Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp942-951

Vol. 21, Issue 2, 2025

MODELING ORGANIZATIONAL VULNERABILITY TO DATA BREACHES USING MODERN CRIME THEORY

[1]Yakkaluri Narendra, MCA Student, Department of MCA

[2] Shaik Haseena, M.Tech, (Ph.D), Assistant Professor, Department of MCA

[12]Dr KV Subba Reddy Institute of Technology, Dupadu, Kurnool

ABSTRACT

Research on data security generally highlights the need to identify the variables associated to security breaches, hoping to avoid future information security disasters. The complexity of protecting sensitive data inside an organisation has increased with the development of digital technologies. Even while data security research is expanding, there aren't many studies that particularly look at the causes of information security breaches in businesses. Previous studies have focused studied the security posture of firms and organizations, concentrating on the breach kind and location. Few studies, nonetheless, have looked at outside variables that can increase an organization's susceptibility to information security breaches. By using contemporary criminal theory (MCT) to examine the exogenous elements impacting the victimisation of public and private organisations to data breach occurrences, the present research fills this gap in the literature. We examine the effects of attraction, visibility, and guardianship on the probability of data breaches using knowledge about the technological, organisational, and financial characteristics of organisations as well as insights from crime theories. To investigate the connection between these variables as separate predictors of data breaches, we develop a theoretical model. A covariance-based structural equation modeling (CB-SEM) based methodology is designed to undertake a complete assessment of the dynamics within the setting of cybercrime. The validity of the suggested constructs is supported by this study's analysis of data gathered from 4,868 organisations, which shows a strong match between the hypothesised model and the data. The study's findings support the application of MCT to information security breach research and make it possible to pinpoint the main exogenous variables affecting data breaches, such as the allure of valuable data and the efficacy of guardianship measures.

I. INTRODUCTION

Organisations and institutions have experienced major data breach events within the last 20 years. Data theft and fraud have become major global threats, and in 2023, they will have a particularly catastrophic effect on businesses everywhere, but notably in the US. The average cost of a breach during this time was around $4.45 million, according to the IBM Cost of a Data Breach Report 2023 [1]. Furthermore, according to the International Data Corporation's (IDC) 2024 Thales Data Threat Report [2], almost two-thirds of US businesses have had at least one data breach recently. Because they cause organisations and corporations to suffer significant financial losses, data breaches are often seen as a major danger that interrupts operations and destroys their assets and image. In order to adequately analyse data breach situations and lessen their detrimental effects, organisations must work with university academics and specialists as data breaches grow more complex and difficult to handle, as stressed by the US government agency [3].

Numerous hacking and phishing situations, including unauthorised access, theft, computer loss, incorrect disclosures, targeting

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp942-951
Vol. 21, Issue 2, 2025

laptops and desktop computers, hacking emails, network servers, portable devices, and other IT devices, may result in data breaches. The security posture of businesses and organisations has been the subject of several studies, most of which have focused on the kind and location of breaches. External variables that can increase their vulnerability to victimisation, however, have received little consideration. To the best of our knowledge, none of these research examined external variables that could lead to public and private organisations becoming victims of data breach occurrences by combining the application of contemporary criminal theory.

Traditional criminological theories often need to be modified and expanded in order to account for the distinct dynamics and features of the digital environment in cybercrime. This study's primary goal is to increase knowledge of the variables linked to an organization's susceptibility to information security breaches. In particular, we look at how well the criminal theory-derived concepts of guardianship, attractiveness, and visibility may predict data breaches. Using routine activity theory as a theoretical framework, this research paper attempts to examine the phenomenon of victimisation in the context of cyberspace, with a particular focus on data breaches. These theories may direct the creation of successful preventative measures and provide insightful information about the situational elements that increase the likelihood of crime.

B. RESEARCH PURPOSE Building on these theoretical frameworks, our goal is to develop a thorough theoretical model that investigates the connections between guardianship, visibility, and an organization's attractiveness as separate predictors of data breaches. The sample of 4,868 organisations that operated in the US between 2018 and 2020 is the subject of our investigation. The dataset contains metrics that evaluate an organization's vulnerability to victimisation. In order to do this, we gather multivariate data from both non-breach and breached organisations, then examine it via the prism of criminal theory. By taking this stance and focussing on the victim rather than the criminal, we want to provide organisations advice and assistance on how to proactively avoid any violations.

The following summarises our manuscript's main contributions: • We use web-scraping methods to gather multivariate data on victim and non-victim organisations.

• We create a set of metrics that represent technical, financial, and organisational aspects.

• We look at how crime theories are used to the analysis of internet security breaches.

• As independent predictors of data breaches on organisations, we provide a theoretical framework that investigates the connection between an organization's guardianship, visibility, and attraction.

• We look at how covariance-based structural equation modelling is used to investigate security breach-related aspects.

• We evaluate the validity and reliability of the suggested model experimentally and identify the most important indications for information security breaches.

Our work's main goal is to verify the use of MCT in information security breach research and help organisations understand the effects of many circumstances that might have led to their victimisation. After that, direct their efforts to put specific security measures into place.

There are six major components to this study article. A thorough assessment of relevant literature is given in Section II. We outline the research topic and formulate the research hypothesis in section III. We outline our approach to answering the research questions in Section IV, where we also describe the study methodology. The results and conclusions drawn

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp942-951
Vol. 21, Issue 2, 2025

from the data analysis are explained in Section V. part VI, the discussion part, we critically review and interpret theimplications of the results, delivering significant insights for organizations, we explain also the study's limits and we provide prospective routes for further research. Lastly, we wrap up the paper.

II. LITERATURE SURVEY

"A visual analysis of research on information security risk using CiteSpace," by X. Li and H. Li 63243–63257 in IEEE Access, vol. 6, 2018.

The topic of information security has spread around the world and raised worries among practitioners and scholars alike. There is a chance that corporate or national military secrets might be compromised during security events, leading to significant harm to the group as a whole. By offering a thorough analysis of the current information security risk (ISR) literature, this study seeks to investigate the knowledge structure, development, and future trends of the information security field. Journal publications from the Web of Science, IEEE, ACM, and Scopus databases were the subject of the visualisation analysis, and the results were mapped into the I-model. Evaluation techniques, including as frequency statistics, clustering coefficient, and centrality computation, are used to examine all of the interconnected matrices that CiteSpace supports, according to 2748 publications. Under a substantial level, several helpful results of various aims are shown, including author, country/territory, cluster, institution, and reference. The future direction of ISR research has been shown by a synthetical analysis. In terms of knowledge and innovation based on the field of ISR, this study proposes an analysis of integrated visualisation for academics and practitioners.

"Awareness, intention, (In)action: Individuals' reactions to data breaches," by P. Mayer, Y. Zou, B. M. Lowens, H. A. Dyer, K. Le, F. Schaub, and A. J. Aviv, ACM Trans. Comput.-Hum. Interact., vol. 30, no. 5, pp. 1–53, Oct. 2023.

Data breaches are common. Through two online surveys, we offer new insights into people's awareness, perception, and reactions to breaches that impact them. In the first survey (n = 413), we showed participants up to three breaches that had an impact on them, and in the second survey (n = 108), we examined whether the main study participants actually carried out their plans to take action. Although 74% of participants were not aware of the breaches that affected them, 73% of participants were impacted by at least one breach overall. The majority of participants thought the breach would not affect them, however some said that they intended to take action. A significant intention-behavior gap was also discovered. When participants were indifferent to breaches, contemplated possible expenses, forgot, or felt defeated about acting, they did not carry out their goal. According to our research, compromised companies need to answer for more aggressively warning and safeguarding impacted customers.

Potentially Unexpected Repercussions of the Sec Limiting Managerial Discretion: Evidence From Cyber Risk Factors and Peer Data Breach, M. Ashraf, document SSRN 3807487, 2021.

I detail the possible unforeseen repercussions of the SEC's limitation of management discretion, paying particular attention to the SEC's 2011 guideline on cyber risk factors. While adjusting for firm and year fixed effects, I use peer data breaches as a salient proxy of non-breached firms that have material exposure to cyber risk. First, I find that peer breaches are linked to more unique disclosures of cyber risk factors when the managers of non-breached firms have more discretion (pre-SEC-2011 period) and to fewer unique disclosures of cyber risk factors after their discretion is limited (post-SEC-2011 period). Next, I discover that businesses are

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp942-951
Vol. 21, Issue 2, 2025

more likely to use the cybersecurity language included in the SEC's 2011 advice, which might be one explanation for the post period's decline. Lastly, I believe that investors' knowledge asymmetry is lessened by more distinctive cyber risk elements. Altogether, my research is consistent with the SEC generating an organizational shift from normative isomorphism to coercive isomorphism and implies that the SEC may be damaging disclosure informativeness by restricting management choice.

A. Bouveret, "Financial sector cyber risk: A quantitative assessment framework," IMF Work. Papers, p. 1, 2018, vol. 18, no. 143.

After recent assaults on financial institutions, cyber risk has become a major danger to financial stability. By examining the many forms of cyber events (fraud, data breaches, and business interruption) and finding trends across a range of datasets, this article offers a new documentation of cyber risk for financial institutions worldwide. A quantitative approach for evaluating cyber risk for the banking industry is the second innovative contribution described. The framework is readily applicable at the national level and is based on a conventional VaR-type framework used to evaluate different kinds of stability risk. Applying the methodology to the available cross-country data, this article provides illustrative aggregated losses for the sample's banking sector under several scenarios, ranging from 10 to 30 percent of net income.

"The breach is dead, long live the breach: A spatial temporal study of healthcare data breaches," by N. Nejjari, K. Zkik, and H. Benbrahim, in Proc. Int. Conf. Sci., Eng. Manag. Inf. Technol., 2022, pp. 287–303.

Data breaches have impacted an increasing number of healthcare organisations in recent years. Preventing data security events in healthcare organisations primarily requires a thorough understanding of the background and the elements that contribute to these dangers. We investigate, from a spatiotemporal perspective, the context and contributing variables to data breaches that target the healthcare industry in the United States (US) from 2009 to 2021 using publicly accessible government data. In order to better understand how the global environment affects data breach instances, we shed light on healthcare data breaches that took place during the Covid19 Pandemic. In our research, the hacking and IT events are the most typical sorts of breaches affecting especially Healthcare providers businesses. In Florida, California, and Texas, victim healthcare organisations are increasingly common. Emails and network servers have emerged as the primary targets of breaches throughout the years. Healthcare IT security experts may reduce the likelihood of leaks by comprehending and detecting elements associated with data breach events. Key words Breach of health care data Time series study of data security data.

III. SYSTEM ANALYSIS AND DESIGN EXISTING SYSTEM

A large study effort has been undertaken in the topic of information security risk (ISR) literature. In order to map knowledge structures and shed light on the ISR environment, Li and Li carried out an analytical study using visualisation methods based on CiteSpace [4]. Their study does not specifically identify research needs, despite their significant contributions. Relatedly, Mayer et al. explore the intention behaviour gap, illuminating barriers and motivators and offering useful advice for solutions [5]. Ashraf [6] investigates the effects of the Securities and Exchange Commission's (SEC) advice on cyber risk factor disclosure in regulatory situations, looking at how peer breaches affect non-breached businesses' cyber risk disclosures. Furthermore,

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp942-951
Vol. 21, Issue 2, 2025

a quantitative methodology for cyber risk assessment is introduced in another research by Bouveret [7], offering a comprehensive viewpoint that is applied to cross-country data. In [8], authors explore, from a spatio-temporal viewpoint, the causes and the context connected to data breaches targeting healthcare sector in the United States.

A number of research aim to improve data breach prediction, such as those by Zhang and Chen [12], Sun et al. [11], Fang et al. [10], and Barati and Yankson [9]. A prediction approach based on historical data is put out by Barati and Yankson to calculate the amount and probability of breaches [9]. Huang et al. provide the Adaptive Weighted Graph Walk model (AGW) to address sparsity in unstructured data [13]. Fang et al. outperform benchmarks in enterprise-level breach prediction by presenting a statistical framework that leverages time series interdependencies [10]. Sun et al. provide a sophisticated method that combines a mixed non-parametric kernel distribution with a hurdle-Poisson model [11]. Zhang and Chen create a hybrid big data breach prediction algorithm that is very accurate and effective [12].

Bouveret questions the rise in data breaches, seeing a steady increase in breach magnitude and frequency [7]. The research finds organisational characteristics that influence the frequency and extent of breaches. Research on the impact of privacy violations on market value shows a brief but significant decline, particularly for bigger businesses [14], highlighting the significance of security and privacy measures for preserving profitability.

Disadvantages

• Data complexity: To identify Assessing Data Breach Factors Through Modern Crime Theory, the majority of machine learning models now in use need to be able to correctly understand sizable and intricate datasets.

• Data availability: In order to provide precise predictions, the majority of machine learning models need a lot of data. The accuracy of the model may degrade if data is not accessible in large enough amounts.

• Inaccurate labelling: The accuracy of the machine learning models that are now in use depends on how well the input dataset was used for training. Inaccurate labelling of the data prevents the model from producing reliable predictions.

PROPOSED SYSTEM

- The implementation of the suggested system The ability of structural equation modelling to thoroughly analyse intricate interactions between many variables at once justifies its use in the study of criminal theory and data breaches. CBSEM promotes the integration of numerous constructs such as organizational attractiveness, visibility, and guardianship into a coherent framework, coinciding with the complex structure of the phenomena under research.
- We may validate theoretical claims and experimentally evaluate the suggested links by using CBSEM to test hypotheses obtained from crime theory.Additionally, CB-SEM facilitates quantitative analysis, enabling model comparison, hypothesis testing, and the quantification of the influence of various factors on the probability of a data breach. All things considered, CB-SEM provides a strong statistical method for comprehending the dynamics of crime theory in relation to data breaches, capturing the complex interactions between variables affecting organisational susceptibility to data breaches and offering empirical backing for theoretical frameworks.

Advantages

International Journal of Engineering Research and Science & Technology

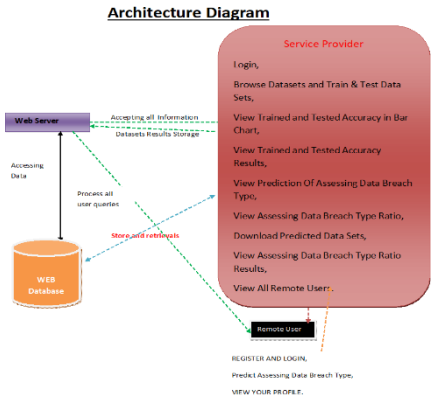
ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp942-951

Vol. 21, Issue 2, 2025

• We use web-scraping techniques to gather multivariate data about victim and non-victim organisations.
• We create a set of metrics that represent technical, financial, and organisational aspects.
• We look at how crime theories are used to the analysis of internet security breaches.
• As independent predictors of data breaches on organisations, we provide a theoretical framework that investigates the connection between an organization's guardianship, visibility, and attraction.
• We look at how covariance-based structural equation modelling is used to investigate security breach-related aspects.
• We evaluate the validity and reliability of the suggested model experimentally and identify the most important indications for handling information security breaches.

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

Modules Description

Service Provider

The Service Provider must use a working user name and password to log in to this module. He can do many tasks after successfully logging in, including browsing datasets and training and testing datasets. View the Results of Trained and Tested Accuracy, View the Bar Chart of Trained and Tested Accuracy, Download Predicted Data Sets, and View the Prediction of Assessing Data Breach Type and Assessing Data Breach Type Ratio View All Remote Users and Evaluate Data Breach Type Ratio Results.

View and Authorize Users

The administrator may see a list of all registered users in this module. Here, the administrator may see the user's information, like name, email, and address, and they can also grant the user permissions.

Remote User

A total of n users are present in this module. Before beginning any actions, the user needs register. Following registration, the user's information will be entered into the database. Following a successful registration, he must use his password and authorised user name to log in. Following a successful login, the user will be able to see their profile, predict the kind of data breach, and register and log in.

ALGORITHIMS

Logistic regression Classifiers

The relationship between a collection of independent (explanatory) factors and a categorical dependent variable is examined using logistic regression analysis. When the dependent variable simply has two values, like 0 and 1 or Yes and No, the term logistic regression is used. When the dependent variable contains three or more distinct values, such as married, single, divorced, or widowed, the technique is sometimes referred to as multinomial logistic regression. While the dependent variable's data type differs from multiple regression's, the procedure's practical application is comparable.

When it comes to categorical-response variable analysis, logistic regression and discriminant analysis are competitors. Compared to discriminant analysis, many statisticians believe that logistic regression is more flexible and appropriate for modelling the majority of scenarios. This is due to the fact that, unlike

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp942-951
Vol. 21, Issue 2, 2025

discriminant analysis, logistic regression does not presume that the independent variables are regularly distributed.

Both binary and multinomial logistic regression are calculated by this software for both category and numerical independent variables. Along with the regression equation, it provides information on likelihood, deviance, odds ratios, confidence limits, and quality of fit. It does a thorough residual analysis that includes diagnostic residual plots and reports. In order to find the optimal regression model with the fewest independent variables, it might conduct an independent variable subset selection search. It offers ROC curves and confidence intervals on expected values to assist in identifying the optimal classification cutoff point. By automatically identifying rows that are not utilised throughout the study, it enables you to confirm your findings.

Gradient boosting

One machine learning method for classification and regression problems is gradient boosting. Usually decision trees, it provides a prediction model in the form of an ensemble of weak prediction models.[1] [2] The resultant technique, known as gradient-boosted trees, often performs better than random forest when a decision tree is the weak learner.Like other boosting techniques, a gradient-boosted trees model is constructed step-by-step; however, it goes one step further by permitting optimisation of an arbitrary differentiable loss function.

SVM

The goal of a discriminant machine learning approach in classification problems is to identify a discriminant function that can accurately predict labels for newly acquired instances based on an independent and identically distributed (iid) training dataset. A discriminant classification function takes a data point x and assigns it to one of the several classes that are part of the classification job, in contrast to generative machine learning techniques that call for calculations of conditional probability distributions. Discriminant techniques are less effective than generative approaches, which are mostly used when prediction entails the identification of outliers. However, they need less training data and processing resources, particularly when dealing with a multidimensional feature space and when just posterior probabilities are required. Finding the equation for a multidimensional surface that optimally divides the various classes in the feature space is the geometric equivalent of learning a classifier.

SVM is a discriminant approach that, unlike genetic algorithms (GAs) or perceptrons, which are both often used for classification in machine learning, always returns the same optimum hyperplane value since it solves the convex optimisation issue analytically. The initialisation and termination criteria have a significant impact on the solutions for perceptrons. While the perceptron and GA classifier models are distinct every time training is started, training yields uniquely specified SVM model parameters for a given training set for a certain kernel that converts the data from the input space to the feature space. The only goal of GAs and perceptrons is to reduce training error, which will result in several hyperplanes satisfying this criterion.

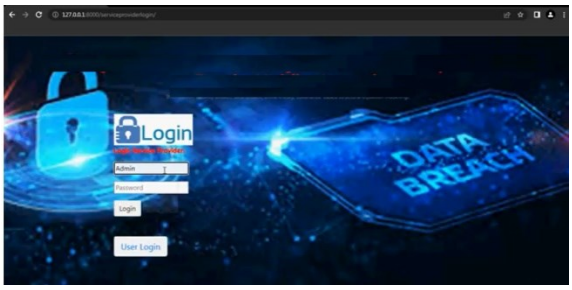
V. SCREEN SHOTS

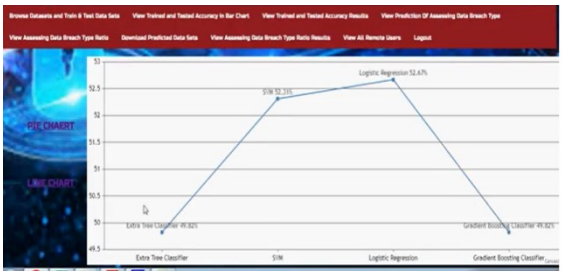
International Journal of Engineering Research and Science & Technology

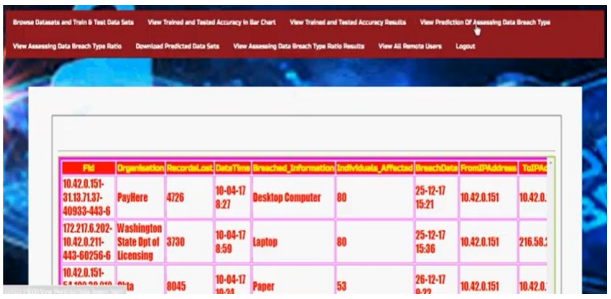
ISSN 2319-5991 www.ijerst.com

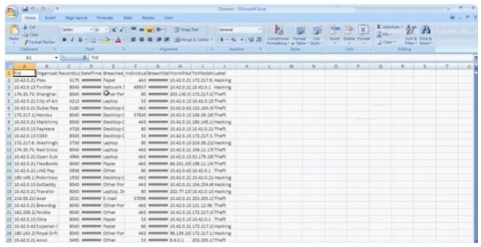
https://doi.org/10.62643/ijerst.2025.v21.i2.pp942-951

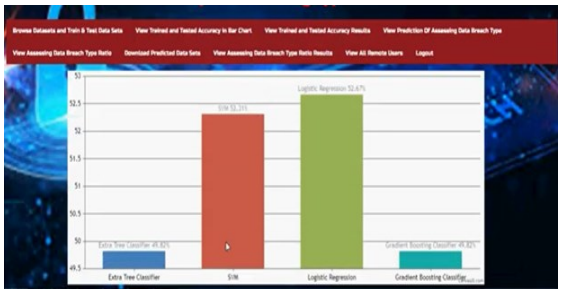
Vol. 21, Issue 2, 2025

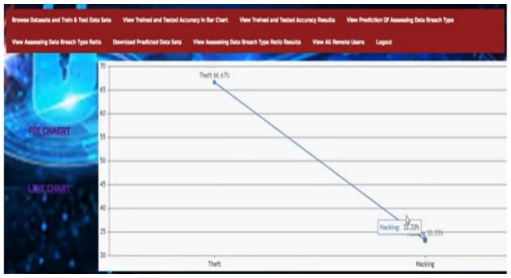


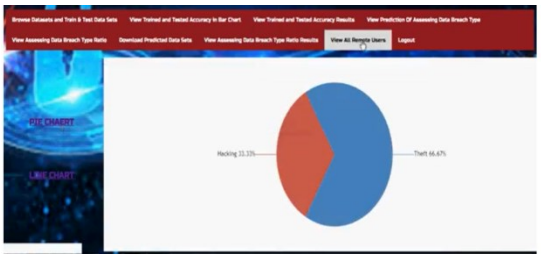












International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp942-951

Vol. 21, Issue 2, 2025

VI. CONCLUSION

In this research, with a particular emphasis on data breaches, we examined how regular activity theory may aid in our understanding of cybervictimization. This hypothesis emphasises how crucial elements like target appeal, visibility, and guardianship are in fostering cybercrime chances. To investigate how these variables affect the probability of data breaches, we created a theoretical model. We suggested that these parameters have a beneficial impact on the probability of data breaches using a CBSEM architecture. CB-SEM provides a thorough examination of the elements that contribute to security breaches as well as the fundamental ideas of criminal theory, providing important information for creating tactics that effectively prevent crime. By applying crime theory to the examination of data breaches, this study aims to further the body of knowledge already available on cybercrime. Through this integration, the study hopes to improve our knowledge of cyberthreats and help sectors find and fix weaknesses in digital systems.

REFERENCES

[1] IBM/Ponemon. (2023). Cost of a Data Breach Report. [Online]. Available: https://www.ibm.com/security/data-breach

[2] (2024). Thales Data Threat Report. [Online]. Available: https://go.thalesesecurity.com/rs/480-LWA-970/images/2024-DTRGlobal- A4-Web-ar.pdf

[3] J. Straub, ‘‘Evaluating the use of technology readiness levels (TRLs) for cybersecurity systems,’’ in Proc. IEEE Int. Syst. Conf., Apr. 2021, pp. 1–6.

[4] X. Li and H. Li, ‘‘A visual analysis of research on information security risk by using CiteSpace,’’ IEEE Access, vol. 6, pp. 63243–63257, 2018.

[5] P. Mayer, Y. Zou, B. M. Lowens, H. A. Dyer, K. Le, F. Schaub, and A. J. Aviv, ‘‘Awareness, intention, (In)action: Individuals’ reactions to data breaches,’’ ACM Trans. Comput.-Hum. Interact., vol. 30, no. 5, pp. 1–53, Oct. 2023.

[6] M. Ashraf, Potentially Unintended Consequences of the Sec Restricting Managerial Discretion: Evidence From Peer Data Breaches and Cyber Risk Factors, document SSRN 3807487, 2021.

[7] A. Bouveret, ‘‘Cyber risk for the financial sector: A framework for quantitative assessment,’’ IMF Work. Papers, vol. 18, no. 143, p. 1, 2018.

[8] N. Nejjari, K. Zkik, and H. Benbrahim, ‘‘The breach is dead, long live the breach: A spatial temporal study of healthcare data breaches,’’ in Proc. Int. Conf. Sci., Eng. Manag. Inf. Technol., 2022, pp. 287–303.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp942-951
Vol. 21, Issue 2, 2025

[9] M. Barati and B. Yankson, ‘‘Predicting the occurrence of a data breach,’’ Int. J. Inf. Manage. Data Insights, vol. 2, no. 2, Nov. 2022, Art. no. 100128.
[10] Z. Fang, M. Xu, S. Xu, and T. Hu, ‘‘A framework for predicting data breach risk: Leveraging dependence to cope with sparsity,’’ IEEE Trans. Inf. Forensics Security, vol. 16, pp. 2186–2201, 2021.
[11] H. Sun, M. Xu, and P. Zhao, ‘‘Modeling malicious hacking data breach risks,’’ North Amer. Actuarial J., vol. 25, no. 4, pp. 484–502, Oct. 2021.
[12] X. Zhang and X. Chen, ‘‘Research on breach prediction for big data through hybrid ensemble learning and logistic regression,’’ J. Phys. Conf. Ser., vol. 1982, no. 1, Jul. 2021, Art. no. 012049.
[13] X. Huang, Y. Lu, D. Li, and M. Ma, ‘‘A novel mechanism for fast detection of transformed data leakage,’’ IEEE Access, vol. 6, pp. 35926–35936, 2018.
[14] A. Acquisti, A. Friedman, and R. Telang, ‘‘Is there a cost to privacy breaches? An event study,’’ in Proc. ICIS, 2006, p. 94.
[15] S. Cook, L. Giommoni, N. Trajtenberg Pareja, M. Levi, and M. L. Williams, ‘‘Fear of economic cybercrime across Europe: A multilevel application of routine activity theory,’’ Brit. J. Criminology, vol. 63, no. 2, pp. 384–406, Mar. 2023.
[16] Z. I. Vakhitova, C. L. Alston-Knox, and R. I. Mawby, ‘‘Online routine activities and self-guardianship against cyber abuse,’’ Victims Offenders, vol. 18, no. 4, pp. 623–645, May 2023. [17] D. Maimon, C. J. Howell, R. C. Perkins, C. N. Muniz, and T. Berenblum, ‘‘A routine activities approach to evidence-based risk assessment: Findings from two simulated phishing attacks,’’ Social Sci. Comput. Rev., vol. 41, no. 1, pp. 286–304, Feb. 2023.
[18] R. Stark, ‘‘Deviant places: A theory of the ecology of crime,’’ Criminology, vol. 25, no. 4, pp. 893–910, Nov. 1987.
[19] J. C. Cross and A. H. Hernández, ‘‘Place, identity, and deviance: A community-based approach to understanding the relationship between deviance and place,’’ Deviant Behav., vol. 32, no. 6, pp. 503–537, Jul. 2011.
[20] P. Puente Guerrero, ‘‘Lifestyle-exposure theory as a framework to analyze victimization of people experiencing homelessness,’’ Deviant Behav.,vol. 44, no. 10, pp. 1549–1569, Oct. 2023.
[21] R. Jervis, ‘‘Deterrence theory revisited,’’ World Politics, vol. 31, no. 2, pp. 289–324, Jan. 1979.
[22] J. D’Arcy and T. Herath, ‘‘A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings,’’ Eur. J. Inf. Syst., vol. 20, no. 6, pp. 643–658, Nov. 2011.
[23] S. L. Green, ‘‘Rational choice theory: An overview,’’ Fac. Develop., Baylor Univ., Waco, TX, USA, 2002, pp. 1–72.
[24] S. Sattler, F. van Veen, F. Hasselhorn, G. Mehlkop, and C. Sauer, ‘‘An experimental test of situational action theory of crime causation: Investigating the perception-choice process,’’ Social Sci. Res., vol. 106, Aug. 2022, Art. no. 102693.
[25] J. Scott, ‘‘Rational choice theory, understanding contemporary society: Theories of the present,’’ Int. Encyclopedia Social Sci., vol. 129, pp. 126–138, Jun. 2000.