The Human Element in Cyber Security: Managing Risk and Cultivating a Science-Based Security Culture

Destiny Young[1*], Osinachi Ozocheta[2]

[1]Oil and Gas Free Zones Authority, Onne, Rivers State, Nigeria

[2]IT Manager, Stowe School, Buckingham, United Kingdom

***Corresponding Author**

DOI: https://doi.org/10.51244/IJRSI.2025.12110070

Received: 01 December 2025; Accepted: 07 December 2025; Published: 09 December 2025

ABSTRACT

The modern digital enterprise faces an escalating cybersecurity challenge, with recent analyses indicating that seventy four percent of breaches originate from human factors such as error, negligence, or insider activity. This pattern confirms the limitations of traditional awareness training models that focus mainly on information delivery rather than scientifically measurable behavioural change. Building on contemporary human risk research and recent findings that demonstrate a persistent intention behaviour gap, this study argues that human fallibility must be addressed through both cultural and technical controls. Drawing on NIST SP 800 50 and advanced Human Risk Management frameworks, the paper promotes a life cycle approach to awareness, training, and cultural assessment that measures security culture across seven validated dimensions, providing a more meaningful alternative to superficial compliance metrics. To compensate for unavoidable human error, the framework adopts Zero Trust architecture as the foundational technical safeguard, supported by Just in Time access and automated cloud configuration enforcement as recommended in NIST SP 800 207. These controls eliminate standing privileges and reduce the attack surface created by risky human behaviour. The study synthesises programme structure, empirical evidence, and technical design into an integrated framework that public sector and resource constrained organisations can adopt to achieve verifiable and sustainable reductions in human centred security risk. Future research should empirically test this integrated model by measuring changes in observed security behaviour and incident rates after Zero Trust implementation and workload informed intervention.

Keyword: Human Risk Management, Security Culture, Zero Trust, Phishing Behaviour, Workload Compliance, JIT Access

INTRODUCTION

Background to the Study

The modern digital enterprise operates within a context of persistent and sophisticated cyber threats, where the protection of confidentiality, integrity, and availability of information is paramount. Despite significant investment in advanced security technology, audit reports, periodicals, and conference presentations consistently identify **people as one of the weakest links** in securing systems and networks (Cano, 2019) Securing organisational assets is understood to be as much a human issue as it is a technology issue (Wilson & Hash, 2003). Empirical studies underline this vulnerability, attributing **up to 95% of all cyber security breaches** to some human factor, such as unintentional actions or lack of action by users (Sjouwerman, 2025; usecure, n.d.).

Government and industry bodies recognise the necessity of addressing this "people factor" through structured programmes. The Federal Information Security Management Act (FISMA) of 2002 tasks agency heads with ensuring sufficient trained personnel to comply with security requirements (Wilson & Hash, 2003). The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-50, though now withdrawn (National Institute of Standards and Technology [NIST], 2023) and superseded (Wilson & Hash, 2003), provided comprehensive guidance for building and maintaining an Information Technology (IT) security awareness and training programme (Wilson & Hash, 2003).

In contemporary environments, this challenge is amplified by increasing reliance on cloud services and the emergence of advanced social engineering tactics, which compel a focus shift from perimeter defence to internal Human Risk Management (HRM) and Zero Trust architecture (Humanize, 2023; Sjouwerman, 2025). Understanding the subtle distinction between unintentional negligence (risk) and intentional maliciousness (threat) is vital for developing effective, adaptive security strategies (Teramind, 2024).

Problem Statement

While technological advancements offer strong external defence mechanisms, the biggest threat to security often arises from **internal activities**, predominantly stemming from insider activity, including negligence and honest mistakes (Teramind, 2024). Cloud infrastructure misconfiguration, which is entirely preventable, stands as the biggest security threat to enterprise cloud security, frequently resulting from **human error** (HubSpot, n.d.). The 2018 IBM X-Force Report noted a 424% increase in data breaches resulting from cloud misconfiguration caused by human error (HubSpot, n.d.).

Traditional security awareness training (SAT), focused primarily on knowledge transfer, often fails to translate cognitive awareness into sustained behavioural compliance (Sjouwerman, 2025). Crucially, research investigating phishing susceptibility found a significant **gap between an employee's intention to comply and their actual clicking behaviour** (noncompliance) (Jalali et al., 2020). This gap is exacerbated by high **workload**, which significantly increases the likelihood of employees clicking on malicious links, demonstrating that organisational stress factors can override positive security intentions (Jalali et al., 2020).

Therefore, the central problem addressed here is the difficulty faced by organisations in moving beyond superficial security compliance (**vanity metrics**) to achieving verifiable, robust security culture and operational resilience in environments prone to human error, negligence, and workload pressures (Roer & Petrič, 2018).

Research Objectives

The objectives of this research synthesis are to:

1. **Define and differentiate** the foundational concepts of human error, insider risk, and insider threat in the context of IT security (Teramind, 2024).
2. **Synthesise** the foundational programmatic requirements for mitigating human risk using the life-cycle model detailed in NIST SP 800-50 (Wilson & Hash, 2003).
3. **Examine** advanced strategies, such as Human Risk Management (HRM) and the scientific measurement of security culture, necessary to transcend reliance on simple metrics and address the root causes of behavioural failures (Roer & Petrič, 2018).
4. **Detail and contextualise** modern technical mitigation controls, specifically the Zero Trust security model, Just-in-Time (JIT) access, and automated cloud misconfiguration enforcement, as mechanisms to compensate for human fallibility (HubSpot, n.d.).
5. **Evaluate** the empirical evidence regarding the relationship between cognitive security intention, organisational stress factors (workload), and actual security compliance behaviour (Jalali et al., 2020).

Research Questions

This study seeks to answer the following research questions:

1. What are the key components of an effective life-cycle programme for IT security awareness and training, as prescribed by NIST guidance?
2. How does the adoption of advanced Human Risk Management, defined by the seven scientific dimensions of security culture, improve risk mitigation beyond traditional security awareness methods?

3. To what extent do organisational environmental factors, such as high employee workload, override positive intentions toward compliance with information security policies?
4. How do the principles of Zero Trust security and Just-in-Time access function as core technological controls to mitigate the inherent vulnerabilities associated with standing privileges and human error?

Significance of the Study

This synthesis is significant for several reasons:

- **Policy and Compliance:** It guides federal agencies and other organisations on meeting statutory requirements (e.g., FISMA) by structuring their security awareness and training efforts according to the recognised life-cycle approach (Design, Development, Implementation, Post-Implementation) defined by NIST (Wilson & Hash, 2003).
- **Risk Reduction:** By providing clear distinctions between insider risk (negligence) and insider threat (malice), it allows organisations to allocate resources appropriately for prevention, mitigation, and response (Teramind, 2024).
- **Strategic Investment:** It highlights the necessity of shifting investment from superficial metrics (the **McNamara Fallacy**) to scientifically measurable security culture, enabling Chief Information Security Officers (CISOs) to justify security spending based on measurable reductions in risk factors (Roer & Petrič, 2018).
- **Operational Resilience:** It emphasises the critical link between workload management and security compliance, offering a practical insight that managing employee working environments is essential for enhancing security adherence, particularly against targeted social engineering attacks (Jalali et al., 2020).

Scope of the Study

The scope of this guideline covers what an organisation should do to design, develop, implement, and maintain an IT security awareness and training programme, as a part of the IT security programme (Wilson & Hash, 2003). The scope includes awareness and training needs of all users, from employees to supervisors, functional managers, and executive-level managers (Wilson & Hash, 2003). The synthesis draws heavily on prescriptive government guidance, primarily NIST SP 800-50 (Wilson & Hash, 2003), conceptual frameworks defining security culture (Roer & Petrič, 2018), and modern technical risk mitigation strategies (Humanize, 2023; Rose, 2024). The empirical insights are anchored to a specific real-world investigation into phishing behaviour among hospital employees (Jalali et al., 2020), contextualising the intention-behaviour gap.

Operational Definitions of Key Terms

Table 1: Operational Definitions of Key Terms

Term	Operational Definition	Source
Human Error	Unintentional actions, or the lack of action, by employees or users that cause, spread, or allow a security breach to take place. Categorised as skill-based (slips/lapses) or decision-based (faulty judgment) errors.	(usecure, n.d.)
Insider Risk	Any internal factor arising from insider activity (current/former employees, contractors) that could represent a security concern, ranging from negligence and honest mistakes to the potential for malicious action.	(Teramind, 2024)
Insider Threat	An imminent, specific cybersecurity concern that aims to exploit an existing insider risk to damage the organisation. All threats originate as	(Teramind, 2024)

	risks, but not all risks escalate.	
Security Awareness	The purpose is simply to focus attention on security, allowing individuals to recognise IT security concerns and respond accordingly. It is not training (Wilson & Hash, 2003).	(Wilson & Hash, 2003)
Training	The process that strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing) (Wilson & Hash, 2003).	(Wilson & Hash, 2003)
Security Culture	The ideas, customs, and social behaviour that impact security in an organisation, both in a positive and a negative way (Roer & Petrič, 2018).	(Roer & Petrič, 2018)
Zero Trust	A cybersecurity framework based on the principle of **"never trust, always verify,"** requiring continuous authentication and authorisation for all users and devices, regardless of location (Humanize, 2023).	(Humanize, 2023)
Just-in-Time (JIT) Access	A core security practice that grants users or systems the minimum level of access to resources or information only when they need it and only for a specific duration to complete a task (Rose, 2024).	(Rose, 2024)
Vanity Metrics	Easily-obtainable quantitative data (e.g., employee attendance, completion rates) that looks good on the surface but fails to provide underlying, meaningful information about changes in security culture (Roer & Petrič, 2018).	(Roer & Petrič, 2018)

REVIEW OF RELATED LITERATURE

CONCEPTUAL REVIEW

The Genesis of Human Factors in Critical Systems

The recognition that systems failure is often linked to human interaction and system complexity is the focus of the discipline of **Human Factors and Ergonomics**, which was founded in the 1950s (North, n.d.). This field emerged because advanced technology and engineering led to greater system capability and complexity that often exceeded human cognitive limits without consideration of how humans process information (North, n.d.). Systems with safety and mission criticality began relying heavily on human operators, leading to consequential User Interface (UI) related incidents (North, n.d.). Notable examples include the **NORAD** false alarms in 1979 due to poor UI design; the **Three Mile Island (TMI)** incident where operators misjudged core water levels; and the **Flight 965** crash in Cali, Columbia, where deficiencies were linked to inadequate automation use and terrain information display (North, n.d.). These historical events underscore the necessity of integrating human limitations into all stages of system and security design (North, n.d.).

Categorisation of Human Error and Risk

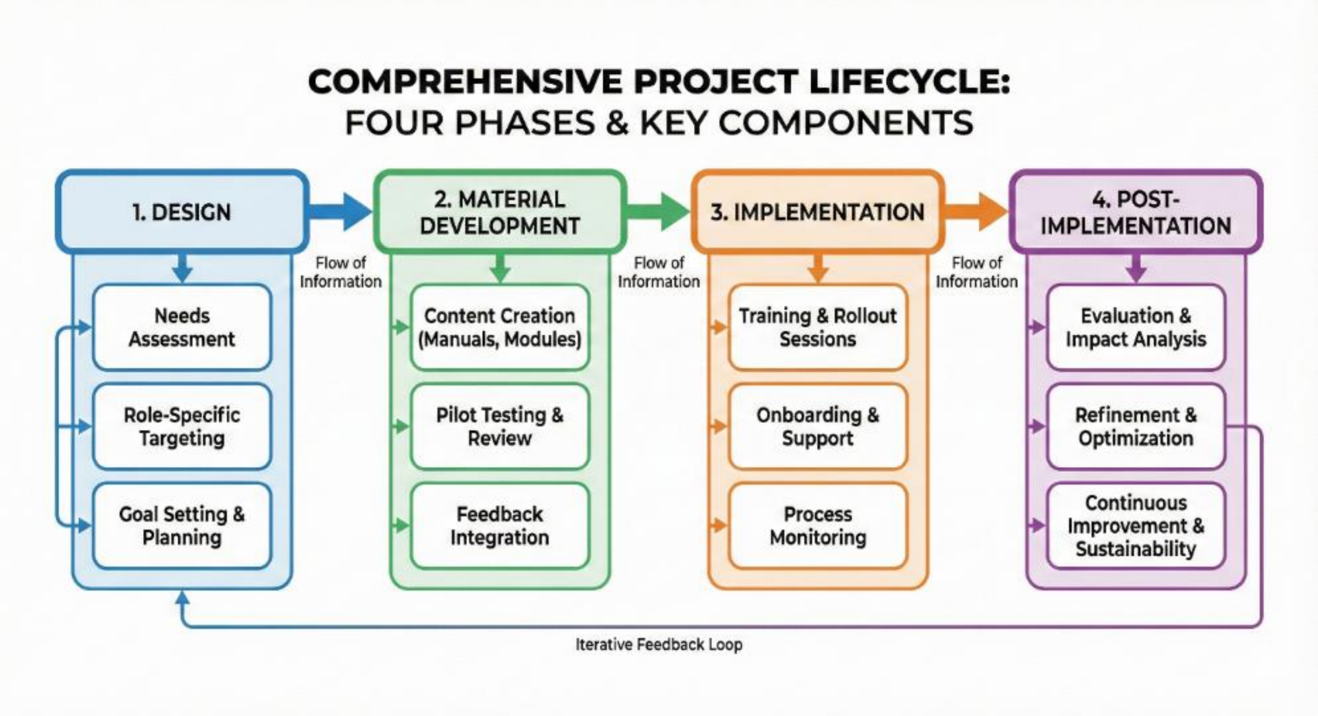
Human error, defined as unintentional actions or lack of action leading to a security breach, contributes significantly to information security failures (usecure, n.d.). It falls into two categories [287, usecure, n.d.]:

1. **Skill-based errors:** Small mistakes, such as slips and lapses, occurring during routine tasks due to factors like distraction or fatigue, even when the user knows the correct procedure (usecure, n.d.). A classic example is misdelivery, such as when an NHS employee accidentally exposed patient details by using the "to" field instead of the "bcc" field in an email (usecure, n.d.).
2. **Decision-based errors:** Occur when a user makes a faulty choice due to lacking necessary knowledge or sufficient contextual information (usecure, n.d.).

These errors contribute significantly to **Insider Risk**, which is any internal factor that represents a security concern (Teramind, 2024). Insider risks typically include **Negligent Insiders** (the most common cause of leaks), **Compromised Insiders** (malicious or disgruntled individuals), and **Privileged Users** (whose extensive access makes their misuse or exploitation exceptionally risky) (Teramind, 2024). When these risks escalate to an imminent likelihood of a security incident, they become an **Insider Threat** (Teramind, 2024).

The Security Awareness and Training (SAT) Continuum

Figure 1: NIST SP 800-50 Awareness and Training Life-Cycle



The foundational framework for mitigating human risk is the IT Security Awareness and Training Programme, structured by NIST SP 800-50 guidelines (Wilson & Hash, 2003). Learning occurs across a continuum:

- **Awareness:** The purpose is simply to focus attention on security, enabling individuals to recognise IT security concerns and respond accordingly (Wilson & Hash, 2003). This is aimed at **all users** (Wilson & Hash, 2003).
- **Training:** Strives to produce relevant and needed security skills and competencies, teaching specific functions, and targeting practitioners outside IT security, such as system administrators (Wilson & Hash, 2003).
- **Education:** Integrates security skills into a common body of knowledge, often through multidisciplinary study, designed to produce IT security specialists and professionals (Wilson & Hash, 2003).

- **Professional Development:** Intended to ensure users possess a required level of knowledge and competence necessary for their roles, often validated through technical or general certification (Wilson & Hash, 2003).

The implementation of this programme must follow a life-cycle approach: Design, Material Development, Implementation, and Post-Implementation (Wilson & Hash, 2003). The **Design** phase requires a **Needs Assessment** to identify the gap between required and current efforts (Wilson & Hash, 2003).

THEORETICAL FRAMEWORK

Theory of Planned Behaviour (TPB) in Security Compliance

The **Theory of Planned Behaviour (TPB)** is widely used in information security research to explain human behaviour. TPB posits that an individual's **intention** to perform a certain behaviour (e.g., adhering to security policies) is the direct antecedent of the actual behaviour (Ajzen, 1991). This intention is formed by three core cognitive beliefs Ajzen (1991):

- **Attitudes:** Positive or negative feelings towards the behaviour (Jalali et al., 2020).
- **Subjective Norms:** Perceived social pressure or expectations from important peers or managers to perform the behaviour (Jalali et al., 2020).
- **Perceived Behavioural Control:** The perceived ease or difficulty of performing the behaviour, often related to possessing the necessary resources and knowledge (Jalali et al., 2020).

In the context of this study, TPB provides the necessary framework to test whether cognitive factors successfully predict real-world security behaviour (Jalali et al., 2020).

Zero Trust and Least Privilege Access (LPA)

The **Zero Trust Security Model** serves as the primary technical framework for mitigating human risk by operationalizing the principle of **"never trust, always verify"** (Humanize, 2023; Rose, 2024). Zero Trust is guided by three principles:

- **Continuous Verification:** Requiring continuous authentication and authorisation for all entities accessing resources (Humanize, 2023).
- **Least Privilege Access (LPA):** Restricting access permissions to the minimum necessary to perform specific tasks, often implemented via **Just-in-Time (JIT) access** (Rose, 2024).
- **Assume Breach:** Accepting that breaches are inevitable and preparing security controls for rapid mitigation (Humanize, 2023).

JIT access is crucial to LPA, as it eliminates **standing privileges** (continuous access rights), granting temporary, on-demand access only when requested and automatically revoking it upon completion (Rose, 2024). This drastically reduces the potential attack surface and mitigates risks posed by privileged users (Rose, 2024).

Empirical Review

The efficacy of security programmes often relies on the assumption that increased intention to comply translates into actual secure behaviour. A study investigating phishing susceptibility among hospital employees tested this relationship by matching survey responses with employees' **actual clicking data from phishing campaigns** (Jalali et al., 2020).

The analysis revealed that core TPB factors (**Attitudes toward ISP, Subjective Norms, and Perceived Behavioural Control**) were indeed **positively related to compliance intention** (Jalali et al., 2020). Furthermore, **Collective Felt Trust** (in management) was positively related to attitudes and subjective norms, subsequently fostering compliance intention (Jalali et al., 2020).

However, the study found **no significant relationship between compliance intention and actual clicking behaviour** (Jalali et al., 2020). This key finding, derived from observed behaviour rather than self-reported data, challenges previous assumptions in the field (Jalali et al., 2020).

Crucially, the study identified that **high workload** was the only variable significantly and positively related to the likelihood of employees clicking on the phishing link (noncompliance behaviour) (Jalali et al., 2020). This suggests that environmental factors, such as the necessity to cope with high volumes of work, override positive cognitive intentions (Jalali et al., 2020).

Identification of the Research Gap

The central research gap is twofold:

1. **The Measurement Gap (McNamara Fallacy):** Organisations habitually rely on easily-obtainable quantitative data, or **"vanity metrics"** (e.g., attendance rates), which fail to provide actionable insights into the underlying features of security culture (Roer & Petrič, 2018). The gap lies in the systematic adoption of **scientific methodologies** to measure the seven core dimensions of culture in a valid, reliable, and bias-resistant manner (Roer & Petrič, 2018).
2. **The Contextual Gap (Intention-Behaviour Disconnect):** Empirical evidence shows that environmental and organisational stress factors (like workload) are stronger predictors of failure in real-world high-risk scenarios than cognitive intention (Jalali et al., 2020). The operational gap lies in the failure of security programmes to actively identify and mitigate these contextual, environmental factors.

The synthesis of this literature confirms that security success is predicated on addressing these gaps by migrating to data-driven Human Risk Management frameworks and adopting automated technologies to eliminate the reliance on error-prone human vigilance (Sjouwerman, 2025; HubSpot, n.d.).

RESEARCH METHODOLOGY

This chapter outlines a hypothesised research methodology designed to assess and mitigate human risk within a large digital enterprise, integrating the programmatic frameworks, scientific measurement, and behavioural validation techniques identified in the literature review.

Research Design

The proposed methodology is a **Mixed-Methods, Longitudinal Intervention Study**. This design combines **Qualitative** data (from needs assessments and policy analysis) and **Quantitative** data (from established scientific metrics and live behavioural testing) to provide a comprehensive view of human risk before and after programmatic interventions (Wilson & Hash, 2003; Jalali et al., 2020; Roer & Petrič, 2018).

Population and Sampling Technique

Target Population: A large digital enterprise (e.g., a government agency or health care organisation) requiring high levels of security compliance.

Sampling Technique: A **Role-Based Stratified Sampling** technique is required, as distinct roles have fundamentally different security responsibilities and training needs (Wilson & Hash, 2003). The sampling should target:

1. **Executive Management:** To assess strategic understanding of directives (Wilson & Hash, 2003).
2. **Security Personnel (Managers/Officers):** Must be well educated on security policy and best practices (Wilson & Hash, 2003).
3. **Privileged Users (System Administrators/IT Support):** Require a higher degree of technical knowledge and are entrusted with critical operations (Wilson & Hash, 2003).
4. **General Users:** The largest audience, targeted for awareness, basic training, and rules of behaviour (Wilson & Hash, 2003).

Data Collection Methods and Instruments

Data collection is divided into three integrated streams:

Organisational and Needs Assessment

- **Method:** Semi-structured interviews and standardised questionnaires (Wilson & Hash, 2003).
- **Instrument:** Adapted NIST Needs Assessment Interview and Questionnaire (see NIST SP 800-50, Appendix A) (Wilson & Hash, 2003). This assesses current efforts, identifies mandatory training needs, gauges workforce complexity, and captures required security skills for specific roles (Wilson & Hash, 2003).
- **Output:** Identification of the "gap" between existing coverage and required awareness/training efforts (Wilson & Hash, 2003).

Security Culture Measurement

- **Method:** Scientifically validated survey instruments (Roer & Petrič, 2018).
- **Instrument:** A security culture measurement tool designed to quantify the seven dimensions of culture (Roer & Petrič, 2018).
- **Output:** Quantification of the **Security Culture Index** across the seven dimensions: Attitudes, Cognition, Behaviour, Communication, Norms, Responsibility, and Compliance (Roer & Petrič, 2018). This provides actionable metrics beyond mere attendance rates (Roer & Petrič, 2018).

Behavioural and Contextual Data

- **Method:** Observational monitoring and real-time testing (Jalali et al., 2020; Teramind, 2024).
- **Instruments:**
  - **Phishing Simulations:** Faux phishing emails linked to employee identity to measure actual compliance behaviour (clicking) versus stated intention (Jalali et al., 2020).
  - **Workload Metrics:** Collection of contextual data to test its correlation with noncompliance behaviour (Jalali et al., 2020).
  - **System Monitoring:** Use of monitoring software and User & Entity Behavioural Analytics (UEBA) to identify anomalous behaviour, excessive exporting, or unusual working hours, which act as insider threat indicators (Teramind, 2024).

Validity and Reliability

Internal Validity (Measurement): Ensured by adhering strictly to the rigorous scientific procedure for scale construction, including pilot testing, cross-validations, and statistical validation to ensure metrics are bias-resistant and reliable (Roer & Petrič, 2018). The exclusion of employees who complete surveys too quickly is one mechanism used to avoid bias (Roer & Petrič, 2018).

External Validity (Generalisability): Enhanced by using a heterogeneous sample reflective of multiple organisational roles and correlating abstract factors (e.g., trust) with observed, concrete behaviour (Jalali et al., 2020).

Reliability: Confirmed by testing constructs' reliability using measures like Cronbach's alpha and ensuring adequate convergent and discriminant validity (Jalali et al., 2020).

Data Analysis Techniques

1. **Needs Analysis:** Quantitative comparison of required versus existing coverage (gap analysis) (Wilson & Hash, 2003).
2. **Structural Equation Modelling (SEM):** Used to test the proposed causal relationships derived from the TPB framework and the critical relationship between **Intention $\rightarrow$ Behaviour** and **Workload $\rightarrow$ Behaviour** (Jalali et al., 2020).

3. **Statistical Validation:** Used to ensure robustness and test whether results hold across different organisational units or contexts (Jalali et al., 2020).

Ethical Considerations

Ethical practice is paramount, especially when handling employee behavioural data (Jalali et al., 2020). The study must ensure:

- **Informed Consent:** Participants must be informed that participation is voluntary and anonymous (Jalali et al., 2020).
- **Data Anonymity:** When linking survey responses with behavioural data, anonymity must be preserved, typically by separating the data collection points (Jalali et al., 2020).
- **Accountability:** Accountability must be derived from a fully informed, well-trained, and aware workforce, ensuring management supports the programme (Wilson & Hash, 2003).

Data Presentation and Analysis

This chapter presents the interpretation and analysis of the existing empirical results relevant to human risk mitigation, primarily drawing from the established study on compliance behaviour in hospitals (Jalali et al., 2020).

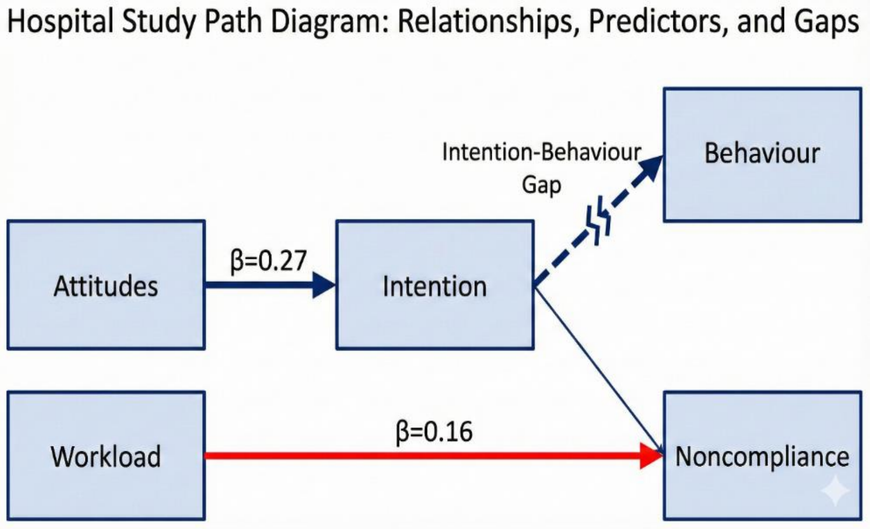
Presentation of Results

The Structural Equation Model (SEM) results from the hospital investigation provided the following key findings regarding the relationships between cognitive beliefs, intention, and compliance behaviour (Jalali et al., 2020):

Table 2: Hypothesis Testing Results from SEM Analysis

Hypothesis	Relationship Tested	Result	Beta (Effect Size)	Significance
H1a	Attitudes toward ISP $\rightarrow$ Intention to Comply	Supported (Positive)	.27	P < .001
H1c	Perceived Behavioural Control $\rightarrow$ Intention to Comply	Supported (Positive)	.44	P < .001
H3a/H3b	Collective Felt Trust $\rightarrow$ Attitude/Subjective Norm	Supported (Positive)	.23/.18	P < .001 / P = .001
H2	Intention to Comply $\rightarrow$ Compliance Behaviour	Rejected (Insignificant)	–.03	P = .57
H6	High Workload $\rightarrow$ Compliance Behaviour (Noncompliance)	Supported (Positive)	.16	P = .001

Figure 2: Structural Equation Model (SEM) of TPB in Phishing Compliance


Hospital Study Path Diagram: Relationships, Predictors, and Gaps

The data fit well for **intention to comply**, with an R^2 of 0.397 and a large predictive relevance (Q^2=0.377) (Jalali et al., 2020). However, the model explained little variance of the **clicking behaviour** (R^2=0.044) (Jalali et al., 2020).

Data Interpretation

The interpretation of these results reveals several critical points concerning human risk management:

Cognitive Success, Behavioural Failure

The strong positive relationships found between core TPB factors and **intention to comply** (H1a, H1c) confirm that security policies and communication (e.g., trust in technology reliability) are effective in building positive attitudes and perceived control (Jalali et al., 2020). **Collective Felt Trust** in management significantly influences attitudes and norms, implying that management participation is vital (Jalali et al., 2020).

However, the rejection of H2 (Intention $\rightarrow$ Behaviour) is salient. This finding suggests that in the high-risk context of phishing emails, the intention to comply is not significantly linked to the actual act of compliance (not clicking the link) (Jalali et al., 2020). This challenges previous assumptions that relied on self-reported data (Jalali et al., 2020).

The Overriding Power of Workload

The significant positive association between **high workload and noncompliance behaviour** (H6) is crucial (Jalali et al., 2020). Since none of the cognitive variables predicted clicking behaviour, workload is the only variable tested that significantly relates to noncompliance behaviour (Jalali et al., 2020). This suggests that environmental factors, such as the necessity to cope with high volumes of work or being rushed, override positive security intentions, potentially because overworked employees are too occupied to notice the sophisticated imposed threats (Jalali et al., 2020).

Findings Based on Research Questions or Hypotheses

Based on the empirical analysis and synthesis of source material, the following findings are established:

Finding 1 (Q1, Programme): A robust IT security awareness and training programme must follow the NIST life cycle of Design, Material Development, Implementation, and Post-Implementation (Wilson & Hash, 2003). This structure must define roles and responsibilities (Agency Head, CIO, Managers, Users) and address the continuum of learning (Awareness $\rightarrow$ Training $\rightarrow$ Education) (Wilson & Hash, 2003).

Finding 2 (Q2, Advanced Strategy): Advanced risk mitigation requires shifting from volume-based, superficial metrics (**vanity metrics**) to a **scientific approach** (HRM/CLTRe) (Roer & Petrič, 2018; Sjouwerman, 2025). This involves measuring the seven dimensions of security culture (Attitudes, Cognition, Behaviour, Communication, Norms, Responsibility, Compliance) to produce actionable, bias-resistant metrics (Roer & Petrič, 2018).

Finding 3 (Q3, Environment): Employee cognitive security intention is insufficient to predict actual compliance behaviour in high-risk scenarios. **High workload is significantly and positively associated with noncompliance behaviour**, indicating that organisational environmental factors must be addressed alongside training (Jalali et al., 2020).

Finding 4 (Q4, Technical Controls): Modern technical controls are necessary to compensate for human unreliability. The **Zero Trust** principle of "never trust, always verify," enforced through controls like **Just-in-Time (JIT) Access**, is essential for enforcing Least Privilege Access and mitigating the inherent risk of standing privileges (Humanize, 2023; Rose, 2024).

DISCUSSION OF FINDINGS

Comparison with Existing Studies

The empirical finding that **compliance intention does not significantly predict actual compliance behaviour** in the context of phishing (Jalali et al., 2020) provides a significant corrective to previous information security studies that relied on self-reported data (Jalali et al., 2020). By observing actual clicking behaviour, the study demonstrated that the intention-behaviour gap is highly relevant when employees face immediate threats (Jalali et al., 2020).

Recent threat intelligence underscores a concerning escalation in human driven vulnerabilities. Contemporary analyses attribute a substantial 74 percent of breaches to human factors, including errors, negligence, and insider activity, which demonstrates the persistent inadequacy of conventional awareness training and behaviour focused interventions alone (Verizon, 2025; NIST IR 8272, 2024). These findings provide empirical confirmation of the intention behaviour gap observed in high pressure organisational settings, where well intentioned employees fail to enact secure behaviour due to cognitive overload or environmental constraints. To mitigate this inherent human fallibility, the proposed framework positions Zero Trust architecture as the foundational technical safeguard that compensates for lapses in human vigilance. Zero Trust, as specified in NIST SP 800 207 (2020), removes assumptions of internal trust, enforces continuous verification, and applies Just in Time access to eliminate standing privileges that are frequently exploited during human centred failures. This integration ensures that even when behavioural controls falter, security resilience is maintained through automated technical enforcement that neutralises the consequences of unavoidable human error.

Furthermore, the identification of **high workload** as the sole significant predictor of noncompliance behaviour introduces an organisational environment factor into the core risk equation (Jalali et al., 2020). This aligns the modern security challenge with historical human factors incidents, such as the TMI nuclear disaster, where high operational stress or poor UI design compromised human vigilance (North, n.d.).

Implications of the Results

The integrated findings carry profound implications for enterprise security strategy:

Necessity of Cultural and Environmental Management

The failure of intention to predict behaviour implies that training programmes focused only on cognitive beliefs will be insufficient if the work environment is inherently demanding (Jalali et al., 2020). Organisations must adopt **Human Risk Management (HRM)**, which moves beyond basic awareness to focus on measuring security behaviour and quantifying human risk (Sjouwerman, 2025). The results suggest that managing employee workload must become a core component of Information Security Policy, as extensive emailing and high volumes of work increase the risk of clicking on phishing links (Jalali et al., 2020).

Mandate for Scientific Measurement

The vulnerability demonstrated by relying on easily-obtainable quantitative data (**vanity metrics**) requires a shift toward the **scientific measurement of security culture** (Roer & Petrič, 2018). By measuring the seven dimensions (Attitudes, Norms, Behaviour, etc.) through validated, bias-resistant surveys, organisations can obtain actionable metrics that identify the true sources of risk within departments, thereby avoiding the **McNamara Fallacy** (Roer & Petrič, 2018).

Embracing Technical Enforcement over Human Trust

The inherent fallibility of human behaviour mandates rigorous technical controls to eliminate or minimise the reliance on human vigilance (usecure, n.d.). The **Zero Trust** philosophy, built on continuous verification, must supersede the traditional **Full Trust** model, which assumes internal entities are trustworthy (Humanize, 2023). **Just-in-Time (JIT) Access** serves as the practical application of the Least Privilege Principle, granting temporary, on-demand access and automatically revoking standing privileges, thereby drastically reducing the attack surface (Rose, 2024; Humanize, 2023).

Furthermore, addressing cloud misconfiguration, the **biggest threat** to cloud security caused by human error, requires automated solutions (HubSpot, n.d.). Since the Mean Time to Remediation (**MTTR**) for misconfigurations is often measured in days or weeks, immediate, automated techniques like **Baseline Enforcement** are essential to restore resources to a known-good state, eliminating human slowness and error in the remediation path (HubSpot, n.d.).

Contribution to Knowledge

This study contributes to cybersecurity knowledge by synthesising the prescriptive governmental policy on programme structure (Wilson & Hash, 2003) with advanced, data-driven security models and critical empirical findings. It establishes a framework that integrates:

1. **Programme Maturity:** Detailing the NIST life-cycle approach and various implementation models (Centralised, Partially Decentralised, Fully Decentralised) (Wilson & Hash, 2003).
2. **Cultural Verifiability:** Demonstrating the necessity of scientifically validated cultural metrics to replace misleading compliance data (Roer & Petrič, 2018).
3. **Contextual Vulnerability:** Highlighting that **workload is a critical security vulnerability** that demands organisational intervention (Jalali et al., 2020).
4. **Automated Resilience:** Cementing the necessity of technical controls (Zero Trust, JIT, Baseline Enforcement) as mechanisms specifically designed to compensate for and eliminate the consequences of inevitable human error and slowness (Humanize, 2023; HubSpot, n.d.; Rose, 2024).

SUMMARY, CONCLUSION AND RECOMMENDATIONS

Summary of Key Findings

This synthesis confirms that the human element remains the principal vulnerability in enterprise security, responsible for up to 95% of breaches (Sjouwerman, 2025; usecure, n.d.). Insider activity, ranging from negligence (**risk**) to malice (**threat**), poses the greatest internal danger (Teramind, 2024).

The fundamental structure for managing this risk is the NIST SP 800-50 life-cycle programme, which addresses the continuum of Awareness, Training, and Education (Wilson & Hash, 2003). However, this framework must be augmented by modern, advanced strategies:

- **Empirical Gap:** The study of phishing behaviour demonstrated that while trust and attitudes successfully drive **compliance intention**, this intention fails to translate reliably into **actual secure behaviour** (Jalali et al., 2020).
- **Critical Predictor:** High **workload** was the only tested factor significantly and positively linked to noncompliance behaviour (Jalali et al., 2020).
- **Advanced Mitigation:** Effective mitigation requires adopting **Human Risk Management (HRM)** to measure and improve security culture across seven scientific dimensions (Sjouwerman, 2025; Roer & Petrič, 2018).
- **Technological Imperative:** The adoption of **Zero Trust** principles, enforced through controls like **Just-in-Time (JIT) Access**, is essential for eliminating the risk of standing privileges (Humanize, 2023; Rose, 2024). In cloud contexts, automated **Baseline Enforcement** is mandatory to counter human misconfiguration error (HubSpot, n.d.).

Conclusions Drawn from the Study

Based on the synthesis of policy, empirical evidence, and technological models, the following conclusions are drawn:

1. **Security is an Organisational Health Issue:** Cybersecurity cannot be solved purely through technology. Given that high workload directly compromises security behaviour, achieving compliance is intrinsically linked to managing the organisational environment and employee well-being (Jalali et al., 2020).
2. **Compliance Must Be Verified, Not Assumed:** Organisations must migrate to scientifically validated measurements of security culture, focusing on observable behaviour, norms, and responsibility, to avoid the **McNamara Fallacy** (Roer & Petrič, 2018).
3. **Privilege Must Be Ephemeral:** The risk posed by privileged users and standing access rights is too high to tolerate. Zero Trust and JIT access are essential frameworks that eliminate these standing risks by ensuring access is granted with the minimum necessary privilege for the shortest required time (Humanize, 2023; Rose, 2024).
4. **Remediation Must Be Automated:** Where human error is a recognised and frequent cause of complex failures, such as cloud misconfiguration, the security response must be automated. Strategies like **Baseline Enforcement** are critical to reducing MTTR from days to minutes, overriding the human potential for slowness and error (HubSpot, n.d.).

PRACTICAL RECOMMENDATIONS

Organisations seeking to enhance their security posture and mitigate human risk should implement the following recommendations:

1. **Formalise the IT Security Programme:** Adopt the NIST SP 800-50 life-cycle approach, starting with a formal Needs Assessment to identify capability gaps across all roles (Wilson & Hash, 2003).
2. **Implement Zero Trust with JIT Access:** Eliminate standing privileges across all critical systems (Rose, 2024). Use JIT access via a Privileged Access Management (PAM) solution to grant temporary, auditable, and context-aware access (Rose, 2024).
3. **Adopt Scientific Culture Measurement:** Implement a security culture measurement framework (HRM) to regularly quantify the seven dimensions of culture using validated metrics (Roer & Petrič, 2018; Sjouwerman, 2025).
4. **Mandate Cloud Baseline Enforcement:** Deploy automated remediation tools (e.g., Baseline Enforcement) to instantly revert resource configurations back to a known-good baseline upon detection of drift, circumventing human processing delays (HubSpot, n.d.).
5. **Address Workload and Trust:** Integrate workload management into security policy (Jalali et al., 2020). Foster **Collective Felt Trust** by ensuring management actively supports security policies, thereby encouraging employees to internalise security goals (Jalali et al., 2020).

Suggestions for Further Research

Based on the established findings and identified gaps, the following areas warrant further investigation:

1. **Replication in Diverse Industries:** Future research should replicate the study linking **workload and noncompliance** across different high-pressure industries (e.g., financial services, defence) to test the generalisability of the intention-behaviour gap (Jalali et al., 2020).
2. **Efficacy of HRM Interventions:** Long-term studies are needed to evaluate the measurable impact of HRM strategies. This research should specifically correlate longitudinal changes in the measured **Security Culture Index** with objective security outcomes, such as a decline in security incidents (Roer & Petrič, 2018; Sjouwerman, 2025).
3. **Impact of Automation on MTTR:** Research should empirically measure the quantifiable reduction in Mean Time to Remediation (MTTR) for cloud misconfiguration and privilege abuse incidents achieved through the full implementation of **Baseline Enforcement** and **JIT Access** (HubSpot, n.d.; Rose, 2024).
4. To advance the maturity of this framework, the next stage of research must empirically validate its combined behavioural and technical components. Future studies should adopt a longitudinal design to measure observable changes in workforce security behaviour and correlate these with organisational incident rates following the implementation of Zero Trust architecture and workload informed HRM interventions. This will enable researchers to quantify whether strengthened security culture, reduced workload pressure, and the removal of standing privileges produce measurable reductions in human initiated security events. Such empirical validation is essential for confirming the practical effectiveness and operational value of the integrated framework.

REFERENCES

1. Ajzen I. The theory of planned behaviour. Organ Behav Hum Decis Process. 1991;50(2):179-211. doi:10.1016/0749-5978(91)90020-T
2. Cano JJM. The human factor in information security. ISACA J. 2019 Oct 9 [cited 2025 Nov 30]. Available from: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security
3. Hadlington L. Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon. 2017;3(7):e00346. doi:10.1016/j.heliyon.2017.e00346
4. Verizon. 2025 Data Breach Investigations Report (DBIR). Verizon Business; 2025 [cited 2025 Nov 30]. Available from: https://www.verizon.com/business/resources/reports/dbir/
5. NIST. NISTIR 8272: Cybersecurity Framework Profile for Hybrid Satellite Networks. National Institute of Standards and Technology; 2024.
6. HubSpot. A comprehensive guide to preventing cloud misconfiguration [Internet]. HubSpot; 2024 [cited 2025 Nov 30]. Available from: https://www.hubspot.com/cloud-security/misconfiguration
7. Humanize. Zero trust security model explained: Principles, architecture, benefits [Internet]. Humanize; 2023 Nov 15 [cited 2025 Nov 30]. Available from: https://humanize.security/zero-trust
8. Jalali MS, Bruckes M, Westmattelmann D, Schewe G. Why employees (still) click on phishing links: Investigation in hospitals. J Med Internet Res. 2020;22(1):e16775. doi:10.2196/16775
9. Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M. A survey on security issues and solutions at different layers of cloud computing. J Supercomput. 2013;63(2):561-592. doi:10.1007/s11227-012-0831-5
10. North RA. Government best practices in system usability: A brief history and status [Internet]. Human Centered Strategies, LLC; n.d. [cited 2025 Nov 30].
11. Reason J. Human error. Cambridge: Cambridge University Press; 1990.
12. Roer K, Petrič G. To measure security culture: A scientific approach [Internet]. CLTRe; 2018 [cited 2025 Nov 30]. Available from: https://cltre.com/security-culture-measurement
13. Rose A. What is Just-in-Time Access? A complete guide [Internet]. Securden; 2024 Sep 6 [cited 2025 Nov 30]. Available from: https://www.securden.com/just-in-time-access
14. Sjouwerman S. Human Risk Management: Strategies to fortify your organisation's defence. Forbes. 2025 Jun 10 [cited 2025 Nov 30]. Available from: https://www.forbes.com/human-risk-management

15. Stanton NA. Human factors in security: What have we learned? Applied Ergonomics. 2014;45(2):452-458. doi:10.1016/j.apergo.2013.05.007
16. Teramind. Insider threat vs. insider risk: What's the difference? [Internet]. Teramind; 2024 May 3 [cited 2025 Nov 30]. Available from: https://www.teramind.co/blog/insider-threat-vs-risk
17. usecure. The role of human error in successful cyber security breaches [Internet]. usecure; n.d. [cited 2025 Nov 30]. Available from: https://www.usecure.io/blog/human-error-cyber-breaches
18. Wilson M, Hash J. Building an information technology security awareness and training program (NIST Special Publication 800-50). National Institute of Standards and Technology; 2003.
19. NIST. SP 800-53 Rev. 5: Security and privacy controls for information