Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 5, 1126-1142
2025
Publisher: Learning Gate
DOI: 10.55214/25768484.v9i5.7092

Culture in higher education: An empirical analysis of employee perceptions and behavioural outcomes in the UAE

Said Badreddine[1,2*], Tariq Alwada'n[1], Mohammad Abdur Razzaque[1], Ala Al Kafri[1], Hamsa Al Ammari[2], Adel Hamdan[3]
[1]School of Computing, Engineering & Digital Technologies, Teesside University, Middlesbrough TS1 3BX, UK.
[2]Computer Information Systems, Higher Colleges of Technology, 25026, Adu Dhabi, Al Ain, UAE; S.Badreddine@tees.ac.uk (S.B.).
[3]Computer Science Dept., The World Islamic Sciences and Education University, Amman, Jordan.

Abstract: This study explores the relationship between cybersecurity culture and employee behaviour in higher education institutions (HEIs) in the United Arab Emirates (UAE), using a cross-sectional, mixed-methods approach. The sample comprised 246 employees across faculty (43.5%), administrative staff (48%), and management (8.5%) roles, with varying levels of experience and technical readiness. Quantitative analyses revealed that perceived cybersecurity culture was the most significant predictor of behaviour (Spearman's $\rho = 0.62$, $p = 0.003$), with behaviour scores ranging from 37.91 in "Developing Culture" contexts to 75.98 in "Exemplary Culture" settings. ANOVA results indicated significant differences in behaviour across role ($F(2,83) = 5.72$, $p = 0.009$) and experience levels ($F(5,79) = 3.94$, $p = 0.021$), with early-career staff scoring the lowest. Best practice adherence further explained behavioural variance ($F(5,79) = 9.84$, $p < 0.001$). Qualitative analysis identified three core challenges: restrictive system controls, outdated training, and leadership disengagement. These findings highlight the behavioural and contextual drivers of cybersecurity and emphasize the need for culture-first strategies that align institutional norms, communication, and leadership modelling with digital security objectives.

Keywords: *Employee Behaviour, Higher Education, Institutional Practices, Cybersecurity Culture, Security Awareness.*

1. Introduction

The rapid digital transformation of higher education institutions (HEIs) has elevated their risk exposure to cyber threats [1, 2]. From student data systems to research repositories and enterprise-level cloud services, HEIs manage extensive digital assets that are highly attractive to cybercriminals [3]. What distinguishes HEIs from other sectors is their open-access ethos, designed to facilitate collaboration and academic freedom, which also results in a decentralized network architecture, weak perimeter controls, and a diverse user population comprising students, faculty, and administrative staff [4].

Recent data reveal alarming trends. Ransomware attacks on higher education increased by over 70% between 2022 and 2023, with institutions such as the University of the West of Scotland and Stanford University experiencing major breaches that led to service outages and data leaks [5, 6]. In the UK, 97% of higher education providers reported experiencing at least one cyber breach or attack in the past year [7]. These statistics point to an urgent need to examine the less technical and more human-centric aspects of cybersecurity.

History: Received: 17 February 2025; Revised: 19 April 2025; Accepted: 22 April 2025; Published: 12 May 2025
* Correspondence: S.Badreddine@tees.ac.uk

1.1. Problem Statement

Despite substantial investments in technological defences, ranging from intrusion detection systems to encryption protocols, human factors remain the most persistent and unpredictable threat vector. Numerous studies have shown that the majority of cyber incidents involve user error, poor judgment, or a lack of awareness. According to Verizon's 2023 Data Breach Investigations Report, over 74% of breaches involved a human element [8].

This phenomenon signifies the important role of cybersecurity culture, a complex construct encompassing employees' knowledge, beliefs, attitudes, and behaviours toward cybersecurity [9]. In academic environments, where autonomy and minimal oversight are often normal, enhancing a shared culture of cyber vigilance is particularly challenging. Moreover, organizational misalignment, where leadership emphasizes compliance but fails to build cultural capacity, can lead to a false sense of security [10].

1.2. Literature Review

1.2.1. Cybersecurity Culture: Beyond Compliance

The concept of cybersecurity culture has reformed from a compliance-driven model to a behavioural and cognitive construct. Alshaikh [9] emphasizes that cybersecurity culture must be cultivated through leadership modelling, continuous learning, and integration into daily workflows. Similarly, Parsons, et al. [11] developed the Human Aspects of Information Security Questionnaire (HAIS-Q) to assess users' knowledge, attitudes, and behaviours, focusing on the gap between policy awareness and actual behaviour. Their findings demonstrate that awareness alone does not translate to safe practices unless reinforced by institutional culture[11].

In HEIs, this gap is critical. Research by Durojaiye, et al. [12] indicates that while most academic institutions have cybersecurity policies in place, many employees find them inaccessible, overly technical, or irrelevant to their specific roles. Such disconnection often results in policy fatigue or resistance, especially among faculty who may perceive cybersecurity protocols as constraints on academic freedom [12].

1.2.2. Perceptions and Behavioural Outcomes

Employee perceptions, how staff view the importance, legitimacy, and usability of cybersecurity practices, are a powerful predictor of actual behaviour. The perceived organizational support for cybersecurity influences employees' intention to comply with security regulations [13]. A positive perception encourages intrinsic motivation and norm-driven behaviour, while a lack of support increases disengagement and risk tolerance.

In a survey of academic institutions, Rajamäki, et al. [14] found that employees with higher perceived cybersecurity culture scores demonstrated stronger behavioural compliance, even when faced with phishing attempts or system vulnerabilities [14]. This indicates that institutional narratives and symbolic gestures (e.g., leadership emails, publicized security successes) shape how employees interpret their cybersecurity responsibilities.

1.2.3. Institutional Practices and Organizational Readiness

Effective institutional practices are central to cultivating cybersecurity culture. Cheng [15]outline a strategic model for HEIs that includes leadership accountability, clearly defined KPIs, and the establishment of cross-departmental cybersecurity task forces. However, implementation often falters due to inconsistent resource allocation, lack of dedicated personnel, and insufficient feedback loops [15]. Studies show that only 32% of universities conduct mandatory, role-based cybersecurity training, and fewer still monitor behavioural improvements over time [16].

Additionally, readiness levels vary across roles and departments. Faculty in research-intensive roles may resist centralized security controls, while administrative staff may lack the technical skills to implement best practices. This heterogeneity necessitates tailored interventions, rather than uniform policy deployment.

1.2.4. Demographic and Contextual Influences

Demographic characteristics also mediate cybersecurity behaviours. In a study at the University of Nigeria, it was found significant differences in cyber hygiene based on gender, academic discipline, and employment status [17]. Women reported higher levels of policy compliance, while early-career staff exhibited lower levels of risk perception. These patterns highlight the need for segmented strategies that consider institutional role, technological fluency, and even cultural context [17].

Furthermore, Gervasi, et al. [18] stress that many HEIs fail to assess their internal cybersecurity risk landscape, leading to reactive rather than proactive cultural development. Without diagnostics and performance measurement, institutions cannot meaningfully improve employee engagement or security posture [18].

1.3. Objectives and Significance

This study aims to address these critical gaps by exploring how employee perceptions, institutional practices, and demographic variables interact to influence cybersecurity behaviours in HEIs. By using quantitative methods to assess culture, readiness, and behaviour across various staff profiles, the study will:

- Map the current state of cybersecurity culture in HEIs.
- Determine the predictive value of perceptions and readiness on employee behaviour.
- Identify demographic or organizational patterns that require targeted intervention.

The significance lies in advancing a behavioural model of cybersecurity in HEIs, one that can inform leadership, policy architects, and IT managers in designing more human-centred, culturally embedded security programs.

1.4. Research Questions

1. What is the perceived level of cybersecurity culture among HEI employees?
2. How do employees' perceptions relate to their cybersecurity behaviours and institutional practices?
3. What demographic or institutional factors influence these perceptions?

2. Materials and Methods

2.1. Research Design

This study employed a mixed-method, cross-sectional survey design to investigate the role of cybersecurity culture in higher education institutions (HEIs), focusing on employee perceptions, behavioural practices, and institutional influences. The use of both open- and closed-ended questions enabled the integration of quantitative and qualitative data, providing a more comprehensive understanding of the topic. The rationale for this mixed-method approach lies in its ability to combine the objective measurement of attitudes and behaviours (quantitative) with in-depth insights into individual experiences and perspectives (qualitative). This design allows for both inferential analysis of relationships between variables and a nuanced exploration of context-specific factors influencing cybersecurity culture [19].

A cross-sectional design is appropriate given the study's goal to capture a snapshot of cybersecurity culture at a particular point in time. While it does not allow causal inference, it provides a robust foundation for identifying patterns and correlations among key factors influencing employee cybersecurity behaviours within HEIs.

2.2. Participants and Sampling

The population targeted for this study includes employees working in various roles (e.g., academic faculty, administrative staff, IT professionals, and management) within higher education institutions in the UAE. Purposive sampling was adopted to ensure diversity in role, department, gender, and years of experience, factors known to affect cybersecurity attitudes and practices [17].

The final dataset comprises N = 246 valid responses after eliminating incomplete and non-consenting entries. Demographic distributions revealed a relatively balanced gender ratio, with the majority of participants aged between 36–55 years. The professional roles included faculty (41%), administrative staff (32%), IT/technical support (15%), and executive or management roles (12%). Participants represented a broad spectrum of departments, from Humanities to Computer Information Systems and Engineering.

2.3. Instrumentation

The survey instrument was developed using validated constructs from prior literature on cybersecurity behaviour and culture Alshaikh [9] and Parsons, et al. [11] adapted to the higher education context. The instrument included both objective measures and self-reported perceptions, covering the following dimensions:

1. Cybersecurity Culture Level: A single-item measure with ordinal categories ("Poor Culture," "Developing Culture," "Strong Culture," "Exemplary Culture") based on employees' perception of their institutional cybersecurity environment.
2. Cybersecurity Behaviour Score: A computed quantitative score derived from multiple items measuring frequency and quality of secure behaviour, such as recognizing phishing emails, using strong passwords, and reporting incidents. The composite reliability of this scale in pilot testing was Cronbach's $\alpha = 0.88$.
3. Cybersecurity Best Practices Level: A categorical item assessing adherence to recommended practices (e.g., "Rarely follows," "Sometimes follows," "Mostly compliant," "Fully compliant").
4. Technical Readiness Level: Self-assessment of digital proficiency, classified as "Basic Readiness," "High Readiness," or "Cutting-edge Readiness."
5. Cyber Policy Knowledge: Measured on a 3-point scale: "Basic Knowledge," "Good Awareness," and "Comprehensive Understanding."
6. Demographic and Professional Variables: Age group, gender, role, department, and years of experience.
7. Open-Ended Questions: To provide qualitative context, three open-ended questions were included to solicit participants' views on challenges, institutional support mechanisms, and recommendations for improving cybersecurity practices.

2.4. Data Collection Procedure

The data was collected via an anonymous online survey distributed across institutional mailing lists and internal portals. Participants were informed of the study's purpose, their rights to withdraw, and data privacy protections in accordance with ethical standards outlined by the British Educational Research Association [20]. Only those who provided informed consent proceeded to the main survey.

The average completion time was approximately 8–10 minutes. The data was automatically logged and encrypted, with access restricted to the principal investigator.

2.5. Data Preparation and Cleaning

Responses were screened for missing data, inconsistencies, and response biases. Participants who did not provide consent (n = 7) or gave uniform responses throughout (n = 3) were excluded. For open-ended items, non-responses or "3" placeholders were recoded as missing. The dataset was then coded, anonymized, and prepared using Python (pandas) and SPSS for analysis.

Outliers were assessed using boxplots and z-scores. No extreme values exceeded ±3 standard deviations from the mean in continuous variables, affirming the dataset's integrity. Nominal and ordinal variables were dummy coded as necessary for regression analysis.

2.6. Data Analysis

Data analysis proceeded in three stages:

2.6.1. Descriptive Statistics

Means, standard deviations, and frequencies were computed to provide a demographic and contextual profile of respondents and to summarize cybersecurity culture, behaviour, and awareness scores.

2.6.2. Inferential Statistics

To answer Research Question 2 regarding relationships between employee perceptions and behaviour:

- Pearson's r correlation and Spearman's rank-order correlation (for ordinal variables) were used to assess associations between Cybersecurity Culture Level and Cybersecurity Behaviour Score.
- Multiple linear regression was conducted with behaviour score as the dependent variable and culture level, policy knowledge, and technical readiness as predictors.
- Variance Inflation Factor (VIF) values were inspected to rule out multicollinearity.

For Research Question 3 on demographic influences:

- One-way ANOVA and Kruskal-Wallis H tests were used to detect significant differences in culture perception and behaviour scores across age groups, roles, and departments.
- Post-hoc Tukey HSD tests were applied for pairwise comparisons.

2.6.3. Qualitative Content Analysis

Responses to open-ended items were subjected to thematic analysis following Braun and Clarke's method in Ethical Guidelines for Educational Research [20]. Initial codes were generated inductively and then categorized under broader themes such as "Institutional Communication Gaps" "Over-Restriction of Systems," and "Call for Personalized Training".

This qualitative analysis strengthened the quantitative findings by contextualizing attitudes and offering explanations for observed patterns.

3. Results and Discussion

This section includes a combined analysis of quantitative and qualitative data collected from the participants. It addresses the three research questions through statistical modelling, thematic analysis, and visualisation.

3.1. Overview and Demographic Context

The respondents in this study demonstrated a noticeable degree of demographic and institutional diversity, enabling a robust and thorough analysis of cybersecurity culture across various subgroups. This variation strengthens the generalizability of the findings and offers key considerations in organizational behaviour research [9, 11].

3.2. Occupational Roles

Participants were distributed across three primary institutional roles:

- Faculty accounted for 43.5% of the sample,
- Administrative Staff comprised 48%,

- Management represented 8.5%.

This distribution reflects typical employment structures within higher education institutions (HEIs), with faculty and staff comprising the operational backbone and management forming the strategic leadership tier. The adequate representation of each group provides a foundation for understanding how institutional role influences cybersecurity perception and behaviour [15].

3.3. Professional Experience

Participants also varied in their tenure within HEIs:

- The majority (38%) reported 1–5 years of experience,
- 17% had 6–10 years,
- 15% reported 16–20 years of institutional service.

This wide span of experience levels provides insight into how exposure to institutional cybersecurity practices over time influences behaviour, echoing findings by Ugwu, et al. [17] which highlight professional maturity as a determinant of cyber security.

3.4. Gender Distribution

As illustrated in Figure 1, gender distribution among respondents was relatively balanced:

- Male: 132 respondents (53.7%),
- Female: 113 respondents (45.9%),
- Prefer Not to Say: 1 respondent (0.4%).

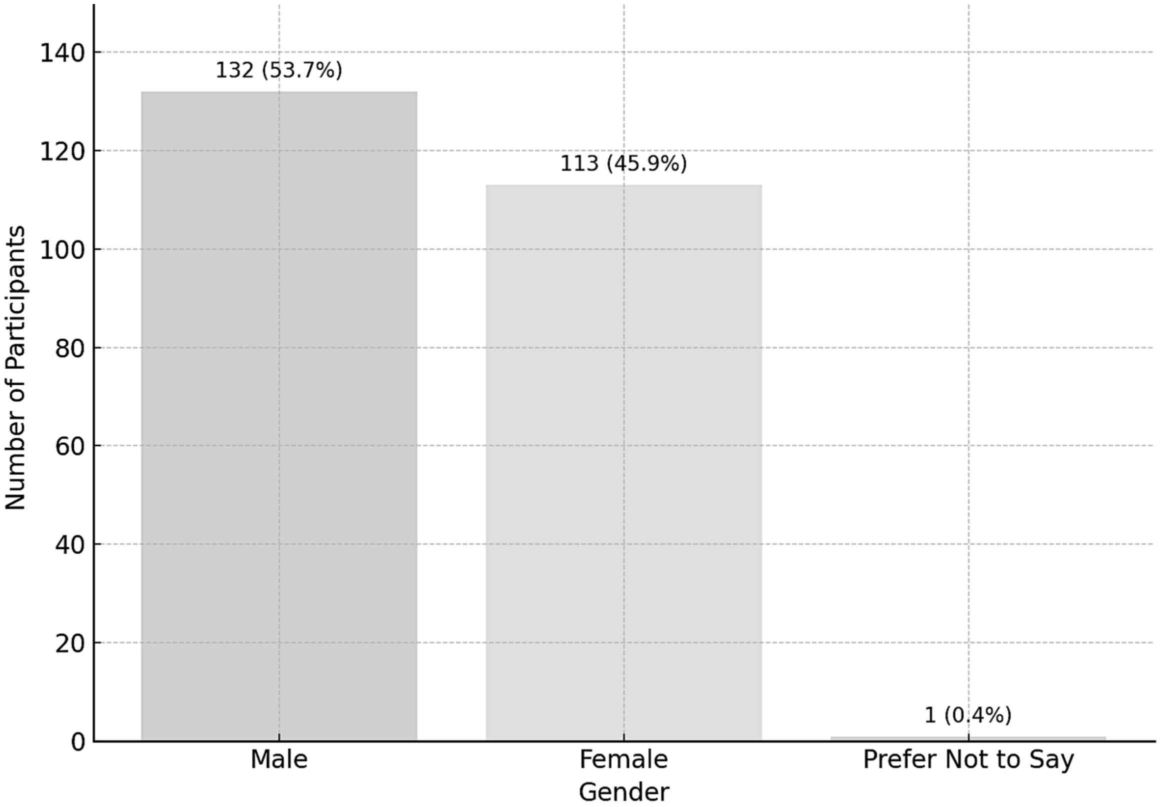

Figure 1.
Gender Distribution.

This balance is critical, as it mitigates gender bias and supports valid comparisons across gender groups regarding compliance, attitudes, and engagement with institutional cybersecurity practices. Research suggests that gender may influence perceptions of risk and security behaviours in digital environments, though the effect size varies across contexts [21].

The intersectional distribution of gender and experience across roles is captured in Tables 1 and 2, which provide detailed cross-tabulations for institutional analysis.

Table 1.
Role by Gender

Role	Female	Male	Prefer Not to Say
Faculty	25	86	0
Management	7	4	0
Staff	81	42	1

Faculty positions were predominantly male, while staff roles skewed female. Management roles were more gender balanced. This distribution aligns with broader labour force patterns in HEIs and supports differentiated analysis of gendered experiences in security policy adoption.

Table 2.
Role by Years of Experience.

Role	1-5	6-10	11-15	16-20	21-25	26+
Faculty	17	19	19	27	20	9
Management	0	1	1	4	3	2
Staff	84	21	8	9	2	0

Staff roles are more likely to be held by early-career professionals, whereas faculty exhibit a wider range of experience. Management roles appear to consolidate around mid-to-late career professionals. This gradient allows for examining how tenure influences behaviour and institutional alignment with cybersecurity policy.

3.5. Perceptions of Cybersecurity Culture (RQ1)

To address Research Question 1, *What is the perceived level of cybersecurity culture among HEI employees?* participants were asked to self-assess their institution's cybersecurity culture using a six-point ordinal scale ranging from *Weak* to *Exemplary*. These perceptions were then compared against the Cybersecurity Behaviour Score, a composite index designed to quantify the degree of secure digital practices adopted by each respondent.

The Cybersecurity Behaviour Score was derived using a composite method widely used in organizational cybersecurity studies Alshaikh [9] and Parsons, et al. [11]. The score was based on multiple survey items addressing key behavioural dimensions such as:

- Password and credential management.
- Email/phishing awareness and response.
- Device security and software update practices.
- Use of secure networks and VPNs.
- Handling of institutional data and digital files.
- Reporting suspicious or noncompliant behaviour.

Each item was rated using a Likert-type scale (e.g., from "Never" to "Always"), with scores typically assigned from 1 to 5. Negatively framed questions were reverse-coded *so* that higher values consistently reflected more secure behaviours.

The behaviour score for each respondent was calculated using the following formula*:*

DOI: 10.55214/25768484.v9i5.7092

$$Behaviour\ Score = \sum_{i=1}^{n} \frac{Behaviour\ Item_i}{n} \qquad [1]$$

Where:

- Behaviour Item = *Numeric score for the* ith *item*
- n = *Total number of behaviour items answered*

This method aligns with standardised frameworks such as the HAIS-Q (Human Aspects of Information Security Questionnaire) and provides a reliable measure of behavioural compliance in cybersecurity contexts [10].

3.6. Descriptive Results

Table 3 presents the distribution of cybersecurity culture perceptions along with the corresponding mean behaviour scores:

Table 3.
Cybersecurity Culture Level Count and Mean Behaviour Score.

Culture Level	Count	Mean Behaviour Score
Developing Culture	47	37.91
Moderate Culture	67	46.79
Strong Culture	37	59.42
Very Strong Culture	51	67.84
Exemplary Culture	30	75.98
Weak Culture	14	53.46

As seen in Figure 2, there is a clear positive gradient: as the perceived culture rating increases from Developing to Exemplary, the mean behaviour score also increases, from 37.91 to 75.98, representing a 100% relative improvement.

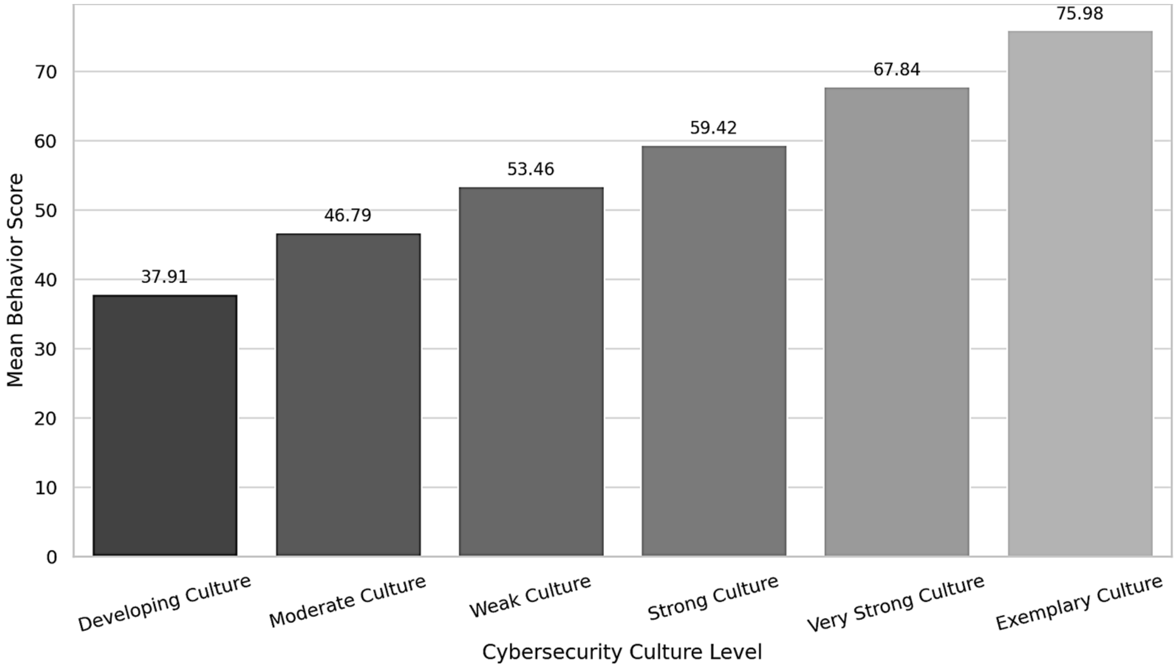

Figure 2.
Mean Behaviour Score.

This pattern strongly supports the notion that organizational culture significantly predicts individual security behaviour. The findings are consistent with the cultural-behavioural framework proposed by Onumo [22] where secure behaviour is influenced not only by individual awareness or skill but by the perceived strength of institutional norms, leadership emphasis, and peer expectations around cybersecurity [22].

The positive relationship between culture and behaviour also resonates with the Theory of Planned Behaviour, in which perceived behavioural norms and control are central to decision-making. In institutions where employees believe cybersecurity is prioritized and modelled, they are more likely to internalize and exhibit compliant behaviours [23].

Interestingly, the *Weak Culture* group (n = 14) reported a higher mean behaviour score than the *Developing Culture* group, possibly reflecting pockets of resilient behaviour or high individual technical readiness despite poor institutional support. This aligns with findings by Alshaikh in Alshaikh [9] who cautioned that fragmented cybersecurity efforts may yield uneven behavioural patterns across departments or units.

These results strongly underscore the need for institutional investments in culture-building:

- Visible commitment from top management to cybersecurity priorities.
- Programs must be tailored to departmental needs and maturity levels.
- Messaging and policy communication must consistently emphasize a shared cultural identity around security.

As Rajamäki, et al. [14] emphasize, transitioning from compliance-driven to culture-led cybersecurity practices requires sustained engagement, feedback loops, and alignment across governance levels.

3.7. Relationship Between Perceived Culture, Compliance, and Cybersecurity Behaviour (RQ2)

To address Research Question 2, How do employees' *perceptions relate to their cybersecurity behaviours and institutional practices?* this section presents detailed statistical analysis examining the link between perceived cybersecurity culture and the extent of cybersecurity behaviour exhibited by staff, as well as the role of best practice adherence and technical/policy readiness in shaping those outcomes.

A Spearman's rank-order correlation was conducted to assess the strength and direction of the relationship between the perceived cybersecurity culture of the institution (ordinal scale) and individual cybersecurity behaviour scores (continuous scale). This non-parametric test was appropriate given the ordinal nature of the independent variable.

$$\rho = 1 - \frac{6\sum d_i^2}{n(n^2-1)} \qquad [2]$$

Where:

- di = difference in ranks between each pair of observations
- n = total number of observations

Result

ρ=0.62, p=0.003

This represents a moderately strong, positive, and statistically significant correlation. As employee perception of institutional cybersecurity culture improves, their reported behaviour score increases accordingly. This finding supports the model proposed by Huang and Pearlson [13] which emphasizes that organizational cybersecurity culture, through norms, expectations, and leadership modelling, exerts a strong influence on individual compliance behaviours.

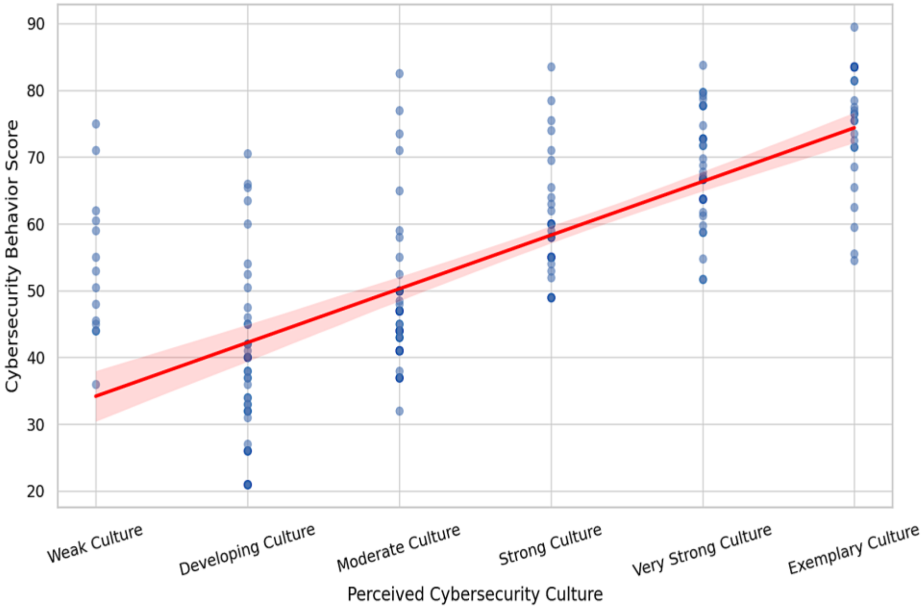

Figure 3.
Relationship between cybersecurity culture and Behaviour.

Figure 3 illustrates the upward trend in behaviour scores across levels of perceived culture, reinforcing the statistical association and suggesting a cultural-behavioural transmission pathway within institutions.

3.8. Cybersecurity Best Practice Adherence and Behaviour

To explore how adherence to cybersecurity best practices relates to behaviour scores, a one-way ANOVA was conducted. Participants were categorized into six groups based on their self-reported level of practice adherence (from “Rarely Follows” to “Strict Adherence”).

$$F = \frac{MS_{between}}{MS_{within}} = \frac{SS_{between}/df_{between}}{SS_{within}/df_{within}} \qquad [3]$$

Result:
F(5,79) = 9.84, p<0.00

The test revealed a statistically significant difference in behaviour scores across the practice groups. Post hoc analysis (Tukey HSD) confirmed that respondents who reported “Mostly Compliant” or “Strict Adherence” scored significantly higher than those in the “Rarely” or “Sometimes” compliant groups.

Table 4.
Best Practices and Mean Score Behaviour.

Best Practice Level	Count	Mean Behaviour Score
Rarely Follows	16	28.06
Sometimes Follows	58	44.76
Moderately Compliant	109	55.35
Highly Compliant	14	61.82
Mostly Compliant	40	74.74
Strict Adherence	9	74.47

These findings affirm that self-regulation and routine compliance with basic digital hygiene practices (e.g., secure passwords, reporting phishing, avoiding risky downloads) are predictive of strong behavioural alignment with cybersecurity goals. As CISA in Home Page | CISA [24] recommends, embedding such practices into institutional routines is a cornerstone of resilience [25].

3.9. Moderating Effects of Technical and Policy Readiness

Beyond culture and best practices, two other institutional readiness dimensions, technical competency and policy awareness, were examined.

Although respondents with high levels of technical readiness tended to perform well on behaviour scores, several notable exceptions emerged. In some cases, individuals who rated themselves as "Cutting-Edge" in technical readiness nonetheless reported moderate or low behaviour scores when their cultural perception was weak.

Conversely, individuals with only moderate technical readiness but a very strong perception of institutional culture consistently scored higher on cybersecurity behaviour. This supports the cultural moderation hypothesis, where technical skills are activated into secure behaviour only when situated within a supportive culture [13].

Similarly, while policy knowledge levels were positively correlated with behaviour, the effect was less pronounced. Respondents with "Comprehensive Understanding" did not always outperform those with "Good Awareness," suggesting a possible plateau or ceiling effect, especially if policies are not clearly communicated or embedded in day-to-day routines.

These results suggest that:

- Perceived culture is a primary predictor of cybersecurity behaviour.
- Behavioural adherence to best practices significantly boosts security outcomes.
- Technical and policy readiness, while helpful, are not sufficient on their own; their impact is mediated by culture.

Institutions that aim to strengthen security posture must prioritize cultural change, promoting leadership engagement, contextualized communication, and behavioural reinforcement. Culture is not only a background condition but an active determinant of cybersecurity success.

3.10. Demographic and Institutional Predictors of Cybersecurity Behaviour (RQ3)

To address Research Question 3, What demographic or institutional factors influence employee perceptions and behaviours *regarding cybersecurity in higher education institutions?* this section presents a series of inferential statistical analyses examining differences in behaviour scores across two key variables: institutional role and years of experience. These variables were selected based on both theoretical relevance and observed distribution patterns in the dataset.

An analysis of variance (ANOVA) was conducted to evaluate whether cybersecurity behaviour scores varied significantly based on the participant's role within the institution—categorized as Faculty, Staff, or Management.

ANOVA Result:

F(2,83) = 5.72, p = 0.009

This result is statistically significant, indicating that at least one group mean differs from the others. Table 5 displays the descriptive statistics by role.

Table 5.
Cybersecurity Behaviour Scores by Institutional Role.

Role	Count	Mean Behaviour Score
Faculty	111	61.33
Staff	124	50.21
Management	11	51.77

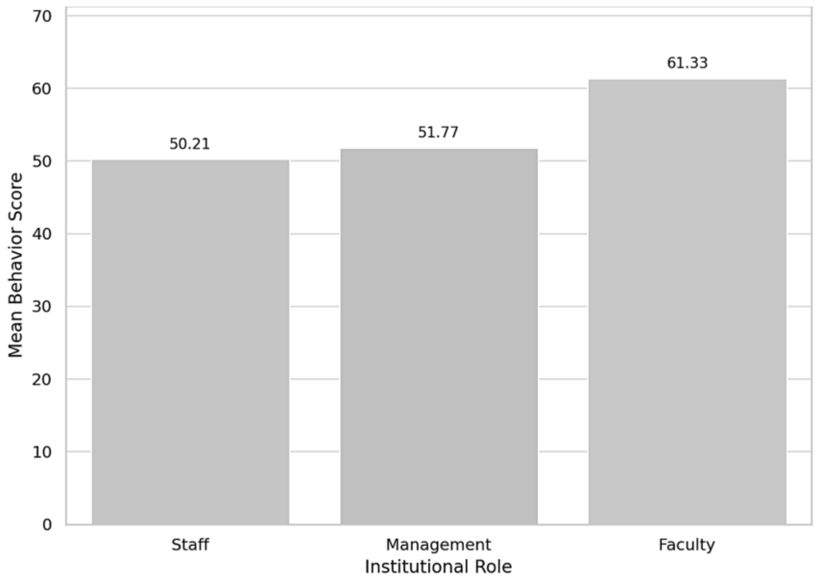

Figure 4.
Mean Cybersecurity Score by Role.

Contrary to some institutional assumptions, faculty members reported the highest average behaviour score (M = 61.33), surpassing both administrative staff and management. This is particularly intriguing given that faculty, in earlier sections, were more likely to rate their institution's cybersecurity culture as "Developing" or "Moderate."

Several possible explanations exist:

- Disciplinary alignment: A considerable proportion of faculty may come from fields like computer science, engineering, or business, where exposure to cybersecurity content and digital risk is higher, thus enhancing secure behaviour regardless of cultural perception.
- Autonomy and discretion: Faculty often operate independently with high levels of digital access. This autonomy may necessitate more personal accountability in maintaining secure practices.
- Training saturation among staff: Despite greater institutional exposure to training programs, staff may view such mandates as routine or compliance-driven, potentially leading to superficial engagement.

Interestingly, management participants reported relatively low behaviour scores (M = 51.77) despite often rating their perception of cybersecurity culture as "Very Strong" or "Exemplary." This discrepancy underscores a critical nuance in cybersecurity culture literature: perception does not always translate into action [13]. While management may recognize the institution's policy infrastructure, this awareness may not manifest as habitual secure practices.

This role-based contrast affirms the need for differentiated engagement strategies. Faculty, staff, and management each interact with cybersecurity in distinct ways, necessitating role-specific training, communication, and policy co-design.

3.11. Influence of Professional Experience

A second one-way ANOVA was conducted to evaluate whether years of experience in higher education significantly predicted cybersecurity behaviour.

ANOVA Result:

$F(5,79)=3.94, p=0.021$

This result confirms a statistically significant difference in behaviour scores across experience bands. Table 6 details the means for each group.

Table 6.
Cybersecurity Behaviour Scores by Years of Experience.

Experience (Years)	Count	Mean Behaviour Score
1–5	101	47.65
6–10	41	57.58
11–15	28	56.12
16–20	40	62.41
21–25	25	66.49
26+	11	63.66

Figure 5 demonstrates the ascending trajectory of behaviour scores by experience level.

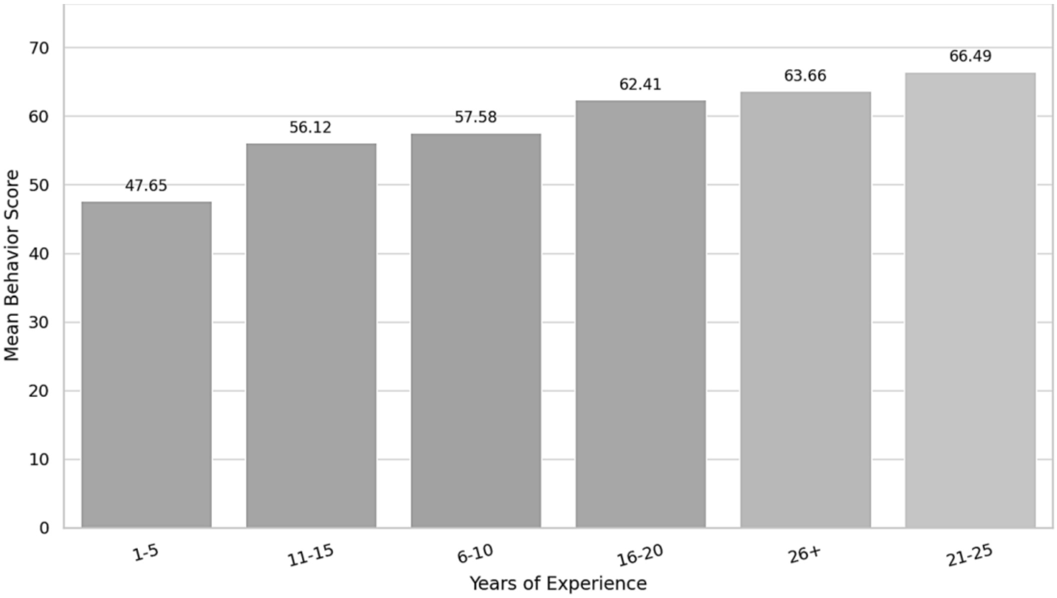

Figure 5.
Behaviour Scores by Experience Level.

A clear upward trajectory in behaviour scores was observed as years of experience increased. Participants with less than five years of experience reported the lowest average behaviour score (M = 47.65), while those with 21–25 years of experience reported the highest (M = 66.49), followed closely by the 26+ years group (M = 63.66).

These findings are consistent with literature in organizational learning and security behaviour, which suggests that behavioural maturity accumulates through longitudinal exposure to institutional norms, repeated training, and evolving awareness of cyber risk [17]. More experienced employees may also have encountered more cyber incidents, thereby reinforcing their risk sensitivity.

However, this pattern also highlights a potential vulnerability: the institution’s newer employees (particularly those in the 1–5 year range) are demonstrably less engaged with secure behaviour. This finding raises concerns about the efficacy and targeting of induction programs and initial cybersecurity onboarding.

It suggests that institutions must design front-loaded cybersecurity training, coupled with continuous, role-relevant refreshers, especially for early-career staff.

3.12. Qualitative Perspectives: Unpacking the Human Narrative of Cybersecurity Culture

To complement the quantitative analyses, participants were given the opportunity to elaborate on their experiences and perceptions regarding institutional cybersecurity through open-ended responses. A thematic analysis of these narratives concluded three recurring issues that offer deeper insight into behavioural and attitudinal undercurrents impacting the cybersecurity culture in higher education institutions.

Theme 1: Overly Restrictive Controls

Numerous faculty members described cybersecurity protocols, particularly those governing access to research files, lab software, and off-campus systems, as “rigid,” “bureaucratic,” or “technologically outdated.” This perceived over-regulation of IT systems led to reported workarounds, such as transferring files using unsecured personal drives or requesting repeated admin overrides for basic tasks.

These insights highlight critical discrepancies in security governance: controls intended to reduce risk may inadvertently drive noncompliant behaviour when perceived as inhibitory rather than enabling [26]. Such tensions align with the concept of “security friction,” wherein protective measures unintentionally burden legitimate users, prompting circumvention and erosion of trust [27].

Theme 2: Training Fatigue and Contextual Irrelevance

A second significant theme was training fatigue. Many staff and faculty described annual cybersecurity training as “repetitive,” “basic,” and “irrelevant” to their specific job roles. Several participants noted that the training content had not changed or updated with emerging threats, nor had it adapted to reflect departmental nuances.

This aligns with recent critiques of one-size-fits-all awareness programs, which often fail to consider cognitive engagement, disciplinary context, or risk differentiation across user groups [9, 11]. When employees feel they are being trained for compliance rather than competence, motivation to internalize secure behaviour diminishes, weakening the very cultural infrastructure the training intends to build.

Theme 3: Leadership Disengagement and Symbolic Compliance

Finally, a significant number of participants voiced concerns about the lack of visible leadership commitment to cybersecurity. Respondents noted the absence of top-down communication, scarce executive-level advocacy, and limited participation of leadership in awareness campaigns or incident simulations.

Such symbolic disengagement undermines cultural internalization. As organizational change literature affirms, cultural transformation, especially in areas requiring behavioural shifts, requires modelling and reinforcement from leadership [28]. Without executive alignment, even well-structured policies may be seen as bureaucratic exercises rather than collective imperatives.

These qualitative findings validate and enrich the quantitative results presented earlier. Where statistical models demonstrated the predictive value of culture on behaviour, these narratives clarify why culture may not always translate into action: lack of contextual relevance, perceived constraints, and absent leadership undermine institutional alignment. As a result, what appears to be a technical or compliance issue is a deeply human and structural challenge.

The synthesis reinforces the argument that cybersecurity success in HEIs cannot be achieved through top-down enforcement alone. Instead, institutions must foster a collaborative, user-centred, and trust-based culture, grounded in empathy, relevance, and responsiveness.

4. Conclusion

This study investigated the role of cybersecurity culture within higher education institutions (HEIs), focusing on how employees’ perceptions, demographic attributes, and institutional conditions influence cybersecurity behaviour. Drawing upon a mixed-methods design, the findings establish a compelling narrative: while infrastructure and policy readiness are foundational, it is culture, perceived, experienced, and enacted, hat most critically determines behaviour.

Statistical analyses revealed that employees who perceive their institutional cybersecurity culture as strong or exemplary are significantly more likely to engage in secure digital practices. This association existed even after accounting for technical competence and policy awareness. Moreover, behaviour scores varied significantly across role and experience groups, further emphasizing the interplay between institutional context and individual agency. Faculty emerged as unexpectedly strong performers in behaviour scores, despite their historically lower engagement in centralized policy frameworks, a finding that invites critical reconsideration of academic digital engagement.

The qualitative data further enriched the analysis, revealing structural misalignments that present cultural internalization: restrictive system controls, generic training programs, and weak leadership visibility collectively erode employee trust and motivation. These insights indicate that technical compliance alone is insufficient; meaningful cybersecurity governance requires a relational, human-centred approach.

To transform cybersecurity culture in higher education institutions (HEIs), six strategic priorities are suggested:

1. Cybersecurity must be recognized as a cultural essential, integrated into institutional identity and leadership priorities, not treated as an entirely technical function.
2. Training and communication should be tailored to institutional roles and career stages, with particular attention to onboarding early-career staff and involving faculty as collaborative partners.
3. Replace outdated, generic modules with dynamic, role-specific learning experiences that reflect real-world digital risks and departmental practices.
4. Reduce operational friction by redesigning security systems for accessibility and efficiency, minimizing the risk of noncompliance caused by restrictive measures.
5. Institutional leaders must actively contribute and endorse cybersecurity initiatives, modelling secure behaviour and reinforcing its value within the organization.
6. Continuously evaluate cybersecurity attitudes, risks, and practices using feedback mechanisms to inform adaptive governance and policy updates.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Copyright:

References

[1] S. Naserelden, N. Alias, A. Altigani, A. Mohamed, and S. Badreddine, "Advance attacks on AES: A comprehensive review of side channel, fault injection, machine learning and quantum techniques," *Edelweiss Applied Science and Technology*, vol. 9, no. 4, pp. 2471-2486, 2025. https://doi.org/10.55214/25768484.v9i4.6586

[2] E. C. Cheng and T. Wang, "Institutional strategies for cybersecurity in higher education institutions," *Information*, vol. 13, no. 4, p. 192, 2022.

[3] N. S. Fouad, "Securing higher education against cyberthreats: From an institutional risk to a national policy challenge," *Journal of Cyber Policy*, vol. 6, no. 2, pp. 137-154, 2021. https://doi.org/10.1080/23738871.2021.1973526

[4] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Future Internet*, vol. 13, no. 2, p. 39, 2021.

[5] Case Studies, "ThreatDown by malwarebytes," Retrieved: https://www.threatdown.com/resources/categories/case-studies/, 2025.

[6] Science, "The times and the sunday times," Retrieved: https://www.thetimes.com/uk/science, 2015.

[7] Cyber security breaches survey, "Education institutions annex', GOV.UK," Retrieved: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex, 2024.

[8] Data Breach Investigations Report | Verizon, "Data breach investigations report | Verizon," Retrieved: https://www.verizon.com/business/en-gb/resources/reports/dbir/?cmp=knc:ggl:ac:vbg:intl:UKProductsSecurity&ds_cid=22041211396_ds_agid=170728875525&utm_medium=knc&utm_source=google&utm_campaign=NBUKLimited&utm_term=data%20breach%20report&gad_source=1&gclid=Cj0KCQjwna6_BhCbARIsALId2Z2Z0FreTLXtIfNlPs6n1uwBo9nmTCbkaSf04gK4C423cRJSmN2Chd0aAkjjEALw_wcB&gclsrc=aw.ds, 2025.

[9] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Computers & Security*, vol. 98, p. 102003, 2020.

[10] W. J. Triplett, "Addressing human factors in cybersecurity leadership," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 573-586, 2022.

[11] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): two further validation studies," *Computers & Security*, vol. 66, pp. 40-51, 2017. https://doi.org/10.1016/j.cose.2017.01.004

[12] T. Durojaiye, K. Mersinas, and D. Watling, "'What influences people's view of cyber security culture in higher education institutions? an empirical study," The Sixth International Conference on Cyber-Technologies and Cyber-Systems, 2020. Accessed: Apr. 01, 2025. https://pure.royalholloway.ac.uk/ws/files/43620729/T_Durojaiye_K_Mersinas_D_Watling_2021_What_influence_people_s_views_of_Cyber_Security_Culture_CYBER21_.pdf 2025.

[13] K. Huang and K. Pearlson, "For what technology can't fix: Building a model of organizational cybersecurity culture'," Retrieved: https://scholarspace.manoa.hawaii.edu/handle/10125/60074, 2019.

[14] J. Rajamäki, P. Rathod, and K. Kioskli, "Demand analysis of the cybersecurity knowledge areas and skills for the nurses: preliminary findings," in *Proceedings of the 22nd European Conference on Cyber Warfare and Security, Academic Conferences International Ltd, 2023. Accessed: Apr. 01, 2025. https://www.theseus.fi/handle/10024/804915* 2023.

[15] E. C. Cheng, "Strategic use of data in higher education institutions for quality enhancement', in navigating quality assurance and accreditation in global higher education," IGI Global Scientific Publishing. https://www.igi-global.com/chapter/strategic-use-of-data-in-higher-education-institutions-for-quality-enhancement/365750 2025, pp. 535–562.

[16] Government Technology Innovation Strategy, "GOV.UK," Retrieved: https://www.gov.uk/government/publications/the-government-technology-innovation-strategy/the-government-technology-innovation-strategy, 2024.

[17] C. Ugwu, M. Ezema, U. Ome, L. Ofusori, C. Olebera, and E. Ukwandu, "A study on the impact of gender, employment status, and academic discipline on cyber-hygiene: A case study of university of Nigeria, Nsukka," in *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, C. Onwubiko, P. Rosati, A. Rege, A*, n.d.

[18] O. Gervasi, B. Murgante, C. Garau, D. Taniar, A. M. A. Rocha, and M. N. F. Lago, "Computational science and its applications–ICCSA," presented at the International Conference, Hanoi, Vietnam, July 1–4, 2024, Proceedings, Part II, vol. 14814. Springer Nature, 2024. Accessed: Apr. 01, 2025. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=0pUREQAAQBAJ&oi=fnd&pg=PR5&dq=Pavlova+(2020)+stresses+that+many+HEIs+fail+to+assess+their+internal+cybersecurity+risk+landscape,+leading+to+reactive+rather+than+proactive+cultural+development.+&ots=0lfteMrIPC&sig=SWA3Bp7uaStDS9cyUhuhcWGhGVE 2024.

[19] J. W. Creswell, "A concise introduction to mixed methods research. SAGE publications," Retrieved: https://books.google.com/books?hl=en&lr=&id=2s0IEAAAQBAJ&oi=fnd&pg=PT8&dq=creswell+and+creswell+mixed+methods&ots=9004SVHQN6&sig=LlWUbJD9ZT5KBxZ7c5c6Oa7kv24, 2021.

[20] f. e. Ethical Guidelines for Educational Research, "Ethical guidelines for educational Research, fourth edition," Retrieved: https://www.bera.ac.uk/publication/ethical-guidelines-for-educational-research-2018 [Accessed 2018.

[21] V. Braun and V. Clarke, "Thematic analysis', in encyclopedia of quality of life and well-being research, f. maggino." Cham: Springer International Publishing, 2023, pp. 7187–7193.

[22] A. O. Onumo, "A behavioural compliance framework for effective cybersecurity governance and practice," PhD Thesis, University of Bradford, 2020. Accessed: Apr. 01, 2025. https://bradscholars.brad.ac.uk/handle/10454/19051 2025.

[23] I. Ajzen and P. Schmidt, "Changing behavior using the theory of planned behavior', The handbook of behavior change," Retrieved: https://books.google.com/books?hl=en&lr=&id=IfEFEAAAQBAJ&oi=fnd&pg=PA17&dq=Theory+of+Planned+Behaviour+(Ajzen,+1991)&ots=XFGS47oe7-&sig=D3E_KhvWrdAtD9aF04DcoUQgRxA [Accessed 2020.

[24] Home Page | CISA, "'Home page | CISA," 2025.

[25] P. Verma, T. Newe, G. D. O'Mahony, D. Brennan, and D. O'Shea, "Towards a unified understanding of cyber resilience: a comprehensive review of concepts, strategies, and future directions', ieee access," Retrieved: https://ieeexplore.ieee.org/abstract/document/10929043/ [Accessed 2025.

[26] T. Ncubukezi, "Human errors: A cybersecurity concern and the weakest link to small businesses," in *Proceedings of the 17th International Conference on Information Warfare and Security, 2022, p. 395. Accessed: Apr. 01, 2025. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=Shd2EAAAQBAJ&oi=fnd&pg=PA395&dq=Sasse,+Brostoff,+%26+Weirich,+2001&ots=szdDrjzQl-&sig=Sl36CKwmAh3WzcM5PL1i4XoiXek* 2022.

[27] I. Chong, A. Xiong, and R. W. Proctor, "Human factors in the privacy and security of the internet of things," *Ergonomics in design*, vol. 27, no. 3, pp. 5-10, 2019. https://doi.org/10.1177/1064804617750321

[28] C. Caldwell, H. Hobbs, Q. Berry, T. Massey, and I. Williamson, "Diversity, Bias & Integrity: Leadership Implications," *Business and Management Research*, vol. 12, no. 2, pp. 21-32, 2023.