Advance Sustainable Science, Engineering and Technology (ASSET)
Vol. 8, No. 4, October 2026, pp. 02604014-01 ~ 02604014-012
ISSN: 2715-4211 DOI: https://doi.org/10.26877/asset.v8i4.2682

Quantifying Routine Activity Theory Factors in Personal Data Protection for Financial Institutions

Irenne Sutanto*, Astari Retnowardhani

Information System Management Department, BINUS Graduate Program – Master of Information System Management, Bina Nusantara University, Jakarta, Indonesia

*irenne@binus.ac.id

Abstract. Personal data protection has become a crucial issue in the financial sector as banking, fintech, and insurance services become increasingly digitized. This study aims to analyze the role of Routine Activity Theory (RAT) through three factors: motivated offender, suitable target, and capable guardianship, in improving the effectiveness of personal data protection. A quantitative method was used with a population of employees directly involved in personal data management, and 233 respondents were obtained through purposive sampling. Multiple regression analysis using SPSS showed that the three RAT constructs had a significant effect, with the capable guardianship factor having the strongest coefficient. The findings emphasize the importance of monitoring, access control, and risk mitigation against data leaks. The implication for financial institutions is the need to develop information security management strategies based on actor behavior, target vulnerability, and supervision mechanisms to increase public trust and digital resilience in the era of digital financial transformation.

Keywords: Data protection, financial institutions, information security, routine activity theory.

(Received 2025-09-04, Revised 2026-06-09, Accepted 2026-06-24, Available Online by 2026-09-22)

1. Introduction

The development of information technology and the digitization of financial services have brought significant changes to the way financial institutions operate in Indonesia. Banks, fintech companies, insurance companies, and other financial service institutions increasingly rely on the processing of customer personal data as a basis for decision-making, service innovation, and increased competitiveness [1,2]. However, this increased use of data is accompanied by a high risk of leaks, misuse, and cyberattacks that can harm companies and undermine public trust in financial institutions [3].

In Indonesia, the urgency of personal data protection has become increasingly prominent following the enactment of Law No. 27 of 2022 on Personal Data Protection. This regulation emphasizes the obligation of financial institutions to ensure the security, confidentiality, and integrity of customer

personal data. However, evidence suggests that data security threats continue to increase, both from internal factors such as negligence or misuse by employees, and from external factors such as hacking, malware, and phishing attacks [4,5]. This indicates that the effectiveness of personal data protection is not only determined by the existence of regulations, but also by a combination of risk factors and control mechanisms implemented in organizations.

The Routine Activity Theory (RAT) introduced by Cohen and Felson (1979) provides a relevant analytical framework for understanding the dynamics of crime, including cybercrime. RAT explains that a violation can occur when there is a motivated offender, a suitable target, and weak or incapable guardianship [6,7]. Therefore, using this framework, the effectiveness of personal data protection can be understood as the result of the interaction between potential threats, system vulnerabilities, and the strength of surveillance and control [8].

Previous studies have applied Routine Activity Theory (RAT) to understand the phenomenon of cybercrime. Bello and Griffiths [9] studied cybercrime in Nigeria using a qualitative approach through semi-structured interviews and documentation. The results of the study show that weak law enforcement, individual greed, and a lack of collaboration between stakeholders contribute to an increase in cases of cybercrime that cause financial losses. Another study conducted by Lee et al. [10] on phishing victims among Malaysian youth found that routine online activities have an impact on vulnerability to phishing attacks and can increase awareness of these threats. Meanwhile, Ahmad and Thurasamy [11], through a systematic literature review, emphasized the need for more detailed specification and operationalization of RAT variables for specific types of cybercrime in order to ensure more accurate interpretation. Research by Özaşçılar et al. [12] also shows that RAT is relevant for use in cybercrime victimization from a gender and geographical perspective, although routine activities that are risky for one type of crime are not necessarily dangerous for another.

However, the majority of these studies focus on the individual level and qualitative approaches, so quantitative empirical evidence at the organizational level, especially financial institutions, is still limited. The financial sector in Indonesia is highly exposed to the risk of data leaks due to the digitization of services, leaving ample room for quantitative RAT testing at the organizational level. This study presents a novelty in the form of RAT testing to assess the influence of motivated offenders, suitable targets, and capable guardianship on the effectiveness of personal data protection in Indonesian financial institutions. Based on this framework, the hypotheses tested are:

H1: Motivated offenders have a positive effect on the effectiveness of personal data protection.

H2: Suitable targets have a positive effect on the effectiveness of personal data protection.

H3: Capable guardianship has a positive effect on the effectiveness of personal data protection.

Based on this background, this study focuses on a quantitative analysis of the factors that influence the effectiveness of personal data protection in Indonesian financial institutions using Routine Activity Theory as a conceptual framework. The results of this study are expected to contribute to the development of a more comprehensive data protection strategy, support the implementation of regulations, and strengthen public trust in financial institutions.

2. **Methods**

This study uses a quantitative approach with the aim of examining the influence of factors within the Routine Activity Theory (RAT) framework on the effectiveness of personal data protection in financial institutions in Indonesia.

2.1 Research Variables and Operationalization

The independent variables in this study consist of motivated offender (X1), suitable target (X2), and capable guardianship (X3), while the dependent variable is the effectiveness of personal data protection (Y).

Table 1. Operationalization of Research Variables

Variable	Operational Definition	Indicators
Motivated Offender (X_1)	The level of potential for internal/external actors motivated to commit personal data breaches	1. Perception of risk of data misuse by employees 2. External threats (hackers, malware, phishing) 3. Incentives/temptations to leak data 4. Ease of unauthorized access to data 5. Employee pressure or dissatisfaction that could trigger data breaches
Suitable Target (X_2)	Level of vulnerability of data/systems as targets for breaches	1. Sensitivity of customer data managed 2. Large volume of data 3. Weaknesses in access control (passwords, authorization) 4. Data stored on less secure media or channels.
Capable Guardianship (X_3)	The power of supervision, control, and protection of personal data	1. Data protection policies/procedures 2. Implementation of security technology. 3. Implementation of SETA (Security Education, Training, and Awareness) 4. Commitment from top management 5. Regular audits and monitoring
Effectiveness of Personal Data Protection (Y)	The success rate of personal data protection implementation in financial institutions	1. Compliance with Personal Data Protection Laws 2. Low incidence of data breaches/leaks 3. Customer data security and confidentiality maintained 4. Increased customer trust 5. Preparedness for cybersecurity incidents

2.2 Population and Sample

The population in this study consisted of employees and staff who were directly involved in the management and protection of personal data in various financial institutions in Indonesia, including banking, fintech, insurance, and other financial services. Respondents were selected because they understood data protection practices, were involved in mitigating the risk of data leaks, and played a role in implementing data security policies. Respondents' positions included strategic and operational roles, such as IT security, data protection officers, compliance officers, IT managers, and operational staff who handle customer data, enabling this study to obtain a comprehensive picture of personal data protection based on their respective experiences and roles.

The sample size in this study was determined by considering practical rules for multiple regression. One commonly used guideline is the formula $N \geq 50 + 8m$, where N is the minimum sample size and m is the number of independent variables in the multivariate linear regression model [13]. This formula is used to ensure that the sample size is large enough so that the regression analysis can produce valid, reliable estimates and has sufficient statistical power to detect the significant effect of independent variables on dependent variables. Considering the number of independent variables in this study, the calculation shows that the minimum sample size required is approximately 74 respondents. However, to improve data representativeness and statistical power, this study set the sample size at 233 respondents from various financial institutions.

2.3 Sampling Technique

Respondents were selected using purposive sampling, which is a technique for determining samples based on specific criteria. The inclusion criteria in this study included: (1) employees who have worked for at least 6 months in a financial institution, (2) employees who are directly involved in personal data management, information technology security, or regulatory compliance, and (3) willing to fill out a questionnaire by providing valid information. Although this technique ensures data from the right respondents, the use of purposive sampling limits external validity, so that research results can only be generalized to populations with similar characteristics.

2.4 Research Instruments

The research instrument was a multi-item questionnaire, developed based on indicators for each construct within the Routine Activity Theory (RAT) framework and the effectiveness of personal data protection. The questionnaire was pre-tested to ensure clarity, relevance, and comprehensibility of the items. Respondents rated each statement using a 5-point Likert scale (1 = strongly disagree, 5 = strongly agree), and construct scores were calculated as the average of the corresponding item scores. Construct reliability and validity were assessed using Cronbach's α, Composite Reliability (CR), Average Variance Extracted (AVE), and factor loadings of each item to ensure internal consistency and convergent validity.

2.5 Data Analysis Techniques

The collected data were analyzed using SPSS, as this method is suitable for research with small to medium sample sizes and is capable of testing the relationship between variables. Before testing the hypotheses, validity and reliability tests were conducted to ensure that the research instrument is reliable and capable of measuring the intended construct consistently.

3. Results and Discussion

3.1 Descriptive Analysis

The results of the descriptive analysis regarding the influence of motivated offenders (X1), suitable targets (X2), and capable guardianship (X3) on the effectiveness of personal data protection (Y) are as follows.

Table 2. Results of Descriptive Analysis

Descriptives

			Statistics	Std. Error
X1	Mean		9.99	.172
	95% Confidence Interval for Mean	Lower Bound	9.65	
		Upper Bound	10.33	
	5% Trimmed Mean		10.02	
	Median		10.00	
	Variance		6.879	
	Standard Deviation		2.623	
	Minimum		3	
	Maximum		15	
	Range		12	
	Interquartile Range		4	
	Skewness		-.125	.159
	Kurtosis		-.170	.318
X2	Mean		17.98	.273
		Lower Bound	17.45	

	95% Confidence Interval for Mean	Upper Bound	18.52	
	5% Trimmed Mean		18.09	
	Median		18.00	
	Variance		17.336	
	Standard Deviation		4.164	
	Minimum		6	
	Maximum		25	
	Range		19	
	Interquartile Range		6	
	Skewness		-.250	.159
	Kurtosis		-.275	.318
X3	Mean		11.69	.178
	95% Confidence Interval for Mean	Lower Bound	11.34	
		Upper Bound	12.04	
	5% Trimmed Mean		11.86	
	Median		12.00	
	Variance		7.413	
	Standard Deviation		2.723	
	Minimum		3	
	Maximum		15	
	Range		12	
	Interquartile Range		4	
	Skewness		-.624	.159
	Kurtosis		-.064	.318
Y	Mean		6.71	.154
	95% Confidence Interval for Mean	Lower Bound	6.41	
		Upper Bound	7.02	
	5% Trimmed Mean		6.79	
	Median		7.00	
	Variance		5.525	
	Standard Deviation		2.350	
	Minimum		2	
	Maximum		10	
	Range		8	
	Interquartile Range		3	
	Skewness		-.341	.159
	Kurtosis		-.699	.318

Based on the results of the descriptive analysis in Table 2, it is known that the Motivated Offender (X1) variable has an average value (mean) of 9.99 with a standard deviation of 2.623, which indicates that the data is quite spread around its middle value. The Suitable Target (X2) variable has a mean of 17.98 with a standard deviation of 4.164, indicating a relatively larger data variation compared to X1. Meanwhile, the Capable Guardianship (X3) variable has a mean of 11.69 with a standard deviation of 2.723, indicating moderate data variability. The Personal Data Protection Effectiveness (Y) variable has a mean of 6.71 with a standard deviation of 2.350, which indicates relatively low variability compared to the other variables.

3.2 Normality Test

The normality test is a statistical analysis technique that aims to evaluate whether data in a study follows

a normal or near-normal distribution. This test is important because many parametric statistical methods require the assumption of normality. Determination of results is generally based on the significance value; if the obtained p-value exceeds the specified significance level, then the data can be said to have a normal distribution [14].

Table 3. Normality Test Results

	Kolmogorov-Smirnova			Shapiro-Wilk		
	Statistics	df	Sig.	Statistics	df	Sig.
X1	.100	233	<.001	.975	233	<.001
X2	.068	233	.012	.976	233	<.001
X3	.124	233	<.001	.923	233	<.001
Y	.124	233	<.001	.936	233	<.001

a. Lilliefors Significance Correction

Based on the results of the normality test shown in Table 3, using the Kolmogorov-Smirnov and Shapiro-Wilk methods, all research variables, namely Motivated Offender (X1), Suitable Target (X2), Capable Guardianship (X3), and Effectiveness of Personal Data Protection (Y), have a significance value (Sig.) of below 0.05. This indicates that these four variables were not normally distributed.

3.3 Reliability Test

Reliability testing is a statistical analysis procedure that aims to assess the extent to which a research instrument is able to produce consistent results. An instrument is considered to have good reliability if repeated measurements on similar objects or conditions produce data that tends to be stable and not very different [15].

Table 4. Reliability Test Results

Cronbach's Alpha	N of Items
.773	4

Based on the reliability test results presented in Table 4, a Cronbach's Alpha value of 0.773 was obtained for the four research variables. This value exceeds the minimum threshold of 0.70 commonly used as a benchmark for assessing reliability. Therefore, this research instrument can be declared to have good internal consistency and is suitable for measuring the variables Motivated Offender, Suitable Target, Capable Guardianship, and Effectiveness of Personal Data Protection.

3.4 Hypothesis Testing

Hypothesis testing is a statistical technique used to assess whether a hypothesis about a population parameter is acceptable based on available sample data. This process begins by establishing the null hypothesis (H_0) as a basic assumption that is considered true, which is then compared with the alternative hypothesis (H_1) which will be used as the basis for acceptance if H_0 is proven to be inconsistent with the data [16].

Table 5. Hypothesis Test Results

Coefficientsa

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	-1.671	.593		-2.818	.005
	X1	.165	.048	.185	3.417	<.001
	X2	.148	.033	.263	4.556	<.001
	X3	.348	.051	.403	6.840	<.001

a. Dependent Variable: Y

Based on Table 5, the results of the hypothesis test show that the three independent variables have a

positive and significant effect on the dependent variable, the Effectiveness of Personal Data Protection (Y). The Motivated Offender (X1) variable has a positive effect with a coefficient value of 0.165 and a significance value of <0.001, indicating that the lower the level of motivated offender, the better the effectiveness of personal data protection. The Suitable Target (X2) variable also has a positive effect with a coefficient of 0.148 and a significance value of <0.001, indicating that the smaller the chance of data being targeted, the greater the effectiveness of personal data protection. Meanwhile, the Capable Guardianship (X3) variable has the most dominant effect with a coefficient of 0.348 and a significance value of <0.001, indicating that the stronger the role of guarding or protection mechanisms, the more optimal the effectiveness of personal data protection. Thus, the research hypothesis stating that there is a positive effect of X1, X2, and X3 on Y can be accepted.

3.5 Correlation Test

A correlation test is a statistical analysis technique used to determine the strength and direction of the relationship between two or more variables. The significance of this relationship is usually determined by the p-value; if the p-value is less than or equal to the significance level (α), the relationship between the variables is considered statistically significant.

Table 6. Correlation Test Results

Correlations

		X1	X2	X3	Y
X1	Pearson Correlation	1	.390**	.434**	.462**
	Sig. (2-tailed)		<.001	<.001	<.001
	N	233	233	233	233
X2	Pearson Correlation	.390**	1	.535**	.550**
	Sig. (2-tailed)	<.001		<.001	<.001
	N	233	233	233	233
X3	Pearson Correlation	.434**	.535**	1	.623**
	Sig. (2-tailed)	<.001	<.001		<.001
	N	233	233	233	233
Y	Pearson Correlation	.462**	.550**	.623**	1
	Sig. (2-tailed)	<.001	<.001	<.001	
	N	233	233	233	233

**. Correlation is significant at the 0.01 level (2-tailed).

Based on Table 6, the results of the correlation test show that all independent variables have a positive and significant relationship with the Effectiveness of Personal Data Protection (Y) at a significance level of 0.01. The Motivated Offender (X1) variable correlates with Y by 0.462, the Suitable Target (X2) variable correlates with Y by 0.550, and the Capable Guardianship (X3) variable shows the highest correlation with Y by 0.623. This finding indicates that the lower the level of motivation of the offender, the smaller the chance of a suitable target, and the stronger the capable guardianship, the higher the effectiveness of personal data protection. In addition, there is also a positive relationship between the independent variables, where the highest correlation occurs between X2 and X3 (0.535), which illustrates a close relationship between the vulnerability of the target and the role of the guardian in supporting the effectiveness of personal data protection.

Discussion

The Influence of Motivated Offenders on the Effectiveness of Personal Data Protection

The results show that the motivated offender factor has a positive effect on the effectiveness of personal data protection. This means that the lower the threat level posed by motivated offenders, the more effective personal data protection can be. This confirms that controlling potential perpetrators who intend to misuse data is a crucial step in maintaining information security.

This perspective is consistent with Routine Activity Theory, which suggests that crime is most likely to occur when three conditions converge: the presence of a motivated offender, the availability of a suitable target, and the absence of capable guardianship. In the context of personal data protection, reducing the motivation of potential perpetrators is just as crucial as strengthening technical safeguards [17]. If individuals perceive that the risks of being detected or punished outweigh the potential benefits of committing cybercrime, their willingness to engage in such activities diminishes significantly. This highlights the importance of integrating deterrence strategies such as strict legal consequences, enhanced monitoring systems, and visible enforcement measures into broader data protection efforts. In addition, previous studies underscore that managing the psychological and behavioral aspects of cybercrime motivation plays a key role in securing information systems [18]. Efforts such as promoting ethical digital behavior, raising awareness of the societal harm caused by cybercrime, and implementing educational programs to reduce malicious intent can complement technical measures [19]. Together, these approaches not only protect data by making it technically harder to breach but also reduce the likelihood that individuals will be motivated to attempt an attack in the first place. This dual focus on limiting opportunities and reducing motivations aligns with Routine Activity Theory's framework and provides a more holistic approach to safeguarding personal data [20].

Furthermore, previous research also confirms that the human factor is a major weakness in information security. Efforts to suppress threats from motivated offenders can be carried out through technical and non-technical prevention mechanisms, such as strengthening regulations, increasing legal awareness, and imposing strict sanctions on violators [21]. This finding reinforces research findings that personal data protection is not only determined by security technology, but is also influenced by social control that can reduce the perpetrator's intention to commit violations [22].

Other research shows that cybercriminals' motivations are often influenced by economic gain, weak oversight, and low user security awareness [23]. Therefore, reducing the threat level from motivated offenders through strict oversight and access control can increase the effectiveness of personal data protection. This is consistent with research findings that the lower the threat from motivated offenders, the more effective the protection of people's personal data [24].

Thus, it can be concluded that managing motivated offenders is key to increasing the effectiveness of personal data protection. Preventive measures, such as increasing legal awareness, strengthening regulations, and implementing robust security systems, are necessary to minimize the potential for violations. This also confirms that the success of personal data protection is determined not only by technology but also by the ability to control potential threats from individuals motivated to commit abuse.

The Influence of Suitable Targets on the Effectiveness of Personal Data Protection

The research results show that suitable targets have a positive impact on the effectiveness of personal data protection. This indicates that the less likely data are to become a vulnerable target, the higher the protection effectiveness that can be achieved. Therefore, reducing data vulnerability is a strategic step in preventing information leaks.

In personal data protection, the concept of target hardening plays a vital role in minimizing the risks of misuse and exploitation. When data systems are poorly protected, they become attractive to cybercriminals who actively seek out weak points to exploit. Weak encryption, lack of access control, and low user awareness collectively create opportunities for breaches, highlighting the urgent need for stronger safeguards [25]. Strengthening security measures such as dual authentication, end-to-end encryption, and strict access management not only reduces the probability of unauthorized access but also shifts the cost-benefit equation for attackers, making data less appealing as a target [26]. Moreover, existing research underscores that the resilience of personal data protection systems depends on how effectively organizations can transform vulnerable targets into resilient ones. By making systems harder to penetrate, the potential gains for cybercriminals decrease while the risks and required effort increase. This aligns with findings that personal data protection is most effective when targets are perceived as unattractive or too costly to compromise. In practice, this means organizations must consistently invest

in technical upgrades, user education, and proactive monitoring to ensure that their security posture remains robust against evolving threats [18].

The higher the level of data security and control, the lower the likelihood of the data becoming a suitable target for perpetrators. In other words, data vulnerability reduction strategies include not only technical protections, but also organizational policies and increasing security literacy among users [27]. This is in line with research findings that effective personal data protection can be achieved by making personal data a difficult-to-reach target, thereby reducing the chance of information leaks [28].

Thus, suitable target management plays a crucial role in maintaining effective personal data protection. Efforts such as strengthening encryption, restricting access, and implementing the principle of least privilege are key strategies for reducing data vulnerability to attacks. This demonstrates that effective data protection depends not only on controlling the perpetrator but also on how data is positioned to prevent it from being easily misused.

The Influence of Capable Guardianship on the Effectiveness of Personal Data Protection

The research results show that capable guardianship has the most dominant influence on the effectiveness of personal data protection. The stronger the guardianship role and oversight mechanisms implemented, the more effective data protection can be achieved. This confirms that strengthening effective oversight systems and security policies is crucial for maintaining the confidentiality and integrity of personal data.

Capable guardianship in the context of personal data protection emphasizes the importance of multilayered defense systems that combine technological, regulatory, and institutional safeguards. Security technologies such as firewalls, intrusion detection systems, and encryption protocols serve as the first line of defense against unauthorized access [29]. At the same time, clear regulations provide a legal framework that guides organizations in handling sensitive information responsibly. Authorized parties, including regulatory bodies and internal compliance officers, ensure these standards are not only adopted but also consistently enforced. Together, these elements create a robust environment where personal data is less vulnerable to misuse. Furthermore, effective guardianship requires continuous monitoring and improvement of data security practices in line with evolving threats. Regular security audits, updates to internal policies, and the active role of oversight institutions help minimize gaps that could be exploited by malicious actors. Empirical studies highlight that organizations with strict supervisory mechanisms experience fewer incidents of data breaches compared to those with weaker controls [30]. This indicates that guardianship is not merely a reactive approach but a proactive commitment to safeguarding information. Thus, the integration of technology, law, and institutional oversight is essential in reducing the likelihood of personal data exploitation and ensuring long-term trust in data management systems.

Previous research also shows that user compliance with security policies is also influenced by the effectiveness of organizational oversight, which simultaneously strengthens the role of oversight as a primary bulwark in preventing breaches [31]. The effectiveness of data protection increases when organizations actively involve capable guardians, both in the form of technology and human resources trained in the field of information security. This shows that strengthening the oversight system depends not only on technology, but also on the awareness, compliance, and competence of those acting as data guardians.

Thus, capable guardianship is a key factor determining the effectiveness of personal data protection. Strengthening the guardians' role through strict regulations, implementing cybersecurity standards, and increasing human resource capacity in oversight are strategic steps to ensure data is properly protected. This demonstrates that the success of maintaining data confidentiality, integrity, and availability depends heavily on the quality of consistently implemented oversight mechanisms and protection systems.

4. Conclusion

The study highlights that the effectiveness of personal data protection is strongly shaped by the presence of capable guardianship, supported by the conditions of motivated offenders and target vulnerability. Practically, this underscores the need for organizations, institutions, and digital service providers to reinforce safeguarding measures through clear security policies, Security Education, Training, and Awareness (SETA) programs, as well as continuous monitoring systems. Nevertheless, the study has certain limitations, including the use of non-probability sampling, reliance on self-reported data, and cross-sectoral coverage that may affect generalizability. Future research is recommended to integrate multi-source data, incorporate objective incident records, and employ longitudinal designs to provide a more comprehensive understanding of personal data protection dynamics.

Acknowledgements
The authors would like to express their deepest gratitude to their supervisor for providing guidance, direction, and valuable input during the process of preparing this research. The authors would also like to thank family, friends, and all those who have provided prayers, moral support, and other forms of assistance so that this research could be completed smoothly.

Declaration of AI and AI-assisted technologies in the writing process
During the preparation of this work, the authors used ChatGPT in order to assist in language refinement, grammar checking, sentence restructuring, and improving the clarity of academic writing. After using this tool/service, the authors carefully reviewed and edited the content as needed and took full responsibility for the publication's content.

Declaration of Competing Interest
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Barroso M, Laborda J. Digital transformation and the emergence of the Fintech sector: Systematic literature review. Digital Business 2022;2:100028. https://doi.org/10.1016/j.digbus.2022.100028.
[2] Aldboush HHH, Ferdous M. Building trust in fintech: an analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. International Journal of Financial Studies 2023;11:90. https://doi.org/10.3390/ijfs11030090.
[3] Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, et al. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract 2022;47:698. https://doi.org/10.1057/s41288-022-00266-6.
[4] Zostant M, Chataut R. Privacy in computer ethics: Navigating the digital age. Computer Science and Information Technologies 2023;4:183–90. https://doi.org/10.11591/csit.v4i2.pp183-190.
[5] Wibowo A, Alawiyah W, Azriadi. The importance of personal data protection in Indonesia's economic development. Cogent Soc Sci 2024;10:2306751. https://doi.org/10.1080/23311886.2024.2306751.
[6] Stadnicki I, Corsini M, Szulkin M. Application of criminology in urban ecology and evolution: Routine Activity Theory and field equipment disappearance dynamics. Ecol Indic 2024;165:112095. https://doi.org/10.1016/j.ecolind.2024.112095.
[7] Madarie R, Weulen Kranenbarg M, de Poot C. Cybersecurity expert perspectives on data thieves' actions in digital environments: Potential refinements for routine activity theory. Deviant Behav 2026;47:544–62. https://doi.org/10.1080/01639625.2025.2453440.

[8] Kamil S, Al-Turfi M, Almukhtar R. Advancements in chemical materials: Exploring smart storage equipment and protection systems. Journal of Applied Engineering and Technological Science (JAETS) 2024;5:1086–101. https://doi.org/10.37385/jaets.v5i2.4096.
[9] Bello M, Griffiths M. Routine activity theory and cybercrime investigation in Nigeria: how capable are law enforcement agencies? Rethinking Cybercrime: Critical Debates, Springer; 2020, p. 213–35. https://doi.org/10.1007/978-3-030-55841-3_11.
[10] Lee YY, Gan CL, Liew TW. Phishing victimization among Malaysian young adults: cyber routine activities theory and attitude in information sharing online. The Journal of Adult Protection 2022;24:179–94. https://doi.org/10.1108/JAP-06-2022-0011.
[11] Ahmad R, Thurasamy R. A systematic literature review of routine activity theory's applicability in cybercrimes. Journal of Cyber Security and Mobility 2022;11:405–32. https://doi.org/10.13052/jcsm2245-1439.1133.
[12] Özaşçılar M, Çalıcı C, Vakhitova Z. Examining cybercrime victimisation among Turkish women using routine activity theory. Crime Prevention and Community Safety 2024;26:112–28. https://doi.org/10.1057/s41300-024-00201-y.
[13] Bekele WB, Ago FY. Sample size for interview in qualitative research in social sciences: A guide to novice researchers. Research in Educational Policy and Management 2022;4:42–50. https://doi.org/10.46303/repam.2022.3.
[14] Demir S. Comparison of normality tests in terms of sample sizes under different skewness and kurtosis coefficients. International Journal of Assessment Tools in Education 2022;9:397–409. https://doi.org/10.21449/ijate.1101295.
[15] Janna N, Herianto H. Konsep uji validitas dan reliabilitas dengan menggunakan SPSS 2021. https://doi.org/10.31219/osf.io/v9j52.
[16] Gonçalves MC, Silva R. The effect of statistical hypothesis testing on machine learning model selection. Brazilian conference on intelligent systems, Springer; 2023, p. 415–27. https://doi.org/10.1007/978-3-031-45389-2_28.
[17] De Kimpe L, Walrave M, Verdegem P, Ponnet K. What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology 2022;41:1796–808. https://doi.org/10.1080/0144929X.2021.1905066.
[18] Mazarr MJ, Rhoades AL, Beauchamp-Mustafaga N, Blanc AA, Eaton D, Feistel K, et al. Disrupting deterrence: Examining the effects of technologies on strategic deterrence in the 21st century 2022.
[19] Wijaya ID, Salam R, Ghozi S, Mubarok FU, Subkhan MF. Perceived security and trust as mechanisms of P2P adoption technology: Evidence from pre-adopters using PLS-SEM approach. International Journal of Environment, Engineering and Education 2026;8:19–34. https://doi.org/10.55151/ijeedu.v8i1.373.
[20] Ireland L. Predicting online target hardening behaviors: An extension of routine activity theory for privacy-enhancing technologies and techniques. Deviant Behav 2021;42:1532–48. https://doi.org/10.1080/01639625.2020.1760418.
[21] Hughes-Lartey K, Li M, Botchey FE, Qin Z. Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon 2021;7. https://doi.org/10.1016/j.heliyon.2021.e06522.
[22] Fontes C, Hohma E, Corrigan CC, Lütge C. AI-powered public surveillance systems: why we (might) need them and how we want them. Technol Soc 2022;71:102137. https://doi.org/10.1016/j.techsoc.2022.102137.
[23] Chen S, Hao M, Ding F, Jiang D, Dong J, Zhang S, et al. Exploring the global geography of cybercrime and its driving forces. Humanit Soc Sci Commun 2023;10:71. https://doi.org/10.1057/s41599-023-01560-x.

[24] Al-Harrasi A, Shaikh AK, Al-Badi A. Towards protecting organisations' data by preventing data theft by malicious insiders. International Journal of Organizational Analysis 2023;31:875–88. https://doi.org/10.1108/IJOA-01-2021-2598.
[25] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics (Basel) 2023;12:1333. https://doi.org/10.3390/electronics12061333.
[26] Lehto M. Cyber-attacks against critical infrastructure. Cyber security: Critical infrastructure protection, Springer; 2022, p. 3–42. https://doi.org/10.1007/978-3-030-91293-2_1.
[27] Sargiotis D. Data security and privacy: Protecting sensitive information. Data governance: a guide, Springer; 2024, p. 217–45. https://doi.org/10.1007/978-3-031-67268-2_6.
[28] Brown H, Lee K, Mireshghallah F, Shokri R, Tramèr F. What does it mean for a language model to preserve privacy? Proceedings of the 2022 ACM conference on fairness, accountability, and transparency, 2022, p. 2280–92. https://doi.org/10.1145/3531146.3534642.
[29] Jamal H, Algeelani NA, Al-Sammarraie N. Safeguarding data privacy: strategies to counteract internal and external hacking threats. Computer Science and Information Technologies 2024;5:46–54. https://doi.org/10.11591/csit.v5i1.pp46-54.
[30] Bouraffa T, Hui K-L. Regulating information and network security: Review and challenges. ACM Comput Surv 2025;57:1–38. https://doi.org/10.1145/3711124.
[31] Delso-Vicente A-T, Diaz-Marcos L, Aguado-Tevar O, de Blanes-Sebastián MG. Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. Future Business Journal 2025;11:28. https://doi.org/10.1186/s43093-025-00452-7.