Summarize the papers.

1\_ [Enterprise data breach causes, challenges, prevention, and future directions.](https://wires.onlinelibrary.wiley.com/doi/10.1002/widm.1211)

(Long Cheng، 2017)This paper reviews enterprise data breach causes, challenges, and future prevention strategies, focusing on the threats of intentional or unintentional data leaks that expose sensitive information like employee and customer data, intellectual property, and medical records. It analyzes recent high-profile incidents, such as Target’s 2013 breach and Yahoo’s 2014 breach, showing the substantial financial and reputational damage that data leaks cause. Research indicates that insiders account for over 40% of breaches, with motivations ranging from espionage to accidental errors. The paper explores various state-of-the-art prevention and detection techniques, such as Data Leak Prevention and Detection (DLPD) systems that monitor and control data flows using policies and behavior modeling. However, the big data era presents new challenges, as modern communication tools (e.g., cloud sharing, email, messaging) increase leak risks. Future directions for reducing data breaches include developing privacy-preserving detection systems, cloud service leak detection, and deep learning-based anomaly detection for insider threats, aiming to transition towards more robust and adaptable solutions in enterprise security.

2\_ [Healthcare Data Breaches Insights and Implications](https://www.mdpi.com/2227-9032/8/2/133):

(Adil Hussain Seh 1ORCID, 2020) pointed to Computerized change in healthcare has progressed openness to treatment, but has moreover expanded helplessness to information breaches, with hacking/IT occurrences being the foremost common shape, taken after by unauthorized inside divulgence From 2005 to 2019, 249.09 million individuals were influenced and 157.4 million were influenced within the final five a long time alone.In 2018, the industry experienced 536 breaches, compromising 41.2 million records.The normal breach taken a toll in 2019 come to $3.92 million, a worldwide tall, reflecting a 12% increment since 2014. The think about connected straightforward moving normal (SMA) and straightforward exponential smoothing (SES) strategies to foresee data breach patterns utilizing information from the PRC database and HIPAA diaries, and found that SMA was more dependable. The comes about uncovered that 64% of restorative data spills since 2005 were due to hacking, and more than 92% of records have been compromised by hacking in later years.In 2019, hacking occurrences expanded by 73.4%, whereas other spills such as theft/loss and disgraceful transfer sorts diminished. The normal taken a toll per restorative breach rose to $6.45 million, and the fetched per record expanded 5.14%. The consider underscores the require for expanded security measures in healthcare and advocates proactive techniques to address the developing hazard and financial effect of information breaches.

3\_ [Pwned The Risk of Exposure from Data Breaches](https://dl.acm.org/doi/10.1145/3292522.3326046):

(Gaurav Sood, 2019)This study examines the prevalence of personal information leaks among Americans in data breaches that lack detailed research, particularly with respect to individual risk. Using a new dataset, the researchers estimated the minimum average number of online accounts compromised per capita by integrating data from a representative YouGov sample with information from Have I Been Pwned (HIBP), which catalogs 293 public information breaches. The results of the analysis of 5,000 e-mails revealed that 14,979 breaches occurred, with an average of three breaches per person and at least 82.84% of Americans experiencing at least one breach. Socioeconomic factors revealed some interesting trends. The frequency of breaches increases with education level, with the average number of breaches for individuals without a high school degree being 2.35, while the more educated are more likely to be breached. The study also found that middle-aged and older accounts face higher risks than younger and older users. Female accounts are 1.12 times more likely to be compromised than male accounts, black accounts are 3.12 times more likely to be compromised than male accounts, and white accounts are 3.16 times more likely to be compromised than white accounts. Of the 15,837 breaches examined, 94.58% were confirmed and one-third were classified as spam listings. The study emphasizes that the relationship between the frequency of breaches and factors such as education and age differs from traditional digital divide concerns, indicating that increased online activity is correlated with a higher risk of breaches, especially among more educated users.

4\_ [Ransomware Reloaded Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration](https://dl.acm.org/doi/10.1145/3691340):

(Timothy McIntosh, 2024)Explain more about Ransomware is a significant cybersecurity threat, causing data breaches and disruptions. However, many studies lack consideration of government strategies, industry guidelines, and cyber intelligence. A study evaluating 212 academic studies found that many were irrelevant to the current reality. The study proposed prioritizing data exfiltration over encryption, considering ransomware in a business-practical manner, and recommending collaboration with the industry to address this evolving threat.

This survey compiled the ransomware evolution history and applied Rogers' Innovation Adoption Curve, predicting the rise of destructive ransomware with espionage. It reviewed 212 academic studies and found that most research has become less relevant in the era of ransomware double extortion with data exfiltration. The survey proposed integrating ransomware risk management into organizational cybersecurity risk management, emphasizing government strategies, industry reports, guidelines, and cyber intelligence. It also discussed innovative research prospects, including generative AI, and suggested future research directions.

5\_ [The Challenges of Leveraging Threat Intelligence to Stop Data Breaches](https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2020.00036/full) :

(Amani Ibrahim, 2020)Despite significant cybersecurity investments, companies face ongoing data breaches that have significant financial and reputational consequences. To protect digital assets and improve threat visibility, threat intelligence employing AI and machine learning is emerging, moving from reactive to proactive defense strategies. This evolution of threat intelligence aims to predict security threats by analyzing and integrating cyber data to gain insights tailored to an organization's unique risk landscape, enhancing both visibility and incident response. It is critical to distinguish between data loss (unintentional) and data breach (intentional), and data loss prevention (DLP) addresses the former while incident response planning addresses the latter, analyzing system logs for forensic purposes after a breach. Effective machine learning solutions in cybersecurity must be aligned with business goals and security standards, and must focus on specific threat scenarios with high-quality training data sets to maximize predictive accuracy and relevance. However, machine learning also introduces vulnerabilities to hostile attacks, so continuous learning is essential to adapt models to changes in the threat environment and mitigate concept drift. Continuous monitoring, root cause analysis (RCA), and improved mapping of infrastructure and threat interdependencies will continue to be essential in managing organization-specific risks and supporting continuous adaptation to the evolving cybersecurity landscape.

# References

Adil Hussain Seh 1ORCID, M. Z. 2. A. 2. K. S. 1. A. 1. K. 1. a. A. K. 1., 2020. *Healthcare Data Breaches: Insights and Implications.* [Online]   
Available at: https://www.mdpi.com/2227-9032/8/2/133

Amani Ibrahim, D. T.-G. S. A., 2020. *The Challenges of Leveraging Threat Intelligence to Stop Data Breaches.* [Online]   
Available at: https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2020.00036/full

Gaurav Sood, K. C., 2019. *Pwned: The Risk of Exposure From Data Breaches.* [Online]   
Available at: https://dl.acm.org/doi/10.1145/3292522.3326046

Long Cheng, F. L. D. (. Y., 2017. *Enterprise data breach: causes, challenges, prevention, and future directions.* [Online]   
Available at: https://wires.onlinelibrary.wiley.com/doi/10.1002/widm.1211

Timothy McIntosh, T. S. T. L. D. X. P. W. D. L. Y. H. A. N. M. H. I. &. C., 2024. *Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration.* [Online]   
Available at: https://dl.acm.org/doi/10.1145/3691340