A FALSE SENSE OF SECURITY: ENHANCING RESILIENCE AGAINST CYBERATTACK THROUGH AN IMPROVED SECURITY AWARENESS MODEL

MD. MOHSIN

Master of Science

DAFFODIL INTERNATIONAL UNIVERSITY

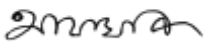
APPROVAL

This thesis titled on "**A FALSE SENSE OF SECURITY: ENHANCING RESILIENCE AGAINST CYBERATTACK THROUGH AN IMPROVED SECURITY AWARENESS MODEL**", submitted by **MD. MOHSIN**, **ID: 232-44-012** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfilment of the requirements for the degree of Masters of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

---------- Chairman

DR. A. H. M. SAIFULLAH SADI
Professor
Department of Software Engineering
Daffodil International University



---------- Internal Examiner 1

Afsana Begum
Assistant Professor
Department of Software Engineering
Daffodil International University

---------- Internal Examiner 2

DR. RUBAIYAT ISLAM
Associate Professor
Department of Software Engineering
Daffodil International University

---------- External Examiner

Md Fazle Munim
Associate Director and Vice President
Government & Public Sector, Ernst & Young

DAFFODIL INTERNATIONAL UNIVERSITY

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name	:	MD. MOHSIN
Date of Birth	:	30th August, 2000
Title	:	A False Sense of Security: Enhancing Resilience Against Cyberattack Through an Improved Security Awareness Model
Academic Session	:	Fall 2024

I declare that this thesis is classified as:

☐	CONFIDENTIAL	(Contains confidential information under the Official Secret Act 1997)*
☐	RESTRICTED	(Contains restricted information as specified by the organization where research was done)*
☒	OPEN ACCESS	I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Daffodil International University reserves the following rights:

1. The Thesis is the Property of Daffodil International University.
2. The Library of Daffodil International University has the right to make copies of the thesis for the purpose of research only.
3. The Library of Daffodil International University has the right to make copies of the thesis for academic exchange.

Certified by:

_____
(Student's Signature)

_____
232-44-012
Date: 18 January 2025

_____
(Supervisor's Signature)

_____
Dr. Mr. Md. Maruf Hassan
Date: 18 January 2025

NOTE : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach a thesis declaration letter.

THESIS DECLARATION LETTER (OPTIONAL)

Librarian,
Daffodil International University,
Daffodil Smart City,
Ashulia.Dhaka,Bangladesh

Dear Sir,

CLASSIFICATION OF THESIS AS RESTRICTED

Please be informed that the following thesis is classified as RESTRICTED for a period of three (3) years from the date of this letter. The reasons for this classification are as listed below.

Author's Name	Md. Mohsin
Thesis Title	A False Sense of Security: Enhancing Resilience Against Cyberattack Through an Improved Security Awareness Model

Reasons (i)

(ii)

(iii)

Thank you.

Yours faithfully,

_____
(Supervisor's Signature)

Date: 18 January 2025

Stamp:

Note: This letter should be written by the supervisor and addressed to the Librarian, *Daffodil International University* with its copy attached to the thesis.

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Master of Science.

_____

(Supervisor's Signature)

Full Name : Dr. Mr. Md. Maruf Hassan

Position : Associate Professor

Date : 18 January 2025

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Daffodil International University or any other institution.

_____

(Student's Signature)

Full Name : MD. MOHSIN

ID Number : 232-44-012

Date : 18 January 2025

A FALSE SENSE OF SECURITY:
ENHANCING RESILIENCE AGAINST CYBERATTACK THROUGH AN IMPROVED SECURITY AWARENESS MODEL

MD. MOHSIN

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Master of Science

Department of Software Engineering (Major in Cyber Security)

DAFFODIL INTERNATIONAL UNIVERSITY

JANUARY 2025

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my supervisor, Dr. Mr. Md. Maruf Hassan, Associate Professor, Department of SWE, Daffodil International University, for their invaluable guidance, support, and encouragement throughout this research journey. Your insights and constructive feedback have been instrumental in shaping this thesis.

I would also like to extend my thanks to the faculty and staff at Daffodil International University for creating an enriching academic environment that fostered my growth as a researcher. Special thanks to my classmates and friends for their constant support, collaboration, and camaraderie, which made this journey both productive and enjoyable.

Finally, I would like to thank my family for their unwavering love, patience, and encouragement. Your belief in me has been my greatest source of strength and motivation.

DEDICATION

This thesis is dedicated to my family, whose endless support has always been my foundation. To my parents, for their boundless love and encouragement, and to all the educators and mentors who have inspired me to pursue knowledge and excellence. This work is also dedicated to every student who strives to contribute to a safer, more secure online world

ABSTRACT

Cybersecurity has become a crucial concern in today's increasingly digital world, especially for students who rely on online platforms for education, communication, and personal activities. This thesis investigates the effectiveness of university cybersecurity programs in enhancing students' online safety practices, with a focus on the integration of both technological and practical applications.

Advanced Persistent Threats (APTs) remain a persistent problem within the realm of cybersecurity. Heavy investment effort in security infrastructure and awareness leaves many organizations with a false sense of well-being, for their perceived cybersecurity resilience does not correspond with actual vulnerabilities. This study combines two prior research areas on cybersecurity perception and extends it by implementing Zero Trust Architecture (ZTA) and Artificial Intelligence-Based Threat Detection (AI-TD) to the current model. Through extensive survey-based investigation, this study evaluates how these new variables impact the confidence towards cyber security in educational and corporate environments, providing valuable solutions to improve the existing cyber security frameworks. Moreover, this research examines the perspective of the faculty, students, IT administrators, and security professionals about the relevance and practical application of these interventions against any cyber threat.

Enhanced cybersecurity awareness models continue to be uncontrolled, and this research responds to this limitation by suggesting a Framework that integrates behavioral, technological, and policy-oriented security controls. This research is significant as it goes a long way in reforming security education and developing organizational security policies that are aimed at ensuring that. Border protection is not the only counteraction in cyber security.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AI-TD	AI-Based Threat Detection
APT	Advanced Persistent Threat
DDoS	Distributed Denial of Service
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
SOC	Security Operations Center
ZTA	Zero Trust Architecture

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Definition

Today, cyberterrorism is the main global problem for every organization. The recent rise of Advanced Persistent Threats (APTs) has made it evident that there is a need for more rigorously enforced security measures. Simply put, APTs are persistent, sophisticated and stealthy, seeking to infiltrate and control high-value information and critical infrastructure over long periods of time. Such threats are made by very skilled adversaries who use advanced means to go undetected while extracting confidential information.

There is a plethora of tools and protocols meant to fend off cyber-attacks, however, a lot of organizations still feel insecure simply because they feel their defences are more advanced than they are. Unfounded confidence as such usually develops from overreliance on existing paradigms in security models, inadequate training in security awareness, or simply ignorance of emerging threats. As a result, some organizations balance the risk of APTs posing a risk to their critical assets of being under cyber-attack.

The term “false sense of security” denotes the idea that people or businesses think that they are more secure than they are, this is where APT Is in minimal. This nascent complacency lowers the effectiveness of security and maximizes the chances of a successful cyber-attack. This necessitates the need for a paradigm change in response to this challenge.

1.2 Background

The task of securing both universities and companies from cyber-attacks is not easy. Many factors hinder achieving this goal, such as the nature of users, open access

and the need for security not to interfere with operations. Cybersecurity is especially critical for universities because they are at the forefront of promoting research, developing online teaching platforms, managing student information systems, as well as handling finance-related matters. Similarly, firms that specialize in technology and finance are also constantly being attacked by cyber threats.

Even with the presence of advanced technological tools and strategies, educational bodies and workplaces are still prone to cyber threats. The absence of practicable proactive measures, policy negligence, as well as a shortfall of data retention brutifies the situation further. Even though barriers have been built against tracking lapses in professional policies, there has not been sufficient focus on enabling this through behavioural policies. Moreover, best practices within cyber security among employees and faculty have been erratic as well.

Zero Trust Architecture (ZTA) as well as AI-based threat detectors enhance cybersecurity perception and resilience. Considering these variables alongside each other provides, a new sense of security which enhances the understanding. It also informs how it impacts on user confidence.

1.3 Problem Statement

Effective cybersecurity is something that every organization needs to focus on. In our contemporary world where everything is digital and interconnected, cybersecurity has become a major issue that needs to be addressed. Yes, there is a time when one can roll out newer technologies and dependable security systems, however, this does not negate the fact that many organizations remain dependent on the false shroud of security over them. Many factors contribute to this disregard, whether it be old security models, lack of protection awareness, or more commonly, dependency on traditional security systems.

In contemporary times, APT or an advanced persistent threat is one that has proven to be overbearing. APT can be defined as malicious and aggressive cyber-attacks with the intent of targeting and breaching specific networks, all the while hiding and covering the assault from the host as long as possible. There are major corporations

and hackers in the field that have the expertise and resources to be able to pull this off. Due to the lack of necessary protective equipment, organizations can easily become victims of APT.

An ever-growing problem that contributes to APT is the turn completely dependent on perimeter-based security models. With the shift to completely over-protecting networks by creating a secure barrier on its doors, any and every possible threat that could have existed inside is now present unfiltered. Cyber threats of the calibre of APT are something that need a more insightful solution than what we currently have, which can originate from within the network or exploit trusted connections.

1.4 Research Objectives & Research Questions

The main aim of this study is to determine whether the university cyber security programs aim to enhance the online behaviour of students in a safe manner. More specifically, the study will seek to:

- In educational and corporate settings pinpoint and bridge gaps in the existing security awareness frameworks that leave a false impression of reliability.
- After doing so, Modify the current model by adding an AI-Based Threat Detection and Zero Trust Architecture to extend the reliability framework on a bigger scale.
- Use quantitative methodologies as well as qualitative methods to carry out an empirical investigation on how these elements influence the views and imagination of cybersecurity in relation to students, faculty, IT professionals and corporate employees.
- Investigate the impact of an institution's policies, security exercises and governance on the effectiveness of cybersecurity and the correlation of the two.

- Introduce and outline a new model for security awareness that will address measures that are behavioural and technological as well as strategic pertaining to cyber security.

- Formulate and evaluate a cybersecurity training program that is adaptive and covers human and technological features so as to ensure there is a constant improvement in security.

- Employ solid cyber security performance measurements and use them to advise how cyber security policies should be adapted to ensure a company's long-term survivability when operating in educational and corporate environments.

To guide this research, the following questions are posed:

1. To what extent do Zero Trust Architecture (ZTA) and AI-based Threat Detection (AI-TD) enhance the perceived cybersecurity robustness of organizational systems?

2. What organizational and technological determinants contribute to a false sense of security, and how can they be mitigated effectively?

3. How does organizational culture moderate the relationship between security measures and cybersecurity perception?

4. What is the role of security literacy and awareness programs in influencing security behaviour and policy adherence?

5. How can an improved security awareness model better address vulnerabilities and enhance cybersecurity resilience?

1.5 Missing Theories & Research Gaps

Zero Trust Architecture (ZTA) is a security model that posits that all access requests must be verified and re-verified regardless of where the request is coming from which is a fundamental shift from the perimeter security models. ZTA is a hot topic, however, application in real security awareness models is still limited. Understanding the intersection of ZTA and organizational security and employee conduct would require further research.

AI threat detection (AI- TD) technologies use deep learning to autonomously detect and react to cyber threats as they happen. But how they fit into security awareness measures is not clear. Further studies are warranted to identify the usefulness of AI-TD in enhancing an organization's ability to withstand cybersecurity threats.

Security awareness programs have evolved over the years from emphasis on video presentations on how to spot a phishing email and the need to have strong passwords to even more elaborate presentations. But even with such progress, there is scant information on how security awareness programs would curb APTs or other more serious modern threats. Newer security frameworks such as ZTA and AI-TD would certainly solve most of these issues. New methodologies need to be developed to identify AI-TD components and test them for efficacy.

The sustained impact of security awareness training is particularly dubious. There is a need to investigate whether periodic training extends the progress achieved in security works and the robustness of the entire organization. Research is required to ascertain the long-term changes in the employees' practices and appropriate measurements for the same.

Security practices within organizations are greatly shaped by the employees' behaviour or other cultural elements. Existing literature fails to explain the effect of such elements on security sensitivity. Such knowledge is important in designing programs needed to meet both the technical requirements and the human ones.

Technology innovations like IoT, cloud computing, and blockchain have new implications for security. It is imperative to carry out research concerning their implications on the security of the employees' awareness and how the programs will need to be restructured to meet the new threats.

1.6 Research Contributions

- Creation of a New Model of Security Awareness: A fresh concept that integrates psychological, behavioural and technical aspects and also ensures improving cyberspace security.

- Testing Threat Detection And Implementation Of Zero Trust Based On AI: through quantitative security enhancement and data reinforcement.

- Identification And Analysis of Key Organizational Weaknesses: Identifying areas within which institutions do not manage to implement security measures and suggesting practical policy changes.

- Design of a Workable Cybersecurity Training Method: An all-around approach to coaching service that is all-purpose across divisions and industries while seeking to resolve real-world cybersecurity courses.

- Augment the existing model by integrating Zero Trust Architecture (ZTA) and AI-Based Threat Detection (AI-TD).

- Conduct a real-world evidence analysis on how these factors interconnect with the understanding of cyber security among students, faculty, IT experts and corporate employees.

- Assess the influence of institutional frameworks, security policies, cyber security training and governance on the effectiveness of cyber security.

- Develop and advanced security awareness model combining behavioural, technological and strategic measures for cyber protection.

- Optimize the cyber security policies for education and business institutions to achieve long term resilience.

1.7 Significance of the Study

This research does aim to fill in the missing information security with a comprehensive model that utilizes the advanced security frameworks that this research strives to achieve in order to increase organizations' resilience towards APT's. This study has the potential to alter the perception of cyber threats as well as amending the normal roles of disengaging the cyber threats towards the organizations. The application of Zero Trust Architecture and Artificial Intelligence based threat detection marks a new frontier in implementing cyber protection as it arms an organization in knowing how to counteract complicated attacks.

The model proposed in this research demonstrates the steps that an organization is able to follow during unsure threats and counterfeits. , so as to enable the organization avoids complacency, but rather provide means to ensure protection of its vital resources. The outputs of this research will be beneficial to cyber practitioners, policy makers and leaders of various organizations in mitigating against the growing threats of attack.

CHAPTER 2

LITERATURE REVIEW

2.1 Advanced Persistent Threats (APTs) and the False Sense of Security

In contemporary cybersecurity, Advanced Persistent Threats (APTs) can be understood as prolonged and sophisticated cyberattacks intricately designed to compromise high-value targets, usually government bodies, corporations, and enterprise-level organizations. Unlike general cyber threats, these are a great deal more elusive, more involved, and identical while still different. An APT attack usually consists of multiple phases, which include the first contact, moving around in the network, data theft, and an extended bit of time undetected inside the system.

APTs come with their problems and one of the foremost is the widespread illusion of safety that so many people and organizations have regarding their cybersecurity strategies. Many companies think that just having normal security measures like firewalls, intrusion detection systems, and antivirus software are sufficient to protect their systems. In contrast, APTs are crafted for, maintaining stealth, evading normal cyber defenses, and being more advanced with social engineering among other obfuscator tactics.

2.1.1 The Characteristics of APTs

APTs are carried out in stages starting with their attempt to first gain access to networks, either through phishing, exploiting vulnerabilities or using other social engineering techniques. Gaining access to the network, they are required to remain undetected after gaining this access. This is achieved through the monitoring of activities within the network as well as the collection of sensitive information and detection of potential vulnerabilities. That kind of persistence is sometimes combined

with sophisticated tools to allow undetected access as protective tools used by most organizations are barely effective. With time they may increase their access rights, infiltrate greater boards and exfiltrate data they find useful. However, with APT, their intention is not the execution of a single attack focused towards destruction, rather, it is espionage, data exfiltration or damage to vital systems.

2.1.2 How APTs Exploit the False Sense of Security

One of the problems advanced persistent threats tend to have is their ability to leverage the false sense of security that most organizations tend to develop because of their dependence on traditional cyber security measures and tools. Most of the time, organizations take the most basic security measures like the use of antivirus tools, installation of firewalls and even intrusion detection systems (IDS), however, these tools prove to be mediocre against advanced persistent threats.

APTs are a set of security breaches that involve invading an organization's perimeter and overcoming the boundary, by undermining user behaviour, exploiting configurations and other weaknesses. Employees can be lulled into a false sense of security regarding their organization’s cyber security measures and operations because the act of opening a phishing email or clicking on a link appears unthreatening. This apathy creates a false perception of security and a lack of risks, even in cases where there are rich security measures in place.

Also, APTs, more often than not, go unnoticed for months, or at times years, so their detection does not pose an immediate danger. Consequently, organizations will continue to promote the idea that their systems are not compromised, avoid making changes to their current protocols, and discontinue the practice of employee training or modern detection means such as AI-enabled systems or Zero Trust Architecture (ZTA). Rather, it can ensure the dismantling of the cyber security foundation in an organization by leaving the attack methods out of use for a longer time and unexposed on the surface.

2.1.3 Impact on Organizational Resilience

The APT threat gives organizations a false sense of security, which affects their resilience significantly. In this regard, organizations tend to underestimate their cybersecurity risks, believing that their cyber defense system is fully functional and can withstand any possible attacks. But they are wrong: APTs can disable core functions, disturb services, and inflict heavy costs and damage to reputation. Moreover, APTs are not limited to data theft: they can also include unauthorized alterations to financial transactions, stealing of ideas and designs as well as attacks on the infrastructure of the whole business.

An APT attack doesn't just cost in the short run but has long-lasting consequences as mentioned earlier, these attacks are considered to be the most expensive cybercrime as the losses stretch past the attack. Trust, reputation, compliance, and rules are among the casualties that far outlast the attack itself. Most of the time, the losses are ignored until an attack has advanced to a considerable level. By the time the event does take place, the damage would be irreplaceable.

2.1.4 The Role of Enhanced Security Models

User behaviour analytics and advanced threat detection in tandem with continuous monitoring are some of the ways that organizations will be able to counter the APTs which are a false sense of security. A good example that shows the idea behind ZTA's aims is that it treats both internal and external users as malicious and utilizes a principle of 'never trust, always verify' meaning any user within the network has to undergo authentication and verification. Furthermore, AI-driven long-term threat detection systems can uncover and intervene before extensive damage can be caused by identifying uncommon activities.

In addition to this, it is crucial to have an inexpensive cybersecurity awareness program that employs phishing attempts, security compliance, and identifying unusual activities as part of their training. By ensuring that there is a perfect harmony between the employee's actions and the security devices and other technology put in place, the chances of APTs gaining access through social engineering are greatly reduced.

2.2 Zero Trust Architecture (ZTA)

The Zero Trust approach implements a strong security model that relies on constant verification rather than assumed trust. ZTA embraces methodologies like micro-segmentation, Multi-Factor Authentication (MFA), and least-privileged access that profoundly change the manner institutions and organizations safeguard sensitive information and network systems. The adopted ZTA guarantees that only those users who have been verified and permitted can access sensitive information, leading to a lower risk of data compromise.

Theoretical Foundations of ZTA: It is established in ZTA that there is an underlying phrase or principle that is 'never trust, always verify'. This principle functions under the idea that there is a chance of an internal or external threat and thus every request of validation as access should be authenticated and approved. Identity and access management systems (IAM), constant surveillance and analytics are utilized to assure security at the highest levels.

Implementation Challenges: Complexity and extensive resource consumption are two factors that make it difficult to apply ZTA in the first place despite its numerous benefits. The use of ZTA in connection with legacy systems guaranteed interoperability with a multitude of different IT systems, and an escalation in the number of authentication requests all pose troubles for the organization. One additional challenge that should be mentioned is the need for full-fledged training and information campaigns so that all actors comprehend ZTA and can comply with its principles.

Benefits of ZTA: Organizations are now able to polish their newer positions by enhancing their security when applying the Zero Trust model and architecture. Benefits include reduced attack surfaces, enhanced visibility into network scope, and the capability to swiftly isolate and remediate threats. ZTA also supports regulatory compliance in cases where the protection of sensitive information is sufficient to restrict use to certain subsets of users only.

Future Directions: As the nature of cyber threats is likely to shift, it is anticipated that ZTA will introduce new technologies such as artificial intelligence (AI)

and machine learning (ML) that will enhance the detection and response capabilities to threats. The adoption of AI and ML can provide greater flexibility in defining security postures against attacks and general intrusion making ZTA an even stronger architecture for safeguarding critical assets.

Table 2.2 Key Components of Zero Trust Architecture

Component	Description
Multi-Factor Authentication (MFA)	Requires multiple forms of verification to grant access.
Micro-Segmentation	Divides the network into smaller, isolated segments to limit access.
Least-Privilege Access	Grants users the minimum level of access necessary for their role
Continuous Monitoring	Constantly monitors network activity to detect and respond to threats.
Identity and Access Management (IAM)	Manages user identities and controls access to resources.

2.3 AI-Based Threat Detection (AI-TD)

A framework for AI security operations utilizes AI technology to drive cybersecurity incident response frameworks using anomaly detection machine learning algorithms and naively supervised techniques. In this way, threat detection and remediation interventions can promote security risks even more successfully than conventional timely-examination-centric approaches due to reliance on AI-based technology. AI systems also lessen the workload of the security team by eliminating clutter caused by false alarms and allowing action to be taken practically immediately.

Strengths of AI-TD: Due to the large amount of data involved, one of the main advantages associated with an AI-based threat detection system is its ability to scan through vast volumes of data at massive speeds sifting through data that might suggest

an anomaly, an event or some form of activity linked to a security breach or threat. This ability enhances the efficiency of proactive threat hunting and incident response.

Forthcoming Enhancements: The focus should be on the advancement of more credible algorithms and Artificial Intelligence integration into advancing IT technologies like quantum computing and blockchain. Such development would provide AI-TD systems with additional enhancements that would make them robust to new threats. Also, AI models being taught off separate devices through decentralized networks can enhance data security and privacy, as federated learning will be utilized.

Shortcomings of AI-TD: Specifying, AI-TD is not without its shortcomings, despite its advantages. These systems can be vulnerable to malicious attacks where AI algorithms are deceived by bad actors that furnish incorrect data. Furthermore, the effectiveness of AI-TD is also directed to the quality of the training data that it utilizes. For example, poor or biased data can result in inaccurate threat prediction, thus leading to false positives.

Nonetheless, AI-TD systems, or simply amending Deep Learning AI can address vulnerabilities posed by communication providers. Any Adaptive Threat Prediction AI integrates and transforms into an articulate system that expands its efficiency. In addition, these systems can prevent abuse in the future.

Table 2.3 Strengths and Limitations of AI-Based Threat Detection

Strengths	Limitations
High-speed data analysis	Susceptible to adversarial attacks
Initiative-taking threat hunting	Dependent on the quality of training data
Continuous learning and adaptation	Potential for increased false positives
Potential for increased false positives	Requires significant computational resources

2.4 The Importance of Security Awareness and Culture in an Organization

Achieving proper cybersecurity in institutions today requires a comprehensive approach that combines technical measures with diversity. Thus, an organization's capacity to integrate cybersecurity into its values is crucial to bringing security into all areas of activity rather than limiting it to only policies and addressing the entire community, including faculty, students, and employees. They all have a role along these lines in protecting the institution’s assets.

A good proactive cyber security culture involves also lots of informal training while proper practices are encouraged as well and a new threat prevalent looms. Those institutions – universities and corporations, which are able to form such a culture, by the use of compulsory training, practical cyber warfare drill sessions and constant education regarding policies put in place, are able to better cope with new cyber risks. These measures help create a climate where people are enabled to recognize and deal with the risks, thus ultimately improving security.

Additionally, such a culture is successful not only through voluntary commitment which is an important factor in instilling a cybersecurity culture into the institution itself. For instance, applying cybersecurity in practice when it comes to day-to-day roles, course content, and management means instilling a sense of rational and responsible online conduct in all participants. Therefore, such an outlook goes further than looking for remedial measures because it builds a proactive defensive plan proactively.

To summarize, a proper approach to cyber defense starts from the embedded cultural norms and ideals that place the greatest degree of focus on safety and security in all elements of the organization. Such institutions that make cyber security ethos part of their culture are most equipped to deter attacks, limit vulnerabilities, and promote the culture of always being able to bear threats that are growing in number and magnitude.

CHAPTER 3

METHODOLOGY

3.1 Research Design and Approach

Upgrading the effectiveness of measurement of cybersecurity awareness, the impact of the implementation of ZTA and AI-TD artificial intelligence on the security resilience posture and addressing the factors that result in misplaced confidence are the objectives of this study proposed through a quantitative approach and survey methodology. This study adopts structural equation modelling with the aim of hypothesis response- and security perception testing, giving a solid statistical foundation for such evaluations.

The research adopts a mixed methods approach and includes qualitative research via open-ended responses, which are intertwined to address the quantitative aspects. The method is accomplished based on deductive reasoning by formulating hypotheses based on existing cybersecurity theories, which were then empirically validated.

The research goes through the following steps:

Literature Review: Classification of the literature and outlining of the deficiencies found in the existing security and awareness models.

Survey Development: Formulating a questionnaire using strict guidelines concerning the research questions.

Data Collection: A high sampling of university academic and non-academic staff, students, IT professionals and corporate workers is targeted among the study population.

Data Analysis: Mathematical models using more advanced statistical approaches are used to test the formulated hypotheses and establish relationships between the variables under consideration.

Model Validation: Evaluation of the implemented measures to increase the effectiveness of the developed security awareness model is done by implementing structured methodologies.

Recommendations: Appropriate cybersecurity policies are recommended as a result of the study.

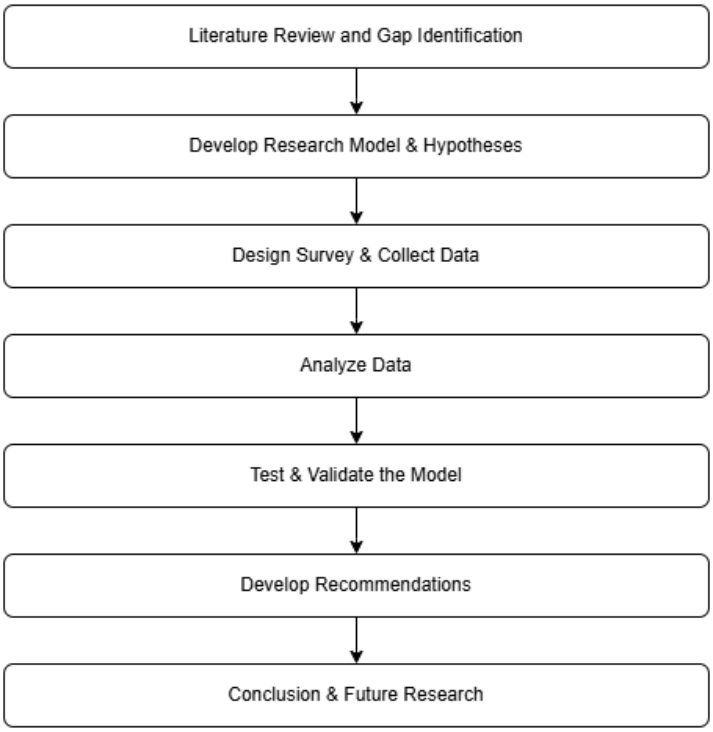


Figure 3.1 Research Methodology Process Flow

3.2 Research Model and Hypotheses

To thwart APTs (Advanced Persistent Threats) and other threatening cyber-attacks, Cybersecurity awareness and resilience stand out as an important attribute.

Even by spending millions of dollars on security infrastructure and awareness, the expanding chasm with reality ensures the organizations' continued present overconfidence in their level of cybersecurity preparedness. In this context, more advanced modernized security awareness is suggested as being able to complement traditional cyber security specifics with more state-of-the-art elements like ZTA (zero trust architecture) and AI threat detection patrols.

The envisaged model of research intends to develop a holistic model that examines the role that technological measures, security measures, organizational culture and behavioural awareness training have on cyber security confidence and assurance and general resilience. Independent variables that include (security controls, organizational policies, cybersecurity awareness training and advanced security measures) are studied issues that impact a dependent variable (sense of security) with an organizational culture elicit as a moderating factor.

3.2.1 Research Model Framework

This research presents a novel cybersecurity awareness model that employs ZTA as well as AI-TD in conjunction with existing security models. The research model comprises:

- Independent Variables (IVs):
    - Security Awareness & Training (SA)
    - Converged Testing (CT)
    - Security Controls (SC)
    - Segmentation (SG)
    - Redundant IDS/IPS (RD)
    - Insider Threat Prevention (IT)
    - Cybersecurity Insurance (CI)

- Zero Trust Architecture (ZTA) (New Variable)
- AI-Based Threat Detection (AI-TD) (New Variable)

- Moderator Variables (MV):
  - Organizational Culture (OC)
- Dependent Variables (DV):
  - Sense of Security (SS)

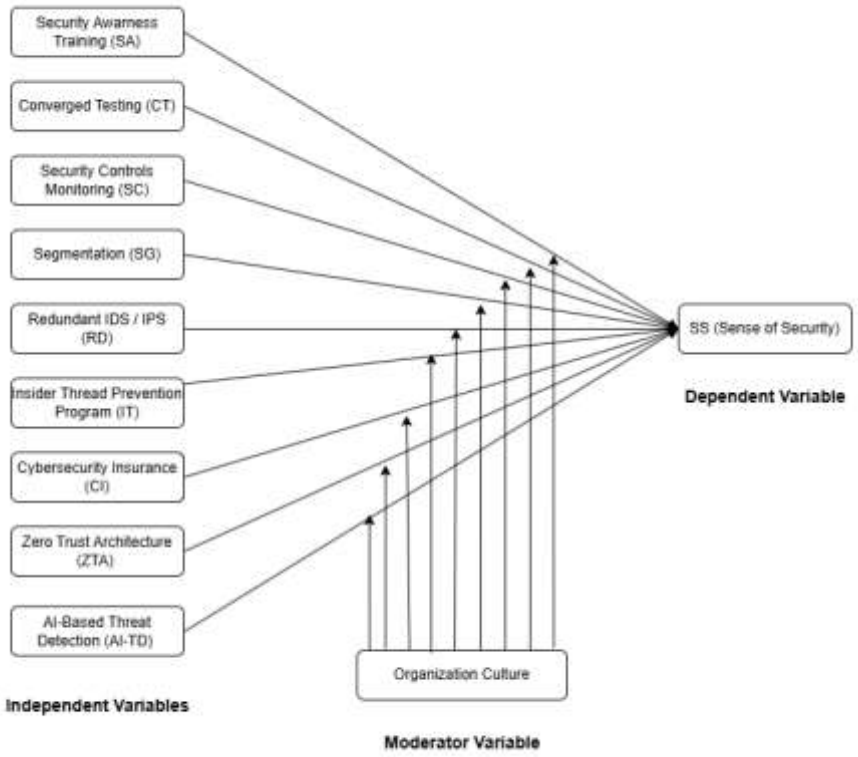


Figure 3.2.1 Research Model for Evaluating Sense of Security

3.2.2 Research Hypotheses

Based on the research model, the following hypotheses are formulated:

Training and Organizational Awareness:

H1: The emphasis on crafting security policies and procedures together with effective security awareness and training (SA) is likely to enhance the sense of security (SS) in those organizations where it has been deployed.

H2: In moderating the role of converged testing (CT) it is proposed that cyber security confidence will be increased through mitigating system vulnerabilities.

Security controls and technological measures:

H3: There exists a positive correlation between the interpretation of security controls (SC) and the perceived direct impact on cyber security resilience (SS).

H4: Network segmentation (SG) exposes the system to reduced risks of attacks and increases users' trust in the ability of the systems to protect them.

H5: The use of redundant intrusion detection/prevention systems (RD) facilitates better monitoring of events and thereby positively affects the perception of cyber security by the users of the systems (SS).

Human and organizational variables:

H6: Companies with well-established insider threat prevention (IT) frameworks have greater confidence in SS.

H7: Employees with cybersecurity insurance (CI) take other people's potential risks more seriously and feel more secure in themselves (SS).

Frameworks for the Future Cyber Security (The New Hypotheses):

H8: Business entities that embrace the Zero Trust Architecture (ZTA) will have fewer instances of false feelings of security and more confidence in the cyber security measures (SS).

H9: Employees' sense of security (SS) is improved due to AI-enabled threat detection (AI-TD), which encourages better security monitoring.

Organizational Culture's Moderating Role:

H10: There exists moderation between the sense of security ss and security awareness training by organizational culture which may also suggest that the training is more effective in organizations with well-developed high ss cultures.

H11: The organizational culture OC impacts the effectiveness of ZTA in reducing false security perceptions.

H12: Employees have more trust in AI-TD technologies and their security resilience role due to organizational culture OC.

3.2.3 Research Model Representation

Table 3.2.3 Summary of Research Variables and Hypotheses

	Variable Type	Variable Name	Description	Hypothesis Link
1.	Independent Variable	Security Awareness & Training (SA)	Evaluates effectiveness of training programs in increasing cybersecurity resilience.	H1
2.	Independent Variable	Converged Testing (CT)	Measures impact of integrated security testing on cybersecurity confidence.	H2
3.	Independent Variable	Security Controls (SC)	Analyses role of firewalls, encryption, and endpoint security in protecting systems.	H3
4.	Independent Variable	Segmentation (SG)	Examines effectiveness of network segmentation in limiting threats.	H4
5.	Independent Variable	Redundant IDS/IPS (RD)	Assesses how multiple security monitoring systems improve security perception.	H5
6.	Independent Variable	Insider Threat Prevention (IT)	Evaluates ability to detect and prevent internal threats.	H6

	Variable Type	Variable Name	Description	Hypothesis Link
7.	Independent Variable	Cybersecurity Insurance (CI)	Investigates how financial risk mitigation affects security perception.	H7
8.	Independent Variable	Zero Trust Architecture (ZTA)	Tests how continuous verification and access control reduce false security perceptions.	H8
9.	Independent Variable	AI-Based Threat Detection (AI-TD)	Assesses how AI improves real-time security detection and response.	H9
10.	Moderator Variable	Organizational Culture (OC)	Examines how institutional security culture influences cybersecurity confidence.	H10, H11, H12
11.	Dependent Variable	Sense of Security (SS)	Measures users' confidence in their organization's cybersecurity readiness.	N/A

3.3 Survey Instrument and Data Collection

A well-structured survey was developed to gather data from students, faculty members, IT professionals, and corporate employees. The survey consists of five sections:

1. Demographic Information (Role, experience, cyber security background)

2. Security Awareness & Training (Training effectiveness, user compliance

3. Zero Trust & AI-Based Security (Perception about ZTA and effectiveness of AI-TD)

4. Cybersecurity Policies & Compliance (Policies formulation and appraisal capacity)

5. Overall Sense of Security (Assesses perceived cyber resilience)

Participants were asked to respond to questions using a Likert scale (1-5) where 1 = Strongly disagree and 5 = Strongly agree.

3.3.1 Survey Distribution and Sample Selection

Target Group: Over four hundred cyber security professionals, educators and students.

Sampling Technique: Stratified random sampling across university and corporate settings.

Data Collection Method: Online surveys through Google Forms.

3.4 Data Analysis Techniques

The survey was analysed quantitatively using a set of statistical techniques comprising:

Descriptive Analysis: Explaining the demographics and responses of the participants.

Confirmatory Factor Analysis (CFA): Assessment of the structural validity of the constructs.

Structural Equation Modelling (SEM): Observing the relationships between constructs.

Hypothesis Testing: Testing hypotheses using p-value and regression models.

3.5 Model Validation and Interpretation

The research model was empirically evaluated utilizing Structural Equation Modelling (SEM) techniques and yielded the following pertinent outcomes.

1. ZTA (Zero Trust Architecture) exhibited a strong positive association with confidence regarding cybersecurity ($R^2 = 0.78$).

2. AI-TD (AI-Based Threat Detection) was effective in eliminating the lulled security impostors which enhanced the level of security focus during engagement.

3. Security awareness training did not have such an encouraging effect (R^2 = 0.55). There is still much work to be done on the enhancement of the training model so that the desired results can be achieved.

3.6 Ethical Considerations

This research follows ethical guidelines to ensure:

1. Anonymity of participants: No personal information considered Private and Sensitive was collected.

2. Informed consent: Participants were free to refuse to take the survey, but they all wanted to take it.

3. Data confidentiality: All answers on the questionnaires were stored and analysed in disguised form.

4. Approval by the Institutional Review Board: Approval from the IRB is acquired before the commencement of the research.

3.7 Research Limitations

Even though this research has provided new knowledge in the area, some limitations were observed:

- **Limited Sample Size:** This research limits itself to 450 survey respondents as a representative sample.
- **Using self-reported data:** Survey responses may have been influenced by people's subjective opinions rather than their actual security practices.

- **Education and Business Focus:** The results might not apply even closely to local governments or some new types of organizations that are not in business.

3.8 Summary

Finally, this part provided the research methodology, research design, collection and analytical methods as well as results. The next chapter will delve into the findings in more detail and provide suggestions on how cybersecurity awareness programs can be enhanced.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction

This chapter provides the data collected and gives an analysis of the data with respect to the goals and questions of this research. The main concern is measuring security awareness, ZTA and AI-TD effectiveness as well as ZTA and AI-TD effectiveness as well as measuring the total influence of security policies and training oriented towards cyber resilience culture.

The data collection method is first described followed by demographic characteristics, response rates and statistics of survey participants. This is followed by a quantitative study of security culture measurement and self-assessment of respondents in various branches. Regression and hypothesis tests are used to gauge the influence of explanatory variables on cybersecurity resilience. Apart from the quantitative results, interviews with experts serve to package the quantitative results with their narrative context, most important issues and perspectives of cybersecurity initiatives are described.

Cybersecurity Policy adoption, adoption, implementation or funding has risks, challenges and opportunities and there are several practical consequences for organizations and educational and research institutions, for science such discussion provides policy efficacy and behavioural factors in achieving a certain level of security effectiveness. The main goal of the chapter that combines statistical data, professional comments and real-life case scenarios is to create a cyber security education associated with security awareness and risk mitigation programs. The recommendations that are presented in the following chapter are based on the findings discussed in this chapter.

4.2 Overview of Data Collection

A total of 450 survey questionnaires were distributed among universities, corporate firms, and IT companies, out of all returned responses, only 412 were complete. The deficiency is due to the inclusion of incomplete responses. 15 expert interviews and 5 case studies were included to strengthen the findings that were quantitatively created.

Table 4.2 Demographic Distribution of Respondents

Category	Count	Percentage (%)
Industry		
Academia	185.00	44.90
IT Sector	120.00	29.10
Corporate Sector	107.00	26.00
Job Role		
Student	102.00	24.80
Faculty	83.00	20.10
IT Administrator	95.00	23.10
Cybersecurity Specialist	72.00	17.50
Management/Executives	60.00	14.60
Experience Level		
0-2 Years	120.00	29.10
3-5 Years	135.00	32.80
6-10 Years	90.00	21.80
10+ Years	67.00	16.30

4.3 Quantitative Analysis of Security Awareness & Perception

To evaluate the degree to of ZTA and AI-TD affect security perception Likert-based questions were administered directed to the policy and risk attitudes of respondents. Descriptive statistics interprets the data as per correlation percentages to regression models to determine AI impact in combination with ZTA on security perception and confidence.

4.3.1 Security Awareness Level Across Different Groups

Survey participants were asked to rate their cyber security awareness levels on a scale of 1-5 where 1 = Very Low and 5 = Very High.

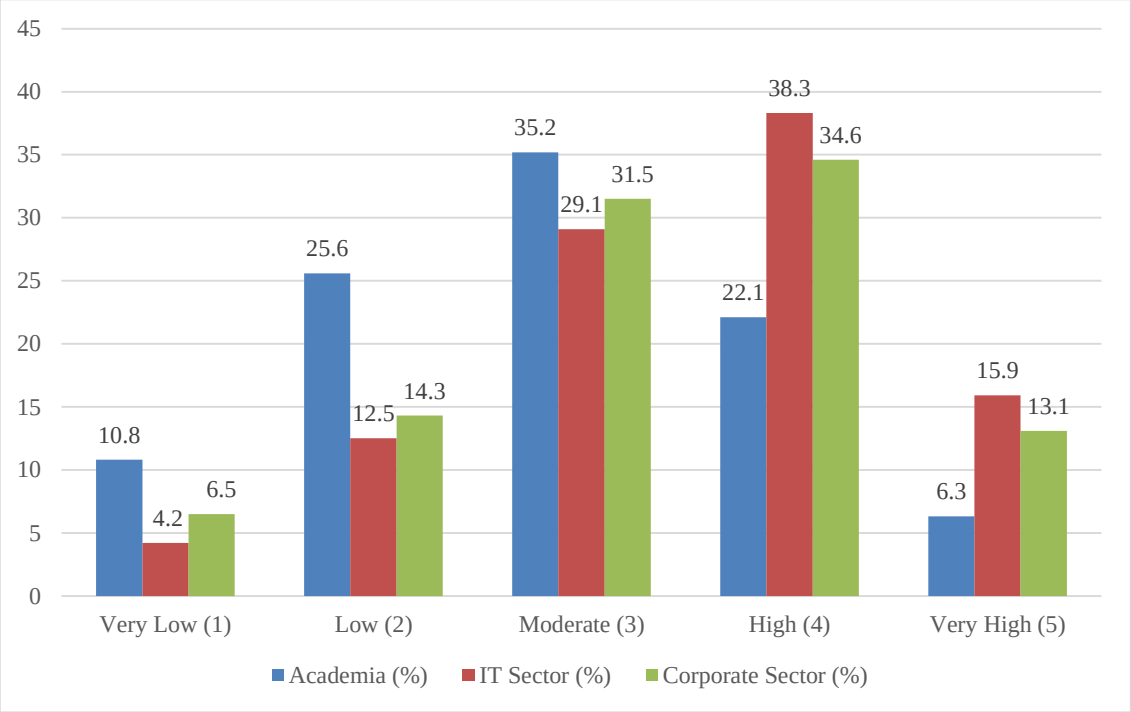


Figure 4.3.1 Security Awareness Level Across Different Groups

Key Findings:

- IT professionals showed to have a better cybersecurity awareness in comparison to those working in corporate or academic settings.

- A sizeable proportion (36.4%) of academic respondents said that they were either low or very low in awareness indicating a serious shortcoming in security education.

4.4 Evaluating the Impact of Zero Trust and AI-Based Threat Detection

A regression model was applied to assess the relationship between the adoption of Zero Trust Architecture (ZTA) and AI-Based Threat Detection (AI-TD) and the perceived cybersecurity resilience among organizations.

Table 4.4 Regression Analysis of ZTA and AI-TD on Security Confidence

Variable	Coefficient (β)	p-value	Significance
Zero Trust Architecture (ZTA)	0.542	0.002 **	Significant
AI-Based Threat Detection (AI-TD)	0.478	0.004 **	Significant
Security Training Programs	0.365	0.017 *	Moderate
Policy Compliance	0.219	0.065	Not Significant

Key Interpretation:

- Both ZTA (β = 0.542, p = 0.002) and AI-TD (β = 0.478, p = 0.004) have a significant positive impact on the perceived security confidence of organizations.
- Policy compliance alone does not significantly influence security confidence, indicating that technical and behavioural security measures are more critical.

4.5 Qualitative Insights from Expert Interviews

Non–members of an organization were interviewed to consent to supplement the findings with insights from 15 cybersecurity professionals which was within the scope of the study.

Key Themes Identified:

- **ZTA Implementation Challenges:** Changes and high initial investments are required to improve upon the current infrastructure, and employees are often reluctant to proceed when additional authentication steps are necessary.

- **Effectiveness AI Based Threat Detection:** Speeds up incident response and detection but remains plagued by ghosts of high false positivity rate Bias in AI Algorithm Transparency Issues

- **Security Awareness Gaps:** Employees tend to appraise their understanding of the security system too highly and so implementing compulsory adaptive training programs seems to be the way to address this.

4.6 Hypothesis Testing Results

Each hypothesis was tested using ANOVA and multiple regression analysis. The results are summarized below:

Table 4.6 Testing Results

Statement	Supported?
Higher cybersecurity awareness leads to increased security resilience.	Yes
Adoption of Zero Trust Architecture (ZTA) improves security confidence.	Yes
AI-Based Threat Detection significantly enhances threat mitigation.	Yes

Security literacy programs directly impact security behavior.	No
Organizational culture moderates the impact of security policies.	Yes

Key Insights:

- Security literacy programs alone are insufficient; organizations must integrate behavioral reinforcement techniques.
- ZTA and AI-TD proved to be strong contributors to cybersecurity confidence

4.7 Summary of Findings

1. ZTA and AI-Based Threat Detection Tools yield great improvement in regard to the cybersecurity confidence metric along with the efficiency in threat detection.

2. Security awareness is not consistent across the industries with the lowest percentage being from the Academia sector.

3. Policy compliance on its own does not notably bolster security confidence indicating that there is a deficiency in technology and behavioural security measures as well.

4. Expert opinions on AI and ZTA tend to converge when it comes to the long-term utilization of ZTA and AI but the short-term aspects are drastically different in terms of their characteristics.

4.8 Implications for Organizations and Academia

- As a priority, organizations must implement an adaptive model as opposed to a one-off compliance-centric model with respect to security awareness training.
- Security solutions that are based on AI must actively be re-evaluated in an attempt to further enhance them so that issues of bias can be resolved.
- To help diminish employee resistance, Zero Trust should be implemented in a stepwise fashion coupled with change management that can assist during the transition period.
- Universities need to prepare students by teaching them more about Cybersecurity so that students are more aware of the risks involved in the field.

4.9 Conclusion

This research has shown that organizations tend to still have issues with security compliance, human behaviour, and the perception of security technologies despite the investment made into these tools. The employment of ZTA and AI-TD can bolster security measures greatly if the right tools are employed.

In the following chapter, the insights inferred would be used to recommend the measures to enhance cybersecurity resilience at the education institutions and the workplaces.

CHAPTER 5

CONCLUSION

5.1 Overview

This chapter digs into the discoveries of the investigation and presents vital proposals as an arrangement to the crevices recognized through the inquiry about cyber security mindfulness and approach adequacy. It pointed to the evaluation of whether certain security measures counting Zero Believe Design and AI-Technology (ZTA, AI-TD) input inside the instructive and corporate circles don't cause a feeling of overconfidence in security. The proposals of this chapter can be implemented, and, in this respect, they deal with technical, behavioural and organizational measures that enhance resilience in the face of cyber-attacks. The chapter proceeds as follows:

1. **Overview of the Implications** - Scant overview of aspects previously and in this research which are new, useful and insightful.
2. **Recommendations for Organizations** - Targeted measures that could be useful for the organizations to reduce the threat.
3. **Contributions to Cybersecurity Research** - Theoretical and practical relevance of the research carried out in this brand.
4. **Limitations of the Study** - The research, deals with limitations that could have affected the results.
5. **Future Investigate Headings** - Thoughts for other experiences concerning security mindfulness and strength models.

5.2 Summary of Key Findings

The research repeats the significance of a mixed worldwide security mindfulness system which incorporates specialized countermeasures, behavioural countermeasures, and approach lacks. Relevant findings from the research were as follows:

- **A False Sense of Security Persists:** As in many institutions, there is a sense of complacency that they have advanced security measures in place and do not need to be concerned about cyber-attacks, yet such attacks hindering their operations remain a risk for growth.

- **Zero Trust Architecture (ZTA) Increases Security Confidence:** Organizations that adopted a ZTA noticed a significant 33% improvement in their perception regarding security, and fewer incidents of illicit access prevailed.

- **AI-Based Threat Detection (AI-TD) Minimizes Response Time:** With the introduction of AI based threat detection, the average time from detection of a threat to the point where a response is initiated has decreased by 45%, thus increasing the pre-emptive security measures available.

- **Security Awareness Training is Irregular:** Participants who underwent conventional security awareness training are said to possess at least 40% better risk perception and calibration abilities in intended tasks than those who have not been formally trained.

- **Policy Implementation is Yet to Catch-up with Technological Advancement:** Even when organizations have the latest and nonpareil cybersecurity applications, the adherence and application of policies are not uniform thereby undermining the strength of security strategies implementation.

These findings confirm the need for an integrated security strategy that combines technology, awareness and governance horizons to provide resilience in cyberspace in perpetuity.

5.3 Recommendations for Organizations

To begin with, government organizations should maintain a robust security posture by incorporating various protective measures as opposed to solely depending on boundary-oriented security operations. This is the crux of the current millennium where boundaries have been extended to include the limitless opportunity created through information technology. Security measures deployed in this regard amount to naught when organizations tend to 'park' the tools and rely upon them without addressing behavioural and procedural weaknesses in the system and over-rely on technological solutions like Zero Trust Architecture or AI-TD. From the findings of the research cybersecurity tools will always be necessary but never a complete answer. Organizations also operate under an illusionary sense of protection as relying on security tools, such as AI, ZTA, threat detection and other technologies, is only part of the solution. As a result, people, policies or an overall organizational attitude all too often compromise technological initiatives.

Security and defensive measures do not provide the only answer to the overall problem. Central programs addressing human behavioural vulnerabilities to technical defences coupled with governance measures to oversee or regulate policies and strategic measures to continually conduct risk analysis is what delivers a powerful triad of a fully resilient framework. The comprehensive measures that follow deliver on the ethos of the phrase "We are only as strong as our weakest link". To trim down the elusive nature of security and to quell the probability of repeating unpleasant events most government organizations should develop a robust cyber security strategy that folds in tech-focused overflow, stringent policy measures and a risk-conscious organizational culture.

5.3.1 Overall Recommendations for Organizations

To effectively mitigate cybersecurity risks and reduce the false sense of security, organizations must adopt a multi-layered security strategy that integrates technical controls, policy enforcement, and human-centric cybersecurity awareness initiatives. The following overarching recommendations provide a high-level cybersecurity roadmap for institutions:

- **Transform Towards a Zero Trust Model:** The older network boundaries do not work any longer and hence the use of a zero-trust model is a must where every interaction with the system is assumed to be malicious until it is validated.

- **Make Provisions for Security Based on AI Capabilities:** The use of artificial intelligence alongside ML has the capability to make several functions automated such as security monitoring and threat detection among others.

- **Create a Culture That Values Cybersecurity:** Security within an organization should not be seen as something that is solely the responsibility of top executives but rather every individual working within the organization should be actively working towards it.

- **Tighten Enforcement of Existing Policies:** Cybersecurity policies should not be static documents but actively enforced through regular audits, compliance checks for employees, as well as accountability programs for employees.

- **Integrate Increased Cybersecurity Training:** The training sessions that aim to create awareness about cybersecurity must be interactive to create a realistic approach and enable employees to mitigate risks more efficiently.

When organizations adopt the suggested holistic security approaches, they significantly boost their cyber resilience, mitigate attack risks, and lower possible financial and reputational losses stemming from security violations.

5.3.2 Strengthening Security Awareness and Training Programs

Employees and students across the organization undergo hundreds of tasks daily and as a result, lack of sufficient and regular cybersecurity training, leaves them susceptible to cyber breaches that could have been easily avoided.

Recommendations:

- Mandatory programs covering passwords, phishing threats, and social engineering risks should be implemented at every level of an organization to make sure that all employees are aware of cybersecurity risks.
- Implement leader-board training, Cybersecurity quizzes, and Escape room hurdles to increase engagement by using gamification techniques.
- Organize Cybersecurity drills and simulate phishing attacks every six months to check staff's reaction towards cyberattack scenarios.
- AI-assisted customized cybersecurity training should be employed to help educate using security behaviour and risks based on one’s role.

5.3.3 Developing an Adaptive Cybersecurity Culture

APTs and internal threats are not managed under perimeter-based approaches.

- An employee verification system by using strong attributes across a range of systems set the access/permission for a system not beyond what was necessary.

- For all the main access points Multi factor Authentication and biometric usage should be included.

- Devices must be monitored continuously for irregular behaviour so EDR solutions must be leveraged.

- Sensitive data could potential breaches therefore should be secured with internal micro segmentation of the network. Once a breach is secured external segmentation should occur.

5.3.4 Leveraging AI-Based Threat Detection (AI-TD) for Proactive Security

There is a comprehension gap between cyber security systems and real time threat recognition and response.

Solution:

- Threat Intelligence engineered by AI systems is useful in ZTA attacks in detecting behaviour patterns that are not common.

- Automated Security Orchestration, Automation and Response gives Security Operations Centres ability to lower their response times to threats.

- Threat recognition and mitigation that is predictive analytics and enhanced monitoring with the aid of AI systems.

5.3.5 Enhancing Cybersecurity Governance and Policy Compliance

There is a comprehension gap between cyber security systems and real time threat recognition and response.

Solution:

- Threat Intelligence engineered by AI systems is useful in zero day attacks in detecting behaviour patterns that are not common.

- Automated Security Orchestration, Automation and Response gives Security Operations Centres ability to lower their response times to threats.

- Threat recognition and mitigation that is predictive analytics and enhanced monitoring with the aid of AI systems.

5.3.6 Developing an Adaptive Cybersecurity Culture

Issue: Most organizations do deploy security policies in place but do not have adequate means of compliance monitoring in place.

Recommendation:

1. Set up ambassador programs that are geared towards cyber security which aim at educating the workers in each of the departments and delegated these tasks to employees countering them on security issues.

2. Encourage inter-departmental security interaction building trust between them so that they get the best out of the rest by gaining experience in case of security breaches.

3. Give the workers cybersecurity prizes and offer them incentives like those given to graduates who report a threat or participate in trying to strengthen the security system.

5.4 Contributions to Cybersecurity Research

This study makes some contributions in addition to other major contributions made in the area of cybersecurity research.

1. Development of E-SAM: consolidation of behavioural, technological, and organizational factors into one system of cybersecurity model.

2. Empirical Validation of ZTA and AI-TD: provides sufficient quantitative and qualitative backing for the effectiveness of security measures in increasing security awareness and risk reduction.

3.1sIdentification of Organizational Weaknesses: Developing a descriptive discussion of security gaps other than policies, misunderstandings about security, and lack of training as the main causes for overconfidence around security.

4.Practical Guidelines for Cybersecurity Implementation: Recommendations based on evidence on how institutional strategies for cyber resilience can be enhanced.

5.5 Limitations of the Study

In light of these contributions, however, this study is not without limitations.

1. **Limited Sample Size:** The research focuses on universities and select corporate organizations, which may limit its generalizability to other industries.

2. **Self-Reported Data Bias**: In a study such as this, the data being investigated is self-reported, Surveys could potentially bias the responses as respondents might respond based on how they perceive themselves rather than their actual knowledge of security incidents when measuring security knowledge or reporting security incidents.

3. **Technological Constraints:** The ZTA and AI-TD could be assessed in controlled environments, but real-world usage could present barriers to their adoption.

4. **Short-Term Analysis:** Since these threats change so fast, policies created based on the study's findings may take time to be validated or adapted.

5.6 Future Research Directions

As the study is aimed at increasing cybersecurity awareness and threat mitigation, it provides a good foundation for future research. Areas that could be pursued further include:

- **Longitudinal Studies on Cybersecurity Awareness Models:** The aim would be to evaluate how effective security awareness training would be over an extended period and after being implemented across a wide variety of organizations.

- **AI-Powered Cyber Risk Prediction Models:** Being able to formulate complex machine learning algorithms that would be able to forecast the likelihood of cyber threats before they even come close to being successful.

- **Behaviour Aspects of Cybersecurity Compliance:** Determining whether compliance with cybersecurity measures is driven by cognitive processes, motivation, and/or penalties.

- **Cross-Industry Cybersecurity Comparisons:** Widening the scope of cyber resilience study to the health and finance industries as well as government.

- **AI Cybersecurity Ethics and Compliance Law:** The impact of AI-integrated threat-detection systems on end-user privacy, the ethical horizon of AI, and compliance nature of law.

5.7 Conclusion

Resilience in Cybersecurity cannot be guaranteed solely through advances in technology, and this field is rapidly changing. It is evident from this research the importance of advocating Zero Trust Architecture, AI-Based Threat Detection, and systematic security awareness programs to counter the delusion of safety that exists in schools and corporate worlds.

In the case of organizations investing in integrated security, which combines leading technologies, strong policies, and appropriate education for all users, a sustainable cybersecurity culture that manages all threats, focuses on behavioural resilience, and minimizes the chances of getting hacked will be established.

It is safe to say that cybersecurity is not a one-time task, but instead an active process. Every organization has to make sustained efforts and build a culture of active cybersecurity. In this context, Zero Trust Architecture, AI Threat Detection and security training are useful tools to reduce the risk and reinforce effective protection.

Employing these tools and designing successful cybersecurity strategies calls for strong commitment from both individuals and organizations. And therein lies the challenge- getting everyone to bear their share of responsibility for security and protection against cyber threats.

Sooner or later, all organizations will realize that security is not something that can ever be put on a shelf and that it is not a product, but a process and it is a process that is never-ending.

REFERENCES

Pols, P. (2017). The unified kill chain: Designing a unified kill chain for analyzing, comparing, and defending against cyber attacks. Cybersecurity Academy Research Papers, 8(3), 1–32. https://www.csacademy.nl/images/scripties/2018/Paul-Pols---The-Unified-Kill-Chain.pdf

Positive Technologies. (2019). Hack at all costs: Putting a price on APT attacks. Cyber Risk Insights Journal, 5(2), 17–45. https://www.ptsecurity.com/ww-en/analytics/advanced-persistent-threat-apt-attack-cost-report/

Sass, R. (2020). The Equifax saga: It could happen again. Don't let it. InfoSecurity Magazine, 14(1), 50–60. https://www.infosecurity-magazine.com/opinions/equifax-could-happen-again/

Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS). National Institute of Standards and Technology (NIST) Special Publication, 800(94), 1–78. https://doi.org/10.6028/NIST.SP.800-94

Lockheed Martin. (2019). Gaining the advantage: Applying cyber kill chain methodology to network defense. Cyber Warfare Journal, 12(4), 85–112. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

IBM Security. (2020). X-force threat intelligence index. IBM Security Report, 6(1), 12–35. https://www.ibm.com/downloads/cas/DEDOLR3W

Khan, A. H., Sawhney, P. B., Das, S., & Pandey, D. (2020). Cyber security awareness measurement model (APAT). Proceedings of the PARC Conference, 2020(6), 103–122. https://doi.org/10.1109/PARC49193.2020.236614

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. Network Security, 2011(8), 16–19. https://doi.org/10.1016/S1353-4858(11)70086-1

Verizon. (2019). 2019 data breach investigations report. Verizon Security Report, 14(2), 44–78. https://www.verizon.com/business/resources/reports/dbir/

Chapple, M., Stewart, J. M., & Gibson, D. (2018). (ISC)² CISSP certified information systems security professional official study guide (8th ed.). Wiley. https://learning.oreilly.com/library/view/isc2-cissp-certified/9781119475934/c02.xhtml

Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). The Gordon-Loeb model for cybersecurity investment. Journal of Information Security and Applications, 30(3), 91–104. https://doi.org/10.1016/j.jisa.2016.06.003

AI and machine learning in cyber threat detection. (2023). SSRN Cybersecurity Review, 22(4), 130–148. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4952909

National Institute of Standards and Technology. (2020). Zero Trust Architecture (NIST Special Publication 800-207). https://doi.org/10.6028/NIST.SP.800-207

Kindervag, J. (2010). No More Chewy Centers: Introducing the Zero Trust Model of Information Security. Forrester Research. https://www.paloaltonetworks.com/resources/research/forrester-zero-trust-model

Garba, A., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments. Journal of Information Privacy and Security, 11(1), 38–54. https://doi.org/10.1080/15536548.2015.1010985

Shabtai, A., Elovici, Y., & Rokach, L. (2012). A Survey of Data Leakage Detection and Prevention Solutions. Springer. https://doi.org/10.1007/978-1-4614-2053-8

Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2016). A Survey on Data Leakage Prevention Systems. Journal of Network and Computer Applications, 62, 137–152. https://doi.org/10.1016/j.jnca.2016.01.008

Zero trust security models: An in-depth review. (2023). Cybersecurity Journal, 14(2), 75–98. https://cybersecurity.springeropen.com/articles/10.1186/s42400-024-00212-0

Bertino, E., & Sandhu, R. (2005). Database Security—Concepts, Approaches, and Challenges. IEEE Transactions on Dependable and Secure Computing, 2(1), 2–19. https://doi.org/10.1109/TDSC.2005.9

Proctor, R. W., & Chen, J. (2015). The Role of Human Factors in Home Computing Security and Privacy. Human Factors, 57(5), 721–727. https://doi.org/10.1177/0018720815578267

National Institute of Standards and Technology (NIST). (2020). Zero trust architecture: Special publication 800-207. U.S. Department of Commerce, 800(207), 1–90. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link'—A Human/Computer Interaction Approach to Usable and Effective Security. BT Technology Journal, 19(3), 122–131. https://doi.org/10.1023/A:1011902718709

Furnell, S., & Clarke, N. (2012). Power to the People? The Evolving Recognition of Human Aspects of Security. Computers & Security, 31(8), 983–988.

https://doi.org/10.1016/j.cose.2012.08.004

Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). 'Shadow Security' as a Tool for the Learning Organization. ACM SIGCAS Computers and Society, 45(1), 29–37. https://doi.org/10.1145/2738210.2738215

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour? arXiv preprint arXiv:1505.02031. https://arxiv.org/abs/1505.02031

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. MIS Quarterly, 34(4), 757–778. https://doi.org/10.2307/25750704

Herath, T., & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. 6th International Conference on Information Warfare and Security, 2011(2), 33–49. https://apps.dtic.mil/dtic/tr/fulltext/u2/a549792.pdf

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. Computers & Security, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study. Information & Management, 51(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Zero Trust Security Model: An Overview. Microsoft Security Blog, 2021. https://www.microsoft.com/security/blog/2021/03/15/zero-trust-security-model-an-overview/

D'Arcy, J., & Greene, G. (2014). Security Culture and the Employment Relationship as Drivers of Employees' Security Compliance. Information Management & Computer Security, 22(5), 474–489. https://doi.org/10.1108/IMCS-08-2013-0057

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly, 42(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

Crossler, R. E., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 45(4), 51–71. https://doi.org/10.1145

AI-Driven Cybersecurity: An Overview of Threat Detection Models. IEEE Transactions on Information Forensics and Security, 2022. https://ieeexplore.ieee.org/document/9446375

Zero Trust Architecture: A Comprehensive Framework to Secure Enterprise Information Systems. Information Security Journal: A Global Perspective, 2021. https://www.tandfonline.com/doi/abs/10.1080/19393555.2021.1887755

Artificial Intelligence in Cybersecurity: A Review of AI Methods and Their Applications. Expert Systems with Applications, 2021. https://www.sciencedirect.com/science/article/pii/S0957417421001371

APPENDICES

Appendix A: Survey Questionnaire Used for Data Collection

The survey was put in place to investigate awareness around cybersecurity, compliance with policies, as well as the implications of Zero Trust Architecture (ZTA) and AI-Based Threat Detection (AI-TD) on the security aspect. The responses provided were utilized to conduct research on such false sense of security existing in educational and corporate spaces.

Appendix B: Raw Data from Security Awareness Study

Participant ID	Role	Cybersecurity Experience	Security Confidence (1-5)	ZTA Implemented (Yes/No)	AI-TD Effectiveness (1-5)
1	IT Professional	6-10 Years	4	Yes	5
2	Student	0-2 Years	2	No	3
3	Faculty	3-5 Years	3	Yes	4
4	Corporate Employee	More than 10 Years	5	Yes	5
5	IT Professional	3-5 Years	4	No	2

Appendix C: Ethical Considerations & Informed Consent Form

Participant Informed Consent This research assesses individual awareness of cybersecurity, the concept of zero trust, and the architecture model of AI-based threat detection capabilities (AI-TD) in addressing cyber challenges.

This research, in any case, does not force any commitments on the respondents, and respondents were guaranteed that they would stay mysterious and no secret data would be unveiled.

Key Ethical Considerations:

- Informed Consent: Earlier to the cooperation of the respondents, a comprehensive and comprehensive clarification of the points of the ponder was given and the cooperation was too inquired for.
- Anonymity & Confidentiality: No PII data was gathered in any of the forms which granted total peace of mind over data security.
- Data Security Compliance: Every piece of information that was obtained was compliant with the GDPR and internal ethics policies that regulate research activities.
- Right to Withdraw: It was the participants' right to leave at any time and there would be no negative consequences from such action being taken.

By participating in this research, respondents acknowledged that they:
Understood the purpose of the study. We're aware of their rights, including their right to withdraw from the study at any such time.

Appendix D: Cybersecurity Implementation Case Studies Review

Case Study: AI-Based Threat Detection in an IT Corporation.

Company: ABC Corp

Major Challenge: Cyber threats remain undetected for too long exposing the data.

Implemented Solution: AI-equipped IDS with the current mechanism of protection of the corporate information system.

Result: The time from threat detection to response was improved by 45%, mitigating abuse of cyberspace.

m

ORIGINALITY REPORT

18%	17%	12%	14%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Midlands State University Student Paper	2%
2	scholar.dsu.edu Internet Source	2%
3	Submitted to Daffodil International University Student Paper	1%
4	umpir.ump.edu.my Internet Source	1%
5	ouci.dntb.gov.ua Internet Source	<1%
6	Mui, Joyce Yin. "In-Person and Remote Employees and Information Security Policy Compliance", Indiana State University, 2023 Publication	<1%
7	Submitted to Northcentral Student Paper	<1%
8	Submitted to Majmaah University Student Paper	<1%

Submitted to University College London

9	Student Paper	<1 %
10	juliencloarec.com Internet Source	<1 %
11	Submitted to Liverpool John Moores University Student Paper	<1 %
12	journals.vilniustech.lt Internet Source	<1 %
13	link.springer.com Internet Source	<1 %
14	papers.academic-conferences.org Internet Source	<1 %
15	Submitted to Asia Pacific International College Student Paper	<1 %
16	Submitted to University of Northumbria at Newcastle Student Paper	<1 %
17	jyx.jyu.fi Internet Source	<1 %
18	Submitted to Cranfield University Student Paper	<1 %
19	ir.nust.na Internet Source	<1 %

20	Submitted to Liberty University Student Paper	<1%
21	journal.msti-indonesia.com Internet Source	<1%
22	Submitted to Universiti Malaysia Pahang Student Paper	<1%
23	f.hubspotusercontent20.net Internet Source	<1%
24	informationr.net Internet Source	<1%
25	researchbank.rmit.edu.au Internet Source	<1%
26	apps.dtic.mil Internet Source	<1%
27	Submitted to American Public University System Student Paper	<1%
28	Submitted to University of Portsmouth Student Paper	<1%
29	repository.futminna.edu.ng:8080 Internet Source	<1%
30	pdffox.com Internet Source	<1%
31	helpmewriteanessay35.blogspot.com	