Ngr. J. Multi. vol-2, issue-8 (Aug-2026) pp-454-467

ISSN: 3108-2750 (E), 3139-8065 (P)

Nexus Global Research Journal of Multidisciplinary

Journal Homepage: https://nexusglobalresearch.com/journal/ngrjm/

Research Article

Student Awareness as Basis for Developing Cybersecurity Program for Avionics Technology

Manuel Luke G. Aritcheta [1*], Prof. Andrew C. Caronongan [2]

[1] Assistant Professor I, Avionics Technology Department, WCC Aeronautical & Technological College – Binalonan, Philippines

[2] Professor, Master in Information Technology Major in Cybersecurity Program, Graduate School, University of Luzon, Dagupan City, Philippines

ABSTRACT:

The digital transformation of the aviation sector necessitates rigorous cybersecurity standards; however, a critical awareness-action gap persists among emerging professionals. This study addressed this imperative by assessing the level of cybersecurity awareness among Avionics Technology students at WCC Aeronautical & Technological College - Binalonan to serve as the empirical foundation for a structured institutional intervention. Employing a hybrid methodology that combined a descriptive survey with elements of Design Science Research, the study was aligned with ISO/IEC 27001:2022 standards. Quantitative data was gathered from one hundred targeted students utilizing a structured 5-point Likert scale evaluation instrument. This tool systematically measured student awareness across four specific threat domains: password management-related issues, social engineering threats, malicious software and wireless network attacks, and endpoint device security. The empirical findings revealed a systemic operational deficiency. While students possessed foundational theoretical knowledge such as effectively recognizing deceptive phishing tactics (mean 4.10) they lacked practical technical defense capabilities. Students exhibited a dangerous reliance on human memory by drastically underutilizing secure encrypted password managers (mean 1.85) and demonstrated alarming vulnerabilities regarding unencrypted wireless network transmissions (mean 2.65). Conversely, the respondents expressed an overwhelming demand for structured, standardized training modules (composite mean 4.78). To rectify these empirical vulnerabilities, the research culminated in the formulation of the Cybersecurity Program for Avionics Technology. This fully operational training architecture integrates standardized vaulting protocols, active threat simulations, and endpoint hardening. Aligned with United Nations Sustainable Development Goals 4: Quality Education and 9: Industry, Innovation, and Infrastructure, this programmatic intervention actively bridges the awareness-action gap, ensuring future graduates enter the industry as highly secure guardians of critical aerospace infrastructure.

Keywords: Student Awareness, Basis, Developing, Cybersecurity Program, Avionics Technology

Citation: Aritcheta, M. L. G., & Caronongan, A. C. (2026). Student awareness as basis for developing cybersecurity program for avionics technology. Nexus Global Research Journal of Multidisciplinary, 2(8), 454–467.

INTRODUCTION:

The digital transformation of the global aviation sector has fundamentally altered how emerging professionals interact with critical technical infrastructure. Modern aircraft maintenance, flight log management, and avionics diagnostic systems are now inextricably linked to complex digital networks and cloud-based databases. Securing these digital perimeters and protecting highly sensitive data has emerged as a critical operational imperative across the international aerospace industry. Consequently, robust cybersecurity awareness is no longer merely an academic recommendation; it is an absolute global requirement. To ensure the resilience of aviation networks against sophisticated cyber threats, educational frameworks must align with the United Nations Sustainable Development Goals 4: Quality Education and 9: Industry, Innovation, and Infrastructure to foster an environment of proactive digital defense.

Within this contemporary landscape, the human element remains the most critical vulnerability. While cryptographic alphanumeric credentials serve as the primary gateway defense, traditional password management policies frequently conflict with human memory capabilities. The stringent requirements for high cryptographic entropy impose an unsustainable cognitive strain, frequently driving high-risk behavioral compromises such as severe

***Corresponding Author:** Manuel Luke G. Aritcheta, Email: avtprof.ml.aritcheta@gmail.com

Received: 05 Aug 2026 | **Accepted:** 20 Aug 2026 | **Published:** 25 Aug 2026

cross-platform credential reuse (Knott & Steube, 2012; Shinde & Deshpande, 2022). Furthermore, modern threat actors increasingly exploit these human limitations through social engineering and deceptive digital tactics, bypassing technical perimeters entirely. This risk is further compounded by localized technical threats, specifically malicious software vulnerabilities, unsecured wireless networks, and the physical compromise of endpoint devices. Protecting institutional data requires addressing this entire spectrum of vulnerabilities.

Avionics Technology students are at a significantly elevated risk within this evolving digital environment. Their highly specialized curriculum requires perpetual interaction with secure university portals, learning management systems, and proprietary aviation diagnostic software. While these students often recognize the inherent vulnerabilities of cyberspace, a profound awareness-action gap persists. They may possess foundational knowledge of cyber threats yet fail to translate this theoretical understanding into secure daily practices. Furthermore, many educational institutions currently lack the proactive, experiential training frameworks necessary to transition students from passive awareness to functional operational defense (Moallem, 2018). Without active technological countermeasures and structured education, the digital identities of these future aviation professionals remain critically exposed.

Addressing this localized vulnerability is an institutional imperative. Therefore, this research empirically investigates the cybersecurity awareness among the Avionics Technology student cohort at WCC Aeronautical and Technological College - Binalonan. By systematically evaluating their understanding of password management, social engineering threats, malicious software, and endpoint device security, the study seeks to definitively quantify their digital readiness. Ultimately, utilizing a descriptive-quantitative methodology structurally aligned with global standards such as ISO/IEC 27001:2022, this study aims to serve as an empirical baseline for the formulation of a comprehensive cybersecurity program. This targeted institutional intervention is designed to systematically mitigate cyber risks and engineer a permanent culture of cyber resilience within the department.

Statement of the Problem

This study aimed to primarily investigate on the awareness of cybersecurity-related issues among Avionics Technology students of WCC Aeronautical & Technological College - Binalonan in order to serve as an empirical baseline for formulating a cybersecurity program in mitigating risks associated to cybersecurity attacks in the educational institution. Specifically, it sought to answer the following questions:

1. What is the level of awareness of the Avionics Technology students in addressing the following cybersecurity threats in the educational institution:

a. Password management-related issues;

b. Social engineering threats and deceptive digital tactics;

c. Malicious software vulnerabilities and wireless network attacks; and

d. Endpoint device security

2. What comprehensive cybersecurity program can be developed to systematically mitigate cyber threats among avionics technology students?

Scope and Delimitation

The primary parameter of this research was bounded by the assessment of digital threat awareness and the subsequent formulation of institutional countermeasures, as encapsulated in the study's title: Student Awareness as Basis for Developing Cybersecurity Program for Avionics Technology. To achieve this, the study's subject matter was strictly confined to evaluating the respondents' level of awareness concerning four specific digital threat domains:

a. Password management-related issues;

b. Social engineering threats and deceptive digital tactics;

c. Malicious software vulnerabilities and wireless network attacks; and

d. Endpoint device security.

Crucially, a significant portion of this research encompassed the development of its definitive output. The empirical data extracted from the aforementioned assessments served as the scientific and structural baseline for designing the comprehensive cybersecurity program. The scope included the systematic drafting and academic alignment of these programmatic frameworks to ensure they effectively mitigated the specific cyber threats identified among the student body.

Demographically, the study focused exclusively on the Avionics Technology students enrolled at WCC Aeronautical & Technological College - Binalonan due to the critical nature of aeronautical technologies and the necessity of instilling advanced digital hygiene among future aviation professionals. Consequently, to maintain empirical focus, faculty members, administrative staff, and students from other academic programs were strictly excluded from the respondent pool. Technically, the research utilized a descriptive-quantitative design focusing on theoretical threat awareness and human-centric cyber behaviors. Therefore, the study was strictly non-intrusive; it did not involve active network penetration testing, digital forensics, vulnerability scanning of the institution's internal IT infrastructure, or the execution of simulated cyber-attacks. Finally, the researcher's parameter was limited strictly to the formulation of the cybersecurity program. The actual institutional enforcement, mandatory integration of this program into official university policies, and longitudinal auditing of its effectiveness fell beyond the jurisdiction of this study and were relegated as recommendations for future administrative action.

Significance of the Study

The culmination of this research, specifically the development of the cybersecurity program, offers profound practical, institutional, and academic value. The empirical data gathered regarding the students' awareness of digital vulnerabilities and the subsequent programmatic countermeasures formulated will directly benefit the following entities:

WCC Aeronautical & Technological College - Binalonan. The findings and the resulting cybersecurity program will directly equip the institution with an evidence-based framework to safeguard its digital ecosystem. By adopting the comprehensive countermeasures formulated in this study, the college can significantly mitigate human-centric cyber vulnerabilities among its student body, thereby protecting vital institutional databases, learning management systems, and academic records against the growing prevalence of digital exploitations.

Avionics Technology Students. As the primary subjects and immediate beneficiaries of this research, these students will gain access to a tailored, data-driven program designed to fortify their digital hygiene. It is imperative for students to be highly knowledgeable about data privacy and system defense; thus, this study empowers them with the exact protocols needed to manage credentials securely, recognize social engineering tactics, mitigate malicious software vulnerabilities, and secure their endpoint devices against contemporary cyber threats.

Cybersecurity Practitioners. The empirical baseline established by this study provides valuable socio-technical insights into the cybersecurity awareness levels of users within a highly specialized, non-IT sector like avionics. Security practitioners and IT administrators can utilize this data to understand specific user vulnerabilities and theoretical knowledge gaps, allowing them to design more intuitive authentication architectures and deploy targeted security awareness campaigns across similar technical industries.

Aviation Maintenance Specialists. Modern aviation relies heavily on interconnected digital systems, diagnostic software, and automated flight networks. The rigorous cyber hygiene habits instilled by the output of this study will prepare these future aviation professionals to secure critical aeronautical infrastructures. By internalizing the principles of this cybersecurity program, emerging specialists ensure that human error does not become the weak link in the highly targeted aviation industry's cyber defense.

To ensure a precise and comprehensive understanding of the core concepts investigated in this study, the following terms are conceptually and

operationally defined strictly based on their application within the context of the research:

Student Awareness

Operationally, this refers to the theoretical comprehension and practical recognition of contemporary digital threats possessed by the respondents. In this study, it is the primary empirical metric evaluated to serve as the baseline for developing institutional countermeasures.

Cybersecurity Program

Operationally, this refers to the definitive academic output of this research (SOP 2). It is a structured, data-driven framework of institutional protocols, training guidelines, and countermeasures scientifically formulated based on the empirical baseline of the students to mitigate human-centric cyber risks.

Avionics Technology Students

Operationally, this refers to the specific demographic of individuals currently enrolled at WCC Aeronautical & Technological College - Binalonan. They serve as the primary respondents of the study whose level of cybersecurity awareness is empirically measured.

Password Management-Related Issues

Conceptually and operationally, this encompasses the vulnerabilities and behaviors associated with digital authentication credentials. In this study, it measures the respondents' awareness regarding the creation, cryptographic complexity, utilization, secure storage, and the risks of reusing passwords across different platforms.

Social Engineering Threats and Deceptive Digital Tactics

Conceptually and operationally, this refers to the psychological manipulation methodologies utilized by cybercriminals to deceive users into voluntarily disclosing confidential data. In this study, it evaluates the students' capacity to identify and avoid malicious schemes such as phishing and identity spoofing.

Malicious Software Vulnerabilities and Wireless Network Attacks

Conceptually and operationally, this encompasses the respondents' understanding of destructive digital payloads such as malware, ransomware, and spyware combined with their recognition of the risks associated with unauthorized intrusions over unsecured or public wireless connections.

Endpoint Device Security

Conceptually and operationally, this pertains to the respondents' awareness regarding the protection of user-accessed hardware. It specifically measures their understanding of how to secure mobile devices, laptops, and avionics workstations against unauthorized physical access, unverified hardware peripherals, and localized breaches.

DESIGN AND METHODOLOGY:

Research Design

This study employed a descriptive-quantitative research design to systematically measure, quantify, and analyze the level of awareness in addressing cybersecurity threats among the target population. This methodological framework is highly appropriate for the investigation because it facilitates the objective collection of empirical data concerning the students' theoretical comprehension and practical recognition of cyber vulnerabilities without manipulating the natural research environment. By utilizing a highly structured quantitative approach, the researcher was able to establish a statistically reliable baseline of the human-centric vulnerabilities present within the academic institution.

Rather than relying on subjective qualitative observation, this quantitative design rigorously assesses specific cybersecurity threat vectors. It mathematically evaluates the students' awareness across four distinct domains: password management-related issues, social engineering threats and deceptive digital tactics, malicious software vulnerabilities and wireless network attacks, and endpoint device security. By statistically defining the precise severity of these behavioral and cognitive gaps, this research design provides the exact empirical foundation required to formulate and develop the proposed comprehensive cybersecurity program for Avionics Technology students.

Program Development and Methodology

Because this study produces a structured institutional policy and educational framework rather than an engineered software application, traditional software development life cycles such as the Waterfall model were not applicable. Instead, the methodological architecture of this study is anchored on a clean combination of a Descriptive Survey method and elements of Design Science Research (DSR), heavily based on ISO/IEC 27001 information security standards.

To visualize this procedural engine, Figure 1 illustrates the linear progression of the methodology, ensuring that empirical data collection strictly dictates the conclusive formulation of the research output.

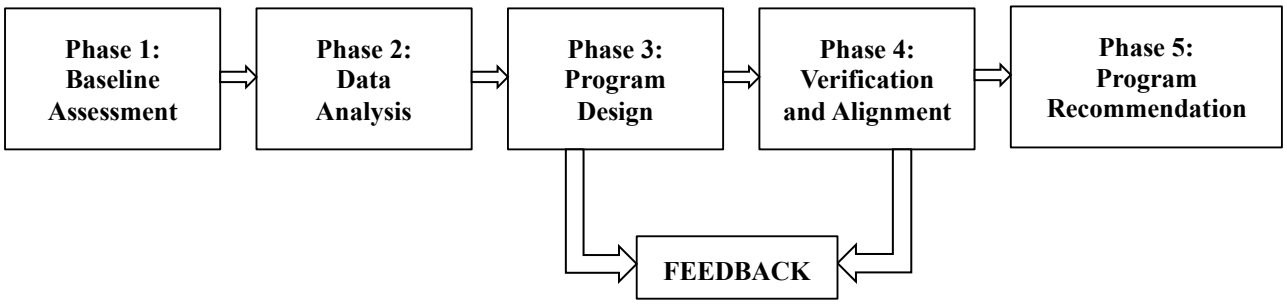

Figure 1. The Methodological Framework for Program Development

This hybrid framework functions through a strict progression outlined as follows:

1. Problem Identification and Baseline Assessment

This initial stage established the foundational baseline of the study by executing the descriptive survey. The researcher engineered and deployed a highly structured, quantitative evaluation instrument utilizing a 5-point Likert scale. This instrument objectively operationalized the identified variables, systematically measuring the students' awareness levels regarding password management, social engineering, malicious software, and endpoint vulnerabilities.

2. Data Analysis and Objective Definition Phase

During this stage, rigorous statistical treatment was applied to the gathered survey data. This phase mathematically defined the specific behavioral vulnerabilities, theoretical gaps, and critical security needs among the student population. By indexing the students' theoretical knowledge against their practical susceptibilities, the researcher translated raw data into clear, actionable objectives for institutional intervention.

3. Program Design and Development Phase

Utilizing the statistical findings from the analysis stage, the researcher systematically drafted the comprehensive cybersecurity program. Applying the principles of Design Science Research, the targeted countermeasures, educational modules, and institutional protocols were engineered to directly address and mitigate the exact empirical vulnerabilities identified among the Avionics Technology student body.

4. Verification and ISO 27001 Alignment Phase

To ensure rigorous academic and industry compliance, the drafted cybersecurity program and its countermeasure protocols were not formulated in a vacuum. They were systematically cross-referenced against the ISO / IEC 27001 information security management standards. This verification guaranteed that the proposed program met the stringent demands of global aviation data security best practices.

5. Program Recommendation and SDG Integration

The workflow culminates in the definitive recommendation of the comprehensive cybersecurity program. Significantly, this procedural methodology and the resulting strategic countermeasures are intrinsically aligned with the United Nations Sustainable Development Goals (SDGs). By pioneering a formalized culture of cyber vigilance, the study directly supports SDG 4: Quality Education, while its rigorous emphasis on resilient data privacy protocols for aviation databases advances SDG 9: Industry, Innovation, and Infrastructure.

Data Gathering Techniques

To systematically execute this quantitative study, the researcher employed a purposive sampling technique, strategically selecting one hundred (100) students currently enrolled in the Avionics Technology program at WCC Aeronautical & Technological College - Binalonan. This specific demographic was deliberately targeted due to their rigorous academic curriculum and their systematic, early exposure to advanced, interconnected aviation infrastructures. As emerging aviation maintenance specialists, these students will inevitably manage highly sensitive flight management databases and diagnostic networks. Consequently, establishing an empirical baseline of their cybersecurity awareness is critical to preserving the digital integrity of the broader aviation industry.

The primary tool for empirical data elicitation was a highly structured, descriptive-quantitative evaluation instrument. Strictly adhering to the quantitative nature of the research design, the instrument utilized a standardized 5-point Likert scale to eliminate ambiguous responses and ensure robust statistical treatment. This instrument was explicitly designed to operationalize the core variables of the study: measuring the students' level of awareness across four specific domains, namely password management-related issues, social engineering threats and deceptive digital tactics, malicious software vulnerabilities and wireless network attacks, and endpoint device security. Additionally, the instrument included a targeted feature preference assessment to determine the recommended training components for the definitive output.

To guarantee international academic rigor and industry validity, the formulation of the evaluation instrument was primarily anchored to the globally recognized ISO/IEC 27001:2022 standards. Specifically, the instrument integrated targeted security controls from the ISO/IEC 27002:2022 framework to accurately and empirically measure student awareness. Annex A Control 5.17 (Authentication Information) was operationalized to rigorously evaluate the students' recognition of risks regarding the secure generation, strict management, and encrypted storage of user credentials. Concurrently, Annex A Control 6.3 (Information Security Awareness, Education, and Training) was utilized to empirically measure the respondents' theoretical knowledge and practical susceptibility to the prevailing cyber threats, specifically assessing their defense against social engineering, malicious network intrusions, and localized endpoint vulnerabilities.

By meticulously aligning the data gathering techniques with these international standards and deploying the instrument to a precisely targeted academic population, the researcher ensured the resulting data was both statistically sound and directly applicable to formulating the proposed comprehensive cybersecurity program for Avionics Technology students.

Ethical Considerations

Given the highly sensitive nature of investigating cybersecurity vulnerabilities and digital hygiene, this study was executed with the utmost adherence to empirical research ethics and statutory data protection mandates, specifically Republic Act No. 10173, also known as the Data Privacy Act of 2012. The researcher implemented strict ethical protocols to ensure that the deployment of the evaluation instrument protected the dignity, rights, and digital safety of the Avionics Technology student respondents at WCC Aeronautical & Technological College - Binalonan.

Informed Consent and Voluntary Participation

Prior to the administration of the 5-point Likert scale evaluation instrument, explicit informed consent was systematically obtained from all one hundred (100) targeted respondents. The respondents were

comprehensively briefed regarding the academic purpose of the study, the specific variables being measured namely, their level of awareness regarding password management-related issues, social engineering threats, malicious software vulnerabilities, and endpoint device security and the ultimate goal of developing the proposed cybersecurity program. Participation was strictly voluntary. The students were explicitly assured that their decision to participate, decline, or withdraw from the study at any juncture would yield no adverse impact on their academic standing or institutional evaluation.

Data Confidentiality and Cryptographic Anonymity

A paramount ethical imperative of this research was ensuring that the data gathering procedure did not introduce new cyber vulnerabilities to the student population. The evaluation instrument was strictly engineered to measure the students' level of cybersecurity awareness rather than extracting sensitive operational data. The researcher explicitly guaranteed that no actual passwords, cryptographic keys, personal identification numbers (PINs), or specific user account details were requested, recorded, or stored at any phase of the study. All gathered quantitative data were aggressively anonymized, ensuring that no specific set of empirical vulnerabilities or knowledge gaps could be traced back to an individual student's identity.

Beneficence and Non-Maleficence

The study was fundamentally guided by the ethical principles of beneficence maximizing benefits and non-maleficence inflicting no harm. The research was designed not to expose or penalize the respondents for poor digital hygiene or a lack of awareness, but rather to empirically identify theoretical and practical gaps to construct a targeted, protective educational program. By strictly aligning the methodology with the United Nations Sustainable Development Goals 4: Quality Education and 9: Industry, Innovation, and Infrastructure, the ultimate ethical objective of this research remains entirely constructive: to pioneer a formalized culture of cyber vigilance that actively safeguards the Avionics Technology student body and fortifies the broader digital infrastructure of the aviation industry against contemporary human-centric threats.

RESULTS AND DISCUSSIONS:

The statistical analysis of the empirical data gathered from one hundred (100) Avionics Technology students at WCC Aeronautical & Technological College - Binalonan reveals profound insights into their digital behaviors and cognitive threat recognition. Utilizing the highly structured, ISO-aligned 5-point Likert scale evaluation instrument, the data exposes a critical operational gap between the respondents' theoretical cybersecurity knowledge and their practical digital defense capabilities. The findings are structurally organized into two master segments, directly addressing the specific problems of the study.

A. Password Management-Related Issues

The first domain evaluated the students' awareness regarding the vulnerabilities associated with credential creation, cross-platform reuse, and unencrypted storage mechanisms. This assessment measures whether students recognize the severe risks embedded in their daily authentication habits.

Table 1. **Level of Awareness Regarding Password Management-Related Issues**

Indicators (ISO/IEC 27002 Control 5.17)	Weighted Mean	Verbal Interpretation
1. Aware of risks associated with short, predictable passwords using personal data.	3.12	Moderately Aware
2. Understands vulnerabilities caused by reusing passwords across multiple platforms.	2.15	Slightly Aware
3. Recognizes severe risks of unencrypted storage versus secure password managers.	1.85	Slightly Aware
Overall Composite Mean	**2.37**	**Rarely**

*Legend: 4.20-5.00 (Highly Aware); 3.40-4.19 (Aware); 2.60-3.39 (Moderately Aware); 1.80-2.59 (Slightly Aware); 1.00-1.79 (Not Aware). *

Table 1 exposes a systemic, high-risk vulnerability among the student population, generating a low composite mean of 2.37 ("Slightly Aware"). The data reveals a dangerous lack of awareness regarding secure digital storage, with the lowest weighted mean (1.85) indicating that students fail to recognize the security disparity between unencrypted notes and encrypted password managers.

B. Social Engineering Threats and Deceptive Digital Tactics

The second domain measured the respondents' theoretical knowledge and practical susceptibility to human-centric psychological manipulation, specifically focusing on phishing, identity spoofing, and unsolicited digital communications.

Table 2. **Level of Awareness Regarding Social Engineering Threats**

Indicators (ISO/IEC 27002 Control 6.3	Weighted Mean	Verbal Interpretation
1. Verifies cryptographic legitimacy of URLs/senders before clicking links.	2.90	Moderately Aware
2. Recognizes psychological manipulation in phishing emails or identity spoofing.	4.10	Aware
3. Aware of dangers of engaging with unsolicited communications claiming official status.	3.85	Aware
Overall Composite Mean	**3.61**	**Aware**

Legend: 4.20-5.00 (Highly Aware); 3.40-4.19 (Aware); 2.60-3.39 (Moderately Aware); 1.80-2.59 (Slightly Aware); 1.00-1.79 (Not Aware).

Table 2 demonstrates a complex disconnect between theoretical recognition and technical execution. The respondents demonstrated a strong foundational awareness of psychological manipulation, successfully recognizing deceptive phishing tactics (4.10, "Aware"). However, their practical digital defense contradicts this theoretical knowledge, as their awareness of verifying the cryptographic legitimacy of URLs dropped significantly (2.90, "Moderately Aware").

C. Malicious Software Vulnerabilities and Wireless Network Attacks

The third domain assessed the students' comprehension of destructive digital payloads, evaluating their ability to recognize threats from malware and the severe vulnerabilities associated with unencrypted wireless transmissions.

Table 3. **Level of Awareness Regarding Malicious Software and Network Attacks**

Indicators (ISO/IEC 27002 Control 6.3)	Weighted Mean	Verbal Interpretation
1. Differentiates functional threats of viruses, worms, and ransomware.	3.35	Moderately Aware
2. Recognizes the threat of hidden spyware and keyloggers bypassing passwords.	3.80	Aware
3. Understands risks of Man-in-the-Middle attacks over unencrypted, public Wi-Fi.	2.65	Moderately Aware
Overall Composite Mean	**3.26**	**Moderately Aware**

Legend: 4.20-5.00 (Highly Recommended); 3.40-4.19 (Recommended); 2.60-3.39 (Neutral / Undecided); 1.80-2.59 (Not Recommended); 1.00-1.79 (Strongly Not Recommended).

Table 3 reveals a moderate structural vulnerability within the students' understanding of

network-level threats (Composite Mean 3.26). While they possess a standard awareness of spyware and keyloggers (3.80), their technical recognition of how these payloads is delivered via wireless infrastructure such as data interception over public Wi-Fi networks is alarmingly low (2.65).

D. Endpoint Device Security

The final domain quantified the respondents' awareness regarding localized, physical hardware protection. This measures their recognition of the risks associated with the physical device's mobile phones, laptops, and workstations that serve as the ultimate gateways to the academic and aviation networks.

Table 4. **Level of Awareness Regarding Endpoint Device Security**

Indicators (ISO/IEC 27002 Control 6.3)	Weighted Mean	Verbal Interpretation
1. Aware of physical security risks when leaving devices unlocked and unattended.	4.15	Aware
2. Understands necessity of active anti-malware, firewalls, and full-disk encryption.	3.20	Moderately Aware
3. Recognizes operational vulnerabilities from connecting untrusted hardware (e.g., USBs).	3.45	Aware
Overall Composite Mean	**3.60**	**Aware**

**Legend: 4.20-5.00 (Highly Recommended); 3.40-4.19 (Recommended); 2.60-3.39 (Neutral / Undecided); 1.80-2.59 (Not Recommended); 1.00-1.79 (Strongly Not Recommended). **

Table 4 confirms that while students recognize basic physical security principles, such as not leaving a device unlocked (4.15), they lack an understanding of advanced programmatic defenses. Their awareness regarding the implementation of full-disk encryption and active firewall maintenance scored lowest in this domain (3.20).

To justify the formulation of the institutional output, the final segment of the evaluation instrument measured the respondents' preference for the inclusion of specific training modules within the proposed program.

Table 5. **Recommended Components for the Proposed Cybersecurity Program**

Training Modules and Protocols	Weighted Mean	Verbal Interpretation
1. Step-by-step training modules on setting up and utilizing encrypted password managers.	4.85	Highly Recommended
2. Formalized institutional checklist for detecting aviation-specific phishing attempts.	4.72	Highly Recommended
3. Standardized protocols and tutorials for accessing databases over public Wi-Fi.	4.78	Highly Recommended
Overall Composite Mean	**4.78**	**Highly Recommended**

**Legend: 4.20-5.00 (Highly Recommended); 3.40-4.19 (Recommended); 2.60-3.39 (Neutral / Undecided); 1.80-2.59 (Not Recommended); 1.00-1.79 (Strongly Not Recommended). **

Table 5 mathematically justifies the fundamental necessity of this research. With an overwhelming composite mean of 4.78 ("Highly Recommended"), the data confirms that Avionics Technology students actively desire a formalized, structured intervention. The exceptionally high score for password manager training modules (4.85) directly correlates to the critical vulnerability identified in Domain A, proving that students are willing to abandon poor memorization habits if provided with clear, standardized education. By endorsing these specific topics, the empirical data provides absolute authorization for the researcher to develop the comprehensive cybersecurity program.

DISCUSSION OF FINDINGS:

The empirical data gathered from the Avionics Technology students reveals a complex intersection connecting theoretical cybersecurity knowledge and practical digital execution. By systematically interpreting the weighted means derived from the ISO-aligned evaluation instrument across four threat domains, the study reveals a profound awareness-action gap that requires immediate institutional intervention.

The most critical finding regarding Domain A, the respondents' credential management is their dangerous reliance on pure human memory. This mathematical finding strongly aligns with the conceptual literature of Adams and Sasse (1999) from Chapter II, which established that human cognitive limits consistently override security protocols. Because students are fundamentally unaware of tools that reduce cognitive load like encrypted managers, they resort to high-risk behavioral shortcuts, leaving aviation databases highly vulnerable to automated credential-stuffing attacks.

Subsequently, Domains B, C, and D measured the students' awareness of contemporary threats, confirming a severe disconnect between passive knowledge and operational defense. For instance, while students theoretically know phishing exists (4.10), they lack the specific, operational methodology required to technically verify a malicious URL (2.90). This directly correlates with the empirical findings of Choi et al. (2020), which proved that unstructured theoretical awareness is insufficient to stop deceptive tactics. Furthermore, as established by Lerner and Lerner (2013), modern payloads traverse unsecured networks; therefore, the students' lack of awareness regarding unencrypted Wi-Fi (2.65) and full-disk encryption (3.20) represents a direct operational hazard to aviation integrity.

Ultimately, this synthesis confirms that passive awareness is inherently insufficient; without the active integration of technical defense mechanisms, the digital identities of the student population remain highly exposed. This empirically justifies the necessity for the definitive output of this research: a structured, operational cybersecurity program that actively spans the awareness-action gap and aligns the institution's digital infrastructure with the United Nations Sustainable Development Goals 4: Quality Education and 9: Industry, Innovation, and Infrastructure.

CYBERSECURITY PROGRAM FOR AVIONICS TECHNOLOGY

I. Program Rationale

The empirical data explicitly identified a critical awareness-action gap among Avionics Technology students. While students possess foundational theoretical knowledge regarding digital threats, they lack the practical, technical mechanisms to defend against them. Because fragmented academic guidelines are insufficient to secure highly sensitive aviation infrastructures, this comprehensive program is engineered as a fully operational training architecture. Structurally anchored to the ISO/IEC 27001:2022 framework, this program transitions the academic environment from passive awareness to a formalized culture of proactive cyber resilience.

II. Program Objectives

1. To eradicate cognitive password strain by standardizing encrypted vaulting operations.
2. To build operational muscle memory against social engineering through active threat simulation.
3. To secure localized endpoint devices and wireless network transmissions used in aviation diagnostics.

III. Program Architecture and Modules

Module 1: Advanced Credential Architecture and Vaulting Operations Target Vulnerability: High cognitive load and cross-platform password reuse (Domain A).

Operational Protocol: The institution shall transition students to a passphrase architecture, mandating the use of 16-to-20-character randomized word strings. Crucially, this module dictates the mandatory deployment of enterprise-grade, zero-knowledge encrypted password managers (e.g., Bitwarden) for all students.

Training Implementation: Students will undergo a mandatory technical onboarding laboratory where they are trained to utilize AES-256 encryption vaults. They will learn to autonomously generate, store, and seamlessly autofill highly complex credentials for their academic and aviation portals, entirely neutralizing credential-stuffing attacks.

Furthermore, Multi-Factor Authentication (MFA) via Time-Based One-Time Passwords (TOTP) will be strictly enforced as a non-negotiable gateway requirement.

Module 2: Active Threat Simulation and Social Engineering Defense Target Vulnerability: Inability to technically verify deceptive communications (Domain B).

Operational Protocol: The university's IT infrastructure will shift the educational paradigm from lecture-based seminars to experiential simulation, deploying ongoing, dynamic cybersecurity tests.

Training Implementation: Unannounced, simulated phishing campaigns and benign identity-spoofing emails will be injected directly into the students' academic inboxes. These controlled drills safely test behavioral responses in real-time. Students who fail to verify cryptographic URL legitimacy or who engage with the simulated threat are immediately routed to a specialized, interactive remediation module. This transforms passive theoretical vulnerabilities into ingrained operational muscle memory.

Module 3: Wireless Infrastructure and Malware Mitigation Protocols Target Vulnerability: Exposure to Man-in-the-Middle attacks and unencrypted data interception (Domain C).

Operational Protocol: Accessing sensitive university or flight maintenance databases over public or unencrypted external Wi-Fi networks is structurally prohibited unless actively routed through an encrypted tunnel.

Training Implementation: Students will be explicitly trained on the operational deployment of Virtual Private Networks (VPNs) and the heuristic verification of secure HTTPS traffic. The module will also provide technical breakdowns of how modern ransomware and hidden keyloggers bypass traditional firewalls, ensuring students understand the strict necessity of encrypting data in transit.

Module 4: Endpoint Hardening and Physical Security Standardization Target Vulnerability: Physical compromise of diagnostic workstations and unverified peripherals (Domain D).

Operational Protocol: All student laptops, mobile devices, and shared avionics diagnostic workstations must comply with strict endpoint security baselines before network access is granted.

Training Implementation: The program provides technical walk-throughs for enabling biometric hardware locks and full-disk encryption (e.g., BitLocker or FileVault) on personal devices. It also institutes a Zero-Trust Peripheral Policy, explicitly training students on the severe risks of connecting unverified external hardware such as unauthorized USB diagnostic drives to network-connected devices, effectively sealing the localized physical perimeter.

Module 5: Continuous Program Auditing and Cyber Resilience Review Target Vulnerability: Policy obsolescence in the face of evolving cyber threats.

Operational Protocol: Cyberspace operates in a state of perpetual evolution. Aligned with the Plan-Do-Check-Act (PDCA) cycle and United Nations Sustainable Development Goal 9: Industry, Innovation, and Infrastructure, the program protocols must undergo a formalized IT and behavioral audit annually.

Implementation Strategy: By continuously measuring student compliance metrics through the simulated phishing campaigns and updating the training modules to align with the latest iterations of global ISO/IEC standards, the institution guarantees a profoundly resilient, future-proof digital learning environment for its future aviation professionals.

CONCLUSIONS:

Through a rigorous empirical analysis of the data gathered from the Avionics Technology student cohort at WCC Aeronautical & Technological College - Binalonan, the researcher presents the following definitive conclusions, systematically aligned with the specific problems of the study.

Regarding the students' level of awareness, the empirical evidence confirms the existence of a profound awareness-action gap across all measured threat domains. In terms of password management-related issues, students exhibit a critical vulnerability driven by severe cognitive overload. Their reliance on human memory and lack of awareness regarding encrypted storage mechanisms directly precipitates high-risk security behaviors, specifically cross-platform password reuse. Furthermore, across the domains of social engineering, malicious software, and endpoint security, students demonstrate a strong foundational theoretical knowledge such as effectively

recognizing deceptive phishing tactics but consistently fail to translate this knowledge into functional technical defense. Their operational inability to deploy technical mechanisms, such as verifying URL cryptography or utilizing encrypted VPNs over public networks, renders their digital identities highly susceptible to compromise.

Regarding the recommended components for the program, the targeted assessment concludes with an overwhelming empirical mandate from the student population. Yielding an exceptional composite mean, the data confirms that students actively acknowledge their operational vulnerabilities and strongly demand structured, standardized technological interventions. The exceptionally high demand for specific training, notably step-by-step modules on encrypted password managers, directly correlates to the vulnerabilities identified in the first domain.

Ultimately, the primary security vulnerability within the Avionics Technology demographic is a persistent awareness-action gap exacerbated by an outdated reliance on manual digital hygiene. The student population remains at a moderate-to-high risk of digital compromise not due to a complete deficit in cyber awareness, but because they lack the technical tools and structured training to operationalize their defense. This empirical reality serves as the absolute academic justification for the formulation of the Cybersecurity Program for Avionics Technology, proving it is not merely a recommendation, but a critical operational imperative to secure the university's digital perimeter.

RECOMMENDATIONS

Derived from the empirical conclusions, the researcher advances a series of strategic, actionable recommendations to ensure the systemic integration and continuous efficacy of the formulated output.

To ensure a smooth transition, WCC Aeronautical & Technological College - Binalonan, through the administration and the Avionics Technology Department, should formally launch a designated pilot testing phase of the proposed Cybersecurity Program. This controlled trial will securely capture real-world behavioral compliance and technical performance data from a micro-cohort of students and faculty.

Crucially, the institution must not treat this pilot program as a static finality. User friction points and technical compliance logs extracted during the trial phase should serve as the empirical catalyst for granular, iterative revisions. This continuous refinement will ensure the program is highly practical and perfectly customized to the operational parameters of the college prior to a full-scale institutional deployment.

To operationalize the students' theoretical knowledge and actively test their defenses, the university's Information Technology (IT) Department must pivot its annual auditing framework from passive compliance checklists to active defense methodologies. This strategic shift must include mandating unannounced simulated phishing campaigns and network vulnerability assessments to dynamically measure and strengthen the institution's human firewall.

Because cognitive credential strain and the awareness-action gap transcend a single discipline, university top management should establish a policy framework to scale this cybersecurity program across all other academic departments. Furthermore, future researchers are highly encouraged to replicate this descriptive-quantitative methodology to track long-term behavioral shifts and investigate emerging automated attack vectors, ensuring the institution remains profoundly resilient against the perpetual evolution of global cyber threats.

The digital frontier of the modern aviation industry demands a workforce that is not only technically proficient in aircraft systems but also profoundly resilient against human-centric cyber threats. The implementation of the formulated cybersecurity program transcends basic academic compliance; it is a foundational investment in the future of aviation security. By transforming vulnerable digital habits into ingrained, proactive defense mechanisms today, the institution ensures that its graduates will enter the global aviation sector as secure, uncompromising guardians of critical aerospace infrastructure.

BIBLIOGRAPHY:

- Altenkirch, T., & Miller, J. (2021). *Cybersecurity in the aviation industry: Risk management and critical infrastructure*. Springer.

- Anderson, R. J. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.
- Halibozek, E. P., & Kovacich, G. L. (2017). *The manager's handbook for corporate security: Establishing and managing a successful assets protection program* (2nd ed.). Butterworth-Heinemann.
- Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An introduction to information security*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-12r1 Cited by: 331
- Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W. W. Norton & Company.
- Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.
- Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.
- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40–46.
- Bottarelli, M., Epiphaniou, G., Mahmood, S., Hooper, M., & Maple, C. (2025). Assessing the trustworthiness of electronic identity management systems: Framework and insights from inception to deployment. *arXiv*. https://doi.org/10.48550/arxiv.2502.10771 Cited by: 4
- Chahid, A. (2026). Developing a cybersecurity awareness framework to safeguard Moroccan students from social media threats. *Frontiers in Education*.
- Choi, Y., Park, J., & Lee, H. (2020). Varying levels of cybersecurity threat awareness among student populations. *Journal of Technology in Higher Education, 15*(3), 112–128.
- Davis, R., & Jones, S. (2021). Behavioral patterns and compliance with recommended password change policies. *Information Systems Review, 12*(2), 45–60.
- Kour, R. (2026). Annoyed by cybersecurity? Human-centric perspectives on cybersecurity. *Frontiers in Computer Science*.
- Kumar, A., & Tiwari, R. (2022). A comparative analysis of password management tools: Usability, security features, and user satisfaction. *Journal of Cybersecurity Technology, 6*(1), 22–38.
- Mohammed, Y., Alsaid, M., & Hossain, G. (2026). Future trends in cybersecurity: A meta-review. *TEM Journal, 15*(1), 167–175.
- Moallem, A. (2019). Cyber security awareness among college students. *Advances in Intelligent Systems and Computing, 782*, 79–87.
- Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work, 24*, 371–390. https://doi.org/10.1007/s10111-021-00683-y Cited by: 390
- Schaltegger, T. (2025). Full article: Human behavior in cybersecurity: an opportunity for risk research. *Journal of Risk Research*. Cited by: 10
- Shinde, S. K., & Deshpande, M. V. (2022). Cognitive load and the challenge of credential management in digital environments. *International Journal of Cyber Behavior and Psychology, 14*(4), 201–215.
- Cybersecurity and Infrastructure Security Agency (CISA). (2024). *Choosing and protecting passwords*. https://www.cisa.gov/secure-our-world/use-strong-passwords
- Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines: Revision 3* (NIST Special Publication 800-63B). National Institute of Standards and Technology. https://pages.nist.gov/800-63-3/sp800-63b.html Cited by: 440
- ISO/IEC. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and*

privacy protection — Information security management systems — Requirements.

- ISO/IEC. (2022). *ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls*.
- Microsoft Security. (2023). *Passwordless authentication and the future of security*. https://www.microsoft.com/en-us/security/business/identity-access/passwordless-authentication.