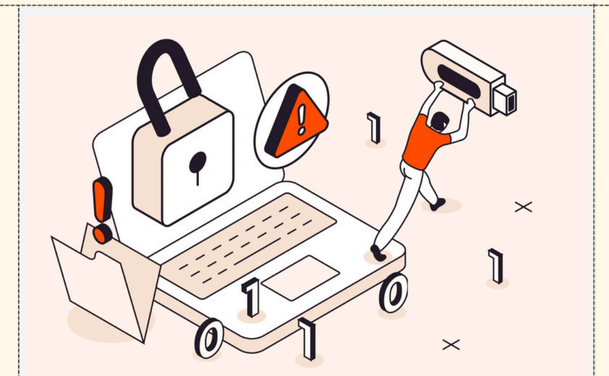
An Empirical Study of Data Breaches and Privacy Issues

Authors
UMANGI KATHROTIA(365701)
RIDDHISH DOBARIYA (366842)

CHARLES DARWIN UNIVERSITY

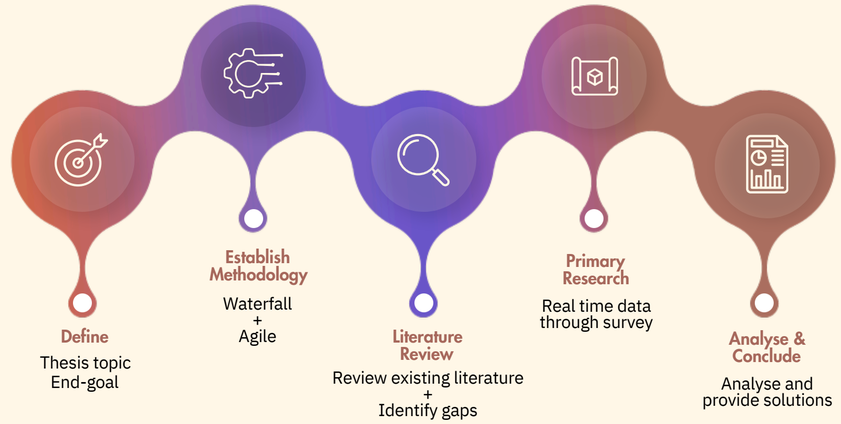
01 Introduction

Investigating the surge of cybersecurity risks linked to technological advances in the financial sector.
This study focuses on uncovering the root causes and consequences of data breaches, with the goal of enhancing current security protocols and defending against future threats.



02 Objective

- Investigate root causes of data breaches in the financial industry.
- Analyze the impacts of data breach attacks.
- Identify preservation and mitigation strategies.
- Propose solutions to prevent future data breaches.
- Assess the role of emerging technologies like AI and blockchain in enhancing cybersecurity.
- Enhance cybersecurity awareness and training to reduce human error.

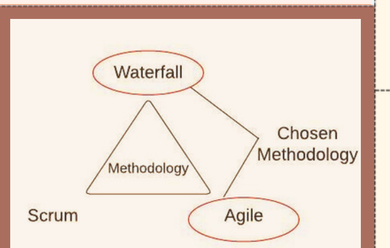


03 Methodology

We adapted the methodologies - Waterfall & Agile for our thesis

For our thesis, we have first followed the waterfall method where existing literature was reviewed by us to understand the existing problem

Followed by this was our questionnaire based result reporting that helped us understand the problems industries facing



04 Existing Literature

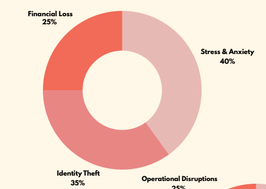
- Cybercriminals are constantly evolving tactics, making traditional security measures like encryption and firewalls inadequate against advanced threats.
- Authentication vulnerabilities and third-party vendors are significant risks for financial institutions.
- Human error, due to lack of training, contributes to many data breaches.
- Research emphasizes the need for AI, blockchain, and regulatory compliance to enhance security and trust.

05 Contributions

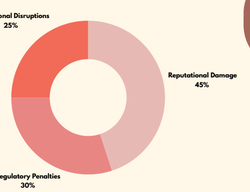
- Identified root causes of data breaches in the financial sector, including human error and vendor risks.
- Evaluated security measures like AI-based detection systems and blockchain for improved protection.
- Developed a predictive model using machine learning to assess breach risks and propose defenses.

06 Results & Findings

Impacts of Data Breach Attack



Individuals



Organizations

Proposed Solutions

- Incident Response Plan Drill
- AI-Based Intruder Detection Monitoring System
- Updated New Account Application Form
- Fixed Internet Provider for Work from Home Employee

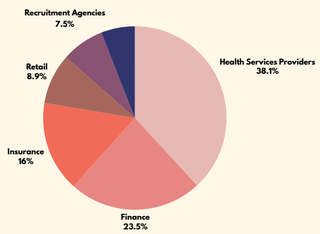
07 Conclusion

Investigate Blockchain, homomorphic encryption, and emerging mitigating technologies.
Develop a predictive model leveraging machine learning to identify potential data breach risks and vulnerabilities.
Effective mitigation requires multilayered defenses, regulatory adherence, and leveraging emerging technologies.
Continued research spanning predictive models, cross-industry collaborations, and policy enhancements.

We Proposed:

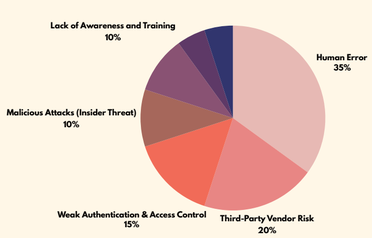
- Enhance incident response plans with regular drills to ensure preparedness for cybersecurity incidents.
- Strengthen third-party risk management through comprehensive vendor assessments.
- Increase cybersecurity awareness training to foster a vigilant organizational culture.

2023 Data Breach Attacks by Industry



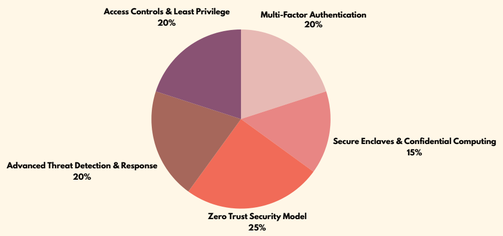
- 38.13% of 2023 data breaches occurred in the Health Services Providers sector, the highest among industries.
- The Finance and Insurance sectors followed with 23.51% and 15.98% of breaches, respectively, while Legal, Accounting, and Management Services accounted for 5.94%.

Root Causes of Data Breach Attacks



- 30% of breaches are caused by Human Error, making it the largest contributor to cyber incidents.
- Third-Party Vendor Risk and Weak Authentication & Access Control follow at 25% and 20%, respectively.

Mitigation Strategy



- The AI-Based Intruder Detection Monitoring System holds the most weight, covering 40% of the focus in mitigation efforts.
- Incident Response Plan Drills and Updated New Account Application Forms take up 25% and 20% of the proposed solutions, respectively.

Cybersecurity Measures Implemented by Companies

- 50% of companies have implemented Multi-Factor Authentication (MFA) as a primary security measure.
- Firewalls and Encryption are also widely adopted, used by 40% of organizations to protect sensitive data.

References

- Epetimehin, F & Fatoki, O n.d., International Journal of Economics, Commerce and Management OPERATIONAL RISK MANAGEMENT AND THE FINANCIAL SECTOR DEVELOPMENT: AN OVERVIEW.
- Wewege, L., Lee, J. & Thomsett, M.C., 2020. Disruptions and Digital Banking Trends. Journal of Applied Finance & Banking, 10(6), pp.15-56.
- Wang, P & Wood, D 2019, 'ECONOMIC COSTS AND IMPACTS OF BUSINESS DATA BREACHES', Issues in Information Systems, vol. 20, no. 2, pp. 162–171.