IJSST Volume 1 Issue 2 | E-ISSN: 302x-xxxx | DOI: https://doi.org/10.55990/20250014

Research Frontiers: International Journal of Social Science and Technology

Journal Homepage:
https://researchfrontiersjournal.com/index.php/pub/index

Research Article

The Multidimensionality Of Cyberterrorism Vulnerability Behavior Among Millennial Employees In The Government: A Sequential Exploratory Mixed-Methods Approach

Lyn Marie C. Centeno, RN, MPA[1] | Glenne B. Lagura, DPA[2]

[1]The University of Mindanao, Professional Schools, Davao City, Philippines
*l.centeno.522997@umindanao.edu.ph

[2]The University of Mindanao, Professional Schools, Davao City, Philippines
Davao del Norte State College, Panabo City, Philippines
glenne.lagura@dnsc.edu.ph

Article Info

Article History:

Received: 12th May 2025
Accepted: 16th June 2025
Published: 28th Oct 2025

Keywords:

public administration, cyberterrorism vulnerability, cyberterrorism risk management, cybersecurity law, cybersecurity policy, e-governance, exploratory design, confirmatory approach

ABSTRACT

The increasing adoption of e-governance in the Philippines enhances government efficiency but also increases exposure to cyberterrorism threats. This study identified and validated the dimensions of cyberterrorism vulnerability behavior among millennial employees in the government. An exploratory sequential design was employed on 1,008 respondents from the different LGU employees in Region XII using purposive sampling for In-Depth Interviews (IDI) in the qualitative phase and stratified random sampling for the survey in the quantitative phase. The Exploratory Factor Analysis (EFA) identified eight dimensions: Organizational Cybersecurity Readiness (OCR), Cyberterrorism Awareness and Risk Perception (CAR), Risky Digital Behaviors (RDB), Personal Cybersecurity Practices (PCP), Secure IT Infrastructure (SII), Perceptions of Cybersecurity Training (PCT), Shared Security Accountability (SSA), and Perceived Cybersecurity Vulnerability (PCV). Using Confirmatory Factor Analysis (CFA), it achieved a strong model fit and high reliability.

[1]Corresponding Author: Lyn Marie C. Centeno
*Corresponding Email: l.centeno.522997@umindanao.edu.ph

INTRODUCTION

The increasing frequency of cyberattacks targeting Philippine government agencies, security institutions, and critical infrastructures underscores the growing threat of cyberterrorism in the country. As the government continues to integrate digital infrastructure into its administrative, operational, and communication processes, reliance on technology has become essential for efficiency and accessibility. The Philippine government has actively promoted e-government initiatives to streamline services, as outlined in the E-Government Master Plan 2022, which envisions a One Digitized Government (Department of Information and Communications Technology (DICT), 2019). With an estimated 1.4 million millennial employees comprising most of the public sector workforce (Civil Service Commission (CSC), 2023), this digital transformation aims to enhance public service delivery. However, these advancements also expose critical systems to cyber threats, emphasizing the urgent need to strengthen cybersecurity measures to safeguard national security and public trust.

The transformative power of technology has brought major contributions across all aspects of society in this modern world. Technology revolutionized how people interact, work, and live, from communication to healthcare, transportation, education, and beyond. However, the virtual environment has become susceptible to various threats because of these rapid technological advancements (Plotnek & Slay, 2021) and escalating digital dependencies (Constantin et al., 2020). Large-scale cyber-attacks are rising at an alarming rate globally, and these attacks are frequently associated with the threat of cyberterrorism (Kamalia et al., 2019). According to the data provided by the Center for Strategic and International Studies (2023), a total of 780 cyber incidents have been documented globally from 2016 to 2023, with five cases reported within the Philippines. These incidents comprised various activities, including state-sponsored actions, espionage operations, and cyberattacks targeting government and private entities. Some of these cyber incidents have led to more than a million dollars in financial losses. Moreover, cases notably increased at the onset of the COVID-19 pandemic when people were most active on the online platform as outdoor activities were restricted. In response to imminent cyber threats against critical infrastructures in the Philippines, the DICT's Cybercrime Investigation and Coordination Center (CICC) implemented the comprehensive National Cybersecurity Strategy Framework 2022 (Department of Information and Communications Technology, 2019).

Cyberterrorism differs from cybercrime by excluding activities such as theft of credit card information, dissemination of explicit content via emails, or unauthorized hacking of websites (Ozeren, 2005). The United Nations Office on Drugs and Crime (2013) defines cybercrime as "acts that can be committed against individuals, organizations, or governments using information and communication technology (ICT), including fraud, identity theft, hacking, and online scams." Meanwhile, Moldovan (2016 cited in Constantin et al., 2020) described cyberterrorism as the merging of the digital

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

realm and acts of terrorism in which non-state actors deliberately attack or threaten civilians, governmental and non-governmental targets to further social or ideological goals resulting in physical, emotional, political, economic, ecological, or other effects outside of cyberspace (Plotnek & Slay, 2021). While the UNODC does not provide an official and universally accepted definition of cyberterrorism, it references a narrow definition of cyberterrorism as a cyber-dependent crime committed for political objectives to provoke fear, intimidate, and/or coerce a target government or population, causing or threatening to cause harm such as sabotage, aligned with the perspectives of Denning, and Jarvis, et al. (2001; 2014 as cited in UNODC, 2019). The threat to national security becomes larger when the acts of cyberterrorism target critical infrastructures such as power grids, telecommunications, healthcare, and transportation systems, as well as financial services, exposing risks to public safety, health, and security, as well as economic development (Naidoo & Jacobs, 2023).

In light of looming terrorism threats, the Human Security Act of 2007, which was later repealed by the Republic Act 11479 or Anti-Terrorism Act of 2020, was enacted to protect and secure life, liberty, and property from terrorism, condemn its acts, and make it a crime against the Filipinos, humanity, and the Law of Nations (GovPH, 2007; GovPH, 2021). Section 4 and Rule 4.3 of the ATA 2020 define terrorism through two key elements: engagement in acts and intent. Acts include causing death or injury, destroying property, disrupting critical infrastructure (e.g., telecommunications, energy, banking, emergency services, information systems, and technology), using weapons or hazardous materials, and triggering large-scale disasters. These acts must aim to intimidate the public, spread fear, coerce governments, destabilize societal structures, or create a public emergency.

In the Philippines, several cases of cyberattacks against government agencies and security institutions aligned with the elements of terrorism as defined by the ATA 2020 may be classified as cyberterrorism attempts. The 2023 PhilHealth Ransomware Attack and the massive data breach affecting the PNP, NBI, and BIR demonstrate deliberate cyberattacks on essential public services, severely compromising national security and eroding public trust (Jaymalin, 2023; Caliwan, 2023). Likewise, breaches targeting military institutions, such as the 2024 Philippine Navy Database Breach and the 2025 Philippine Army Network Breach, pose significant threats to national defense by potentially exposing sensitive military operations and classified information (Mangosing & Subingsubing, 2024; GMA Integrated News, 2025). Moreover, cyber intrusions originating from foreign actors, including 2024 China-based hacking attempts and the 2025 Advanced Persistent Threat (APT) attacks on intelligence data, suggest sophisticated, state-sponsored cyber operations designed to destabilize the country's political and security landscape (Reuters, 2024; Lema & Flores, 2025).

Several factors may influence cyberterrorism vulnerability behavior among millennial employees in the government. The existence of smartphones and the prevalence of social media platforms like Facebook, YouTube, blogs, Twitter, and

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

messaging apps such as WhatsApp and Telegram in the Millennial era have exposed this generation and those that follow to the risk of cyberterrorism (Kamalia et al., 2019). The behaviors and attitudes of millennial employees are significant crucial points in understanding and addressing cyberterrorism vulnerabilities as the demographic landscape within government organizations shifts.

Millennials, who are often considered digital natives growing in a digital environment, can be too overconfident in their familiarity with technology, resulting in risky online behaviors (Dimock, 2019). Despite being tech-savvy, they are easy targets for cybercriminals, with 40 percent of the generation having experienced it (Norton Cyber Security Insights Report, 2016). They are more comfortable with technology and connected to the internet and social media sites for almost twenty-four hours a week (Hayes, 2013; Srinivasan, 2012, as cited in Tyson, 2018). Based on the report, a few reasons for millennials' vulnerability to cybercrime include password promiscuity and the use of public Wi-Fi. In India, more than 55 percent of millennials have been victims of cybercrime (The Economic Times, 2017). While 36 percent of this generation say they should be doing more to protect their digital security, 33 percent believe they are "too dull" to be a victim of a cyber-attack (Security Brief Australia, 2020). In 2021, a study showed that 44 percent of Millennials are likelier to experience a cyber threat, while 25 percent said their identities had been stolen (National Cybersecurity Alliance, 2021).

Organizational culture in government agencies also affects how employees approach cybersecurity. Millennials are keen to be influenced by organizational culture, practices, and management. They could resign from their job due to a lack of social relevance. Guo et al. (2011, as cited in Tyson, 2018) found that employees commonly engage in Non-Malicious Security Violation (NMSV) behaviors for convenience and aiding colleagues. Moreover, D'Arcy et al. (2014), Njenga (2017), and Peoria et al. (2017, as cited in Tyson, 2018) highlighted motivational factors leading to employees violating Information Systems policy, such as work overload and internet interruptions, emphasizing the human factor as the weakest link in cybersecurity. Instead of cybersecurity training, Woodward et al. (2015, as cited in Tyson, 2018) noted that millennials expressed a need for problem-solving training.

The cyberattacks are anticipated to evolve and become more sophisticated in the future. Reshaping the organizational structure (Willie, 2023), emphasizing cybersecurity, and improving specialized manpower (Moşteanu, 2020) are imperative to address emerging cybersecurity threats and enhance resilience. Relatedly, the effectiveness of cybersecurity training and awareness programs within agencies impacts their behaviors. Each employee of an organization is responsible for its security. Insufficient awareness undermines even the most advanced information systems in the government (Dash & Ansari, 2022).

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

An individual's perception of cybersecurity risks and the severity of potential threats can also influence their vulnerability behavior. Factors that may include knowledge of threats, perceived severity, perceived vulnerability, protection habits, perceived barriers, self-efficacy, and response efficacy influence a government employee's cybersecurity behavior (Sulaiman et al., 2022).

Several researchers investigated cybersecurity behavior and awareness (Almansoori et al., 2023; Khan et al., 2022; Herath et al., 2022; Alzubaidi, 2021). Alghamdi (2022) reviewed 27 research papers to investigate vulnerabilities in human factors in cybersecurity from 2009 to 2020. This resulted in identifying 14 human factors that impact cybersecurity for organizations, which are categorized into three sections: demographic factors, cognitive factors, and knowledge and skills factors. Further studies have been conducted to uncover human cybersecurity behaviors among organizational employees (Alshaikh, 2020; John, 2021; Sulaiman, et al., 2022; Klein & Zwilling, 2023). However, there are still significant limitations, gaps, or weaknesses in the cyberterrorism perspective within academic research. McDonald et al. (2022) listed access to data with 30.9 percent as the top of the significant gaps or limitations in the field. However, the focus on vulnerabilities, with 2.1 percent, is still recognized as one of the weaknesses in the scholarly inquiry.

In response to the growing threats of cyberterrorism, studies were conducted on its taxonomy and patterns (Seissa et al., 2017; Ramadhan, 2020; Chandrika et al., 2018; Plotnek & Slay, 2021; Murray, et al., 2019; Almansoori et al., 2023), emerging threats and vulnerabilities (Valeriia, 2022; Cohen-Almagor, 2018; Zubko, 2021; Khan, et al., 2022), counter strategies and law enforcement efforts (Bakry et al., 2021; Constantin, et al., 2020; Moustafa & Bello, 2021), as well as cybersecurity practices (Uchendu, et al., 2021).

This study is anchored on the Protection Motivation Theory (PMT) of R.W. Rogers (1975). It tries to figure out and predict a person's behavioral intentions by looking at how they think about a threat and how well they can deal with things. This research is based on the full PMT nomology and explains problems related to behavior in an information security setting (Boss et al., 2015; Posey et al., 2015, cited in Aurigemma, 2019). This model has two cognitive processes: 1) threat appraisal and 2) coping responses. Fear appeals, which produce threats, are used to encourage people to adopt protective security behaviors. The study by Warkentin et al. (2016, as cited in Ghazali, Hassan, and Ahmad, 2023) showed how important PMT is for developing ways to get people to talk about how to protect themselves from cyber threats.

The Theory of Planned Behavior (TPB) and the Unified Theory of Acceptance and Use of Technology (UTAUT) are two well-known theories that this study uses to explain behaviors in the context of cybersecurity. The TPB explains behavioral intentions, which are shaped by attitudes, subjective norms, and perceived behavioral control. It stresses how subjective norms affect behavior, including starting and keeping it up, as well as how

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

people think about their behavior and their attitudes toward using technology (Vafaei-Zadeh et al., 2019; Al-Emran et al., 2022, as cited in Almansoori et al., 2023).

To explain user intentions regarding the use of an information system and the resulting patterns of usage behavior, recent studies have used Venkatesh et al. (2003)'s UTAUT model to investigate cybersecurity. Social influence, performance expectancy, effort expectancy, and facilitating conditions are the four main ideas that affect a person's intention to use technology as well as their actual use of it. Age, gender, experience, and voluntary use all act as moderators of these constructs.

This study integrates the common constructs of the theories of PMT, TPB, and UTAUT in investigating the multidimensionality of cyberterrorism vulnerability behavior among millennial employees in the government, with primary consideration of the demographic, cognitive knowledge, and skills factors identified to pose an impact on cybersecurity for organizations (Alghamdi, 2022). This framework suggests that cyberterrorism vulnerability behavior is determined by the behavioral intentions and facilitating conditions observed by millennial government employees. These behavioral intentions depend on the direct effect of constructs, namely Perceived Behavior and Attitudes, Efficacy, and Social Influence. In other words, fear and risk perception mediate the path between perceived behavior and attitudes, as well as behavioral intentions. It also proposes that the process is mediated by the voluntariness of use and demographic factors, namely age, gender, and experience.

Perceived Behaviors and Attitudes describe how millennial employees subjectively assess the necessity, appropriateness, and efficacy of taking cybersecurity precautions to lessen the risk of cyberterrorism. Efficacy refers to the millennial employees' perceptions of their ability to execute cybersecurity measures to protect against cyberterrorism threats successfully. Facilitating Conditions denote perceived behavioral control and perceived resources and support necessary for millennial employees to engage in cybersecurity behaviors within the organization effectively. Social Influence refers to the impact of interpersonal relationships, organizational culture, and leadership support on millennial employees' intentions and behaviors against the threat of cyberterrorism.

This study is distinct from previous literature as it focuses on cyberterrorism vulnerability behavior. As of this writing, no studies have been conducted in the Philippines. However, terrorism is still one of the security challenges that is currently addressed by the national government, anticipating imminent threats in cyberspace that pose significant risks to its critical infrastructures and people. This research also reinforces recent findings on the need for optimal digital governance among LGUs, highlighting gaps in data privacy and technical infrastructure (Lagura, 2025).

The main objective of this study is to explore the multiple dimensions of cyberterrorism vulnerability behavior of millennials employed in government offices in

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

Region XII, employing a mixed-methods exploratory sequential approach. Specifically, the researcher aims 1) to determine factor structures of cyberterrorism vulnerability behavior among millennial employees in the government, 2) to generate a multidimensional framework, and 3) to validate the framework using a Confirmatory Factor Analysis.

In the context of this study, cyberterrorism vulnerability behavior refers to the actions, attitudes, and practices of millennial government employees that increase the risk of cyberterrorism threats and attacks. It encompasses a range of factors that contribute to an organization's susceptibility to cyberterrorism, which may include technical vulnerabilities, human factors, and organizational culture.

This study fills a crucial gap in the literature on cyberterrorism by focusing on the frequently disregarded behavioral vulnerabilities of the millennial workforce, which has substantial global and local relevance. The study contributes to the United Nations Sustainable Development Goals (SDG), specifically SDG #9 (Industry, Innovation, and Infrastructure) and SDG #16 (Peace, Justice, and Strong Institutions), by illuminating how this population engages with cyber threats. It supports international initiatives to protect digital infrastructure and strengthen institutional governance and trust in the face of cyberterrorism.

The study may also offer insightful information for different Philippine institutions. The results may be used by the DICT to develop more focused cybersecurity guidelines and initiatives to increase the skills of millennial government workers. Likewise, the findings may support the National Privacy Commission (NPC) in its regulatory plans to improve data security procedures. To build a more secure and digitally resilient public sector, local government unit (LGU) associations may also use the study to raise cybersecurity awareness and resilience at the local level. This will encourage knowledge-sharing and cooperative ventures.

METHODS

Study Participants/Research Subject

The target population for the qualitative phase of this study, which was the first part of the Framework Development, consisted of millennial employees aged 26 to 41 years old working in the Local Government Units (LGUs) of Region XII, Philippines, who participated in In-Depth Interviews (IDIs). These individuals shared common characteristics, such as being digitally savvy, adaptable to technological advancements,

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

and actively engaged in government affairs. The sample size for the IDIs involved selecting two participants per province within the region, resulting in a total of eight participants. The in-depth interviews were structured to elicit a profound understanding of the participants' viewpoints (Rutledge & Hogg, 2020). Purposive sampling was employed for the IDIs to ensure that participants possessed rich and diverse experiences relevant to the study's objectives (Creswell and Poth, 2018, as cited in Kegler et al., 2018). This sampling method, commonly used in qualitative research, was applied to select cases rich in information, ensuring the efficient allocation of limited resources (Patton, 2002, cited in Palinkas et al., 2015).

Meanwhile, the quantitative phase of this study consisted of two sub-phases: the continuation of the Framework Development and Framework Validation. In this phase, 1,000 millennial employees working within the LGUs of Region XII were selected as respondents. Of these, 100 respondents were initially allocated for the pilot test, 400 respondents for the framework development phase, and 500 respondents for the validation phase. A stratified random sampling method was employed to generate the sample size, with each province representing a stratum. From each stratum, a random sample of 225 millennial employees was selected, excluding the pilot test population. This process ensured that the sample was representative of the entire population of millennial employees across all four provinces of Region XII, enabling meaningful analysis of cyberterrorism vulnerability behavior within the region. Stratified random sampling, widely accepted in survey research, ensured adequate representation of subgroups within the population [54]. By stratifying the population by province, this method facilitated the inclusion of diverse perspectives and characteristics across different provinces of Region XII, ultimately enhancing the generalizability and reliability of the study's findings.

Materials/Instruments

This study employed an exploratory sequential design to investigate cyberterrorism vulnerability behavior among millennial employees of LGUs in Region XII. The qualitative phase began with in-depth interviews (IDIs) involving eight respondents, guided by a validated semi-structured interview guide. This guide was developed based on Protection Motivation Theory, Theory of Planned Behavior, and Unified Theory of Acceptance and Use of Technology, ensuring validity through expert consultations and comprehensive literature reviews. Participants' responses were meticulously transcribed, analyzed, and coded to extract key themes and factors, which were then used to design a survey instrument. The survey, featuring a 5-point Likert scale to measure perceptions and attitudes, underwent expert validation and a pilot test with 100 millennial employees, yielding a Cronbach's alpha reliability score of 0.935.

In the quantitative phase, the validated survey instrument was distributed to 400 millennial government employees across various provincial, municipal, and city LGUs for

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

framework validation using Exploratory Factor Analysis (EFA). EFA assessed sampling adequacy via the Kaiser-Meyer-Olkin Measure, interrelations using Bartlett's Test of Sphericity, and identified factors based on Eigenvalues above 1.0, with VARIMAX rotation simplifying interpretation. A scree plot was used to determine the number of factors to retain. Subsequently, an additional survey of 500 millennial employees refined the framework through CFA, evaluating model fit indices such as Comparative Fit Index (CFI), Tucker-Lewis Index (TLI), Root Mean Square Error of Approximation (RMSEA), and Standardized Root Mean Square Residual (SRMR). This rigorous mixed-methods approach provided a multidimensional understanding of cyberterrorism vulnerability, supporting the development of a validated framework for addressing this phenomenon among government employees.

Design and Procedure

This study combined qualitative and quantitative research methods in an exploratory sequential design. Gaining a thorough grasp of the aspects of cyberterrorism vulnerability behavior among millennial employees of LGUs in Region XII was the driving force behind this design. The qualitative phase was carried out first, and then the quantitative phase.

According to J.W. Creswell and J.D. Creswell (2018), the exploratory sequential mixed-methods design consists of three stages: first, researchers gather and analyze qualitative data; next, they develop a quantitative feature, such as a survey instrument; and finally, they proceed to a quantitative phase for testing and validation. This method guarantees that the quantitative element is influenced by deep qualitative insights, enabling the development of experimental protocols or measurement instruments that are pertinent to the context. According to Creswell and Creswell (2018), the framework in Figure 1 shows the flow from qualitative investigation to quantitative testing and interpretation. By incorporating results from an initial qualitative phase into a structured quantitative investigation, this design improves the study's rigor and applicability, especially when the instruments currently in use are insufficient.

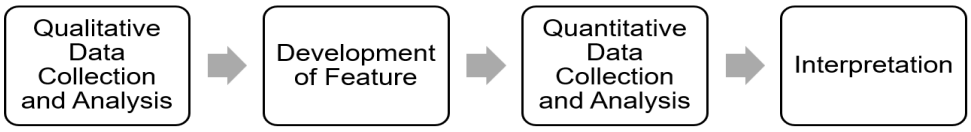

Figure 1
Exploratory Sequential Mixed-Methods Framework

The "building" integration strategy from Fetters et al. (2013, as cited in Fetters & Tajima, 2022) also guides this design. The first qualitative results, which included schemes, codes, and quotes, were used to make the scales, stems, and items for the next quantitative data collection tool. In the second phase of the sequential design, this tool

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

was given out. The researcher used this integration strategy to make sure that the quantitative phase was closely related to and informed by the qualitative phase. This helped to fully explore how millennial government employees in Region XII are vulnerable to cyberterrorism. Figure 2 shows the model procedure for an exploratory sequential study based on the ideas of J.W. Creswell and J.D. Creswell (2018) and Fetters et al. (2013).

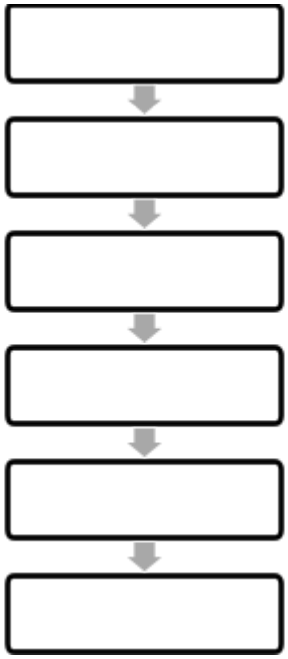

Figure 3
Model Procedure of Exploratory Sequential Study

Qualitative Phase

Eight participants were chosen through collaboration with the provincial governors and the provincial human resource management offices (PHRMOs) of North Cotabato, South Cotabato, Sultan Kudarat, and Sarangani, and the qualitative phase started with in-depth interviews (IDIs). The researcher used a validated instrument to guide the interviews, which lasted between 60 and 90 minutes and were recorded with consent after gaining the required permissions and informed consent. Their responses were transcribed, and key statements that aligned with the research objectives were extracted and coded. These codes informed the initial development of a survey tool, which was reviewed and validated by experts for clarity and relevance.

Quantitative Phase

For the pilot testing, the researcher coordinated with the City Mayor of Tacurong in Sultan Kudarat province and requested permission to conduct pilot testing for 100 millennial employees of the city government. After getting permission, the researcher

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

worked with the City Government's HRMO to send out survey questionnaires to gather data. The researcher worked with a statistician to look at the data and figure out how consistent and reliable the survey tool was by calculating Cronbach's alpha, which yielded a value of 0.935.

Following the successful completion of the reliability test, the researcher collaborated with the four provincial government offices in the area to develop a framework by surveying 400 millennial employees working for each office. To identify the underlying factors that account for the relationships between observed variables, the data collected during this phase was processed using inferential statistics, particularly Exploratory Factor Analysis (EFA) (Watkins, 2018). EFA provides insights into the intricacy of the phenomenon by assisting in the identification of the structure of cyberterrorism vulnerability behavior among millennial government employees.

In order to ascertain whether the variables are sufficiently related for significant factor analysis, the EFA procedure comprised performing Bartlett's Test of Sphericity and evaluating sampling adequacy using the Kaiser Meyer-Olkin (KMO) Measure. To find out how much variance each factor explains, the initial Eigenvalue was calculated; factors worth keeping had values of 1.0 or higher. Aiming for a straightforward structure with each variable having high loadings on just one factor, VARIMAX Rotation was also used to maximize variance and facilitate factor interpretation. Lastly, a Cattell Scree Plot was utilized to visually assess the eigenvalues, indicating the number of factors to retain.

After completing the initial quantitative phase of the Framework Validation, the study continued with the survey of another 500 millennial government employees in the region, utilizing the survey instrument processed with EFA. Then, the data gathered was subjected to Confirmatory Factor Analysis (CFA).

In CFA, the researcher evaluated the fit between the observed data and the proposed framework, verifying the validity of the structure. The primary analysis in CFA involved evaluating the fit indices of the model, including the Comparative Fit Index (CFI), Tucker-Lewis Index (TLI), Root Mean Square Error of Approximation (RMSEA), and Standardized Root Mean Square Residual (SRMR), with higher values indicating a better fit. Additionally, chi-square tests evaluated the model's overall goodness of fit.

RESULTS AND DISCUSSION

Framework Development

The qualitative phase resulted in the identification of codes which represent cyberterrorism vulnerability behaviors in terms of technological limitations, policy and organizational gaps, behavioral and cultural challenges, and external dynamics threats as perceived by the government employees. Table 1 presents 33 relevant items or initial

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

codes extracted from the responses of the participants, represented as Ps, during the IDIs, and were used to develop the questionnaire. From these codes, the researcher formulated 60-item statements for the instrument.

Table 1
Initial Codes

Codes	P1	P2	P3	P4	P5	P6	P7	P8
1. Limited IT Resources and Workforce	✔	✔	✔		✔	✔		
2. Uncontrollable Employee Behavior	✔	✔	✔	✔	✔	✔	✔	✔
3. Lack of Robust Cybersecurity Policy	✔	✔	✔		✔	✔	✔	✔
4. Limited Cybersecurity Awareness and Education	✔	✔	✔	✔	✔	✔	✔	✔
5. Unsecured Data Storage and Transmission of Office Communications	✔	✔	✔	✔	✔	✔		
6. Download or Use of Unauthorized, Unlicensed or Cracked Software/Applications	✔	✔	✔	✔	✔	✔	✔	✔
7. Superficial Data Protection Management and Cybersecurity Training	✔	✔			✔	✔	✔	✔
8. Cybersecurity as a Low Priority	✔	✔	✔	✔	✔	✔	✔	✔
9. Decentralized Data Management System	✔	✔	✔		✔	✔		
10. Employment Status and Cybersecurity Consciousness	✔	✔	✔	✔	✔	✔		
11. Lack of PLGU Support for ICT Infrastructure	✔	✔	✔		✔	✔		
12. Password Mismanagement	✔	✔	✔	✔	✔	✔	✔	✔
13. Unsecured Network Connections	✔	✔	✔	✔	✔	✔	✔	✔
14. Vulnerability of Government as Target of Cyberterrorism	✔	✔	✔	✔	✔	✔	✔	✔
15. Experience of Cyberattacks (hacking, phishing, ransomware, online scams)	✔	✔	✔	✔	✔	✔	✔	✔
16. Increase Social Media Activities	✔	✔	✔	✔	✔	✔	✔	✔
17. Unrestricted Access to the Internet and Dark Web	✔	✔	✔	✔	✔	✔	✔	✔
18. Lack of IT Infrastructure	✔	✔	✔		✔	✔		
19. Motives of Cyberattacks as Political Sabotage	✔	✔	✔	✔	✔	✔		
20. No Established Access Control Policy	✔	✔	✔	✔	✔	✔	✔	✔
21. Use of Personal Devices for Work or Workstation for Personal Activities	✔	✔	✔	✔	✔	✔	✔	✔
22. Weak Empowerment of Non-IT Workforce	✔	✔			✔	✔		
23. Independent PLGU cybersecurity practices	✔	✔	✔		✔	✔	✔	✔
24. Mismatch of IT Roles	✔	✔	✔		✔	✔		
25. Reliance on Office Warnings and Disciplinary Actions			✔				✔	✔

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

26.	Voluntary Attendance to Training and Passive Learning	✔				✔	✔	✔	✔
27.	Not Regularly Updating Software/Applications	✔	✔	✔	✔	✔	✔	✔	✔
28.	Over-reliance on IT employees	✔	✔	✔		✔	✔		
29.	Knowledge on IT exploited to Bypass PLGU Security System			✔					
30.	Poor Performance of Cybersecurity Software			✔		✔	✔	✔	
31.	Reliance on Third-party Web Hosting			✔					
32.	Rapid Evolution of Cyberspace and Cybersecurity Solutions			✔				✔	✔
33.	Use of Free Firewall Versions	✔	✔			✔	✔		

The 60-item survey instrument was tested for validity and deployed for pilot testing among 100 millennial employees of the City Government of Tacurong in Sultan Kudarat province. The reliability analysis of the instrument, as shown in Table 2, yielded a Cronbach's Alpha coefficient of 0.935, indicating an excellent level of internal consistency among the 60 items. When standardized, Cronbach's Alpha further improved to 0.944, demonstrating that the scale is highly reliable and suitable for measuring the intended constructs. The scale statistics also resulted in a mean of 238.39 with a variance of 597.13 and a standard deviation of 24.44, indicating moderate dispersion of responses around the mean. These findings confirm that the instrument is consistent and dependable for data collection, strengthening its validity for use in the study.

Table 2
Reliability and Scale Statistics

Reliability Statistics		Scale Statistics	
Cronbach's Alpha Coefficient	0.935	Aggregated Mean	238.39
Cronbach's Alpha Based on Standardized Items	0.944	Variance	597.13
		Std. Deviation	24.44
No. of Items = 60			

Table 3 shows the distribution of respondents for the qualitative and quantitative data collection phases. The IDI involved eight participants with 4 or 50 percent of the total population, who were under the age group of 38-41 years old. The majority of the respondents were male, with 7 or 88 percent, graduates of a bachelor's degree with 6 or 75 percent, and had a length of service of 10 years and above with 5 or 63 percent. Meanwhile, there were 400 respondents in the survey for EFA. Out of the total population, 145 or 36.25 percent of the participants belonged to the age group of 26-29 years old. There were 257 or 64.25 percent female and 139 or 34.75 percent male respondents.

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

Table 3

Demographic Profile of Respondents

Variable		*n**	Percentage
a. In-Depth Interview Participants			
Age Group	26-29	0	0
	30-33	2	25
	34-37	2	25
	38-41	4	50
Sex	Male	7	87.50
	Female	1	12.50
	Prefer not to say	0	0
Educational Attainment	Bachelor's Degree	6	75
	Graduate Degree	2	25
	Others	0	0
Length of Service	Below 1 year	0	0
	1-3 years	0	0
	4-6 years	2	25
	7-10 years	1	12.50
	10 yrs above	5	62.50
Total		8	100
b. Survey Respondents for EFA			
Age Group	26-29	145	36.25
	30-33	92	23
	34-37	70	17.5
	38-41	93	23.25
Sex	Male	139	34.75
	Female	257	64.25
	Prefer not to say	4	1
Educational Attainment	Bachelor's Degree	308	77
	Graduate Degree	60	15
	Others	32	8
Length of Service	Below 1 year	56	14
	1-3 years	101	25.25
	4-6 years	126	31.5
	7-10 years	61	15.25
	10 yrs above	56	14
Total		400	100
c. Survey Respondents for CFA			
Age Group	26-29	225	45
	30-33	107	21.4
	34-37	82	16.4
	38-41	86	17.2
Sex	Male	287	39.4
	Female	197	57.4
	Prefer not to say	16	3.2
Educational Attainment	Bachelor's Degree	328	65.6
	Graduate Degree	89	17.8
	Others	83	16.6
Length of Service	Below 1 year	91	18.2
	1-3 years	125	25
	4-6 years	143	28.6
	7-10 years	71	14.2
	10 yrs above	70	14

[1]Corresponding Author: Lyn Marie C. Centeno
*Corresponding Email: l.centeno.522997@umindanao.edu.ph

Total	500	100

n = Population per Subgroup*

Within the population, there were 308 or 77 percent of participants with bachelor's Degrees, while 60 or 15 percent had Graduate Degrees. The majority, comprising 126 respondents or 31.5 percent of the total population, have 4 to 6 years of service. Lastly, another set of 500 respondents took part in the survey for CFA. Majority of the respondents belonged to an age group of 26-29 comprising 225 or 45 percent of the total population, male respondents with 287 or 39 percent, those who completed bachelor's degree with 328 or 66 percent, and had a length of service of 4-46 years with 143 respondents or 29 percent.

Presented in Table 4 are the results affirming the sample's suitability for Exploratory Factor Analysis (EFA). The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy yielded a high value of 0.927, exceeding the acceptable threshold of 0.5, indicating the dataset's robustness for identifying distinct factors. According to the KMO standards (Olkin and Samson, 2001), this high KMO value indicates that the dataset is well-suited for identifying distinct factors. Furthermore, Bartlett's test of sphericity showed significant results ($p < 0$), confirming interrelationships among variables and supporting the dataset's appropriateness for factor analysis. This test assessed whether the correlation matrix (R-matrix) significantly differs from an identity matrix.

Table 4
KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.927
Bartlett's Test of Sphericity	Approx. Chi-Square	20791.593
	df	1770
	Sig.	0

The latent roots criterion of the nine extracted factors and their variance are presented in Table 5. The first factor has an eigenvalue of 20.831 (34.719 percent variance), the second factor has an eigenvalue of 6.676 (11.126 percent variance), and the third factor has an eigenvalue of 4.489 (7.481percent variance). Overall, these factors explain 69.282 percent of the vulnerability behaviors of millennial government employees toward cyberterrorism.

Table 5
Total Variance Explained

	Total	Percentage of Variance	Cumulative Percentage
1	20.831	34.719	34.719
2	6.676	11.126	45.845
3	4.489	7.481	53.326

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

4	2.07	3.449	56.776
5	2.017	3.361	60.137
6	1.663	2.772	62.909
7	1.467	2.445	65.354
8	1.232	2.053	67.408
9	1.125	1.876	69.283
		69.282	

Illustrated in Figure 4 is the scree plot from the secondary Exploratory Factor Analysis (EFA), which charts eigenvalues on the vertical axis against factors on the horizontal axis. As outlined by Cattell (1966), the "elbow" in the plot, where the eigenvalue magnitude sharply declines, indicates the number of meaningful factors for analysis. In this study, the plot reveals a significant drop after the third factor, confirming the instrument's multidimensional structure. Gorsuch (1997) noted that the effectiveness of the Scree Test depends on sufficient sample size and well-defined factors, both of which are met in this investigation.

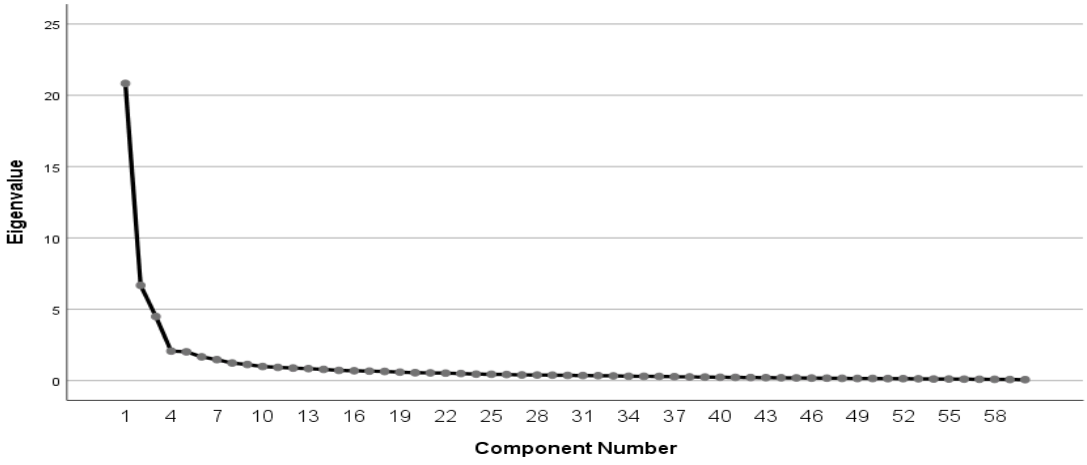

Figure 4
Scree Plot

The EFA grouped 60 items into nine factors defining cyberterrorism vulnerability among millennial government employees: Organizational Cybersecurity Readiness, Cyberterrorism Awareness and Risk Perception, Risky Digital Behaviors, Personal Cybersecurity Practices, Secure IT Infrastructure, Perceptions of Cybersecurity Training, Shared Security Accountability, Perceived Cybersecurity Vulnerability, and Unsecure Data Transfer Practices.

The factor loadings and thematic analysis as presented in Table 6 confirmed these distinct factors, with all factor loadings exceeding the acceptable threshold of 0.40 and most items loading above 0.50, indicating strong item reliability and construct validity.

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

However, the ninth factor, which contained fewer than three items, was removed in accordance with guidelines from MacCallum et al. (1999), Raubenheimer (2004), and others (Fuentes & Gono, 2023; Gono Jr et al., 2021; 2024). Therefore, item number 60 under Unsecure Data Transfer Practice, highlighted in red font, was eliminated based on EFA guidelines.

Table 6

Factor Loading and Thematic Analysis

Factors	Items	Rotated Component Matrix								
		1	2	3	4	5	6	7	8	9
1. Organizational Cybersecurity Readiness (OCR)	1	0.85								
	2	0.841								
	3	0.837								
	4	0.835								
	5	0.831								
	6	0.828								
	7	0.826								
	8	0.823								
	9	0.807								
	10	0.803								
	11	0.802								
	12	0.799								
	13	0.786								
	14	0.765								
	15	0.739								
	16	0.738								
	17	0.717								
	18	0.703								
	19	0.671								
	20	0.671								
	21	0.584								
	22	0.511								
2. Cyberterrorism Awareness and Risk Perception (CAR)	23		0.831							
	24		0.828							
	25		0.765							
	26		0.743							
	27		0.698							
	28		0.546							
3. Risky Digital Behaviors (RDB)	29			0.852						
	30			0.846						
	31			0.817						
	32			0.769						
	33			0.696						
	34			0.577						
	35			0.528						
	36			0.409						
4. Personal Cybersecurity Practices (PCP)	37				0.789					
	38				0.724					
	39				0.718					
	40				0.642					
	41				0.641					
	42				0.46					
5. Secure IT Infrastructure (SII)	43					0.653				
	44					0.642				
	45					0.627				
	46					0.615				
	47					0.609				
6. Perceptions of Cybersecurity Training (PCT)	48						0.739			
	49						0.701			
	50						0.656			
	51						0.6			
	52						0.554			
7. Shared Security Accountability (SSA)	53							0.741		
	54							0.612		
	55							0.535		
	56							0.503		
8. Perceived Cybersecurity Vulnerability (PCV)	57								0.63	
	58								0.536	
	59								0.47	

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

9. Unsecure Data Transfer Practice (UDTP)	60		0.742

Extraction Method: Principal Component Analysis.
Factor Loading Threshold: 0.40

Rotation Method: Varimax with Kaiser Normalization.

A Rotation converged in 14 iterations.

The factor loadings and thematic analysis as presented in Table 6 confirmed these distinct factors, with all factor loadings exceeding the acceptable threshold of 0.40 and most items loading above 0.50, indicating strong item reliability and construct validity. However, the ninth factor, which contained fewer than three items, was removed in accordance with guidelines from MacCallum et al. (1999), Raubenheimer (2004), and others (Fuentes & Gono, 2023; Gono Jr et al., 2021; 2024). Therefore, item number 60 under Unsecure Data Transfer Practice, highlighted in red font, was eliminated based on EFA guidelines.

OCR emphasizes the value of readiness in bolstering government institutions' resistance to cyberattacks, including clear cybersecurity policies, proactive tactics, and sufficient funding. Since increased awareness has a direct impact on proactive cybersecurity behaviors, CAR emphasizes the necessity for staff members to comprehend and evaluate cyber risks. On the other hand, RDB—such as downloading illegal software, using incorrect passwords, and sharing data in an unsecure manner—becomes a major source of vulnerabilities. On the other hand, PCP is essential for reducing cyber risks at the individual level. This includes secure password management and frequent software updates.

The study also highlights the technological and organizational aspects of cybersecurity. SII highlights that in order to resist cyberterrorism, strong networks, safe data storage, and dependable communication platforms are essential. PCT displays the opinions of the staff regarding the applicability and accessibility of training courses that have a big impact on their readiness and consciousness. SSEA reflects the importance of fostering a collective responsibility among all levels of employees to secure organizational systems and promoting adherence to policies. Lastly, PCV highlights how employees' awareness of their organization's susceptibility to threats can shape their behaviors, either encourage proactive actions or trigger risk-avoidance tendencies. These factors offer a comprehensive framework for understanding and addressing cybersecurity vulnerabilities in government institutions.

Framework Validation

A 59-item refined survey, derived from EFA results, was administered to 500 respondents for CFA. Illustrated in Figure 5 is the baseline model of cyberterrorism vulnerability behavior as a result of the CFA generated with AMOS software. The model presents interrelationship between the eight factors of cyberterrorism vulnerability

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

behavior and their respective indicators identified during factor loadings and thematic analysis.

The baseline model demonstrated a reasonable fit with a Chi-Square Ratio (X^2/df) of 2.987, which is within the acceptable threshold of 3.00. However, the Incremental Fit Indices (IFI, CFI, and TLI) were all below the acceptable value of 0.90, indicating poor model fit. The Root Mean Square Error of Approximation (RMSEA) was 0.084, slightly above the acceptable threshold of 0.08, suggesting marginal misfit, while the PCLOSE value of 0.00 confirmed the RMSEA was not statistically acceptable.

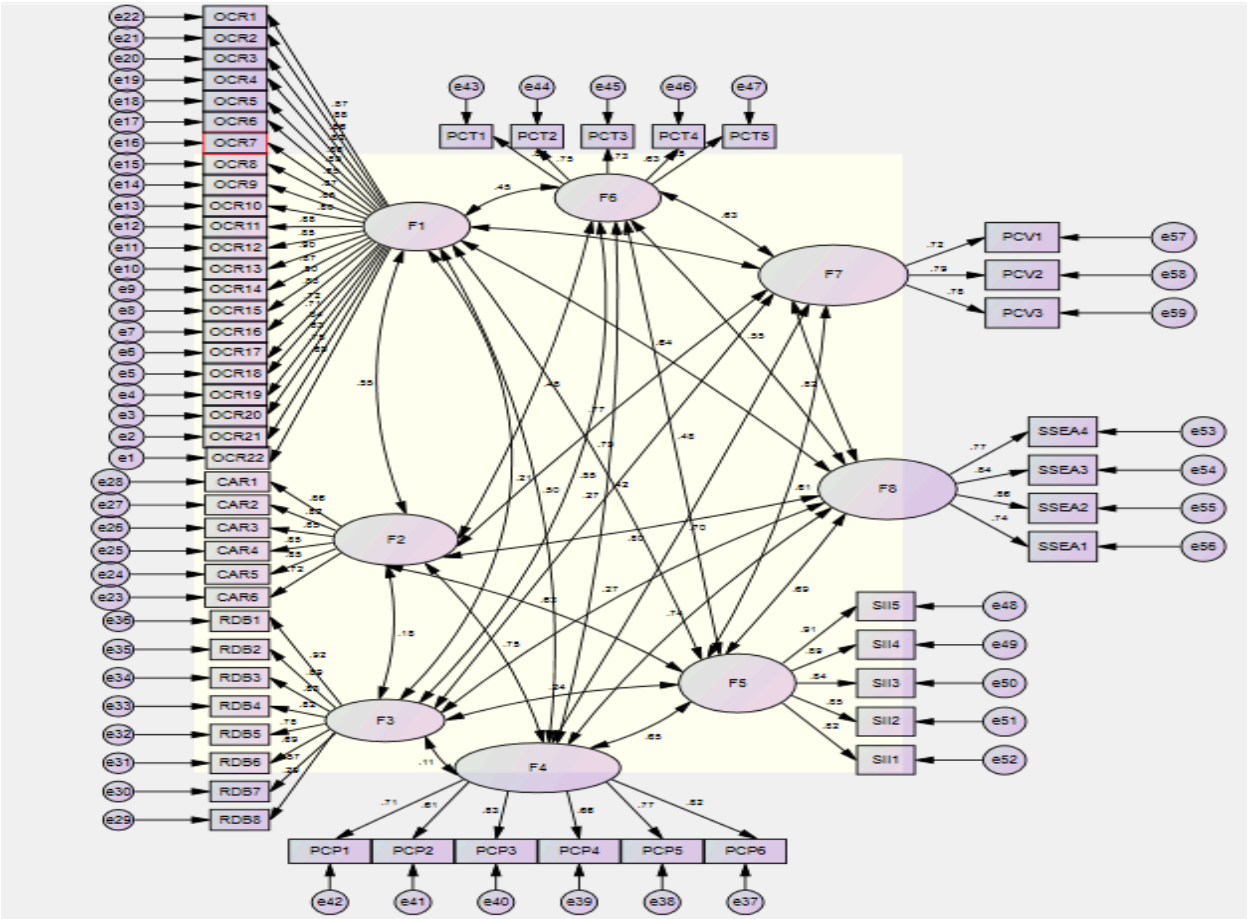

Figure 5
Baseline Model

Legend:

OCR – Organizational Cybersecurity Readiness (F1)
CAR – Cybersecurity Awareness and Risk Perception (F2)
RDB – Risky Digital Behavior (F3)
PCP – Personal Cybersecurity Practices (F4)
SII – Secure IT Infrastructure (F5)
PCT – Perceptions of Cybersecurity Training (F6)
PCV – Perceived Cybersecurity Vulnerability (F7)

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

SSEA – Shared Security Accountability (F8)

Table 7 presents the model fit indices for the baseline model and the six successive modifications made to derive the best-fit model for cyberterrorism vulnerability behavior. Each modification aimed to improve model fit based on statistical criteria and theoretical justifications, ensuring a more accurate representation of the factors influencing cyberterrorism vulnerability.

Table 7
Model Fit Indices

	X2	X2/df	IFI	CFI	TLI	RMSEA	PCLOSE
Baseline Model	4850.719	2.987	0.815	0.814	0.804	0.084	0.00
1. Modification 1 Delete items with standardized weights <0.7	3396.953	2.962	0.853	0.852	0.842	0.081	0.00
2. Modification 2 Delete Factors standardized weights <0.5	2949.71	3.192	0.853	0.853	0.842	0.086	0.00
3. Modification 3 Delete items with standardized weights <0.7 Correlate error	1708.264	2.210	0.932	0.931	0.915	0.064	0.00
4. Modification 4 Delete Factor 6	1442.086	2.198	0.940	0.939	0.924	0.063	0.00
5.Modification 5 Delete items <0.8 and delete factor <3 items	463.088	2.215	0.97	0.970	0.957	0.064	0.002
6.Modification 5 Delete Factor 5	231.162	2.212	0.983	0.983	0.970	0.061	0.047

[1]Corresponding Author: Lyn Marie C. Centeno
*Corresponding Email: l.centeno.522997@umindanao.edu.ph

7. Modification 6 Delete items <0.8	152.710	1.933	0.988	0.988	0.979	0.056	0.224
Acceptable Values	-	<3.00	0.90	0.90	0.90	<0.08	>0.05
Good Fit Values	p<0.05		0.95	0.95	0.95	<0.08	>0.05

In Modification 1, items with standardized weights below 0.7 were deleted, leading to slight improvements in the fit indices, with IFI, CFI, and TLI increasing to approximately 0.85 and RMSEA reducing to 0.081, though the overall fit remained marginal. Modification 2, which involved deleting factors with standardized weights below 0.5, slightly worsened the model fit, as indicated by an increase in X^2/df to 3.192 and RMSEA to 0.086, with no change in the incremental fit indices (~0.853).

In Modification 3, further improvement was achieved by deleting items with standardized weights below 0.7 and correlating errors, resulting in significant enhancement of the incremental fit indices to ~0.93 and RMSEA reducing to 0.064, meeting acceptable thresholds. Subsequent refinement in Modification 4, which involved deleting Factor 6, further improved the fit, with IFI, CFI, and TLI reaching ~0.94 and RMSEA slightly decreasing to 0.063, achieving close-to-good fit values. Modification 5 involved deleting items with standardized weights below 0.8 and factors with fewer than three items, yielding substantial improvements, with the incremental fit indices increasing to ~0.97 and RMSEA remaining at 0.064. The PCLOSE value also improved to 0.002, nearing the good-fit criteria.

In Modification 6, deleting Factor 5 resulted in excellent model fit, with incremental fit indices exceeding 0.98, RMSEA decreasing to 0.061, and PCLOSE improving to 0.047, signaling strong improvement. The final modification, which involved deleting items with standardized weights below 0.8, yielded the best-fit model with X^2/df reduced to 1.933, incremental fit indices further improving to ~0.988, RMSEA reduced to 0.056, and PCLOSE increasing to 0.224. This final model met or exceeded all good-fit criteria.

The final modification (Modification 6, deleting items <0.8) as presented in Figure 6 achieves the best model fit, with all indices meeting or exceeding the good-fit thresholds. Earlier modifications show progressive improvement, with Modification 3 onwards contributing significant gains in fit quality.

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

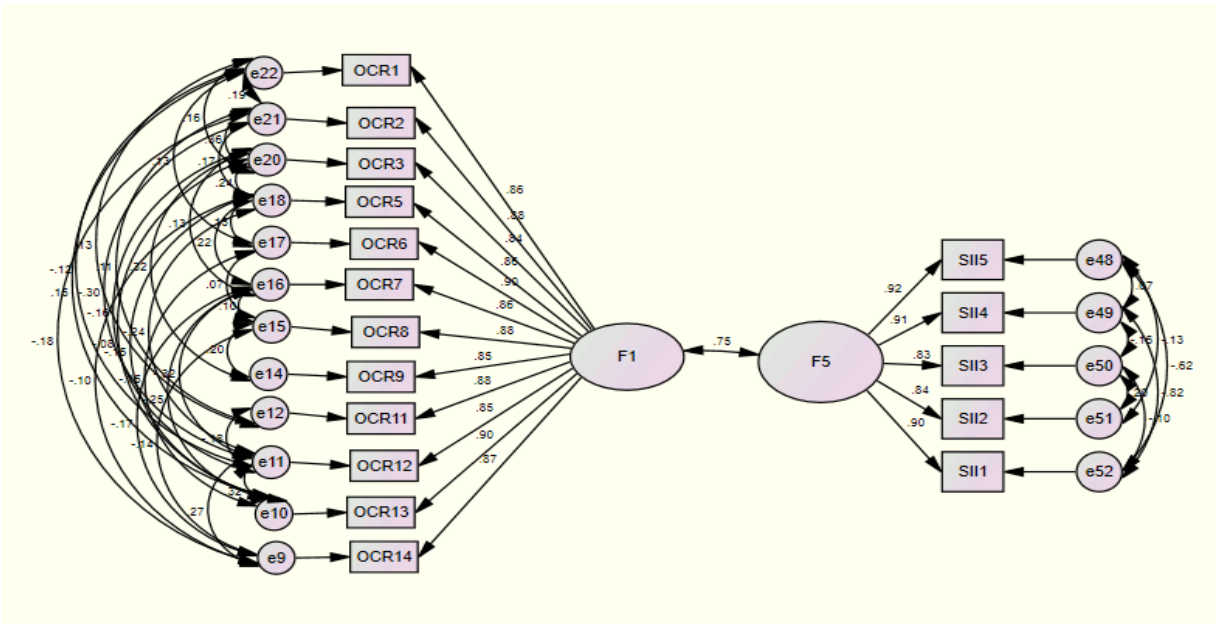

Figure 6
Best Fit Model Structure

Legend:
OCR – Organizational Cybersecurity Readiness (F1)
SII – Secure IT Infrastructure (F5)

Table 8 presents the results for items loading onto Organizational Cybersecurity Readiness (F1) and Secure IT Infrastructure (F5), including estimates of factor loadings, standard errors (S.E.), critical ratios (C.R.), and significance levels (P). These results are essential for assessing composite reliability (CR) and convergent validity.

For Factor 1 (OCR), loadings range from 0.937 to 1.138, demonstrating strong contributions of all items to the latent construct and excellent alignment with the underlying dimension. The standard errors range from 0.045 to 0.059, indicating precise and reliable estimates, while the critical ratios range from 18.400 to 23.489, significantly exceeding the threshold of 1.96, confirming statistical significance at $p < 0.001$. These results indicate that all items for Factor 1 are reliable indicators, strongly supporting convergent validity.

Table 8
Results of composite reliability and convergent validity testing

			Estimate	S.E.	C.R.	P
OCR14	<---	F1	1.066	.052	20.297	***
OCR13	<---	F1	1.061	.045	23.489	***
OCR12	<---	F1	1.078	.059	18.400	***
OCR11	<---	F1	1.060	.047	22.659	***

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

			Estimate	S.E.	C.R.	P
OCR9	<---	F1	1.075	.054	19.878	***
OCR8	<---	F1	1.138	.055	20.851	***
OCR7	<---	F1	.937	.047	19.848	***
OCR1	<---	F1	1.000			
OCR3	<---	F1	.962	.046	21.125	***
OCR5	<---	F1	.944	.048	19.716	***
OCR6	<---	F1	1.069	.046	23.392	***
OCR2	<---	F1	1.034	.045	23.214	***
SII5	<---	F5	1.000			
SII4	<---	F5	.987	.041	23.867	***
SII3	<---	F5	.771	.047	16.469	***
SII2	<---	F5	.851	.048	17.861	***
SII1	<---	F5	.890	.048	18.359	***

Similarly, for Factor 5 (SII), the loadings range from 0.771 to 1.000, indicating strong contributions to the construct, with all but one item exceeding the typical threshold of 0.70. The standard errors range from 0.041 to 0.048, reflecting high precision, and the critical ratios range from 16.469 to 23.867, also significantly above 1.96, and confirming statistical significance at $p < 0.001$. These results support the convergent validity of F5.

Both factors meet the criteria for convergent validity, with high and statistically significant loadings and low standard errors, confirming that items within each factor effectively measure the same underlying construct. Although discriminant validity is not explicitly tested in the table, the strong internal loadings for F1 and F5 suggest that the factors remain distinct and measure separate constructs. Composite reliability is supported by the high factor loadings across both factors, which also show excellent internal consistency.

In summary, F1 and F5 show strong convergent validity and composite reliability, indicating that the items measure their respective latent constructs robustly and make a substantial contribution to the model's overall validity and reliability.

In order to assess convergent and discriminant validity, Table 9 analyzes the correlation estimate, standard error (S.E.), critical ratio (C.R.), and significance level (P-value) of OCR (F1) and SII (F5).

Table 9
Convergent/Discriminant Validity

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

			Estimate	S.E.	C.R.	P
F5	<-->	F1	.478	.051	9.359	***

A moderately positive relationship is indicated by the estimated correlation of 0.478 between OCR and SII. The value is significantly below the threshold of 0.85, which is frequently used to suggest excessive correlation and a possible lack of discriminant validity, even though it suggests some overlap between the two factors. The precision of this correlation estimate is demonstrated by the standard error of 0.051, and the statistical significance of the relationship at $p < 0.001$ is confirmed by the critical ratio of 9.359, which is significantly above the 1.96 threshold.

From a convergent validity perspective, the moderate correlation indicates that OCR and SII are related constructs that share some common variance. Meanwhile, the correlation of 0.478, being well below the threshold of 0.85, provides evidence of discriminant validity, affirming that OCR and SII are sufficiently distinct and measure different underlying constructs. While the factors are related, their significant yet moderate relationship confirms they are not redundant.

In conclusion, OCR and SII demonstrated a balanced relationship that supports both convergent and discriminant validity, contributing to the overall validity of the measurement model.

Table 10 presents the reliability assessment of the sub-scales, evaluated using Cronbach's Alpha, which measures the internal consistency of items within each factor.

Table 10
Level of Reliability

Sub-scale	Number of Items	Cronbach's Alpha
1. OCR (F1)	12	0.979
2. SII (F5)	5	0.942
Total	17	0.976

OCR, which has 12 items, has a Cronbach's Alpha of 0.979, which shows that the construct is consistently measured and has very high reliability. Similar to this, SII, which consists of five items, exhibits strong internal consistency and stability with a Cronbach's Alpha of 0.942. Using 17 items from both factors, the total scale has an excellent overall reliability of 0.976, as measured by Cronbach's Alpha.

Both OCR and SII, as well as the entire scale, surpass the requirements for robust internal consistency based on widely recognized thresholds for Cronbach's Alpha, where values ≥ 0.9 indicate excellent reliability. These findings imply that each factor's items

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

measure their respective constructs consistently, and that the instrument as a whole can be used with confidence in research to accurately and consistently assess the constructs that the factors OCR and SII represent. In summary, the stability and validity of the measurement model are supported by the high reliability of OCR, SII, and the total scale.

The final scale, validated by CFA, is shown in Table 11 and represents the model structure that best fits the theoretical constructs of cyberterrorism vulnerability behavior among millennial government employees.

Table 11
Final Cyberterrorism Vulnerability Behavior Scale

Item Statements	Rating Scale				
	5	4	3	2	1
A. Organizational Cybersecurity Readiness					
1. Our LGU has sufficient funds to stay updated with the latest cybersecurity tools					
2. Our LGU has an IT team that is equipped with adequate training and resources to stay up-to-date with cyber threats.					
3. Our LGU has IT department that is well-funded and equipped to maintain cybersecurity systems.					
4. Our LGU has defined consequences for employees who violate cybersecurity policies.					
5. Our LGU conducts Cybersecurity awareness and education.					
6. Our LGU has employees who receive cybersecurity orientation hired.					
7. Our LGU foster Cybersecurity as part of its long-term organizational goals.					
8. Our LGU has clear cybersecurity policies that are strictly enforced.					
9. Our LGU prioritizes Cybersecurity awareness and education.					
10. Our LGU receives adequate support and resources from management to promote cybersecurity.					
11. Our LGU has adequate staff and resources to support cybersecurity capabilities.					
12. Our LGU promptly addresses cybersecurity threats when they arise.					
B. Secure IT Infrastructure					
13. Our LGU's department has workstations that are securely connected to a centralized data system.					
14. Our LGU's department has workstations that are securely connected to a centralized data system.					
15. Our LGU's department ensures that all communication platforms are secure for official use.					
16. Our LGU's department has database systems that are adequately secured and regularly monitored.					
17. Our LGU's department uses secure methods for data sharing within the departments.					

The two factors, OCR and SII, provided the best model fit, according to the CFA done on the survey data gathered from LGU employees. The OCR emphasizes how crucial policies, training, and readiness are to reducing vulnerabilities. Employee perceptions of

[1]Corresponding Author: Lyn Marie C. Centeno
*Corresponding Email: l.centeno.522997@umindanao.edu.ph

the value of organizational readiness, policies, and training in reducing cyber vulnerabilities are reflected in this factor. It highlights how employees' perceptions of organizational expectations and available resources impact their cybersecurity behaviors, which is consistent with the Theory of Planned Behavior's concepts of attitude toward behavior, subjective norms, and perceived behavioral control (Ajzen, 1991; Zubko, 2021).

Additionally, by emphasizing how policies and training improve awareness and self-efficacy in fending off threats, OCR supports the Protection Motivation Theory's (PMT) focus on threat and coping appraisals (Rogers, 1975). According to the Unified Theory of Acceptance and Use of Technology (UTAUT), OCR emphasizes the significance of social influence, performance expectancy, effort expectancy, and facilitating conditions in promoting secure behaviors. It also shows that organizational support has a major impact on employees' willingness to participate in cybersecurity practices (Venkatesh et al., 2003; Oliveira et al., 2020).

Likewise, the SII emphasizes how strong technological tools and systems can lessen vulnerability to cyberattacks. It highlights how robust tools and systems can lessen vulnerability to online threats. In line with TPB's constructs of attitude, subjective norms, and perceived behavioral control, SII builds employee trust and confidence by showcasing the company's dedication to cybersecurity (Ajzen, 1991; Choi et al., 2021). By demonstrating how effective secure technology systems are at reducing risks, this construct also supports PMT's coping appraisal and increases employees' motivation to take protective actions (Bülthoff & Karnowski, 2019; Rogers, 1975). In terms of UTAUT, SII deals with performance expectations and enabling conditions, making sure that workers have the resources and technical assistance they need to follow safe procedures (Venkatesh et al., 2003; Alotaibi et al., 2021).

The results emphasize how organizational, technological, and behavioral factors influence LGU employees' susceptibility to cyberterrorism. Whereas PMT describes the motivational dynamics of threat and coping appraisals in adopting protective behaviors, TPB emphasizes how attitudes, social norms, and perceived control drive individual behaviors. UTAUT highlights how crucial organizational support, performance expectations, and enabling circumstances are in influencing workers' propensity to use secure practices. Together, these theories demonstrate that the behavior of cyberterrorism vulnerability is a complex phenomenon impacted by organizational and human factors. Moreover, the findings underscore the critical role of organizational readiness and robust IT infrastructure in mitigating cyber risks, particularly in the context of LGUs where resource limitations often challenge cybersecurity efforts (Choi, Lee & Kim, 2021; Oliveira et al, 2020).

CONCLUSION AND RECOMMENDATIONS

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

The multifaceted concept of cyberterrorism vulnerability behavior is greatly influenced by organizational and human factors. The findings highlight the critical role that organizational readiness and strong technological systems play in mitigating cyber risks by identifying eight critical dimensions, with OCR and SII emerging as the most influential. A thorough framework for comprehending how attitudes, perceived risks, organizational norms, and technological support all work together to influence cybersecurity behaviors is offered by the combination of the TPB, PMT, and UTAUT. These observations are especially pertinent, though not exclusive, to LGUs, where persistent cyber challenges are caused by a lack of resources and changing threats. In order to effectively address cyber vulnerabilities, the study emphasizes the need for focused interventions like improving training programs, fortifying policies, and investing in IT infrastructure.

Stronger IT infrastructure increased digital literacy, and improved government cybersecurity readiness are all clear outcomes of the DICT, NPC, and LGUs' continuous efforts to promote cybersecurity and data privacy. Raising awareness of cyberthreats and increasing access to safe digital resources have been made possible by a number of national initiatives. Similarly, security measures in various sectors have been strengthened by regulatory initiatives targeted at data privacy protection, compliance monitoring, and public awareness. In response to the increasing risks associated with cyber threats, the LGU has taken action to implement IT security policies and cybersecurity awareness programs. However, additional steps might need to be investigated in order to guarantee a more thorough and proactive approach in addressing cyberterrorism vulnerability among LGU employees.

According to the study's findings, LGUs should create a Standardized Cybersecurity Compliance Framework in order to help ensure that cybersecurity measures are implemented consistently. The lack of a specific cybersecurity framework for LGUs suggests gaps in risk assessments, regular cybersecurity audits, and compliance reporting mechanisms, even though government agencies are guided by existing data privacy policies. Furthermore, given that current procedures seem to lack a systematic approach, the results suggest that LGUs may need to strengthen cybersecurity risk assessment and vulnerability analysis. In order to regularly assess LGU vulnerabilities and offer customized security recommendations, the NPC, working with DICT, may find it helpful to implement a Cybersecurity Readiness and Risk Evaluation Program.

Localized cybersecurity and data protection regulations may also be able to help LGUs with their particular problems, such as limited funding, a lack of technical know-how, and inadequate IT infrastructure. These guidelines' alignment with international cybersecurity standards might be a sign of a more robust strategy for thwarting changing cyberthreats. Furthermore, since the results show that specific capacity-building efforts beyond broad digital literacy programs are required, the creation of a Cyber Resilience Training Program for LGU Employees may be taken into

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

consideration. A more cybersecurity-aware workforce within LGUs could result from training programs that emphasize social engineering awareness, phishing detection, cyber hygiene practices, and incident response procedures.

It also suggests that LGU-level cybersecurity policy enforcement mechanisms might need to be improved. DICT's adoption of a Cybersecurity Compliance Monitoring and Enforcement System may be a sign of a more methodical approach to carrying out regular security assessments, guaranteeing adherence to security procedures, and mitigating hazards that have been identified. According to the findings, LGU compliance may be impeded by financial constraints. As a result, a Cybersecurity Infrastructure Grant Program may be necessary to help acquire secure IT infrastructure, endpoint security solutions, and real-time threat detection systems.

Lastly, the findings show how beneficial it could be for LGUs to create a centralized cyber threat intelligence and early warning system. The creation of an LGU-focused cyber threat intelligence network may indicate a more focused approach in offering real-time monitoring, threat intelligence sharing, and coordinated response strategies, even though DICT currently keeps an eye on national cybersecurity threats. By putting these suggestions into practice, LGUs may become more cybersecurity resilient, lower their risk of cyberterrorism, and strengthen their defenses against cyberattacks and the loss of vital government data.

This study is subject to several limitations. First, the data collection was confined to Region XII, Philippines limiting the generalizability of the findings to other regions, levels of the government or industries. The framework could also be applied to other sectors like private industries, healthcare, financial institutions, educational institutions, military and defense agencies, or other local or national government agencies. Second, the study primarily focused on millennials, potentially overlooking generational differences in cybersecurity behavior. Third, the cross-sectional design of the study limits the ability to establish causal relationships between constructs. A longitudinal study would also help identify trends, shifts in cybersecurity awareness, and the effectiveness of interventions over time. Finally, while the study incorporated TPB, PMT, and UTAUT, additional theoretical frameworks, such as organizational culture theories, may provide deeper insights into the contextual factors influencing cybersecurity practices.

FUNDING

The authors did not receive financing for the development of this research.

INSTITUTIONAL REVIEW BOARD STATEMENT

This study adhered to the full ethical standards set by the University of Mindanao Professional Schools. The UM Ethics Review Committee reviewed the norms of this

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

dissertation, which cover privacy and confidentiality, informed consent, voluntary participation, benefits, recruitment, risks, fabrication, plagiarism, falsification, deceit, permission from organizations/locations, conflict of interest (COI), and authorship. This study was issued with UMERC Certification No. UMERC-2024-318 after having complied with the research ethics requirements.

INFORMED CONSENT

The researcher obtained informed consent from participants by providing clear information about the study's purpose, procedures, potential risks, confidentiality measures, and the voluntary nature of participation. Only those employed in regional and local government units (LGUs) in Region XII who gave their consent were included, while those who declined or did not meet the criteria were excluded. Participants were assured of their right to privacy, confidentiality, and the freedom to withdraw at any time without penalty. The consent process also addressed possible cognitive risks and outlined mitigation and follow-up measures.

ACKNOWLEDGEMENTS

The authors would like to thank the respective LGU heads, admin staffs and respondents in Region XII, Philippines for their active participation and support to this study.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211.

Alghamdi, A. (2022). A systematic review on human factors in cybersecurity. IJCSNS International Journal of Computer Science and Network Security, 22(10), 282. https://doi.org/10.22937/IJCSNS.2022.22.10.36

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. Applied Sciences, 13(9), 5700. https://doi.org/10.3390/app13095700

Alotaibi, R. M., Houghton, L., & Sandhu, K. (2021). Exploring cybersecurity awareness in Saudi Arabia. Computers & Security, 104, 102203. https://doi.org/10.1016/j.cose.2021.102203

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

Alzubaidi, A. (2021). Measuring the level of cybersecurity awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

Aurigemma, S., Mattson, T., & Leonard, L. (2019). Evaluating the core and full protection motivation theory nomologies for the voluntary adoption of password manager applications. AIS Transactions on Replication Research, 5, 1–21. https://doi.org/10.17705/1atrr.00035

Bakry, M., Syatar, A., Abubakar, A., Risal, C., Ahmad, A., & Amiruddin, M. M. (2021). Strengthening the cyber terrorism law enforcement in Indonesia: Assimilation from Islamic jurisdiction. International Journal of Criminology and Sociology, 10, 1267–1276. https://doi.org/10.6000/1929-4409.2021.10.146

Bülthoff, A., & Karnowski, V. (2019). Coping with cyber risks: Exploring protective motivation and preventive measures. Cyberpsychology, Behavior, and Social Networking, 22(7), 463–471. https://doi.org/10.1089/cyber.2018.0733

Caliwan, C. L. (2023). PNP-ACG probes "massive" data breach | Philippine News Agency. Pna.gov.ph. https://www.pna.gov.ph/articles/1199811

Cattell, R. B. (1966). The scree test for the number of factors. Multivariate Behavioral Research, 1(2), 245–276.

Center for Strategic and International Studies. (2023). Significant cyber incidents. CSIS. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Chandrika, K. L., Adiperkasa, R. P., & Ningtyas, Y. (2018). Cyber terrorism in Indonesia. Bulletin of Social Informatics Theory and Application, 2(2), 65–72.

Choi, H., Lee, Y., & Kim, J. (2021). A model of cybersecurity behavior: The role of individual and organizational factors. Journal of Information Security and Applications, 58, 102800. https://doi.org/10.1016/j.jisa.2021.102800

Civil Service Commission. (2023). Statistics and reports. CSC. https://www.csc.gov.ph/downloads/statistics-and-reports/category/426-2023

Cohen-Almagor, R. (2018). Cyberterrorism. In The SAGE encyclopedia of the internet (pp. 169–171). SAGE Publications.

Constantin, M., Bortea, A.-N., & Costovici, D.-A. (2020). Risks and vulnerabilities in digital public services: Threat of cyberterrorism vs. Romania's cybersecurity strategy. Holistica Journal of Business and Public Administration, 11(2), 74–84. https://doi.org/10.2478/hjbpa-2020-0020

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and Mixed Methods Approaches (5th ed.). SAGE Publications. https://extranet.ogs.edu/ogsdial/upload/OXFORD/2024/2643/resources/Creswell_2018.pdf

Dash, B., & Ansari, M. F. (2022). An effective cybersecurity awareness training model: First defense of an organizational security strategy.

Dear millennials, here is why you are a soft target for cybercriminals. (2017, October 10). The Economic Times. https://economictimes.indiatimes.com/tech/internet/dear-millennials-here-is-why-you-are-a-soft-target-for-cyber-criminals/articleshow/61020568.cms

Department of Information and Communications Technology. (2017). National Cybersecurity Plan 2022. https://dict.gov.ph/national-cybersecurity-plan-2022/

Department of Information and Communications Technology. (2019). E-Government Masterplan 2022. https://dict.gov.ph/ictstatistics/wp-content/uploads/2020/03/EGMP-2022.pdf

Dimock, M. (2019). Defining generations: Where Millennials end and Generation Z begins. Pew Research Center. https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins

Fetters, M. D., & Tajima, C. (2022). Joint displays of integrated data collection in mixed methods research. International Journal of Qualitative Methods, 21, 160940692211045. https://doi.org/10.1177/16094069221104564

Fuentes, J. M., & Gono, E. R. (2023). Factors characterizing students' attitude toward learning social studies: An exploratory factor analysis. European Journal of Social Sciences Studies, 8(4).

Ghazali, N. N., Hassan, S., & Ahmad, R. (2023). Fortifying against cyber fraud: Instrument development with the protection motivation theory. International Journal of Advanced Computer Science and Applications, 14(10).

GMA Integrated News. (2025). PH Army confirms "illegal access" attempt on cyber network. GMA News Online. https://www.gmanetwork.com/news/topstories/nation/937244/ph-army-confirms-illegal-access-attempt-on-cyber-network/story/

Gono Jr, E. R. (2024). Determining the students' attitude towards research: An exploratory factor analysis. European Journal of Education Studies, 11(6).

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

Gono Jr, E. R., & Pacoy, E. P. (2021). Redefinition of the parameters of meaningful mathematics learning. Turkish Journal of Computer and Mathematics Education, 12(13), 6524–6542.

Gono, E. J., & Sales, S. L. T. (2024). Dimensionality of strategies in learning mathematics among engineering students: An exploratory factor analysis. TWIST, 19(1), 445–453. https://twistjournal.net/twist/article/view/180

Gorsuch, R. L. (1997). Factor analysis (2nd ed.). Lawrence Erlbaum Associates.

GOVPH. (2007). Republic Act No. 9372. Official Gazette of the Republic of the Philippines. https://www.officialgazette.gov.ph/2007/03/06/republic-act-no-9372/

GOVPH. (2021). Anti-Terrorism Act of 2020. Official Gazette of the Republic of the Philippines. https://www.officialgazette.gov.ph/downloads/2020/06jun/20200703-RA-11479-RRD.pdf

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: A systematic literature review. Journal of Cybersecurity and Privacy, 2(1), 1–18. https://doi.org/10.3390/jcp2010001

Jaymalin, M. (2023, October 19). PhilHealth: 13 million members affected by data breach. Philstar.com. https://www.philstar.com/headlines/2023/10/19/2304835/philhealth-13-million-members-affected-data-breach

John, Y. (2021). Generational differences: A quantitative study in employees' information security knowledge, attitudes, and behavioral intentions [Doctoral dissertation, ProQuest]. https://search.proquest.com/openview/f29a6688ab6b44c27feb513c835bc3f3/1?pq-origsite=gscholar&cbl=18750&diss=y

Kamalia, S., Indartono, S., & Islamiah, R. (2019, June). The role of families on internalization of the tolerance values for millennial generation to decrease the potential of intolerant conflict and radicalism behavior within the multi-religion society. In International Conference on Social Science and Character Educations (IcoSSCE 2018) and International Conference on Social Studies, Moral, and Character Education (ICSMC 2018) (pp. 316–325). Atlantis Press.

Kegler, M. C., Raskind, I. G., Comeau, D. L., Griffith, D. M., Cooper, H. L. F., & Shelton, R. C. (2018). Study design and use of inquiry frameworks in qualitative research published in health education and behavior. Health Education and Behavior, 46(1), 24–31. https://doi.org/10.1177/1090198118795018

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2022). Cybersecurity and risky behaviors in a developing country context: A Pakistani perspective. Security Journal. https://doi.org/10.1057/s41284-022-00343-4

Klein, G., & Zwilling, M. (2023). The weakest link: Employee cyber-defense behaviors while working from home. Journal of Computer Information Systems, 1–15. https://doi.org/10.1080/08874417.2023.2221200

Lagura, G. (2025). Towards Digital Governance Divide Index Development: Evaluating City Government Websites in the Philippines. Journal of Community Development Research (Humanities and Social Sciences), 18(1), 1–17. https://doi.org/10.69650/jcdrhs.2025.717

Lema, K., & Flores, M. (2025, February 18). Philippines reports foreign cyber intrusions targeting intelligence data, but no breaches. Reuters. https://www.reuters.com/technology/cybersecurity/philippines-reports-foreign-cyber-intrusions-targeting-intelligence-data-no-2025-02-18/

MacCallum, R. C., Widaman, K. F., Zhang, S., & Hong, S. (1991). Sample size in factor analysis. Psychological Methods, 4(1), 84–99.

Mangosing, F., & Subingsubing, K. (2024, July). PH Navy foils "hundreds" of hacking attempts. INQUIRER.net. https://newsinfo.inquirer.net/1962403/ph-navy-foils-hundreds-of-hacking-attempts

Moşteanu, N. R. (2020). Challenges for organizational structure and design as a result of digitalization and cybersecurity. The Business and Management Review, 11(1), 278–286.

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behavior in improving cyber security management. Frontiers in Psychology, 12(12). https://doi.org/10.3389/fpsyg.2021.561011

Murray, G. R., Albert, C. D., Davies, K., Griffith, C., Heslen, J., Hunter, L. Y., Jilani-Hyler, N., & Ratan, S. (2019). Toward creating a new research tool: Operationally defining cyberterrorism.

Naidoo, R., & Jacobs, C. (2023). Cyber warfare and cyber terrorism threats targeting critical infrastructure: A HCPS-based threat modeling intelligence framework. European Conference on Cyber Warfare and Security, 22(1), 311–318. https://doi.org/10.34190/eccws.22.1.1443

National Cybersecurity Alliance. (2021). Study: Millennials and Gen Z say they are bigger victims of cybercrime.

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

https://staysafeonline.org/press-release/study-millennials-and-gen-z-say-they-are-bigger-victims-of-cybercrime

Norton. (2016). 2016 Norton Cyber Security Insights Report. https://asia.norton.com/cyber-security-insights-2016

Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2020). Information technology adoption: Going beyond UTAUT and integrating contextual factors. Information and Management, 57(5), 103284. https://doi.org/10.1016/j.im.2019.103284

Olkin, I., & Sampson, A. R. (2001). Multivariate analysis: Overview. ScienceDirect. https://www.sciencedirect.com/science/article/abs/pii/B0080430767004721

Ozeren, S. (2005). Global response to cyberterrorism and cybercrime: A matrix for international cooperation and vulnerability assessment [Doctoral dissertation, University of North Texas]. https://digital.library.unt.edu/ark:/67531/metadc4847/

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed-method implementation research. Administration and Policy in Mental Health and Mental Health Services Research, 42(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y

Plotnek, J. J., & Slay, J. (2021). Cyber terrorism: A homogenized taxonomy and definition. Computers and Security, 102, 102145. https://doi.org/10.1016/j.cose.2020.102145

Ramadhan, I. (2020). Cyber-terrorism in the context of proselytizing, coordination, security, and mobility. Journal of Islamic World and Politics, 4(2). https://doi.org/10.18196/jiwp.4252

Raubenheimer, J. E. (2004). An item selection procedure to maximize scale reliability and validity. SA Journal of Industrial Psychology, 30(4), 59–64.

Reuters. (2024, February 5). Philippines wards off cyber attacks from China-based hackers. Reuters. https://www.reuters.com/world/asia-pacific/philippines-wards-off-cyber-attacks-china-based-hackers-2024-02-05/

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114.

Rutledge, P., & Hogg, J. L. (2020). In-depth interviews. International Encyclopedia of Media Psychology, 1–6. https://doi.org/10.1002/9781119011071.iemp0019

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

Security Brief Australia. (2020). A third of millennials think they're 'too boring' to be victim of cyber attack. https://securitybrief.com.au/story/a-third-of-millennials-think-they-re-too-boring-to-be-victim-of-cyber-attack

Seissa, I. G., Ibrahim, J., & Yahaya, N. (2017). Cyberterrorism definition patterns and mitigation strategies: A literature review. International Journal of Science and Research (IJSR, 6(1), 180–186.

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. Information, 13(9), 413. https://doi.org/10.3390/info13090413

Trong, D., Nguyen, Shih, M.-H., Srivastava, D., Tirthapura, S., & Xu, B. (2019). Stratified random sampling from streaming and stored data. https://www.ece.iastate.edu/snt/files/2019/01/sss-edbt-2019.pdf

Tyson, B. (2018). Generational examination of the factors perceived to affect organizational cybersecurity awareness: A quantitative correlation study [Doctoral dissertation, University of Phoenix].

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cybersecurity culture: Current practices and future needs. Computers & Security, 109, 102387. https://doi.org/10.1016/j.cose.2021.102387

United Nations Office on Drugs and Crime. (2019). Cybercrime Module 14 Key Issues: Cyberterrorism. Unodc.org. https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html

United Nations. (2015). The 17 sustainable development goals. United Nations. https://sdgs.un.org/goals

United Nations: United Nations Office on Drugs and Crime. (2013). COMPREHENSIVE STUDY ON CYBERCRIME - Draft February 2013. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Valeriia, M. (2022, May). Cyberterrorism as a threat to national security of modern states. In The 11th International Scientific and Practical Conference: International Scientific Innovations in Human Life (pp. 598). Cognum Publishing House.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478.

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph

Watkins, M. W. (2018). Exploratory factor analysis: A guide to best practice. Journal of Black Psychology, 44(3), 219–246. https://doi.org/10.1177/0095798418771807

Willie, M. M. (2023). The role of organizational culture in cybersecurity: Building a security-first culture. Social Science Research Network. https://doi.org/10.2139/ssrn.4564291

Zubko, M. (2021). Cyberterrorism: A global threat to financial institutions. Financial Markets, 2021, 145.

[1]Corresponding Author: Lyn Marie C. Centeno
[*]Corresponding Email: l.centeno.522997@umindanao.edu.ph