience with its implementation. From this feedback, the overall sentiment among the respondents is that there is some awareness about Zero-Trust Architecture, albeit not extensive figures.

4. Discussion and Conclusions

The study gathered information about the state of cybersecurity incidents in manufacturers, the types of vulnerabilities contributing to these incidents, their impact on the manufacturers, and real-world applications of Zero-Trust Architecture as an effective solution. As a result, some of the study's primary findings relate to prevalent cybersecurity incidents, vulnerabilities, risks posed by employee activities, and the preparedness of manufacturers to handle and recover from cybersecurity incidents.

First, the research sheds light on the frequency of cybersecurity incidents within the manufacturing industry. Despite the different types of incidents, the respondents indicated that Phishing and ATM Skimming Attacks were the most prevalent cybersecurity incidents, which pose a significant risk. This finding is supported by the data presented in Figure 3 from the survey. In addition to this data, the prevalence of Phishing and ATM skimming attacks has been highlighted as posing a continuous challenge to the security infrastructure of manufacturers. The research also concludes that "Outdated Software and Systems", "Insufficient Employee Training," and "Weak Access Controls" are some of the common vulnerabilities contributing significantly to the increasing rate of cybersecurity incidents in manufacturers, as shown in the survey results. These results call for a multifaceted approach by manufacturers to effectively mitigate cybersecurity risks. The respondents also demonstrated a lack of confidence in the technological measures implemented by manufacturers to mitigate cybersecurity risks. This finding is presented in Table 2, where 68.5% of respondents expressed Negative Confidence. This calls for manufacturers to assess and enhance the cybersecurity defenses of their IT infrastructure to encourage trust and confidence among employees and customers.

Table 3: Level of Awareness of Zero-Trust Architecture.

Likert 5-Point Scale / Survey Questions	Highly Aware (5)	Aware (4)	Neutral (3)	Limited Awareness (2)	No Awareness (1)
What is your level of awareness of Zero-Trust Architecture	15.5	24.5	10.0	45.0	5.0

Additionally, the paper sheds light on the confidence of employees in the preparedness of manufacturers to handle and recover from cybersecurity incidents. From the feedback provided in Table 2, 77.1% of respondents expressed a lack of confidence in this preparedness. This finding thus concludes that manufacturers must adopt better approaches to managing cybersecurity incidents to promote confidence and ensure robust security practices. Also, on the extent to which respondents anticipate challenges to the successful implementation of ZTA in Manufacturers, 60% of the respondents expressed the view that even though there may be challenges, the challenges will not be significant enough to prevent its successful implementation, as shown in Table 3.

Lastly, when the respondents were asked to what extent improvement in technology, process, and people can enhance the overall cybersecurity posture of manufacturers, it was revealed that 80% of the respondents believed that an overall improvement in these areas can significantly improve cybersecurity in the manufacturing industry. This research thus concludes that manufacturers must implement an integrated cybersecurity model such as ZTA to address current cybersecurity challenges as well as future anticipated ones, considering the interconnected nature of these risks. This could be furthered in terms of Artificial Intelligence (AI), induced automation, and driving concerns and patterns from Large Learning Models to provide and equip a robust ZTA.

Abbreviations

ADM	Agricultural Development Manufacturer
APTs	Advanced Persistent Threats
ATM	Automated Teller Machine
CISA	Cybersecurity & Infrastructure Security Agency
CIA	Confidentiality, Integrity, and Availability
DoS	Denial of Service
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
IT	Information Technology
IDPS	Intrusion Detection and Prevention System
MCQ	Multiple Choice Questions
NAC	Network Access Control
NIST	National Institute of Standards and Technology
PAM	Privilege Access Management
SMEs	Small and Medium-Sized Enterprises
VPN	Virtual Private Network
WAFs	Web Application Firewalls
ZTA	Zero-Trust Architecture

Author Contributions

The contributions made by the author in the preparation of the article is well stated and agreed.

Availability of Data and Materials

The author consents to provide the materials upon request. All cited works are listed in the references.

Consent for Publication

No consent for publication is required, as the manuscript does not involve any individual personal data, images, videos, or other materials that would necessitate consent.

Conflicts of Interest

It is here to disclose that there is no potential conflict of interest in their manuscripts under the section "Conflicts of Interest".

Funding

No external funding was received for this research.

Acknowledgments

I, as the author, thank the represented institutions for their support during the research.

References

[1] National Institute of Standards and Technology (NIST), "*Zero Trust Architecture (NIST Special Publication 800-207)*," NIST, Gaithersburg, MD, USA, 2020. [CrossRef]

[2] National Cyber Security Centre (NCSC), "*Annual Cyber Security Threat Assessment Report*," National Cyber Security Centre, Washington, DC, USA, 2021. Available online: https://www.ncsc.gov.uk/annual-review/2020/ncsc-accessible-version/index.html

[3] H. Wang and M. Li, "Challenges and Opportunities in Implementing Zero Trust Architecture: A Survey," *Future Gener. Comput. Syst.*, vol. 115, pp. 83–94, 2021. Available online: https://onlinelibrary.wiley.com/doi/pdf/10.1155/2022/6476274

[4] Palo Alto Networks, "*Zero Trust: The Fundamentals of a Zero Trust Architecture*," Palo Alto Networks, Santa Clara, CA, USA, 2020. Available online: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

[5] M. Fojude, "Insider Threat Agent: A Behavioral Based Zero Trust Access Control Using Machine Learning Agent," Master's Thesis, Georgia Southern University, Statesboro, GA, USA, 2025. Available online: https://digitalcommons.georgiasouthern.edu/cgi/viewcontent.cgi?article=4197&context=etd

[6] M. A. Rosenthal and S. Manohar, "*Implementing Zero Trust in Financial Services: Principles and Case Studies*," Financial Services Information Sharing and Analysis Center (FS-ISAC), Reston, VA, USA, 2021. Avail-

able online: https://www.fsisac.com/insights/zero-days-are-here-to-stay-heres-how-you-can-prepare

[7] R. J. Robinson, "Inference on Business Best Practices Affinity Despite Conceptual AI Exposure," *Horiz. J. Hum. Soc. Sci. Res.*, vol. 5, no. 2, pp. 121–131, 2023. [CrossRef]

[8] V. Gorecha and R. J. Robinson, "AI Adoption Patterns Among Major Original Equipement Manufacturers (OEMs) in Automotive Industry,". in: *Proceedings of the 2024 IEEE International Conference on Electrical and Computer Engineering Research (ICECER)*, Gaborone, Botswana, 2024. [CrossRef]

[9] R. Kitchin and M. Dodge, "The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention," in: "*Smart Cities and Innovative Urban Technologies*," Routledge, New York, NY, USA, 2020, pp. 47–65. [CrossRef]

[10] KPMG, "*Cybersecurity Considerations for Financial Institutions*," KPMG, London, UK, 2020. Available online: https://assets.kpmg.com/content/dam/kpmgsites/uk/pdf/2020/11/all-hands-on-deck.pdf

[11] IBM Security, "*Building a Zero Trust Environment in Manufacturing*," IBM Security, New York, NY, USA, 2020. Available online: https://www.ibm.com/think/topics/zero-trust

[12] R. J. Robinson, "Digital Security: A Critical Evaluation Process for IT-Security Products," *Math. Comput. Sci. Contemp. Dev.*, vol. 6, pp. 18–30, 2024. [CrossRef]

[13] H. Kang, G. Liu, Q. Wang, L. Meng and J. Liu, "Theory and Application of Zero Trust Security: A Brief Survey," *Entropy*, vol. 25, no. 12, p. 1595, 2023. [CrossRef] [PubMed] [PubMed Central]

[14] K. A. Owusu and S. K. Antwi, "Cybersecurity Challenges Facing the Banking Industry in Ghana: A Case Study of Selected Banks," *Int. J. Comput. Appl.*, vol. 975, pp. 8887–8889, 2020. [CrossRef]

[15] J. R. Rachel, "Cybersecurity Compliance Frameworks—A Pragmatic View with an IT Outsourcing Company Case Study," *Soc. Lens*, vol. 1, pp. 15–25, 2024. [CrossRef]

[16] S. Màrquez Postigo, "*Criminal Compliance System: Implementation of a Compliance Model in the Information Technology Security Sector*," 2024. Available online: https://diposit.ub.edu/dspace/bitstream/2445/214556/1/TFG_M%C3%A0rquez_Postigo_Sandra.pdf (accessed on 1 January 2025).

[17] Bank of Ghana, "*Cybercrime and ATM Fraud in Ghana 2023*," Bank of Ghana, Accra, Ghana, 2023. Available online: https://www.bog.gov.gh/news/banks-sdis-psps-2023-fraud-report/

[18] R. Garg, A. Gupta and A. Srivastava, "A Comprehensive Review on Transforming Security and Privacy with NLP," in: "*International Conference on Cryptology & Network Security with Machine Learning*," Springer Nature Singapore, Singapore, 2023, pp. 147–159. [CrossRef]

[19] S. Dzomira, "Cybersecurity Threats and Manufacturing Sector Stability: An Analysis of Vulnerabilities," *J. Financ. Crime*, vol. 27, pp. 789–803, 2020. [CrossRef]

[20] Deloitte, "*Cybersecurity in Financial Sector: Strategies for Implementing Zero Trust Architecture*," Deloitte, Boston, MA, USA, 2021. Available online: https://www.deloitte.com/global/en/services/consulting-risk/services/zero-trust.html

[21] R. J. Robinson, "*Insights on Cloud Security Management. Cloud Computing and Data Science*," 2023, pp. 212–222. Available online: https://ojs.wiserpub.com/index.php/CCDS/article/view/3292 (accessed on 1 January 2025).

[22] D. Smit, S. Eybers, A. van der Merwe and N. Human, "Designing a Technical Framework for Enabling Enterprise AI Adoption," in: "*Science and Information Conference*," Springer Nature, Cham, Switzerland, 2024, pp. 167–181. [CrossRef]