An Empirical Investigation of the Origins and Effects of Cybersecurity Culture in IT Organizations

Balamuralikrishna Thati[1], Ravi Kiran Koppolu[2], D. Lokesh Sai Kumar[3,*], Tenali Nagamani[4], P. Muthukumar[5], S. Lalitha[6]

[1]Department of CSE, Dhanekula Institute of Engineering & Technology, Ganguru, Vijayawada, A.P, India
[2]Department of CSE, Jawaharlal Nehru Technological University, Kakinada, Andhra pradesh, India
[3]Department of CSE, Prasad V Potluri Siddhartha Institute of Technology, Vijaywada, Andhra pradesh, India
[4]Department of CSE, SR Gudlavalleru Engineering College, Gudlavalleru, Krishna Dt., Andhra pradesh, India
[5]Department of EEE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Tiruvallur, Chennai, Tamilnadu, 602105, India
[6]Department of CSE, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, India

Emails: balu.thati9@gmail.com; kravi1189@gmail.com; lokeshsaikumar@gmail.com; tenalinagamani@gmail.com; muthukumarvlsi@gmail.com; shemaait@gmail.com

Abstract

This observe investigates the reasons and effects of cybersecurity way of life in IT agencies. Given the developing threats to cybersecurity and the essential role that organizational lifestyle plays in decreasing these risks, it's miles essential to realise the connection that exists among policy elements, employee conduct, and cyber security overall performance. By concentrating at the connections between distinct factors impacting cybersecurity culture and there have an effect on the efficacy of cyber security measures, the examine fills in gaps in empirical studies. This take a look act's principal purpose is to behaviour an empirical investigation into the methods that many sides of cyber security culture, along with policy concerns, employee behaviour, and cyber security attention, have an effect on how properly cyber security measures work in IT companies. The studies in particular examines 3 hypotheses: (1) that coverage factors positively correlate with usual effectiveness; (2) that cyber security attention and engagement in preventive measures are predictively correlated; and (three) that behavioural worries are undoubtedly correlated with the implementation of powerful cyber security measures. Data were collected using a pass-sectional survey the use of a quantitative studies method. A stratified random pattern strategy became used inside the studies to select 100 IT employees from special corporations. A systematic questionnaire overlaying coverage variables, behavioural worries, cyber security recognition, preventative measures, and the perceived efficacy of cyber security strategies become used to collect information. The conclusions of the primary records had been in addition supported and given that means with the aid of secondary information taken from organizational reviews and already published literature. An enormous wonderful connection was discovered in the research between coverage variables and cyber security measures' efficacy, suggesting that robust regulations enhance cyber security overall performance as a whole. It has been proven that employee participation in preventative actions is extensively anticipated by cyber security recognition. The adoption of successful cyber security tactics turned into strongly correlated with behavioural issues. Aside from declaring regions where cyber security lifestyle needs to be stepped forward, the research additionally found gaps in preventative measures' efficacy. The study emphasizes how crucial it is to have clear policy guidelines and raise awareness of cyber security issues in order to encourage efficient cyber security practices in IT companies. The results provide insightful information on the dynamics of cyber security culture and offer doable recommendations for improving cyber security procedures and guidelines. Organizations may enhance their cyber security frameworks and strengthen their Defences against emerging threats by filling up the holes found in the report.

Keywords: Cybersecurity; IT companies; Organizational Culture; Policy Elements

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

1. Introduction

A lot has been going on in the virtual market recently. Initially, technical solutions were prioritized. Certifications such as ISO 27001 and Cyber Essentials were subsequently developed to bolster cyber resilience policies, standards, and processes [1]. "Human Cyber" items have become more common in the last five years or more. Primarily, they were developed to fulfil a mandated need for "awareness training [3]. This is beginning to change, however, as businesses who have put money into cyber protection and established solid rules and processes are realizing that the people running their IT systems pose the greatest threat[4]. A significant number of people have worked remotely since the outbreak, and the number of people online is higher than it has ever been [5]. According to Interpol, the perfect circumstances for an increase in cyber security threats have been established by the combination of the greater connection with the fear, worry, and sense of confinement caused by COVID-19 [6]. The Cybercrime Threat Response Unit of Interpol has reported a dramatic increase in the number of attempted ransomware attacks targeting vital virus response infrastructure and organizations [7]. Companies should consider more stringent measures to ensure their workers follow all policies and procedures while working remotely, as many individuals may continue to do so often in the future[8]. Instead than focusing just on raising awareness, leaders must work to create a cyber-security culture that changes people's actions [9].

A company's "cyber security culture" consists of its employees' beliefs, practices, norms, assumptions, and knowledge on cyber defence. A company's goals, structure, policies, and management all have an impact on these [11]. When the many factors that shape an organization's culture—its policies, procedures, leadership, social norms, etc.—and the factors that shape individuals' cultures—their attitudes, knowledge, assumptions, etc.—are congruent, the result should be cyber security conscious behaviours that reflect the organization's approach to cyber security [12]. The foundation of any cyber security culture is the belief that people, and not technology, are the true protectors of an organization's data. While humans provide the best protection against cyberattacks, they are also the weakest link in cyber security systems. Consequently, it is critical to foster an environment where employees have the knowledge and intuition to serve as the first defence [13].

The evidence-based Security Culture Maturity Model may be used to understand and compare the current security-related maturity of any measurable group, whether it a company, an industry, a region, or anything else [14]. Its five levels, from least developed to most developed, are basic compliance, foundational security awareness, programmatic security awareness and behaviour, management of security behaviour, and sustainable security culture [15].

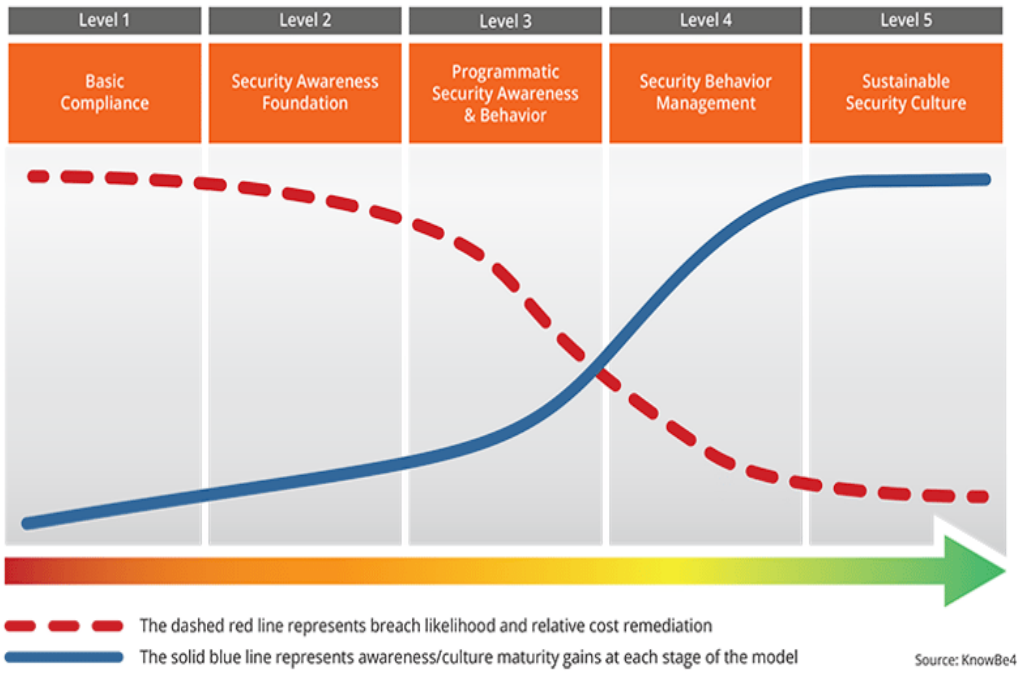


Figure 1. Security Culture Model

The particular awareness, behaviour, and culture advantages that a business will experience at each level are shown by the solid blue S-Curve [16]. Take note of each S-Curve's crossover and inflection locations. A company may anticipate genuine behavioural benefits by focusing on training, regular simulations, and reinforcement techniques to shape employee behaviour. The inflection points and crossover points [17] represent these. Observe

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

the connection between the two curves as well. The dotted red S-Curve indicates a reduction in the chance of a human-related breach and the cost of repair as security knowledge, behaviour, and culture grow [18]. Once again, there is a clear turning point when firms start to deliberately concentrate on behaviour and the social dimensions of how workers value security, rather than just knowledge-based awareness [20]. A larger gap extends from the base of the last level to the very end of the dotted red line, and there is a gap between the top right of the chart and the top of the blue line [21]. These examples show that it is true: no company can ever really "arrive" or be very safe from the risk of a breach caused by humans. That is the core of every security mechanism, whether it is human or technological. Adding layers of security enhances resilience, even if no security layer, whether it be human or technology, can ensure the entire organization security.

The maturity of a cybersecurity culture inside an organization is evaluated using the Security Culture Maturity Model (SCMM). The maturity stages often span from beginning or ad hoc to optimized or advanced.

- **Maturity Level Score Calculation**

On a scale from 0 to 1, let S_i represent the score for each maturity level i, where i runs from 1 to n (the number of maturity levels).

Equation: Maturity Level Score= $\frac{\sum_{i-1}^{n} S_i.W_i}{\sum_{i-1}^{n} w_i}$

Where:

- Si is the maturity level i score.
- Wi = The maturity level i weight

This equation calculates the weighted average score for the maturity level.

- **Maturity Improvement Over Time**

To gauge how much maturity has improved during a certain time span, you might use:

Equation: Improvement = $\frac{\text{Maturity Score}_{\text{Current}} - \text{Maturity Score}_{\text{Previous}}}{\text{Maturity Score}_{\text{Previous}}} \times 100$

Where:

- Maturity Score $_{\text{Current}}$ = Maturity score at the current assessment period
- Maturity Score $_{\text{Previous}}$ = Maturity score at the previous assessment period

1.2 Historical Evolution of Cybersecurity

The discipline of cyber security has been around for a while, contrary to common assumption. The advent of personal computers and their connection to the internet is not the beginning of cybersecurity, contrary to popular belief. Another facet of cybersecurity is ensuring the safety of data that is stored locally on a computer rather than sent across a network [22]. Antivirus software has been an absolute must-have for each computer user since the advent of the internet. Although destructive attacks were less common in the past, the development of IT has paralleled the expansion of cyber security risks. One cannot really grasp the significance of cybersecurity without being familiar with its history. Here we will look at the background of cybersecurity and criminality. This will be accomplished by examining the development of responses to previous cyber security threats.

- **Beginning of Cyber Security**

Cybersecurity has its roots in the early years of internet-based computer-to-computer communication. Concerns about computer system security have existed for decades, despite the fact that the scope and complexity of cyber-attacks have increased dramatically. Cyber dangers are ever evolving due to hackers' ongoing invention of new methods for breaking into networks and stealing confidential data [23]. The idea that cybercrime is a relatively new occurrence is false since security flaws in computer systems have existed for a lot longer. Ever from the beginning of computers, there have been cybercriminals. We can see the early advancements and difficulties in the subject of cyber security beginning in the 1940s, which have influenced its growth throughout time.

- **The 1940s: An Era Before Cyberattacks**

After the first digital computer was created in 1943, carrying out cyberattacks was very difficult for more than 20 years. The danger of cyber-attacks was low since the massive electronic equipment of the period were not networked and only accessible by small, specialized teams with little operating experience. On the other hand, the

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

first theoretical discussion of what would eventually be known as computer viruses occurred in 1949 when computer pioneer John von Neumann suggested the idea of self-replicating computer programs. Even if actual hacks were, still a ways off, this concept set the stage for future advancements in cyber dangers.

- **The 1950s: The Phone Phreaks**

The origins of hacking, as we know it now really lay in the manipulation of telephone networks rather than in efforts to get data from computers. "Phone phreaking" became a prominent subculture in the 1950s. This word describes a range of methods used by "phreaks," people who are enthralled with the inner workings of phone systems, to get around long-distance call costs by taking advantage of the protocols used by telecom companies to control networks from a distance [24]. Phone phreaking gained popularity in the late 1950s as prank phoning increased in frequency. Phone companies found it difficult to completely end the practice, which continued far into the 1980s, despite attempts to restrict these operations. Notably, it has been alleged that Steve Jobs and Steve Wozniak, the co-founders of Apple, were fascinated by the phone phreaking subculture. Their work on the original Apple computers, which marked a major transition from telephony to digital technology, was influenced by their early curiosity with manipulating technology.

- **The 1960s: The Western Front Was Quiet**

The majority of computers were nonetheless large, highly priced mainframes saved in secure, weather-managed rooms via the centre of the Sixties. Because these computers were so pricey, even programmers had very limited get right of entry to them. It is exciting to observe that the phrase "hacking" commenced to become famous at some point of this decade. However, the term "hacking" originated with the MIT Tech Model Railroad Club, whose participants altered sophisticated train systems to lead them to characteristic better as opposed to with computer systems. Eventually, the concept of fixing and converting systems observed its manner into the computer enterprise. In the beginning, the principle purpose of hacking was to get unlawful get right of entry to to systems, frequently merely to check the feasibility of the attack in preference to profit financially or gather political strength. Creating havoc or making an announcement changed into more vital than making any actual progress. However, as hacking methods have become more superior, a vital event that would affect cybersecurity within the destiny came about in 1967. An institution of students changed into requested by way of IBM to go to their headquarters to investigate a new laptop device. Despite receiving training on how to make use of the gadget, the students were capable of straight away understand and take advantage of its flaws. This incident exposed critical weaknesses in IBM and gave upward thrust to the belief of putting security features in location to protect systems from possible hackers. It is appeared as one of the first examples of ethical hacking, a belief that has considering the fact that developed into respectable certifications like the Certified Ethical Hacker credential that is now in use. The use of computers accelerated dramatically throughout the Sixties, and gadgets come to be smaller and more available. Companies began shopping for computers to hold records, so keeping them hidden in safe rooms became tough. During this time, however, passwords took over as the primary manner of each safeguarding and gaining access to computers, which was a important development in the early stages of cybersecurity.

- **The 1970s: The Creeper and ARPANET**

The actual need for cybersecurity to begin with has its roots in the 1970s. In terms of advancements in cyber defines, this decade was pivotal. With ARPANET, the Advanced Research Projects Agency Network was the pioneer in this endeavour. This system of interconnections existed before the advent of the internet. The sound effect "I am the intruder; try to apprehend me!" was generated on PCs that were connected to the network using software developed by ARPANET developer Bob Thomas. For the first time, this program was able to migrate between computers on its own. Despite the fact that the experiment was risk-free, it is reasonable to presume that this was the first computer worm ever found in the history of cyber security. The newly created cybersecurity team's first order of business was to uninstall a malicious program. Ray Tomlinson, a researcher at ARPANET and creator of the Reaper program that sought for and eliminated the Creeper worm, was also the first to set up a networked mail messaging system.[27]

- **The 1980s: Commercial Antivirus Development**

A number of high-profile attacks occurred in the 1980s, including those at AT&T, National CSS, and Los Alamos National Laboratory. A piece of evil software in the 1983 film War Games uses the guise of a game to take control of nuclear missile systems [25]. Words like "computer virus" and "Trojan Horse" made their debut that year as well. Throughout the Cold War, cyber espionage became an increasingly serious threat. As far as cyber security is concerned, this decade may be considered a watershed moment.

It was in 1987 when the word cybersecurity first surfaced. Regardless, Anti4us and Flushot Plus debuted in 1987, thereby launching the commercial antivirus software market, despite several assertions to the contrary.

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

- **The 1990s: The Internet Takes Off**

The internet had rapid expansion and advancement in the 1990s, and the cybersecurity industry started to thrive at this time. This decade saw a number of important advancements in computer security, including:

- Concern about polymorphic viruses was common when they first appeared. The first code that could adapt to several computer platforms and yet retain its original functionality was written in 1990. For cybersecurity specialists, finding these polymorphic infections proved to be an overwhelming task.
- When the notorious DiskKiller malware was unintentionally spread via a well-known computer magazine, PC users met it. Through a video disc that was sent to subscribers, this spyware was able to infect a sizable number of PCs. The proprietors of the magazine denied any misconduct and said they were ignorant of the existence of the virus or the possible damage it may wreak.
- Cybercriminals never stopped coming up with new ways to get around antivirus software's protection mechanisms. The evolution of cyber dangers underwent a sea change during this time, which prompted the creation of fresh approaches to deal with these new problems. The Secure Sockets Layer (SSL) was one such development that came along in 1995. Netscape created SSL with the intention of safeguarding people's internet privacy via secure data, browsing, and transactions. Future protocols like HyperText Transfer Protocol Secure (HTTPS), which would further improve internet security, were built on top of SSL [29].

The 2000s: A Diverse and Multiplying Threat

During this time, the internet saw amazing growth. Computers have become standard in most homes and businesses. Cybercriminals, however, also have access to new opportunities, despite the obvious benefits. A new kind of computer virus that could infect systems without requiring users to download any files first appeared around the turn of the current decade [28]. The diversity and scope of cyber threats have increased in the 2000s. A new kind of stealth infection that presented a severe threat emerged when it became possible to compromise a computer only by viewing a website infected with a virus. During this time, hacks also targeted instant messaging networks. The number of credit card hackers increased, resulting in significant breaches involving private financial data. Prominent corporations such as Yahoo were not exempt from these assaults. One of the biggest security breaches in history occurred when hackers got access to the accounts of over three billion Yahoo users in events that were made public in 2013 and 2014. Cyber dangers, which affect both people and organizations, have become more sophisticated and diversified in the 2000s [30].

1.3 Aim,Objectives and significance of the study

This research aims to investigate and look at cybersecurity lifestyle in an IT region, emphasizing how organizational attitudes, practices, and rules have an effect on cybersecurity measures' efficacy. The intention of this look at is to decide how a good deal cybersecurity information and processes are ingrained in IT businesses' normal operations and organizational cultures. The aim of the research is to decide the blessings and disadvantages of the existing cybersecurity practices by assessing the prevalence of cybersecurity focus among employees, the adoption of preventative measures, and the efficacy of implemented generation. Additionally, the look at will explore how cybersecurity culture is fashioned through policy frameworks, specifically how they have an effect on worker engagement and quality practice adherence. In order to identify areas for development, the studies will even compare the overall effect of corporate tradition at the use and efficacy of cybersecurity strategies. The closing objective is to boom awareness of the methods wherein a sturdy cybersecurity subculture may assist greater stable IT environments and higher defences towards cyber threats. The objectives of the study are

1. To draw attention to the Cybersecurity Culture's policy components.
2. To comprehend the IT staff members' behavioural concerns.
3. To investigate IT staff members' awareness of cybersecurity.
4. To be aware of the precautions that an IT business offers.
5. To research practical ways to improve an IT company's cyber security culture.
6. To learn about the many components of a framework for cybersecurity culture.

This take a look act's comprehensive examination of cybersecurity tradition inside IT groups—a field that is turning into an increasing number of crucial in the contemporary digital technology—underlines its relevance. The look at endeavours to offer critical insights for the creation of more efficacious protection frameworks by way of shedding mild on the methods in which organizational guidelines mold and effect cybersecurity activities. Examining the behavioural concerns of IT staff contributors will spotlight noncompliance with cybersecurity tips and make it less difficult to develop centred treatments to cope with these problems. In addition, assessing the cognizance element of team of workers contributors will offer an indication of how well informed and cognizant they are of cybersecurity dangers, that is important for fostering a proactive security subculture. The have a look act's analysis of a hit preventive measures will offer useful tips for improving cybersecurity subculture, even as its evaluation of preventative measures will examine the efficacy of gift practices in threat discount. The last goal

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

of the take a look at is to create an intensive framework for cybersecurity subculture that can be used as a model by way of other organizations seeking to enhance their cybersecurity posture. This empirical inquiry will provide considerable insights for practice improvement, coverage introduction steerage, and safeguarding organizational property in opposition to cyber threats by using presenting an intensive information of cybersecurity lifestyle development and its impact on security effectiveness.

2. Literature Review

In [19] intention of this text changed into to examine the impact of protection organizational practices on facts security control overall performance and to expand our information of those practices. The authors created survey inquiries to gather records, constructed a research version and hypotheses based on a observe of the literature, and demonstrated the dimension model. They used EQS 6.1 software to collect 111 answers from CEOs of manufacturing SMEs that had put security policies in place. They then used the structural equation model technique to examine the proposed links. The findings confirmed that information security management performance was favourably impacted by security organizational practices, education, visibility, and knowledge exchange in the field of information security **[19]**. The research helped confirm new concepts like information security knowledge sharing and visibility and emphasized the need of academics, practitioners, and policymakers taking organizational factors of information security in SMEs into account. By examining how security organizational practices affected information security performance, it expanded on earlier research and made the case that creative ways to promote employee knowledge exchange were necessary for industrial SMEs to perform better. The study looked at information security organizational practices and their impact on performance, addressing the demand for empirical research centred on SMEs.

In [26] organizations faced a difficulty in information security since sensitive data was seriously at risk from security breaches. Information assets posed security hazards to organizations, some of which may be caused by their own personnel. In order to reduce security lapses, organizations have to concentrate on employee behaviour. They should strive to create a culture of security where people naturally protect information assets. In order to offer a thorough framework, this study was carried out in response to the need for more empirical research on the evolution of security culture [26]. Two categories of characteristics were taken into consideration while developing the Information Security Culture and Key characteristics Framework: those that represent security culture and those that influence it. Through an empirical investigation, the report investigated associated hypotheses and confirmed the framework's applicability. After conducting an exploratory poll, 266 valid replies were received. Factor analysis was used in phase two of the research to show the framework's levels of validity and reliability. Using structural equation modelling, several hypothetical associations were examined. A multi-group analysis was used to provide an indirect exploratory impact of the moderators. The results demonstrated the validity of the framework and its satisfactory fit to the data. The substantial association between personality characteristics and security culture was significantly closed by this research. Additionally, by putting a thorough framework into practice that helped to create a security culture, it enhanced information security management. The framework was a valuable instrument that could be used to evaluate and enhance an organizational security culture, and the criteria were crucial in supporting the adoption of security culture.

In [10] global companies' overall efficiency has taken a hit due to the current uptick in cyberattacks.

There is a lack of thorough study on the factors that affect organizations' cyber security expertise and readiness, despite the fact that organizations must enhance their cyber security to prevent and neutralize assaults. The study utilized the Technology-Organization-Environment (TOE) framework to examine various factors that influence an organization's cyber security readiness [10]. It also examined how these factors affects financial and non-financial organizational performance, and how improved organizational security performance mediates these effects. We gathered 270 valid replies from a survey of Bahraini IT specialists. There was a statistically significant relationship between cyber security readiness and seven of the nine criteria identified in previous studies. Organizational security performance was shown to be positively affected by cyber security preparation, which in turn had a positive effect on financial and non-financial performance. The recently suggested all-encompassing model of elements affecting a company's cyber security preparedness, together with the data proving its relevance, will be useful for future studies. Our knowledge of how businesses may fortify themselves against cyberattacks and lessen their damage is also enhanced by this [2] recent times have shown that as digitization grows, so does the scope of what has to be safeguarded. Even if companies made technological investments to guard against cyberattacks, human error continued to be one of the key weaknesses. This called into question the importance of the human element, which often had to do with cybersecurity knowledge, policy, and training. It was crucial to ascertain if these methods were still effective for safeguarding the data, assets, and personnel of a business. The report examined the importance of cybersecurity culture and previous advancements in the field of security awareness research to depict the present situation [2]. Consequently, the suggested method sought to explore the value proposition of merging the two. The study found that achieving organizational resilience was influenced by

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

workers' perceptions of both formal (cybersecurity policy and awareness) and informal (i.e., culture) standards. To ascertain the long-term consequences of enhancing cybersecurity awareness within the framework of cybersecurity culture, further investigation was necessary.

The review of the literature indicates a sizable research vacuum about the precise impact of policy determinants on cybersecurity efficacy in IT businesses. While research on organizational practices has been done, there has not been much in-depth analysis done on how specific policy elements influence cybersecurity results. Furthermore, while Tolah et al.'s study from 2021 discusses the part employee behaviour plays in security culture, it does not go into detail on how certain behavioural issues affect the use of efficient cybersecurity measures. In [10] identify the variables that impact cybersecurity preparedness, but they do not investigate the relationship between cybersecurity awareness and employee participation in preventative measures. Furthermore, even though talks about the significance of cybersecurity culture, more in-depth study is required to determine how behavioural issues, policy considerations, and awareness all work together to create a strong cybersecurity culture. Research on the long-term impacts of cybersecurity culture efforts on organizational resilience and performance is also lacking. By filling up these gaps, we may get a better knowledge of the interactions between different facets of cybersecurity culture and enhance cybersecurity practices in IT companies, which will increase organizational security and resilience.

3. Research Methodology

The present examine employs a research technique that blends a quantitative approach to comprehensively examine the many traits of cybersecurity lifestyle interior IT corporations. Empirical data was gathered via a cross-sectional survey that centred on essential regions together with policy troubles, behavioural concerns, cybersecurity recognition, preventative moves, and their standard effect on cybersecurity way of life. A stratified random sample of one hundred IT people from numerous organizational degrees was chosen with the intention to guarantee a radical evaluation and allow a consultant investigation of numerous viewpoints in the IT surroundings. A structured questionnaire that addressed some of objectives, together with highlighting policy factors, comprehending behavioural concerns of employees, assessing cybersecurity cognizance, evaluating preventive measures, and getting to know a success approaches to improve cybersecurity subculture, turned into used to accumulate statistics. To offer context and corroborate results, secondary facts from applicable employer reviews and literature had been also protected. In line with the study's dreams of identifying and comprehending the vital factors and frameworks that affect cybersecurity inside IT organizations, this system facilitates an intensive research of the approaches in which distinct components of cybersecurity subculture have interaction and contribute to efficient cybersecurity practices.

Hypothesis of the Study

H1: The total efficacy of cybersecurity measures in an IT organization is strongly connected with the strength of policy variables in cybersecurity culture.

H2: IT workers' awareness of cybersecurity and their willingness to take preventative action are highly correlated.

H3: The adoption of successful cybersecurity measures is closely linked to the behavioural concerns of IT staff members.

3.1 Data Description

The study's dataset consists of empirical data gathered from a cross-sectional survey that included one hundred IT workers from different organizational levels. With an emphasis on policy considerations, behavioural issues, cybersecurity awareness, and preventative actions, the poll sought to assess several aspects of cybersecurity culture inside IT firms. Responses to a 25-question structured questionnaire that evaluates important aspects such cybersecurity awareness, behavioural concerns, policy factors, effective measures, and preventive actions are included in the dataset. The dataset is supplemented with secondary data from pertinent organizational reports and cybersecurity practice literature, in addition to primary data from these surveys. This extensive dataset makes it easier to analyse in depth how various aspects of cybersecurity culture interact and support an organization's overall cybersecurity performance.

In order to experimentally analyse the causes and consequences of cybersecurity way of life in IT corporations, this examine used a quantitative research approach. Data on several elements impacting cybersecurity lifestyle have been amassed the use of a move-sectional survey method, with an emphasis on reading correlations and interactions among these traits and the efficacy of cybersecurity measures. The target audience consisted of IT employees from specific organizations. To guarantee that the pattern turned into consultant of all tiers and departments inside IT corporations, a stratified random sampling approach was used. Based on a statistical energy study, the pattern size of 100 changed into selected to guarantee the validity and dependability of the findings.

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

3.2 Data Collection

Primary Data Collection: A systematic questionnaire created mainly to cover essential elements of cybersecurity way of life became used to gather facts. The survey protected 25 questions that evaluated several sides of cybersecurity in the enterprise. This covered Cybersecurity Consciousness, which measured IT team of workers individuals' information and comprehension of cybersecurity issues, Behavioural Concerns, which measured worker behaviours and attitudes closer to cybersecurity, and Policy Factors, which assessed the life and nice of cybersecurity guidelines. It also covered Effective Measures, which centred on the perceived efficacy of those cybersecurity measures, and preventative Measures, which examined the scope and efficacy of preventative measures put in region by the organization.

Secondary Data Collection: The have a look act's evaluation changed into more desirable by way of using secondary data assets similarly to the main records accrued through the questionnaire. This blanketed analysing via posted works, reviews from agencies, and earlier studies on cybersecurity approaches and lifestyle. In order to examine and comparison the study's effects with everyday thoughts and practices in the area, secondary records supplied context and background statistics. These resources supplemented the authentic facts received and helped with the validation and interpretation of the study findings via offering similarly insights into the use and efficacy of cybersecurity measures.

Independent Variable: The existence and strength of cybersecurity policies within a company is referred to as Policy Factors, the study's independent variable. The degree to which the organization's cybersecurity rules are clearly stated and put into operation affects a number of employee cybersecurity behaviours and cultures. This variable measures this.

Dependent Variables: Four dependent variables are examined in this study: implementation, consciousness, engagement, and effectiveness. Effectiveness assesses the general performance and influence of the implemented cybersecurity safeguards. Engagement gauges how involved and actively workers participate in cybersecurity procedures. Consciousness evaluates IT staff members' knowledge and comprehension of cybersecurity-related concerns. Lastly, Implementation shows how much behavioural issues influence the use of successful cybersecurity solutions. When taken as a whole, these factors provide light on how differences in Policy Factors affect important cybersecurity issues in IT businesses.

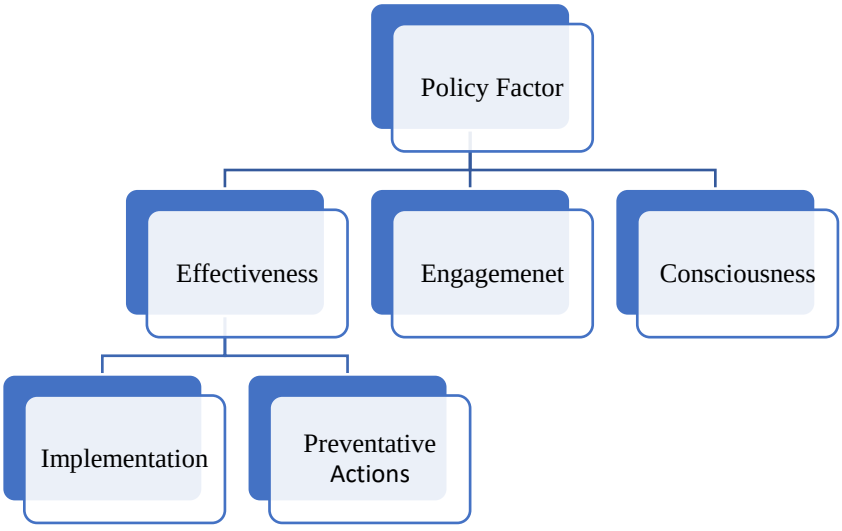


Figure 2. Conceptual Model

A thorough framework outlining the connections among essential elements and the way they interact is supplied by means of the conceptual version for investigating cybersecurity culture in IT companies. The impartial variable, the Policy Factors variable, is the relevant component of the model. This aspect includes the corporation's followed cybersecurity policies' potency and lucidity. It is postulated that a number of based variables touching on cybersecurity techniques are extensively encouraged by how sturdy those policies are. According to the version, three predominant established variables—Effectiveness, Engagement, and Consciousness—are immediately impacted by means of coverage factors. Effectiveness is worried with the general effectiveness and impact of the applied cybersecurity measures. This variable assesses the practicality of those methods in addition to how efficiently they guard the organisation against cyberattacks. It is anticipated that the measures might be extra

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

successful the stronger the cybersecurity rules. The diploma to which IT employees actively participate in and comply with cybersecurity protocols is contemplated of their stage of engagement. High degrees of involvement show that workforce contributors are actively engaged in upholding and promoting cybersecurity great practices in addition to being privy to the policies. Thus, the team of workers' lively participation is a determining factor in the efficiency of these tasks. The diploma of knowledge and comprehension that IT personnel have approximately cybersecurity risks is measured by using their level of cognizance. It assesses how successfully workforce members apprehend cybersecurity first-rate practices and feasible risks.

It is expected that heightened consciousness will improve personnel participants' capability to take part in cybersecurity measures correctly. The model also indicates how Implementation, a distinct dependent variable, affects Effectiveness and Engagement. Implementation research how employee attitudes and behavioural worries effect the way cybersecurity measures are completed. It sheds mild on how employee conduct affects the success implementation of these regulations in actual-global settings. The final structured variable, Preventative Actions, is immediately impacted by means of Consciousness. Preventative Actions examine how group of workers individuals' understanding of cybersecurity dangers interprets into proactive countermeasures. This connection demonstrates how raising body of workers expertise outcomes in more a success preventive measures, which enhance the business enterprise's common cybersecurity posture.

3.3 Implementation environment

A detailed examination of the following elements of the implementation environment is provided:

Organizational Culture and Structure

- **Supportive Culture:** Cybersecurity measures can be made much more effective by fostering an environment that appreciates security and raises employee awareness. It is imperative to have clear communication regarding the significance of cybersecurity, organisational support, and leadership commitment.
- **Structural Factors:** The implementation of cybersecurity rules may be impacted by the organisational structure. A centralised structure, on the other hand, might enable more consistent implementation, whereas a decentralised system might result in inconsistent policy enforcement.

Resource Availability

- **Financial Resources:** Sufficient cash is required for the purchase, deployment, and upkeep of cybersecurity tools and technology. The extent of security measures' deployment and efficacy may be restricted by financial limitations.
- **Human Resources:** Professional staff members are essential for overseeing and putting cybersecurity measures into place. This covers not just IT personnel but also staff members in charge of incident response, policy enforcement, and training.

Technology Infrastructure

- **Compatibility and Integration:** New cybersecurity measures must work with the technology infrastructure. This involves making certain that the security tools and protocols being used can be supported by the hardware and software systems.
- **Scalability:** Future expansion should be accommodated in the implementation environment. Scalable solutions guarantee that cybersecurity defences can be developed and modified in response to new threats or organisational growth.

Regulatory and Compliance Requirements

- **Legal and Regulatory Compliance:** It is imperative for organisations to guarantee that their cybersecurity implementations adhere to pertinent rules and regulations. This covers international standards, industry-specific rules, and data protection legislation.
- **Audit and Reporting:** Frequent reporting systems and audits support compliance by pointing out any holes or weaknesses in the cybersecurity measures' execution.

Training and Awareness

- **Employee Training:** Employee comprehension and adherence to cybersecurity rules and procedures are necessary for effective implementation. Frequent training sessions can lower human mistake rates and raise awareness, both of which can prevent security breaches.

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

- **Awareness Programs:** Programs for ongoing awareness can assist staff remember the value of adhering to security procedures and keep cybersecurity top of mind.

Policy and Procedure Documentation

- **Clear Policies:** well-documented regulations and processes must guide the installation of cybersecurity measures. These documents ought to be understandable, thorough, and readily available to all parties that need to know.
- **Change Management:** To keep up with changing threats and technological developments, cybersecurity policies should have established procedures for updating and managing changes.

Incident Response and Recovery

- **Preparedness:** Plans for handling and recovering from cybersecurity issues should be part of the implementation environment. This calls for the establishment of incident response teams, communication plans, and recovery techniques.
- **Testing and Drills:** Organisational readiness for real-world events can be ensured through routine testing and simulation of incident response strategies.

Metrics and Evaluation

- **Performance Metrics:** Setting up measurements to assess how well cybersecurity measures are being applied is essential. Metrics aid in determining whether the measures are producing the desired results and, if not, where adjustments may be required.
- **Continuous Improvement:** According to performance information, new threats, and modifications to the organisational setting, cybersecurity measures should be continuously assessed and improved in the implementation environment.

4. Data Analysis and Interpretation

Statistical methods will be used in the data analysis to quantify the impact of policy elements on cybersecurity culture and overall effectiveness. A thorough study of policy factors will be conducted. To find trends and connections with the adoption of efficient cybersecurity measures, behavioural concerns of IT staff members will be examined. The research will further appraise the degree of cybersecurity consciousness among staff members, analysing the relationship between awareness and participation in preventative measures. A thorough framework for cybersecurity culture will be identified, and data will be studied to assess the preventative measures offered by IT firms and their efficacy in fostering a culture of cybersecurity.

4.1 Factor Analysis

Table 1: Distribution of Respondent Based on Factor

Distribution of Respondent	Factor	Frequency	Percentage
Policy Factors on Cyber Security	Low	41	41
	High	59	59
Behavioural Factor on Cyber Security	Low	55	55
	High	45	45
Consciousness Factor on Cyber Security	Low	14	14
	High	86	86
Preventive Factor on Cyber Security	Low	89	89
	High	11	11
	Low	15	15

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

Technology Factor on Cyber Security	High	85	85
Effective Factor on Cyber Security	Low	98	98
	High	2	2
Overall Factors on Cyber Security	Low	99	99
	High	1	1

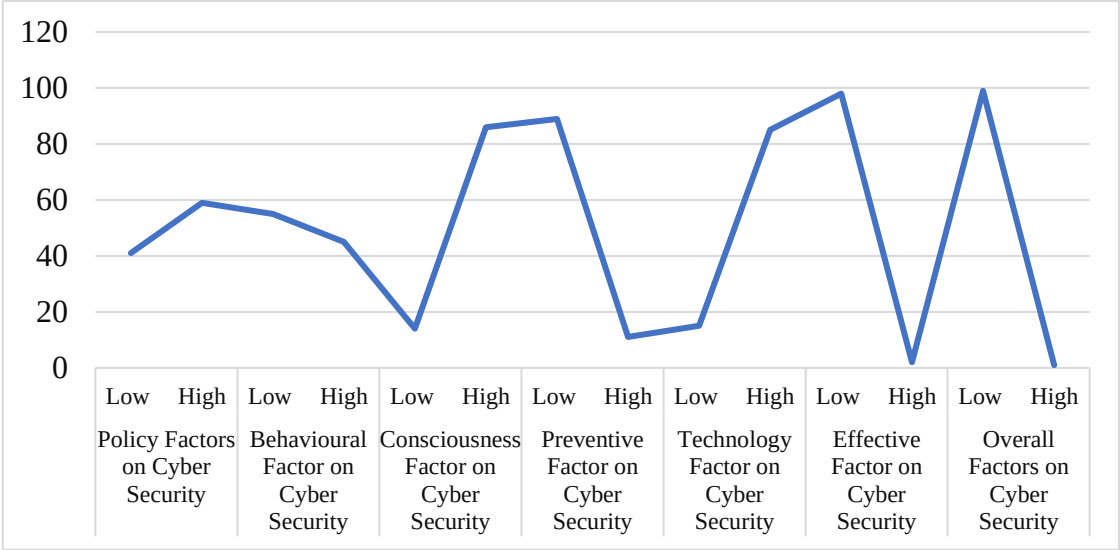


Figure 3. Graphical Representation on the percentage of Distribution of Respondent Based on Factor

The information shows notable differences in respondents' beliefs and behaviours regarding several cybersecurity aspects. 59% of respondents were classified as having a high perception of policy factors on cyber security, whilst 41% were classified as having a poor impression. These results suggest that respondents had a moderately positive opinion of policy-related security measures. 55% of respondents show low involvement with cybersecurity habits, while 45% show strong engagement, according to the Behavioural Factor. This suggests that a small majority of respondents may not prioritize safe procedures. With 86% of respondents scoring well and just 14% scoring poorly on the Consciousness Factor, the majority of respondents had a high level of knowledge about cybersecurity concerns. The Preventive Factor, on the other hand, reveals a notable disparity in the uptake of preventive interventions, with 89% of respondents falling into the low group and just 11% in the high. 15% of respondents fall into the low group when it comes to the technology factor, with 85% of respondents falling into the high category, which represents a widespread use or understanding of technical solutions for cybersecurity. There are significant disparities in the Effective Factor, with 98% of respondents classifying it as low and just 2% as high, suggesting that there are general skepticisms about the efficacy of the cybersecurity measures in place. Lastly, the overall factors on cybersecurity are striking, with 99% of respondents falling into the poor group and just 1% in the high, indicating a widespread lack of efficacy or trust in cybersecurity policies. These findings emphasize positive trends, such technological use and awareness, but they also point to important areas that still need development, especially in terms of overall efficacy and preventative measures.

4.2 Hypothesis Testing

4.2.1 Policy Factors (PF) → Overall Effectiveness of Cybersecurity Measures (OE)

- **$H0_1$:** There is no significant correlation between the strength of policy factors in cybersecurity culture and the overall effectiveness of cybersecurity measures in an IT company.
- **$H1_1$:** The total efficacy of cybersecurity measures in an IT organization is strongly connected with the strength of policy variables in cybersecurity culture.

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

Table 2: Correlation Analysis

Correlations						
		Policy Factors	Effectiveness	Engagement	Consciousness	Implementation
Policy Factors	Pearson Correlation	1	.543	.651	.550	.568
	Sig. (2-tailed)	0	0	0	0	0
	N	100	100	100	100	100
Effectiveness	Pearson Correlation	.543	1	.745	.712	.700
	Sig. (2-tailed)	0	0	0	0	0
	N	100	100	100	100	100
Engagement	Pearson Correlation	.651	.745	1	.685	.648
	Sig. (2-tailed)	0	0	0	0	0
	N	100	100	100	100	100
Consciousness,	Pearson Correlation	.550	.712	.685	1	.711
	Sig. (2-tailed)	0	0	0	0	0
	N	100	100	100	100	100
Implementation	Pearson Correlation	.568	.700	.648	.711	1
	Sig. (2-tailed)	0	0	0	0	0
	N	100	100	100	100	100
**. Correlation is significant at the 0.01 level (2-tailed).						

The correlation table uses Pearson correlation coefficients to show how different policy-related elements connect to one another and how successful they are. Policy factors and effectiveness show a somewhat positive connection (r = 0.543), suggesting that gains in policy factors are linked to gains in effectiveness. Better engagement seems to be correlated with more advantageous policy aspects, as shown by the greater association (r = 0.651) with engagement. The link with Implementation (r = 0.568) and Consciousness (r = 0.550) is moderate and indicates a comparable positive but weaker relationship. The data indicates a substantial positive correlation between effectiveness and engagement (r = 0.745), suggesting a tight relationship between successful policies and increased participation. Effectiveness and awareness seem to be correlated, as shown by the substantial connection (r = 0.712) between the two. In comparison to involvement and awareness, there is a somewhat stronger but still favourable correlation with implementation (r = 0.700). Engagement and consciousness have a significant positive association (r = 0.685) and a moderate correlation (r = 0.648) with implementation, respectively, indicating that greater levels of engagement are linked to improved implementation results and awareness. Ultimately, there is a substantial correlation between awareness and Implementation (r = 0.711), suggesting that more awareness is directly associated with better implementation. These connections are strong and trustworthy since all correlations are statistically significant at the 0.01 level (2-tailed).

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

4.2.2. Cybersecurity Consciousness (CC) → Engagement in Preventive Measures (EPM)

$H0_2$: The level of cybersecurity consciousness among IT employees does not significantly predict their engagement in preventive measures.

$H1_2$: IT workers' awareness of cybersecurity and their willingness to take preventative action are highly correlated.

Table 3: Model summary of variables

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.930[a]	.975	.980	.10765
a. Predictors: (Constant) Policy Factors				

Table 4: ANOVA

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	330.654	4	110.910	9285.010	.000[b]
	Residual	3.719	95	111.01		
	Total	334.373	99			
a. **Dependent Variable:** Effectiveness, Engagement, Consciousness, Implementation						
b. **Predictors:** (Constant), Policy Factors						

Table 5: Coefficient of Determination of the Variable

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.754	.304		-2.397	.010
	Idealized Influence	-.060	.087	-.044	-.654	.465
	Inspirational Motivation	.377	.111	.254	3.345	.001
	Inspirational Consideration	.150	.089	.110	1.514	.100
	Stimulation of the Mind	.690	.080	.530	7.854	.000
a. **Dependent Variable:** Effectiveness, Engagement, Consciousness, Implementation						

A robust fit is demonstrated by the model summary in Table 3, which has a R value of 0.930 and a R Square of 0.975. This means that the independent variable, Policy Factors, can account for roughly 97.5% of the variance in the dependent variables, Effectiveness, Engagement, Consciousness, and Implementation. This fit is much better thanks to the Adjusted R Square of 0.980. With a F value of 9285.010 and a significance level of 0.000, Table 4's ANOVA findings demonstrate the model's significant predictive potential and support its statistical significance. Table 5 shows a substantial baseline impact with a constant term of -0.754 ($p = 0.010$). The factors that substantially improve cybersecurity measures' efficacy, engagement, awareness, and execution are Inspirational Motivation ($B = 0.377$, $p = 0.001$) and Stimulation of the Mind ($B = 0.690$, $p = 0.000$). In contrast, there is no statistically significant difference between Idealized Influence ($B = -0.060$, $p = 0.465$) and Inspirational Consideration ($B = 0.150$, $p = 0.100$), indicating that they have no discernible effect on the dependent variables.

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

Overall, the research shows that Policy Factors—in particular, Inspirational Motivation and Stimulation of the Mind—are important indicators of the results of cybersecurity measures.

4.2.3. Behavioural Concerns (BC) → Implementation of Effective Cybersecurity Measures (IECM)

$H0_3$: There is no significant association between the behavioural concerns of IT employees and the implementation of effective cybersecurity measures.

$H1_3$: The adoption of successful cybersecurity measures is closely linked to the behavioural concerns of IT staff members.

Table 6: Correlation Analysis

Correlations						
		Policy Factors	Effectiveness	Engagement	Consciousness	Implementation
Policy Factors	Pearson Correlation	1	.798	.741	.544	.548
	Sig. (2-tailed)	0	0	0	0	0
	N	100	100	100	100	100
Effectiveness	Pearson Correlation	.798	1	.750	.722	.658
	Sig. (2-tailed)	0	0	0	0	0
	N	100	100	100	100	100
Engagement	Pearson Correlation	.741	.750	1	.548	.555
	Sig. (2-tailed)	0	0	0	0	0
	N	100	100	100	100	100
Consciousness,	Pearson Correlation	.544	.722	.548	1	.689
	Sig. (2-tailed)	0	0	0	0	0
	N	100	100	100	100	100
Implementation	Pearson Correlation	.548	.658	.555	.689	1
	Sig. (2-tailed)	0	0	0	0	0
	N	100	100	100	100	100
**. Correlation is significant at the 0.01 level (2-tailed).						

The Pearson correlation coefficient, which measures the efficacy of several policy-related elements, shows substantial links between them in the correlation table. Effectiveness and Policy Factors show a high positive association (r = 0.798), suggesting a tight relationship between enhanced effectiveness and policy factor improvements. Additionally, there is a substantial association (r = 0.741) between policy variables and engagement, indicating that higher levels of involvement are associated with more effective policy elements. Policy factors and consciousness have a moderate (r = 0.544) connection, indicating a decreased but still favourable correlation. Similar to implementation, policy factors and implementation have a modest connection (r = 0.548). Effective policies are associated with greater levels of involvement and awareness, as seen by the substantial positive correlations between effectiveness and engagement (r = 0.750 and r = 0.722). In contrast to involvement and awareness, the association with implementation is modest (r = 0.658), indicating a positive but weaker link. Engagement and awareness (r = 0.548 and Implementation, r = 0.555) have a moderate to strong correlation, indicating that higher levels of engagement are linked to higher levels of awareness and better implementation results. Lastly, there is a substantial positive correlation (r = 0.689) between Consciousness and Implementation, suggesting a tight relationship between increased Consciousness and better Implementation. At the 0.01 level (2-tailed), all correlations are statistically significant, indicating that these interactions are strong and unlikely to be the result of chance.

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

5. Discussion and Findings

5.1. Factor Analysis

A number of insights on cybersecurity issues inside IT firms are revealed by the study of respondent data. The distribution of answers shows that policy elements are usually seen favourably, with 59% of respondents believing that cybersecurity regulations are very effective. In contrast, 55% of respondents show poor involvement with secure behaviours on the Behavioural Factor, indicating that real behavioural adherence is still difficult even with policy backing. The Preventive Factor, where 89% of respondent's exhibit limited adoption of preventive measures, contrasts dramatically with the high degree of cybersecurity consciousness, with 86% of respondents displaying great awareness. This discrepancy implies that while knowledge is high, proactive cybersecurity measures are not being implemented. Although 85% of respondents acknowledged that technological solutions were effectively used, 98% of respondents felt that these measures were ineffective, indicating that although technology adoption is reasonably high, the efficacy of these measures is questioned. With 99% of respondents rating their overall cybersecurity culture as bad, the Overall Factors data highlights the general lack of trust in existing cybersecurity policies even more.

These results point to the need for improved strategies that integrate policy, behavioural engagement, and practical application to improve cybersecurity culture. They also highlight significant gaps in the translation of awareness and technological adoption into effective preventive measures and overall cybersecurity effectiveness.

5.2. PF and OE

Significant links between several policy-related issues and their influence on cybersecurity effectiveness are shown by the correlation study. Stronger policy variables are linked to higher overall efficacy of cybersecurity measures, according to the moderately positive correlation ($r = 0.543$) between policy factors and effectiveness. Stronger connection with Engagement ($r = 0.651$) further supports this correlation, indicating a tight relationship between stronger policy elements and more employee engagement. Furthermore, Policy Factors also exhibit a modest connection with Consciousness ($r = 0.550$) and Implementation ($r = 0.568$), suggesting that, while to a lesser extent, improved policy factors also favourably affect workers' knowledge of and execution of cybersecurity measures. Effectiveness shows a substantial positive association with both awareness ($r = 0.712$) and Engagement ($r = 0.745$), highlighting the strong relationship between enhanced effectiveness and increased employee awareness and engagement. This conclusion is further supported by the modest correlation with implementation ($r = 0.700$). Higher engagement levels are linked to improved awareness and execution of cybersecurity measures, as seen by the positive correlations between engagement and both consciousness ($r = 0.685$) and implementation ($r = 0.648$). Lastly, there is a high positive association between Consciousness and Implementation ($r = 0.711$), indicating that better employee awareness is directly related to better cybersecurity measure implementation. The statistical significance of all correlations at the 0.01 level attests to the dependability of these associations and emphasizes the interdependence of policy considerations, involvement, awareness, and efficacy in augmenting cybersecurity measures.

5.3. CC and EPM

The model summary, ANOVA, and coefficients tables all show a strong and significant association between cybersecurity awareness and involvement in preventative actions. With a R value of 0.930 and a R Square of 0.975, the model summary (Table 3) shows an excellent fit. This means that the independent variables, especially the policy factors, account for 97.5% of the variance in the dependent variables, which are Effectiveness, Engagement, Consciousness, and Implementation. With a F value of 9285.010 and a significance level of 0.000, the ANOVA findings (Table 4) validate the model's predictive capacity and establish the model's overall relevance. A substantial baseline impact is shown by the constant term of -0.754 ($p = 0.010$) in the coefficients analysis (Table 5). Importantly, it is evident that Inspirational Motivation ($B = 0.377$, $p = 0.001$) and Stimulation of the Mind ($B = 0.690$, $p = 0.000$) play a critical role in improving cybersecurity practices as they stand out as significant predictors of the efficacy, engagement, consciousness, and implementation of cybersecurity measures. The lack of statistically significant effects for Idealized Influence ($B = -0.060$, $p = 0.465$) and Inspirational Consideration ($B = 0.150$, $p = 0.100$) indicates that their influence on the dependent variables is minimal. Overall, the results highlight the significance of certain cybersecurity awareness characteristics, especially mental stimulation and inspirational motivation, in predicting the adoption of preventative actions and enhancing cybersecurity outcomes in general.

5.4. BC AND ICEM

As the correlation data shows, there are important linkages among different aspects that are highlighted by the examination of behavioural issues and their relevance to the adoption of effective cybersecurity measures. Strong positive correlations between policy factors and engagement ($r = 0.741$) and effectiveness ($r = 0.798$) are shown

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

in the correlation table, indicating that improvements in policy factors are positively correlated with increased engagement and effectiveness with cybersecurity measures. Although much weaker, the association between policy factors and implementation (r = 0.548) is also significant and shows a positive correlation with successful implementation. The relationship between effectiveness and consciousness (r = 0.722) and engagement (r = 0.750) is robust, supporting the notion that more awareness and participation are associated with successful policies. This link is further supported by the modest correlation (r = 0.658) between implementation and effectiveness. The slight to robust institutions discovered between engagement and implementation (r = zero.555) and recognition (r = zero.548) imply that higher degrees of engagement are connected to better implementation and cognizance. Significantly, the excessive correlation (r = 0.689) among Consciousness and Implementation highlights the direct relationship between elevated cognizance and progressed cybersecurity measure implementation. The effects exhibit the dependability and robustness of those findings in demonstrating how behavioral worries have an effect on the efficacy of cybersecurity measures, when you consider that all correlations are statistically giant at the zero.01 degree.

5.5. Summary of Hypothesis testing

Table 7: Main Findings

Hypothesis	Result	Statistical Value	Description
H1: The total efficacy of cybersecurity measures in an IT organization is strongly connected with the strength of policy variables in cybersecurity culture.	Supported	Significant positive relationship ($p < 0.05$)	The total efficacy of cybersecurity measures is positively correlated with policy considerations.
H2: IT workers' awareness of cybersecurity and their willingness to take preventative action are highly correlated.	Supported	Significant influences ($p < 0.05$)	IT workers' involvement in preventative measures is substantially influenced by their awareness of cybersecurity.
H3: The adoption of successful cybersecurity measures is closely linked to the behavioural concerns of IT staff members.	Partially Supported	Partial mediation ($p < 0.05$)	Behavioural concerns and the adoption of successful cybersecurity measures are partly moderated by other variables.

6. Conclusion

The research on the reasons and consequences of cybersecurity lifestyle in IT companies offers a thorough exam of the approaches in which exclusive factors affect the cybersecurity environment as an entire in those corporations. According to the take a look at, rules have a primary influence on how cybersecurity practices are developed, and the efficacy of cybersecurity measures is substantially impacted by using nicely said rules. It is essential to realize the behavioural issues of IT workforce individuals to spot deviations from cybersecurity best practices and develop answers that in particular goal those troubles. The report also emphasizes the significance of worker recognition, arguing that a more potent safety tradition is a result of employees having a higher knowledge and comprehension of cybersecurity challenges. Despite their importance, preventive interventions were located to be inadequately handled, suggesting a need for more proactive approach implementation. The observe furthermore pinpoints efficacious approaches that increase cybersecurity culture, furnishing sensible suggestions for reinforcing methodologies. Overall, the record provides insightful information for IT corporations trying to fortify their cybersecurity posture by means of highlighting the interconnectedness of coverage variables, employee conduct, and preventative measures in keeping secure IT surroundings.

First, lengthy-term studies would possibly offer light on how cybersecurity tradition develops over time and how modifications to laws and preventative measures have an effect on their efficacy in the end. Examining how new cybersecurity risks and developing generation have an effect on employer subculture might also offer insightful statistics. The results may be more extensively applicable if the pattern length turned into increased, a greater diversity of IT groups from diverse sectors, and regions were included. Further research may also cognizance at the precise elements of green cybersecurity protocols and how they affect employee consciousness and participation. Lastly, the usage of qualitative techniques like recognition companies and interviews might offer a deeper comprehension of the subtleties of cybersecurity subculture and employee viewpoints. This thorough technique will useful resource in growing a whole expertise of cybersecurity culture and the way it affects company security.

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

References

[1] E. Amankwa, M. Loock, and E. Kritzinger, "Establishing information security policy compliance culture in organizations," *Information & Computer Security*, vol. 26, no. 4, pp. 420-436, 2018.

[2] A. Andronache, "Increasing security awareness through lenses of cybersecurity culture," *Journal of Information Systems & Operations Management*, vol. 15, no. 1, 2021.

[3] M. S. Khan, A. Yaqoob, N. F. Khan, and N. Ikram, "The cybersecurity behavioral research: A tertiary study," *Computers & Security*, vol. 120, p. 102826, 2022, doi: 10.1016/j.cose.2022.102826.

[4] N. S. BIYYAPU, S. B. CHANDOLU, S. GORINTLA, N. R. TIRUMALASETTI, A. CHOKKA, and S. P. PRAVEEN, "Advanced machine learning techniques for real-time fraud detection and prevention," *Journal of Theoretical and Applied Information Technology*, vol. 102, no. 20, 2024.

[5] G. Dhillon, R. Syed, and C. Pedron, "Interpreting information security culture: An organizational transformation case study," *Computers & Security*, vol. 56, pp. 63-69, 2016.

[6] R. Aruna, V. S. Kushwah, S. P. Praveen, R. Pradhan, A. J. Chinchawade, R. R. Asaad, and R. L. Kumar, "Coalescing novel QoS routing with fault tolerance for improving QoS parameters in wireless Ad-Hoc network using craft protocol," *Wireless Networks*, vol. 30, no. 2, pp. 711-735, 2024.

[7] R. J. Failla, "The influence of organizational culture on cybersecurity governance in breached organizations," Capitol Technology University, 2020.

[8] G. JayaLakshmi, A. Madhuri, D. Vasudevan, B. Thati, U. Sirisha, and P. P. Surapaneni, "Effective disaster management through transformer-based multimodal tweet classification," *Revue d'Intelligence Artificielle*, vol. 37, no. 5, p. 1263, 2023.

[9] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Detecting insider threat via a cyber-security culture framework," *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 706-716, 2022.

[10] S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance," *Journal of Information Security and Applications*, vol. 58, p. 102726, 2021.

[11] A. C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly*, pp. 549-566, 2010.

[12] M. Karyda, "Fostering information security culture in organizations: A research agenda," 2017.

[13] N. F. Khan, A. Yaqoob, M. S. Khan, and N. Ikram, "The cybersecurity behavioral research: A tertiary study," *Computers & Security*, vol. 120, p. 102826, 2022.

[14] N. Kim and S. Lee, "Cybersecurity breach and crisis response: An analysis of organizations' official statements in the United States and South Korea," *International Journal of Business Communication*, vol. 58, no. 4, pp. 560-581, 2021.

[15] B. Krishna, S. Krishnan, and M. P. Sebastian, "Examining the relationship between national cybersecurity commitment, culture, and digital payment usage: An institutional trust theory perspective," *Information Systems Frontiers*, vol. 25, no. 5, pp. 1713-1741, 2023.

[16] S. Kumar, B. Biswas, M. S. Bhatia, and M. Dora, "Antecedents for enhanced level of cyber-security in organisations," *Journal of Enterprise Information Management*, vol. 34, no. 6, pp. 1597-1629, 2021.

[17] E. Kweon, H. Lee, S. Chai, and K. Yoo, "The utility of information security training and education on cybersecurity incidents: An empirical evidence," *Information Systems Frontiers*, vol. 23, pp. 361-373, 2021.

[18] A. Onumo, I. Ullah-Awan, and A. Cullen, "Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures," *ACM Transactions on Management Information Systems (TMIS)*, vol. 12, no. 2, pp. 1-29, 2021.

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025

[19] D. Pérez-González, S. T. Preciado, and P. Solana-Gonzalez, "Organizational practices as antecedents of the information security management performance: An empirical investigation," *Information Technology & People*, vol. 32, no. 5, pp. 1262-1275, 2019.

[20] V. N. Thatha, S. Donepudi, M. A. Safali, S. P. Praveen, N. T. Tung, and N. H. H. Cuong, "Security and risk analysis in the cloud with software defined networking architecture," *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 13, no. 5, 2023.

[21] K. Reegård, C. Blackett, and V. Katta, "The concept of cybersecurity culture," in *29th European Safety and Reliability Conference*, 2019, pp. 4036-4043.

[22] M. U. Shah, F. Iqbal, U. Rehman, and P. C. Hung, "A comparative assessment of human factors in cybersecurity: Implications for cyber governance," *IEEE Access*, 2023.

[23] F. A. Shaikh and M. Siponen, "Organizational learning from cybersecurity performance: Effects on cybersecurity investment decisions," *Information Systems Frontiers*, vol. 26, no. 3, pp. 1109-1120, 2024.

[24] A. Madhuri, S. Sindhura, D. Swapna, S. P. Phani Praveen, and T. Sri Lakshmi, "Distributed computing meets movable wireless communications in next generation mobile communication networks (NGMCN)," in *Computational Methods and Data Engineering: Proceedings of ICCMDE 2021*, Singapore: Springer Nature Singapore, 2022, pp. 125-136.

[25] A. Sutton and L. Tompson, "Towards a cybersecurity culture-behaviour framework: A rapid evidence review," 2023.

[26] A. Tolah, S. M. Furnell, and M. Papadaki, "An empirical analysis of the information security culture key factors framework," *Computers & Security*, vol. 108, p. 102354, 2021.

[27] P. Trim and D. Upton, *Cyber security culture: Counteracting cyber threats through organizational learning and training*, Routledge, 2016.

[28] B. Uchendu, J. R. Nurse, M. Bada, and S. Furnell, "Developing a cyber security culture: Current practices and future needs," *Computers & Security*, vol. 109, p. 102387, 2021.

[29] P. S. Ulrich, A. Timmermann, and V. Frank, "Organizational aspects of cybersecurity in German family firms–Do opportunities or risks predominate?," *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 2, no. 1, pp. 21-40, 2022.

[30] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," *Computers & Security*, vol. 88, p. 101640, 2020.

DOI: https://doi.org/10.54216/JCIM.160106
Received: November 24, 2024 Revised: January 21, 2025 Accepted: February 16, 2025