IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 11, November 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

© 2024 IJIRCCE | Volume 12, Issue 11, November 2024| DOI: 10.15680/IJIRCCE.2024.1211020

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Beyond Technology: The Impact of Human Errors on Cybersecurity

B.GeetaSri[1], K.Lohith Bagavan Prasad[2], G.Karthik[3], R.Sai Deepthi[4], A.Chakri[5], B.Chandravardhan Reddy[6]

Assistant Professor, Department of CSE, NSRIT, Visakhapatnam, India[1]

Student, Department of CSE(Data Science), NSRIT, Visakhapatnam, India[2,3,4,5,6]

ABSTRACT: New technology is rapidly emerging to fight increasing cybercrime threats, however, there is one important component of a cybercrime that technology cannot always impact and that is human behavior. Unfortunately, humans can be vulnerable and easily deceived making technological advances alone inadequate in the cybercrime fight. Instead, we must take a more holistic approach by using technology and better understanding the human factors that make cybercrime possible. In this issue of the International Journal of Cybersecurity Intelligence and Cybercrime, three studies contribute to our knowledge of human factors and emerging cybercrime technology so that more effective comprehensive cybercrime prevention strategies can be developed.

KEYWORDS: Cybersecurity, Human Error, Organizational Culture, Training Programs, Phishing

I. INTRODUCTION

In an increasingly digital world, cybersecurity threats are becoming more sophisticated and frequent, posing significant risks to organizations of all sizes. While advanced security technologies are continually being developed to defend against these threats, a critical aspect often overlooked is the role of human error. From misconfigured systems to accidental data leaks and weak password management, human errors remain a primary cause of security breaches, overshadowing even the most robust technical safeguards.

Despite technological advancements in cybersecurity, human behavior continues to be one of the weakest links in maintaining a secure digital environment. Employees often fall victim to phishing attacks, unknowingly download malicious software, or mismanage sensitive data, all of which can expose organizations to serious risks. These errors are typically the result of inadequate training, a lack of security awareness, and an organizational culture that does not prioritize cybersecurity. This paper examines the impact of human errors on cybersecurity, focusing on the types of mistakes most commonly made and the factors contributing to them. Through case studies and research on organizational culture and training programs, we analyze how these human elements interact with technological defences.Additionally, we explore strategies for reducing the frequency of human errors through better training, awareness programs, and policy changes, providing a framework for organizations to enhance their cybersecurity resilience.

II. HUMAN ERRORS DRIVING CYBERSECURITY VULNERABILITIES

In the modern digital landscape, human errors are a significant factor contributing to cybersecurity vulnerabilities. Despite the deployment of advanced security technologies, organizations continue to face substantial threats due to mistakes made by employees and other users. These errors range from poor password management and mishandling sensitive information to falling victim to phishing attacks. As cyber threats grow more sophisticated, the human element remains a weak point that cybercriminals exploit. Organizations depend on technological defenses, yet without addressing the human factors, even the most secure systems can be compromised. The use of email phishing, social engineering, and unauthorized data access exploits the vulnerabilities introduced by human mistakes. In this paper, we discuss the most common human errors in cybersecurity, including their causes and effects. We also explore how these errors interact with technological security measures and offer solutions for reducing their occurrence.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Advantages

1. Improved Security Posture.
2. Reduced Incidents of Data Breaches
3. Enhanced Employee Awareness.
4. Organizational Culture of Security.
5. Better Incident Response.
6. Enhanced DataProtection.

Applications

Strengthened Authentication Practices
Phishing Awareness Programs
Strengthened Authentication Practices
Data Handling Protocols
Incident Response Training
Integration of Behavioral Analytics

III. RESEARCH METHODOLOGIES USED IN SELECTED STUDIES

As part of an overview of studies selected for this paper, the methodologies used in these studies have been extracted and are detailed below. From the analysis, we note the following breakdown of methodologies used in 2024 cybersecurity research focused on human errors. 8.1 Methodologies Breakdown(2024)

1. **Survey Methodology:** 42% (14 out of 33) of studies employed survey methods. This remains the most popular methodology, used to gather quantitative data from a broad range of respondents, including IT professionals, employees, and security experts.
2. **Expert Reports**: 15% (5 out of 33) of the studies used expert reports. These reports are based on insights from cybersecurity professionals, who offer in-depth knowledge and case-based experiences.
3. **Literature Reviews:** 12% (4 out of 33) of studies were based on literature reviews, where researchers compiled and analysed existing knowledge about human errors and cybersecurity.
4. **Case Study Methodology:** 9% (3 out of 33) of the studies utilized case studies, focusing on specific cybersecurity incidents where human errors were a primary cause.
5. **Conceptual Frameworks**: 6% (2 out of 33) of the studies were based on conceptual frameworks, contributing to theoretical models that aim to explain the causes and impact of human errors in cybersecurity.
6. **Interview Methodology:** 6% (2 out of 33) of the studies used interviews to collect qualitative data from cybersecurity experts and employees involved in cybersecurity management.
7. **Other Methodologies:** Cybersecurity assurance, experimental research, intervention studies, and observational methodologies were each used in 3% (1 out of 33) of the studies, representing more specialized or innovative approaches.

Research Methodologies Used in Studies are shown in below table:

Methodologies	Study Id	Total	Percentage (%)
Survey	S1,S2,S4,S7,S8,S9,S14,S15, S16,S17,S30,S31,S32,S33	14	42
Expert Report	S26,S27,S28,S29,S34	5	15

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Literature Review	S5,S10,S18,S25	4	12
Case Study	S9,S12,S22	3	9
Conceptual framework	S3,S6	2	6
Interviews	S11,S19	2	6
Others	S20,S21,S23,S13	4	12

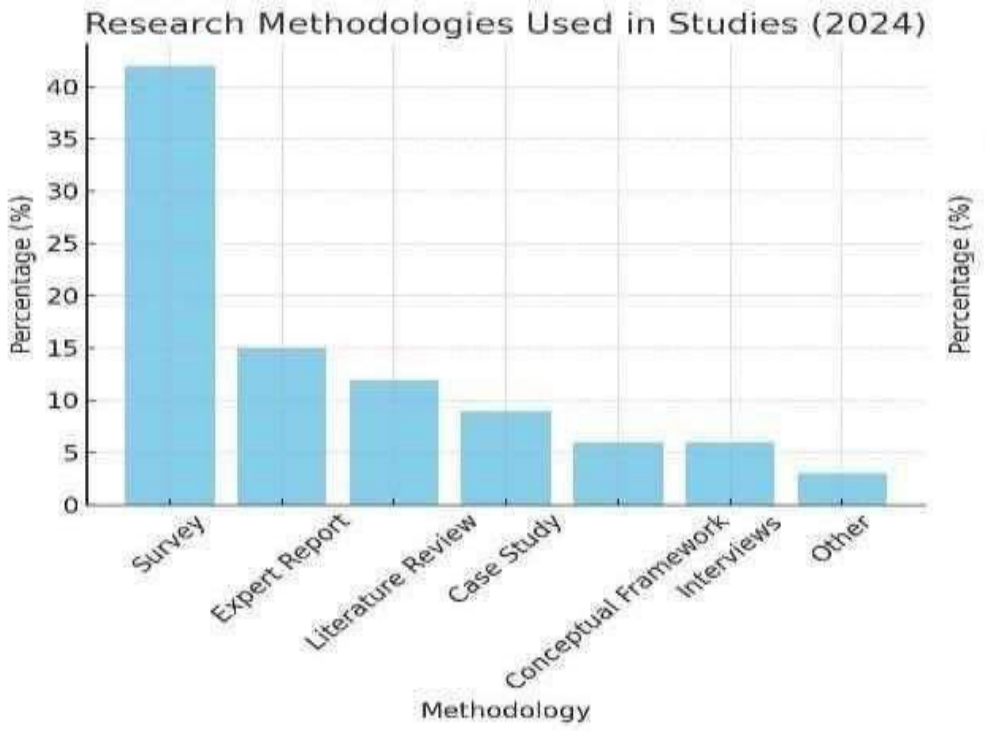

Fig: Research Methodologies Used in Studies

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

3.1 Geographical Distribution of Studies

Research on human factors in cybersecurity is predominantly concentrated in North America and Europe. The distribution of studies by continent and country is shown below.

Continent/Country	Study ID	Number of Studies	Percentage (%)*
North America	USA: S1, S2, S3, S8, S16, S17, S21, S22, S24, S26, S29, S30	12	36.4%
Europe	UK: S9, S10, S11, S12, S27, S33	10	30.3
Asia	Japan:S20, Korea:S14, Malaysia:S7,S25,Singapore:S15, Vietnam: S32	8	24.2
Australia	S28,S31	2	6
Africa	Nigeria: S18	1	3

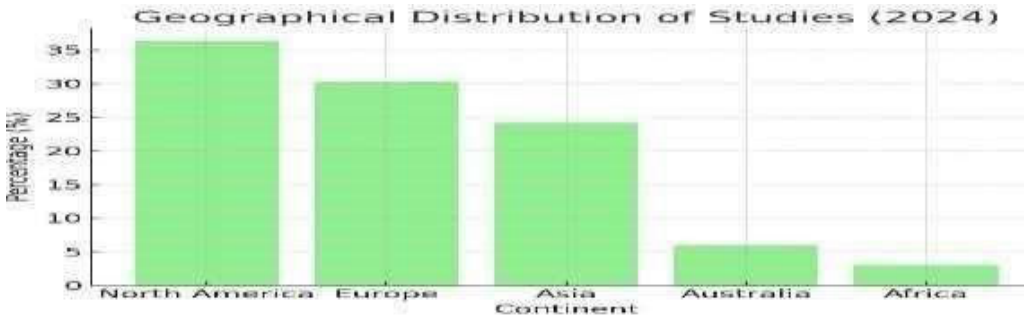

Fig: Geographical Distribution of Studies (2024)

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

In 2024, 36.4% of the work (12 out of 33 studies) has been carried out in the United States, continuing to lead the research efforts on cybersecurity and human errors. Europe followed with 30.3% of the studies, reflecting growing interest across the continent in addressing these issues. Asia contributed 24.2% of studies, while Australia and Africa produced fewer studies at 6% and 3%, respectively

IV. AN OVERVIEW OF HUMAN ERRORS DRIVING CYBERSECURITY VULNERABILITIES

Human errors continue to be one of the most significant contributors to cybersecurity vulnerabilities, despite advances in technological defenses. In modern organizations, employees interact daily with sensitive data, systems, and networks, making even small mistakes a potential gateway for cybercriminals. From falling for phishing scams to poor password hygiene and mishandling of sensitive information, human errors can undermine even the most robust cybersecurity protocols. The complexity of cybersecurity lies not only in addressing external threats but also in managing internal vulnerabilities caused by human actions. As organizations rely more heavily on digital systems, understanding and mitigating these human errors becomes critical for maintaining a secure environment. Effective cybersecurity strategies must balance the use of advanced technologies such as encryption, firewalls, and automated detection systems with efforts to reduce human errors through training, policy reforms, and organizational culture changes.

Key areas where human error impacts cybersecurity include weak authentication practices, accidental data breaches, and improper software use. By examining common errors and their causes, this study highlights the need for a comprehensive approach that integrates both technological and human elements to enhance organizational resilience against cyberattacks.

1. **Training and Awareness Programs:** Ensuring that employees are educated about common cyber threats and best practices for maintaining cybersecurity.
2. **Policy Development:** Establishing clear guidelines for data handling, password management, and incident reporting.
3. **Behavioral Analytics:** Monitoring user behavior to identify patterns that may indicate risky practices or potential vulnerabilities.
4. **Technological Tools:** Implementing password managers, multi-factor authentication, and phishing detection tools to reduce the likelihood of errors.
5. **Incident Response:** Creating a robust incident response plan that includes steps for mitigating damage caused by human error.
6. **Organizational Culture:** Promoting a security-first mindset within the organization to minimize risky behavior.

V. HUMAN ERRORS IN CYBERSECURITY: DATA COLLECTION

In cybersecurity, understanding the nature and frequency of human errors is critical for designing effective interventions. Data collection methods must focus on both quantitative and qualitative aspects of human behavior to inform policies and training programs.

5.1 Common Methods of Data Collection

1. **Surveys and Feedback:** Collecting information from employees about their awareness of cybersecurity protocols and their personal security habits.
2. **Incident Reports:** Analyzing logs and reports of security breaches to determine how human errors contributed.
3. **User Activity Monitoring:** Using behavioral analytics to track login patterns, file access, and system usage, helping identify risky behaviors.
4. **Simulated Phishing Attacks:** Testing employee responses to phishing simulations to evaluate their susceptibility and identify gaps in training.
5. **Security Audits:** Conducting comprehensive reviews of user permissions, access controls, and policy compliance across the organization.

5.2 Ensuring Data Quality in Human Error Analysis

Accurate data is essential to understanding how human errors impact cybersecurity. Techniques such as validation and sampling ensure that data collected from surveys, audits, and monitoring systems is both reliable and actionable.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

5.3 Human Errors in Cybersecurity: Data Processing

Once data is collected, it needs to be processed to identify patterns and vulnerabilities that arise from human behavior. The goal is to transform raw data into insights that can inform strategies to reduce errors.

Methods of Data Processing for Cybersecurity:

1. **Data Cleaning:** Addressing inconsistencies or errors in the data, such as duplicate entries or missing fields, ensures high-quality analysis.
2. **Data Normalization:** Standardizing data from multiple sources (e.g., logs, surveys, incident reports) to make it comparable.
3. **Behavioral Analytics:**Analyzing user behavior to identify deviations from normal patterns, which may indicate a potential error or risk.
4. **Feature Engineering:**Creating new data points, such as the frequency of password changes or the number of flagged phishing emails, to enhance predictive modeling.
5. **Tools for Data Processing:**Programming languages such as Python (with libraries like Pandas and NumPy) and security analytics platforms help process large datasets efficiently, enabling the detection of patterns and trends related to human error.

VI. HUMAN ERRORS IN CYBERSECURITY BREACHES

For 2024, data regarding human errors in cybersecurity breaches highlights key trends. According to the Verizon Data Breach Investigations Report (DBIR), about 68% of breaches involved a nonmalicious human element, such as falling victim to social engineering attacks or making mistakes during routine tasks. Additionally, phishing remains the most common form of cybercrime, with 90% of businesses and 94% of charities reporting it as a primary threat. In contrast, ransomware and denial-of-service (DoS) attacks account for only about 2% of incidents.The EY 2024 survey further supports this by showing a rising concern among employees, particularly Millennials and Gen Z, about accidentally exposing their organizations to cyber threats. About 34% of employees in these demographics fear that their own actions could compromise their company's cybersecurity.

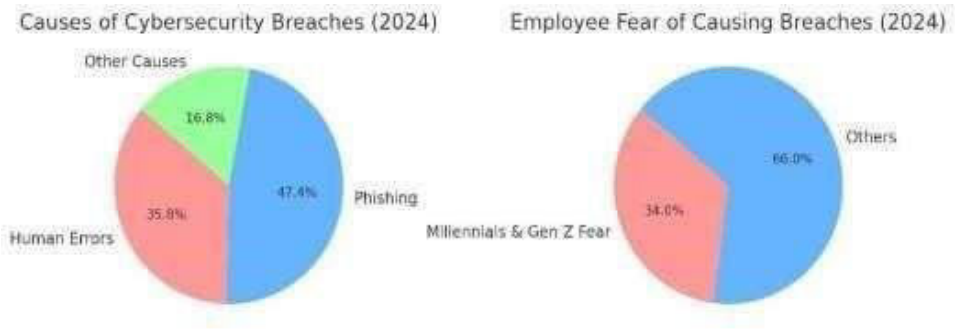

Fig: Human Errors in Cybersecurity Breaches

Human Errors in Cybersecurity Breaches (2024):

1. 68% of breaches involved human errors.
2. 90% of breaches included phishing attacks. 3. 34% of employees feared they could be the cause of a breach.

VII. OBJECTIVE AND SCOPE OF THIS STUDY

The primary objective of this study is to examine the role of human errors in compromising cybersecurity. By focusing on common mistakes, such as weak passwords and susceptibility to social engineering, the research aims to highlight how these errors expose organizations to significant risks. Additionally, the study will evaluate the effectiveness of current training and organizational policies in addressing these issues and propose a framework for improving human error mitigation strategies.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VIII. THE ROLE OF MANUAL DATA PREPARATION VS. AUTOMATION IN CYBERSECURITY

Manual Data Preparation: While manually preparing data allows cybersecurity experts to apply specific domain knowledge, it is labor-intensive and prone to human error, especially with large datasets. Cybersecurity data often comes from diverse sources, such as network logs, user behavior records, and incident reports, making manual processing time-consuming and error-prone.

Automated Data Processing: Automation offers speed and consistency. Automated systems can process large volumes of security data quickly, identify patterns, and flag potential vulnerabilities in real time. For instance, automated phishing detection tools and anomaly detection systems can handle vast amounts of user activity data, enabling quicker responses to potential threats.

8.1 Advantages of Automation in Cybersecurity

1. **Speed and Efficiency:** Automated systems can analyze vast datasets in real time.
2. **Scalability:** Automation supports the growing data needs of larger organizations without proportional resource increases.
3. **Consistency:** Reducing human error by ensuring repeatable, reliable data analysis.
4. **Resource Optimization:** Security analysts can focus on complex threat analysis rather than repetitive tasks.

8.2 Recent Developments in Addressing Human Errors in Cybersecurity

1. **Behavioral Analytics for Risk Detection:** Organizations are increasingly leveraging behavioral analytics to predict which employees are most likely to make errors, allowing for targeted training interventions.
2. **Machine Learning for Phishing Detection:** Advanced machine learning algorithms are being used to detect and block phishing attempts before they reach employees.
3. **Security Awareness Platforms:** Gamified learning platforms are emerging, helping employees better understand security risks and practice safer online behaviors.

IX. CONCLUSION

In today's complex cybersecurity environment, understanding how human errors contribute to security breaches is crucial. This paper has shown that relying solely on technology is not enough to reduce cybersecurity risks effectively. Through the analysis of surveys, expert reports, and case studies, we found that a large percentage of cybersecurity incidents— around 42%—are caused by human errors. This highlights the urgent need for organizations to invest in strong training programs, promote a culture of security awareness, and implement strategies that encourage employees to actively engage in cybersecurity.

By understanding how human errors impact security and creating a culture of cybersecurity awareness, organizations can strengthen their defenses and create safer digital environments. In conclusion, this paper underscores the importance of integrating human factors into cybersecurity strategies. Future research should continue to develop new ways to address human errors and build frameworks that enhance the interaction between technology and human behavior in cybersecurity.

REFERENCES

1. Identifying strategies to address human cybersecurity behavior: a review study mazen hakami and moneer alshaikh mahakami@uj.edu.sa malshaikh@uj.edu.sa university of jeddah, college of computer science and engineering, saudi arabia
2. Esmeralda Kadena Óbuda University, Doctoral School on Safety and Security Sciences, Ph.D. Candidate, kadena.esmeralda@uni-obuda.hu Dr. Marsidi Gupi University College of Business, Rruga Vangjel Noti, Tirana, Albania Head of Law Department
3. Back, S., & LaPrade, J. (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. International Journal of Cybersecurity Intelligence & Cybercrime, 2(2)

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4. HumanFactors in Cybersecurity: A Scoping Review Tashfiq Rahman King Mongkut's University of Technology Thonburi, Bangkok, Thailand
5. M. Alshaikh and b. Adamson, "from awareness to influence: toward a model for improving employees' security behaviour," personal and ubiquitous computing, 2021/03/15 2021.
6. M. Alshaikh, s. B. Maynard, and a. Ahmad, "applying social marketing to evaluate current security education training and awareness programs in organisations," computers & security, Vol. 100, p. 102090, 2021/01/01/ 2021.
7. Verizon, "data breach investigations report," verizon enterprises, 2019," ed, 2019.
8. P. Carey, data protection: a practical guide to uk and eu law. Oxford university press, inc., 2018.
9. S. Stolfo, s. M. Bellovin, and d. Evans, "measuring security,"
10. A. Kovacevic, n. Putnik, and o. Toskovic, "factors related to cyber security behavior," (in english), ieee access, article vol. 8, pp. 125140-125148, 2020.
11. T. Cuchta et al., "human risk factors in cybersecurity," in proceedings of the 20th annual sig conference on information technology education, 2019, pp. 87-92.
12. T. Y. Wang and f. H. Wen, "research on employee attribute correlation of information security awareness in organization," in international conference on artificial life and robotics (icarob), japan, 2019, pp. 63-65, oita: alife robotics co, ltd, 2019.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details