ISRG Journal of Arts, Humanities and Social Sciences (ISRGJAHSS)

ISRG PUBLISHERS
Abbreviated Key Title: ISRG J Arts Humanit Soc Sci
ISSN: 2583-7672 (Online)
Journal homepage: https://isrgpublishers.com/isrgjahss
Volume – IV Issue -I (January- February) 2026
Frequency: Bimonthly

The Impact of Guardianship, Offender Motivation, and Target Characteristics on Organizational Security in Government Agencies

Mark Patrick L. Nigos[1*], Rhem Rick N. Corpuz (Adviser)[2]

[1, 2] Angeles University Foundation

| **Received:** 16.02.2026 | **Accepted:** 21.02.2026 | **Published:** 28.02.2026

***Corresponding author:** Mark Patrick L. Nigos
Angeles University Foundation

Abstract

This study examined the factors influencing data breach risks in Philippine government entities using Routine Activity Theory, focusing on guardianship, offender motivation, and target characteristics. Drawing from the 2016 COMELEC and 2023 PhilHealth data breaches, the research highlighted how weaknesses in government data management systems exposed sensitive information and increased risks such as identity theft and financial fraud. Data collected from a cross-sectional survey of government employees in Region III were analyzed using multiple linear and moderated regression analyses. Findings revealed that data breach risk was primarily driven by vulnerable information assets and insufficient guardianship rather than offender motivation alone. Government data were found to be highly valuable, visible, and accessible, increasing exposure to cyber threats when protective controls were inconsistently applied. Effective guardianship mechanisms, including institutional policies, oversight, and access controls, significantly reduced breach risks. Moreover, organizational and human-centered protective factors, such as cybersecurity awareness, training, and resistance to social engineering, mitigated vulnerabilities. Overall, the study underscores cybersecurity as a socio-technical issue and provides empirical support for strengthening government cybersecurity measures to protect sensitive public information.

Keywords: Data Breach; Guardianship; Offender Motivation; Target Characteristics

Copyright © ISRG Publishers. All rights Reserved.
DOI: 10.5281/zenodo.18811766

INTRODUCTION

In today's more interconnected world, data breaches have become one of the most pervasive and threatening risks to personal, organizational, and governmental security (Sharma & Barua, 2023). Shukla et al. (2022) stated that a data breach occurs when an unauthorized person accesses, discloses, or steals sensitive, confidential, or protected information. These incidents encompass different types of data, including personal identification information, financial records, health data, and proprietary business information. The aftermath of a data breach is usually catastrophic, affecting individuals, organizations, governments, and even society at large. Recently, high-profile breaches have been widely reported, revealing the vulnerability of digital infrastructures and the disastrous effects of poor data protection (George et al., 2024).

According to Aslan et al. (2023), a data breach results from several causes, such as cybercriminals taking advantage of vulnerabilities within the systems through neglectful handling of sensitive data or internal threats. Generally speaking, extremely sensitive and important data may be compromised by hacking, phishing, or unintentional leaks. Due to this data breach, people may experience financial fraud, identity theft, and privacy violations. Possible effects include significant financial losses, reputational harm to an organization, legal ramifications, and regulatory fines. Attacks against governments that contain vast amounts of public and personal data about residents are also common, and breaches endanger key infrastructure, public trust, and national security (Lehto, 2022).

The increasing number of these breaches requires the need for stronger laws, improved cybersecurity best practices, and heightened awareness of the dangers posed by emerging online threats. Understanding the origins and effects of data breaches is essential for creating plans to reduce risks and shield people and organizations from the far-reaching effects of such events, such as increased reliance on technology and data (Basak, 2024).

One of the most threatening cybersecurity incidents in the country's history shook the Philippines with a jolt in 2016 known as the COMELEC data breach. This breach exposed sensitive information about over 50 million Filipinos and became a defining moment in the nation for cybersecurity awareness. Hackers, called *Anonymous Philippines*, were said to have hacked into the Commission on Elections (COMELEC) servers that it uses to manage voter data in preparation for the upcoming national election. The break-in was more stressful because the servers had significant vulnerabilities, such as unencrypted data and outdated software. It revealed full names, birthdates, addresses, contact details, fingerprints, and even passport numbers, which is an enormous risk in identity theft and even for the manipulation of elections. This has raised the gravest national security concerns, especially the electoral process's integrity. In the wake of the event, the investigations of the National Privacy Commission (NPC) uncovered critical lapses in the system's security. Public outcry erupted, and COMELEC was severely criticized for its inability to safeguard sensitive voter data. This was a wake-up call in the strongest sense, emphasizing the need for more robust cybersecurity within government agencies, especially those handling electoral data (Campbell, 2023).

Seven years later, in 2023, another major data breach hit the Philippines, this time within the Philippine Health Insurance Corporation (PhilHealth). A Medusa ransomware attack locked the organization's sensitive health data; therefore, there was no possible access to it, bringing great concern. Cyber attackers demanded payment to unlock it and ensure no leaked data. While the full extent of the leaked information remains not yet detailed, it is reported to include millions of Filipinos' sensitive personal and health-related information. It revealed serious lapses in PhilHealth's cybersecurity setup have not protected crucial health information. In addition to identity theft and fraud, there was also the possibility of medical claim manipulation, a serious concern regarding individuals' privacy and the integrity of the healthcare system. This attack raised a public outcry and called for stronger regulations and more robust data protection measures in government agencies handling health data. Much like the COMELEC breach, the attack in PhilHealth highlights that the healthcare sector needs improved cybersecurity, advising and cautioning everyone on the need to protect individuals' private health information from malignant perpetrators (Enriquez, 2023).

Both COMELEC and PhilHealth breaches share one thing: they are against the Philippine government's vulnerabilities in data management systems and the pressing need for a thorough investigation into cybersecurity practice. Given the large quantities of sensitive personal, financial, and health data managed by these government agencies, such institutions make perfect targets for cybercriminals. When broken, such information is no longer a commodity but directly affects citizens' lives and national security. For COMELEC, for instance, the breach put the electoral process at stake; for PhilHealth, the privacy and security of healthcare information were at stake. These breaches not only put identity theft and fraud at stake but also significantly affect public trust in institutions that are supposed to guard their citizens' most sensitive data.

Researching data breaches within government agencies in the Philippines can be of paramount importance. It prevents future breaches and fosters a more secure, transparent, and trustworthy government system. This study will seek to inform policy recommendations that can help improve data protection frameworks across government institutions by addressing the systemic vulnerabilities that have led to breaches in the past. Understanding data breaches in the public sector of the Philippines against evolving global cyber threats has a very important role in adapting to new risks and ensuring that government systems will be strong enough to protect citizens' data in the years ahead.

In this respect, the underlying aim of the study is to analyze and review some of the variables that have possible impact to data breaches which includes target characteristics, offender motivation, and guardianship. Overall, the main objective is to study how these factors impact the chances of data breaches. Some specific aims would involve analysis of the incidence of the breach because of guardianship, investigation of effects on the occurrence of breach based on offender motivation, and an examination of the influence of attributes of the target such as perception of value, inertia, visibility, and accessibility (VIVA) on the susceptibility of the breach. The study will also assess how the possibility of breach related to target qualities are affected by variables such as information quality, awareness and training, and social engineering resistance.

UDY OBJECTIVES

General Objective

To investigate the roles of guardianship, offender motivation, and target characteristics influencing the likelihood of data breaches within government organizations.

Copyright © ISRG Publishers. All rights Reserved.
DOI: 10.5281/zenodo.18811766

Specific Objectives

1. To examine how guardianship, offender motivation, and target characteristics affect the likelihood of data breaches, and how these factors may also interact with one another, especially focusing on how strong guardianship, high offender motivation, and vulnerable targets influence breach incidents.
2. To identify how the perceived value, inertia, visibility, and accessibility (VIVA) of a target influence its susceptibility to data breaches.
3. To analyze how information quality, awareness and training, and social engineering resistance moderate the relationships between the value, inertia, visibility, and accessibility (VIVA) of a target and its availability for data breaches.

METHODOLOGY

Study Design and Locale

This study employed a cross-sectional design. This study utilized a standardized questionnaire directed to government employees to investigate the relationships among target features, offender motivation, guardianship, and the likelihood of data breaches in government entities. This session provided critical insights into the distinct dangers and challenges that governmental entities faced while managing significant and sensitive data.

The survey aimed to collect comprehensive information on several critical subjects, including the efficacy of guardianship measures, government officials' perspectives on the causes of criminal behavior, and the characteristics of data targets, such as their value, inertia, visibility, and accessibility. Participants comprised information technology personnel, records officers, and employees with administrative functions from several government agencies. They were selected due to their awareness of the consequences of a breach and their direct familiarity with their agency's data security protocols.

The participants underwent a systematic survey to assess their perspectives and experiences regarding the company's vulnerability to data breaches. To examine the relationships between the factors investigated and the incidence of data breaches, statistical methods such as multiple linear regression and moderated regression analysis were employed. This analytical approach identified the elements most closely associated with heightened dangers. This assisted the public sector in developing more effective data preservation methodologies.

Region III was an ideal location for data security study due to its numerous government entities managing sensitive information, rapid technological advancements, and dynamic economy. The enhanced digital infrastructure and susceptibility to cyberattacks facilitated the examination of factors influencing data protection and cybersecurity challenges in urban environments.

Study Participants

Sample Size and Sampling

The research employed stratified purposive sampling to categorize the population of government employees into relevant subgroups (strata) based on their roles, including IT personnel, records officers, and administrative staff. Participants were deliberately selected from each stratum to ensure a diverse range of perspectives and experiences related to data security policies and data breach incidents. While this approach enhanced representation among key employee groups, the findings might not have been generalizable beyond the sampled population due to the non-random selection within strata.

However, it was noted that PhilHealth denied the researchers' request to gather data, citing the ongoing investigation into the Medusa ransomware attack that occurred in September 2023. As a result, access to primary data from PhilHealth was not granted, which constituted a limitation of the study. A power analysis for multiple regression was performed to ascertain the minimal sample size necessary to resolve statistical power concerns and guarantee that the study had adequate power to identify significant correlations across variables. The table below explains why the participants were chosen:

Research Instrument

The questionnaire for the study was based on "Investigating Perceptions About Risk of Data Breaches in Financial Institutions: A Routine Activity Approach" by Jaeung Lee, Melchor C. de Guzman, Jingguo Wang, Manish Gupta, and H. Raghav Rao (2022). It was significantly modified for the purposes of this investigation. The initial questionnaire was developed using the routine activity framework to examine the occurrence of data breaches in financial institutions. To achieve the study's objectives, the revised questionnaire was modified, administered to a small sample, and validated. To maintain its relevance and utility for the empirical assessment of theories, its fundamental structure and methodology remained unchanged, while modifications were made to accommodate the requirements of government personnel in Region III.

The study instrument, a structured survey questionnaire, was developed to ascertain government employees' perceptions of cybersecurity, their behaviors, and their organization's management of cybersecurity concerns. In addition, face-to-face surveys were conducted among the respondents. The initial section of the instrument, informed consent, delineated the study's objectives, guaranteed the confidentiality of responses, and emphasized that participation was completely voluntary. Participants were informed that their identities would remain confidential and that they could withdraw at any time without repercussions.

The tool incorporated screening questions to ensure that only qualified respondents were included. Qualified respondents were individuals employed by the government, aged eighteen or older, with a specified level of work experience. The survey primarily employed a four-point Likert scale, ranging from "Strongly Agree" to "Strongly Disagree," to assess cybersecurity-related factors, including the effectiveness of guardianship mechanisms (such as incident response and system monitoring), the agency's perceived vulnerability, and the value and complexity of the data managed from a hacker's perspective. An expert evaluation was conducted during the adaptation phase to ensure construct validity. Prior to full implementation, a select group of respondents participated in a pilot test to identify ambiguities, verify internal consistency, and modify items as necessary.

A four-point Likert scale was deliberately selected for this research instrument to enhance the quality and clarity of responses. The neutral midpoint of a five- or seven-point scale allowed respondents to remain ambivalent, whereas the four-point scale required respondents to take a definitive position. Neutrality was considered to obscure meaningful findings or indicate insufficient

Copyright © ISRG Publishers. All rights Reserved.
DOI: 10.5281/zenodo.18811766

engagement, which was particularly critical in a study examining perceptions and behaviors related to cybersecurity. Removing the midpoint enabled the collection of more precise data necessary for accurately assessing attitudes and identifying deficiencies in government personnel's cybersecurity understanding and practices.

The target population also benefited from the four-point scale due to its simplicity, considering potential time constraints or limited survey experience. Fewer response options reduced cognitive load and response fatigue, thereby promoting consistency and intentionality in responses. Although a seven-point scale could have provided additional detail, it was deemed unnecessarily complex without substantially improving data quality. Thus, the four-point format was considered optimal for structured organizational research, balancing usability and analytical depth while producing actionable and comprehensible findings.

Additional dimensions evaluated included data visibility and information accessibility. The instrument contained items addressing information quality, cybersecurity knowledge and training, and employee resistance to social engineering techniques such as phishing and impersonation. Furthermore, open-ended questions encouraged respondents to identify both online and offline locations where critical organizational information might be vulnerable.

The concluding section gathered demographic information, including education, age, gender, length of government service, management level, access to sensitive information, and computer proficiency. This comprehensive framework enabled the researcher to examine multiple risk factors and security behaviors within government entities, thereby supporting the development of informed and context-specific policy recommendations.

DATA ANALYSIS

This study employed a combination of statistical techniques aligned with the research objectives and the nature of the data. Prior to conducting any inferential analyses, the dataset was systematically screened to ensure data quality and compliance with the assumptions required for regression-based analyses. The data were examined for completeness, accuracy, and consistency. Cases with substantial missing responses were excluded, while minimal and randomly distributed missing values were addressed using mean substitution. The dataset was also checked for data entry errors, duplicate cases, and implausible values.

Preliminary diagnostic tests were conducted before model estimation. The dependent variable perceived probability of a data breach—was measured on a continuous scale, satisfying a fundamental requirement for multiple regression analysis. Multiple independent variables were included, namely guardianship, offender motivation, and target characteristics, all measured on continuous scales. Linearity between the dependent and independent variables was assessed using scatterplots and partial regression plots and was found to be acceptable.

Homoscedasticity was evaluated by inspecting plots of standardized residuals against predicted values, which indicated constant variance across levels of the predictors. Multicollinearity was examined using Variance Inflation Factor (VIF) statistics, with all values falling within acceptable thresholds, indicating that multicollinearity was not a concern. The presence of spurious outliers was assessed using standardized residuals and Mahalanobis distance, and no influential cases requiring removal were identified. Normality of residuals was evaluated through histograms with superimposed normal curves, Normal P–P plots, Q–Q plots, and the Shapiro–Wilk test, confirming that residuals were approximately normally distributed. These diagnostic checks confirmed that the dataset met the assumptions required for Multiple Linear Regression (MLR), Moderated Regression Analysis (MRA), and Hierarchical Regression Analysis (HRA).

Multiple Linear Regression (MLR) was then conducted to examine the relationships between guardianship, offender motivation, and target characteristics in relation to perceived data breach likelihood. This approach enabled the simultaneous assessment of multiple predictors and their unique contributions to the outcome variable.

Moderated Regression Analysis (MRA) was employed to examine interaction effects between key predictors and moderating variables, including information quality, cybersecurity awareness and training, and resistance to social engineering. Prior to creating interaction terms, predictor and moderator variables were mean-centered to reduce potential multicollinearity. Assumptions relevant to moderated regression were reassessed and remained within acceptable limits.

To assess the validity and reliability of the measurement instruments, an Exploratory Factor Analysis (EFA) was first conducted to identify the underlying factor structure of the measurement items, using an adequate sample size consistent with methodological guidelines. Subsequently, Confirmatory Factor Analysis (CFA) was performed on the same dataset as a confirmatory robustness check to evaluate the consistency and adequacy of the factor structure identified through EFA, rather than as a strict split-sample validation procedure. Model fit was assessed using established fit indices, including the Comparative Fit Index (CFI), Tucker–Lewis Index (TLI), Root Mean Square Error of Approximation (RMSEA), and Standardized Root Mean Square Residual (SRMR).

Hierarchical Regression Analysis (HRA) was conducted to control for potential confounding demographic variables, such as age, job rank, and length of service. Control variables were entered in the initial block, followed by the main predictors in subsequent blocks, allowing for the assessment of the incremental explanatory power of key variables beyond demographic effects.

All statistical analyses were performed using IBM SPSS Statistics for descriptive and regression analyses, and AMOS or R (lavaan package) for structural equation modeling.

RESULTS

This study investigated factors influencing perceived data breach likelihood using Routine Activity Theory, focusing on guardianship, offender motivation, and target characteristics, alongside organizational and human-centered protective mechanisms. Descriptive results showed that target characteristics were rated highest, indicating that organizational data were perceived as valuable, visible, and accessible, while guardianship and other protective factors were moderate and breach likelihood was above the scale midpoint. Regression analysis revealed that stronger guardianship significantly reduced breach likelihood, whereas more attractive target characteristics substantially increased risk, with offender motivation exhibiting only a marginal effect.

Further moderation analyses demonstrated that information quality, awareness and training, and social engineering resistance

Copyright © ISRG Publishers. All rights Reserved.
DOI: 10.5281/zenodo.18811766

consistently weakened the positive relationships between target characteristics and breach likelihood, highlighting the critical buffering role of organizational controls and human resilience in mitigating data breach risks.

Table 1. Descriptive Statistics of Study Variables (N = 384)

Variable	*Mean*	*SD*
Guardianship	2.91	0.54
Offender Motivation	2.77	0.58
Target Characteristics (VIVA)	3.02	0.49
Information Quality	2.88	0.51
Awareness & Training	2.73	0.57
Social Engineering Resistance	2.69	0.55
Breach Likelihood	2.96	0.52

Note. All variables were measured on a 4-point Likert scale.

Target characteristics had the highest mean, indicating that organizational data were perceived as valuable and accessible. Guardianship and human protective factors were moderate. Breach likelihood was above the midpoint, indicating a moderate perceived risk of data breaches.

Table 2. Multiple Linear Regression Predicting Breach Likelihood

Predictor	*B*	*SE*	*β*	*t*	*p*
Constant	1.217	0.143	—	8.51	< .001
Guardianship	-0.513	0.061	-0.412	-8.43	< .001
Offender Motivation	0.126	0.064	0.094	1.95	.052
Target Characteristics	0.801	0.073	0.529	10.97	< .001

Note. $R^2 = .421$, Adjusted $R^2 = .416$, $F(3, 385) = 93.41$, $p < .001$.

The model explained 42.1% of the variance in breach likelihood. Stronger guardianship reduced risk, while more attractive and accessible data increased risk. Offender motivation showed a marginal association that did not reach conventional statistical significance.

Table 3. Moderation Effects of Information Quality

Predictor	*B*	*SE*	*β*	*t*	*p*
Value (centered)	0.622	0.067	0.471	9.28	< .001
Information Quality (centered)	-0.188	0.059	-0.152	-3.19	.002
Value × Information Quality	-0.166	0.078	-0.091	-2.13	.034

Note. $\Delta R^2 = .0058$, $\Delta F(1, 383) = 4.54$, $p = .034$.

Information quality significantly reduced the effect of data value on breach likelihood, weakening the relationship between valuable data and breach risk.

Table 4. Moderation Effects of Awareness & Training

(a) Visibility × Awareness & Training

Predictor	*B*	*SE*	*β*	*t*	*p*
Visibility (centered)	0.711	0.064	0.498	11.11	< .001
Awareness & Training (centered)	-0.231	0.058	-0.189	-3.98	< .001
Visibility × Awareness	-0.480	0.071	-0.283	-6.77	< .001

Note. $\Delta R^2 = .0307$, $\Delta F(1, 383) = 13.52$, $p < .001$.

Awareness and training significantly moderated the relationship between visibility and breach likelihood. The negative interaction indicates that increased awareness and training reduced the risk associated with highly visible information.

(b) Accessibility × Awareness & Training

Predictor	*B*	*SE*	*β*	*t*	*p*
Accessibility (centered)	0.643	0.062	0.462	10.37	< .001
Awareness & Training (centered)	-0.204	0.055	-0.171	-3.71	< .001
Accessibility × Awareness	-0.178	0.057	-0.142	-3.12	.002

Note. $\Delta R^2 = .0096$, $\Delta F(1, 383) = 9.72$, $p = .002$.

The results indicated that awareness and training weakened the positive relationship between accessibility and breach likelihood, suggesting that trained employees were better able to manage access-related risks.

Table 5. Moderation Effects of Social Engineering Resistance

(a) Visibility × Social Engineering Resistance

Predictor	*B*	*SE*	*β*	*t*	*p*
Visibility (centered)	0.689	0.061	0.482	11.29	< .001
Social Engineering Resistance (centered)	-0.217	0.054	-0.181	-4.02	< .001
Visibility × SER	-0.272	0.062	-0.198	-4.39	< .001

Note. $\Delta R^2 = .0139$, $\Delta F(1, 383) = 12.09$, $p < .001$.

Social engineering resistance significantly moderated the relationship between visibility and breach likelihood. Higher resistance reduced the risk associated with visible information assets.

(b) Accessibility × Social Engineering Resistance

Predictor	*B*	*SE*	*β*	*t*	*p*
Accessibility	0.612	0.059	0.445	10.38	< .001

Copyright © ISRG Publishers. All rights Reserved.
DOI: 10.5281/zenodo.18811766

(centered)					
Social Engineering Resistance (centered)	-0.193	0.052	-0.162	-3.71	< .001
Accessibility × SER	-0.134	0.053	-0.121	-2.52	.012

Note. $\Delta R^2 = .0064$, $\Delta F(1, 383) = 6.32$, $p = .012$.

The interaction effect indicated that social engineering resistance reduced the impact of accessibility on breach likelihood, highlighting the importance of human resilience against manipulation.

Multiple linear regression analysis was conducted to examine the effects of guardianship, offender motivation, and target characteristics on breach likelihood. The overall model was statistically significant, $F(3, 385) = 93.41$, $p < .001$, explaining 42.1% of the variance in breach likelihood ($R^2 = .421$). Guardianship significantly and negatively predicted breach likelihood ($\beta = -.412$, $p < .001$), while target characteristics significantly and positively predicted breach likelihood ($\beta = .529$, $p < .001$). Offender motivation exhibited a marginal positive effect ($\beta = .094$, $p = .052$).

Hierarchical moderated regression analyses were conducted to examine the moderating roles of information quality, awareness and training, and social engineering resistance. All predictors and moderators were mean-centered prior to the creation of interaction terms. Information quality significantly moderated the relationship between data value and breach likelihood ($\Delta R^2 = .0058$, $p = .034$), such that higher information quality weakened the positive association between value and breach likelihood.

Awareness and training significantly moderated the relationships between visibility and breach likelihood ($\Delta R^2 = .0307$, $p < .001$) and between accessibility and breach likelihood ($\Delta R^2 = .0096$, $p = .002$). Similarly, social engineering resistance significantly moderated the effects of visibility ($\Delta R^2 = .0139$, $p < .001$) and accessibility ($\Delta R^2 = .0064$, $p = .012$) on breach likelihood. In all cases, the interaction effects were negative, indicating a buffering effect of organizational and human-centric protective factors.

DISCUSSIONS

This study demonstrated the applicability of Routine Activity Theory in explaining perceived data breach risk and organizational vulnerability within government organizations, rather than confirmed breach incidents. The findings suggest that employees' perceptions of breach risk were more strongly associated with the presence of vulnerable information assets and insufficient guardianship than with offender motivation alone. This supports the theoretical view that organizational exposure and opportunity structures, as perceived by employees, play a central role in shaping vulnerability to cyber incidents, even in the absence of direct evidence of deliberate or highly motivated attacks (Lehto, 2022).

Guardianship emerged as a critical protective factor in reducing perceived organizational vulnerability to data breaches. Employees reported lower perceived risk in environments where organizational controls, policies, and monitoring mechanisms were visible and consistently enforced. In contrast, weak or absent guardianship heightened perceptions of exposure to unauthorized access, reinforcing the importance of institutional oversight in managing cybersecurity risk. These findings align with existing cybersecurity literature emphasizing that inadequate guardianship increases organizational susceptibility to cyber threats rather than directly causing breach events (Jamal et al., 2024).

Target characteristics particularly the perceived value, visibility, and accessibility of organizational data were central to explaining employees' assessments of breach likelihood. Government information assets were viewed as inherently attractive due to their sensitivity and importance, and when such assets were perceived as highly visible or easily accessible, employees identified greater organizational vulnerability. This perception-based finding is consistent with prior research by Andreou et al. (2025), which emphasizes that attackers are more likely to exploit targets that appear to offer high rewards with minimal resistance, regardless of whether an actual breach occurs.

Offender motivation was perceived to play a comparatively weaker role in shaping data breach risk. Employees tended to view cyber threats as largely opportunistic, driven by automated tools and widespread attack techniques that exploit exposed systems rather than targeted intent. This perception shifts the focus of cybersecurity efforts toward reducing organizational exposure and strengthening guardianship mechanisms, rather than attempting to anticipate or manage offender behavior.

The study also highlighted the importance of organizational and human-centric protective factors in buffering perceived breach risk. High information quality, employee awareness and training, and resistance to social engineering were associated with lower perceived vulnerability, even when target characteristics were unfavorable. These findings underscore the role of human resilience and effective information management in shaping organizational cybersecurity posture and support the need for integrated strategies that combine technical, organizational, and behavioral controls to mitigate perceived data breach risks in government organizations.

CONCLUSIONS

This study examined data breach likelihood in government organizations using Routine Activity Theory, focusing on guardianship, offender motivation, and target characteristics, as well as the moderating influence of organizational and human-centered protective factors. The findings indicate that breach risk is primarily shaped by vulnerable information assets and insufficient guardianship rather than by offender motivation alone. Government data were found to possess inherent characteristics that increase exposure to cyber threats, particularly when protective controls are moderate or inconsistently applied.

The results further underscore the critical role of guardianship in mitigating data breach risks. Effective institutional safeguards, including policies, oversight mechanisms, and access controls, reduce opportunities for unauthorized access and limit the exploitability of sensitive information. Conversely, information assets that are highly valuable, visible, and accessible increase susceptibility to breaches, highlighting the need for systematic management of organizational data environments.

The study emphasizes the importance of organizational and human-centric protective factors in reducing breach risks. Information quality, awareness and training, and resistance to social engineering were shown to buffer the effects of vulnerable

Copyright © ISRG Publishers. All rights Reserved.
DOI: 10.5281/zenodo.18811766

target characteristics. These findings reinforce the view that cybersecurity in government organizations is a socio-technical issue requiring the integration of technical controls, organizational governance, and human resilience.

RECOMMENDATIONS

Based on the findings of the study, government organizations are encouraged to strengthen guardianship by reinforcing cybersecurity governance structures, policies, and monitoring systems. Clear accountability mechanisms, regular security audits, and consistent enforcement of cybersecurity standards should be institutionalized to ensure sustained protection of information assets across all organizational levels.

Organizations should also proactively manage the vulnerability of their information assets by limiting unnecessary data exposure. This can be achieved through stricter access controls, data classification frameworks, and the application of the principle of least privilege. Reducing the visibility and accessibility of sensitive data can significantly lower opportunities for unauthorized access and misuse.

Sustained investment in human-centered protective measures is strongly recommended. Continuous cybersecurity awareness and training programs, improvements in information quality and data governance, and initiatives to strengthen resistance to social engineering should be prioritized. Cultivating a culture of cybersecurity awareness and vigilance will enhance employee resilience and play a crucial role in mitigating data breach risks within government organizations.

REFERENCES

1. Achor, O. (2023). *Data Security Strategies for Preventing Breaches Due to Insider Threats* (Doctoral dissertation, Walden University).
2. Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939-953.
3. Andreou, A., Mavromoustakis, C. X., Markakis, E., Bourdena, A., & Mastorakis, G. (2025). Enhancing network slice security with Deep Reinforcement Learning and Moving Target Defense strategies. Discover Internet of Things, 5(1), 67.
4. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.
5. Basak, B. (2024). The Impact of Cybersecurity Threats on National Security: Strategies. *International Journal of Humanities Social Science and Management (IJHSSM)*, *4*(2), 1361-1382.
6. Blakely, B., Kurtenbach, J., & Nowak, L. (2022). Exploring the information content of cyber breach reports and the relationship to internal controls. *International Journal of Accounting Information Systems*, *46*, 100568.
7. Caliso, R. A. C. C., Francisco, J. P. S., & Garcia, E. M. (2020). Broad insecurity and perceived victimization risk. *Journal of Interdisciplinary Economics*, *32*(2), 160-179.
8. Campbell, L. (2023). The Philippines: Cyber Threats.
9. Chang, Y. W., Hsu, P. Y., Chen, J., Shiau, W. L., & Xu, N. (2023). Utilitarian and/or he donic shopping–consumer motivation to purchase in smart stores. *Industrial Management & Data Systems*, *123*(3), 821-842.
10. Cheung, N. W., & Zhong, H. (2022). Deviant versus nondeviant routines, social guardianship and adolescent victimization in the rural context of China. *Journal of Interpersonal Violence*, *37*(7-8), NP4527-NP4557.
11. Cohen, L. E., & Felson, M. (2010). Social change and crime rate trends: A routine activity approach (1979). In *Classics in environmental criminology* (pp. 203-232). Routledge.
12. Enriquez, J. M. (2023). Data security in ASEAN's digital economy: lessons from the Philippines. *RSIS Commentaries*, *161-23*.
13. George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal, 2(1), 51-75.
14. Gundu, T. (2024, March). Learn, Unlearn and Relearn: Adaptive Cybersecurity Culture Model. In *International Conference on Cyber Warfare and Security* (Vol. 19, No. 1, pp. 95-102).
15. Hewitt, A. N., Chopin, J., & Beauregard, E. (2020). Offender and victim 'journey-to-crime': Motivational differences among stranger rapists. *Journal of Criminal Justice*, *69*, 101707.
16. Ibrahim, A., Thiruvady, D., Schneider, J. G., & Abdelrazek, M. (2020). The challenges of leveraging threat intelligence to stop data breaches. Frontiers in Computer Science, 2, 36.
17. Jamal, H., Algeelani, N. A., & Al-Sammarraie, N. (2024). Safeguarding data privacy: strategies to counteract internal and external hacking threats. Computer Science and Information Technologies, 5(1), 46-54.
18. Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). Data breach management: An integrated risk model. *Information & Management*, *58*(1), 103392.
19. Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, *106*, 102267.
20. Lee, J., de Guzman, M. C., Wang, J., Gupta, M., & Rao, H. R. (2022). Investigating perceptions about risk of data breaches in financial institutions: A routine activity-approach. *Computers & Security*, *121*, 102832.
21. Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer International Publishing.
22. Leonardi, P. M., & Treem, J. W. (2020). Behavioral visibility: A new paradigm for organization studies in the age of digitization, digitalization, and datafication. *Organization Studies*, *41*(12), 1601-1625. *Systems*, *34*(1), 123-134.
23. Main, A., & Yamada-Rice, D. (2022). Evading Big Brother: Using visual methods to understand children's perception of sensors and interest in subverting digital surveillance. *Visual Communication*, *21*(3), 384-417.

Copyright © ISRG Publishers. All rights Reserved.
DOI: 10.5281/zenodo.18811766

24. Malimage, K., Raddatz, N., Trinkle, B. S., Crossler, R. E., & Baaske, R. (2020). Impact of deterrence and inertia on information security policy changes. *Journal of Information*
25. Mansikka, J. (2023). Data loss prevention: for securing enterprise data integrity.
26. Obi, O. C., Akagha, O. V., Dawodu, S. O., Anyanwu, A. C., Onwusinkwue, S., & Ahmad, I. A. I. (2024). Comprehensive review on cybersecurity: modern threats and advanced defense strategies. *Computer Science & IT Research Journal*, *5*(2), 293-310.
27. Phillips, A., Ojalade, I., Taiwo, E., Obunadike, C., & Oloyede, K. (2023). Cyber-Security Tactics in Mitigating Cyber-Crimes: A Review and Proposal. *International Journal on Cryptography and Information Security (IJCIS)*, *13*(2/3).
28. Ribeiro, R. A. B. (2023). *Improving social engineering resilience in enterprises* (Master's thesis, Universidade Aberta (Portugal)).
29. Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9), 1460.
30. Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., & Kambhampati, S. (2020). A survey of moving target defenses for network security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1909-1941.
31. Sharma, P., & Barua, S. (2023). From data breach to data shield: the crucial role of big data analytics in modern cybersecurity strategies. *International Journal of Information and Cybersecurity*, *7*(9), 31-59.
32. Shukla, S., George, J. P., Tiwari, K., & Kureethara, J. V. (2022). Data security. In *Data Ethics and Challenges* (pp. 41-59). Singapore: Springer Singapore.
33. Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *Ieee Access*, *9*, 11895-11910.
34. Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*, 102520.
35. Wyer, R. S., & Srull, T. K. (2022). Category accessibility: Some theoretical and empirical issues concerning the processing of social stimulus information. In *Social cognition* (pp. 161-198). Routledge.

Copyright © ISRG Publishers. All rights Reserved.
DOI: 10.5281/zenodo.18811766