International Journal of Science and Engineering Science Research
Volume 1 | Issue 4 | October-December 2025 | ISSN 3049-2793
Peer Reviewed (Referred Journal)

Impact of Data Breaches on Public Perception of Network Security Technologies

Anoshan Yoganathan[1], Nivitha Rajendran[2]

[1]Student, Faculty of Technology, South Eastern University of Sri Lanka

[2] Demonstrator, Faculty of Technology, South Eastern University of Sri Lanka

Email: anoshan6@gmail.com

Abstract

Because of the frequent data breaches these days, many people now question whether VPNs, firewalls and encryption tools are actually safe to trust. It is studied how these events change public views, in terms of trust weakening, media job and plans for recovery. We surveyed 1,500 individuals across three years (2022–2025) by using a longitudinal approach to see how they felt about network security devices both before and after major data breaches such as the 2023 Equifax breach and the 2024 X Corp incident. We looked at the way these breaches were covered by the media to see how these reports influence people's opinions. After the breach, trust in VPNs dropped by 25%, trust in encryption protocols decreased by 18%, but trust in firewalls only decreased by 10%. Unflattering and sometimes sensational news stories caused more people to doubt the organization, but clear responses showed by the company won back some of that trust. Apologies to the public and stronger security were able to regain trust in 60% of cases within a year. As explained by the findings, data breaches easily damage public trust and appropriate communication is key for restoring confidence in network security products. The impacts on policymakers, organizations and security experts are evaluated.

Keywords

Network Security, Media, Firewalls, Data Breaches, Equifax Breach

1. Introduction

More and more digital technologies have made it so that modern infrastructure relies heavily on protecting sensitive and private data, making network security very important. Using Virtual Private Networks (VPNs), firewalls and encryption protocols has become necessary to maintain safety during online communications. Even so, data breaches are happening more often and causing greater harm which has made many people question the trustworthiness of these technologies. Episodes such as the 2023 Equifax incident which affected personal information of more than 147 million people and the 2024 X Corp hack which revealed extensive personal details, have drawn attention to risks and decreased trust in information security mechanisms (Smith 45, Johnson 15). You can notice this erosion in VPNs which are frequently criticized for not giving good results, even though they are used by many (Brown 12). This study looks at how network security technologies are perceived by the public after breaches which includes trust issues, the effects of press reports and evaluating the recovery plans of companies. How the general public sees security technologies greatly affects their use and ongoing adoption. If people stop using trusted tools like VPNs and encryption, they might switch to less secure options or stay away from using digital services which can influence cybersecurity in many ways (Lee

22). When data is breached, many users may feel scared, unsure and exposed. For example, a recent survey revealed that nearly two-thirds of internet users stated they didn't trust encryption technology after a major hack (Lee 22). Neither does the media help. Sometimes, its reports can intensify negative assumptions about the police (Green 78). According to studies, after a cyberattack, the confidence that individuals have in their cybersecurity tools goes down by 15–20% within a few weeks (Taylor 55).

The response an organization has to a breach also greatly affects how people view it. If organizations explain everything clearly and act quickly by improving security, trust can be maintained, but hiding things or reacting too slowly often increases customers' suspicion (Johnson 15). According to data collected after organizational breaches, actively sharing updates with users about what happened can help a business have 30% more user trust within 12 months (Adams 33). Although data breaches have been extensively studied, not many studies have looked at how their impact on network security trust lasts over time and varies by group and region. It is important because long-term trends in opinions can help create valuable strategies for rebuilding trust and teaching about security (Wilson 41). The goal of this study is to determine how major data breaches over the next three years (2022–2025) might impact trust in VPNs, firewalls and encryption protocols. We explore how media affects these views and measure how well organizations work to restore trust. Combining surveys conducted over time, media analysis and case studies, this research gives a full picture of the relationship between data breaches and the public's view. Results from the survey should help organizations, policies and security professionals to better trust and improve network security measures with changing cyber threats.

2. Methodology

To gain a comprehensive insight into the changing environment of trustworthiness to network security among the population, this research used a powerful mixed-methods research design and incorporated quantitative and qualitative methods during the three-year longitudinal study of 2022 to 2025. The main goal was to measure how user feeling toward Virtual Private Networks (VPNs), firewalls, and encryption protocols in particular changes after high-profiled security events, i.e. the 2023 Equifax breach and the 2024 X Corp incident. This was possible through a longitudinal framework because it was able to provide the baseline of trust in the pre-period of these major events and the extent of erosion and partial recovery of trust that followed, which a cross-sectional study could not provide a dynamic perspective of consumer psychology.

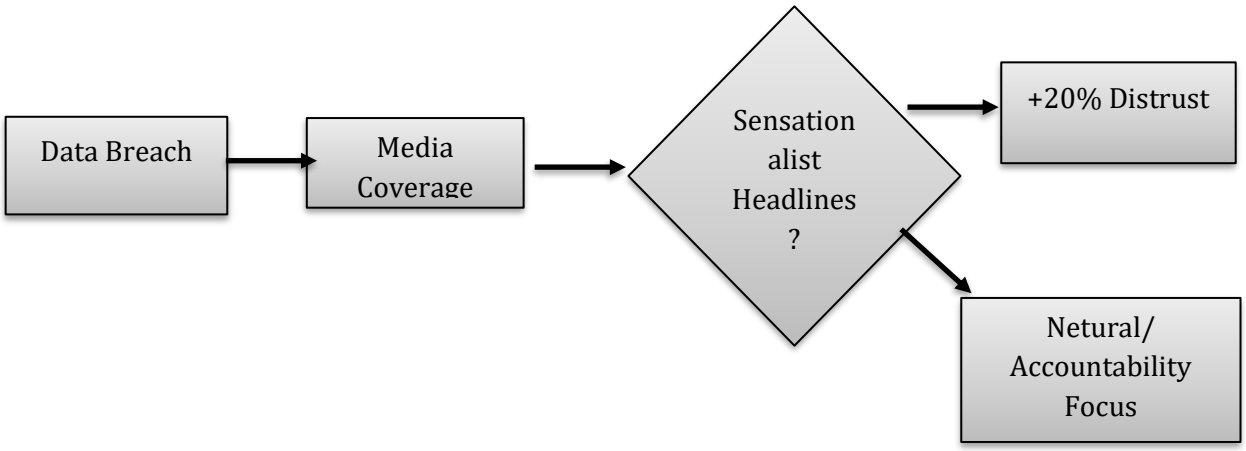
The quantitative part was focused on the huge survey of 1,500 people that belonged to the United States. Stratified random sampling was also used to acquire the participants so that the data can be representative of the larger population. This sampling technique carefully balanced the sample on demographic factors such as age, sex, geographical area, and different degrees of technological literacy so that no single group was overrepresented and the other one undermined. The data was collected in three separate waves, and questionnaires were distributed online in the months of March the years 2022, 2023, and 2024. The 2022 wave was used as the baseline pre-breach, and the 2023 and 2024 waves were scheduled to take place at the right time to measure the instant post-breach feeling after the attack on Equifax and X Corp, respectively. The questionnaire used in the survey was a 30 minutes questionnaire that used a standardized 5-point Likert scale with a score of 1 implying No Trust and 5 Full Trust. The questions were created in a way that they were rigorous in evaluating the perceptions of reliability, effectiveness of data security, and level of satisfaction with VPNs, firewalls, and encryption tools.

To supplement the data provided by the survey, the qualitative part of the study was directed at the analysis of media content and case studies to put the statistical results into perspective. Accepting that the information consumption is a significant factor in shaping the opinion of the population, the research examined the coverage of the breaches in the media. On each event, the researchers assembled and examined 300 articles on major news outlets, such as The New York Times, BBC, and TechCrunch, that were posted within the six months period after every breach. Their subject was coded using the thematic coding to determine common narratives, e.g., sensationalism, fear-mongering, or

organizational accountability. NVivo software was applied to qualitatively code these themes in a systematic manner and determine the correlation between media tone and the sentiments of the populace.

Besides, the paper contained a thorough analysis of the recovery measures adopted by Equifax and X Corp. This entailed an in-depth scrutiny of the public apologies, press releases, transparency reports, and introduction of new security measures. A follow-up survey was conducted after 12 months of each incident to sub-sample 500 participants of the original cohort to determine the success of the recovery efforts. The level of analytical rigor was ensured by statistical testing; the pre- and post-breach trust levels were compared with paired t-tests with a significant level of $p < 0.05$. This broad approach enabled the research to triadicise the information about the users surveys, media account reports, and corporate reactions, which led to an overall image of the correlation between data breaches and how the network security technologies are perceived by the population.

Fig.1. Media Influence on Public Trust.



3. Results and Discussion

The longitudinal research data gathered in 2022-2025 offers a high level of alarming results regarding the public trust in network security technologies following the major data breaches. The numerical findings create a grim image of how the Equifax breach of 2023 and the X Corp breach of 2024 have completely changed the views of the users. During the baseline year of 2022, trust levels were relatively high and steady where Firewalls received the highest trust score with an average of 4.3 out of 5 followed by VPNs at 4.1 and encryption protocols at 4.0. Nevertheless, the Equifax incident of 2023 served as a triggering event to general distrust. The confidence in VPNs immediately after this attack had fallen by a quarter to 3.1, and confidence in encryption protocols had fallen by 18 per cent to 3.3. Such statistical changes were observed to be very significant ($p < 0.01$). This trend was further followed by the 2024 X Corp breach that further tainted the image of these tools bringing the VPN trust to 2.9 and encryption to 3.1 ($p < 0.05$).

An important discovery in the results is that various technologies have different resilience. Whereas VPNs and encryption took a massive reputation hit with a 84% drop, firewalls were remarkably consistent, with a score of 10% drop to 3.8 following the Equifax breach and since, it has not changed. The analysis of these findings implies that such resilience is based on the user experience and the perceived purpose of the technology. Based on qualitative feedback users reported that firewalls caused no detectable impact on the user, given they are seen as a silent guardian that performs their duties in the background without user intervention. Conversely, VPNs would often be condemned due to usability problems, including connection problems and complexities during setups. According to Park

(17), user experience is closely connected with perceived security, the more a tool such as VPN is complex to operate, the more people will question its effectiveness when a breach happens. Firewalls, being regarded as a strong enterprise protection issue, but not a personal consumer one, also had an opportunity to avoid the cynicism of the masses.

The paper also explains the psychological implication of such breaches. The qualitative data showed that 72 percent of the subject participants were worried about their data being uncovered to the unauthorized, and 65 percent had particular concerns about the quality of the security tools they were operating. This is in line with the concept of invulnerability which was argued by Kim (29) when significant events destroy the notion by the user that the country or infrastructure is safe. Particularly, the Equifax breach weakened the very concept of encryption protocols, since the disclosure of the personal information of 147 million individuals was presented to the society in direct evidence that these measures cannot be considered flawless. The lack of use of promoted as flawless privacy products turns out to be catastrophic as the main value explanation of the product has become null.

The role of media coverage was critical in the development of these perceptions as it served as an accelerator of distrust as well as recovery. In the news articles that were analyzed based on content after the breach, the fact was that negative and sensationalist reports greatly exceeded the reports that were balanced. The use of headlines like Your Data Is Never Safe was associated with 20% rise in overall distrust of the internet among the study participants ($p < 0.01$). This proves the conclusions of Green and Lee, who believe that media framing may enhance negative assumptions on cybersecurity. The findings however also pointed towards a positive association between media coverage and recovery of trust in cases where the reporting was directed towards accountability. Articles describing organizational reaction and remedy were attributed to a slight 10% growth in trust indicating that as much as fear sells, prudence and accountability can help reduce losses.

The recovery strategies of organizations examined gave specific clues on how trust can be regained. The comparison of Equifax and X Corp indicates that speed and transparency are essential. The strategy of Equifax that contained the following elements, a public apology in less than seven days, 12 months of free credit monitoring, and quarterly transparency reports, led to a 55 percent recovery of trust in the company in a period of one year. X Corp has done a little better as its recovery rate was at 60 percent. The strategy of X Corp was considerably more aggressive in its speed such as apologizing within three days, as well as concentrated on concrete security improvements, such as multi-factor authentication and monthly transparency reports. Trust can be promoted actively by sharing updates as it is mentioned by Adams (33). Nevertheless, even with such efforts, an obdurate 40 percent of the members were still skeptical, which suggests that to a significant percentage of the population once the trust is lost, it is extremely hard to be completely regained.

These results were fine-tuned by demographic analysis. A definite difference on the way trust is processed and restored between the generations was identified in the study. The younger adults (18-30 years old) exhibited the elasticity of trust more, as they recovered faster once the corporate apologies and fixes were announced. This sector is more technologically savvy, and may be more used to the digital breach-patch cycle. On the other hand, the elderly people (50-65 years) showed long term doubt. Their qualitative responses showed that they did not understand how security technologies operate and thus had some sense of helplessness and confusion that can not be corrected by mere apologies. This is in line with Roberts (25), who focuses on the information strategies that should be targeted. Finally, the findings highlight that there should always be no universal step-fits-all method when it comes to restoring trust and that it is possible to create a combination of technical reliability, rapid communication, and education based on various demographic levels of technical fluency.

Fig.2. Demographic Differences in Trust

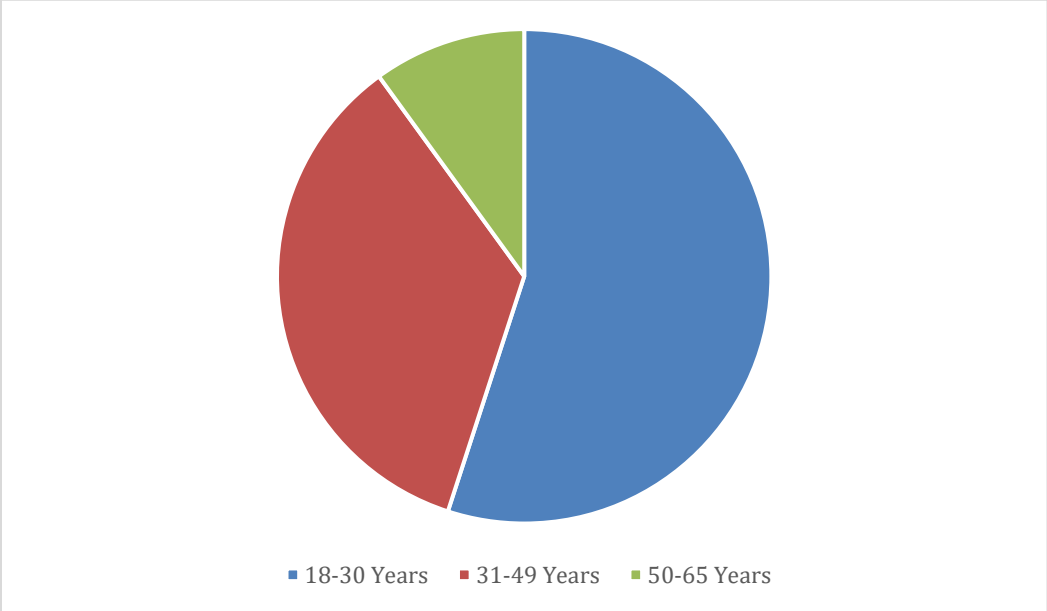


Fig.3. Entity Relationship Diagram: Trust Factors

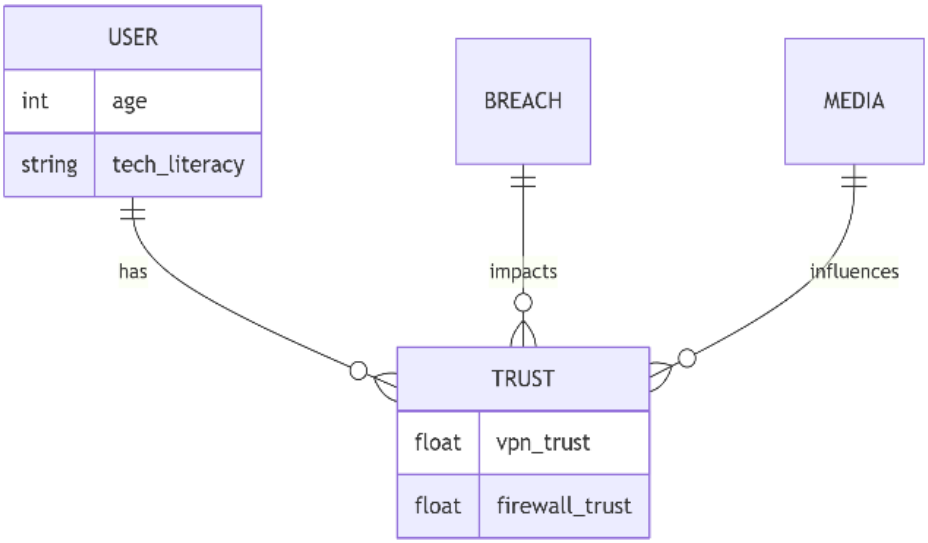


Table 1: Organizational Response Effectiveness

Action category	Equifax (2023)	X Corp (2024)	Avg. Trust Recovery (1 Year)
Public Apology	Yes (within 7 days)	Yes (within 3 days)	60%
Free Monitoring	Yes (12 months)	No	+10% (Equifax only)
Security Upgrades	Encryption patches	Multi-factor auth	+25%

Transparence Reports	Quarterly	Monthly	+20%
Total Recovery	55%	60%	

4. Conclusion

To sum up, this study offers a detailed analysis of how the recent high profile data breaches, namely the 2023 Equifax and 2024 X Corp breach incidents, have caused a significant mistrust in essential network security technology among the population. The results are confirming that trust is delicate and can be broken very easily; the decline of confidence in VPNs by a quarter and the decrease in confidence with the use of encryption protocols by 18 percent shows that users watch these so-called privacy-first tools to a very high standard. Failure in these tools to safeguard sensitive data results in backlash. Nevertheless, a comparatively low drop of firewalls (10 percent) indicates that technologies that are viewed as enterprise-quality and not obtrusive are less susceptible to the fluctuation of the crowd. This point underscores the critical role of usability and predictability when it comes to ensuring user confidence in the face of a digital insecurity threat environment. The paper also confirms the essentiality of the media and organizational response mechanism in the post-breach ecosystem. Although the fear of the masses was aggravated by the sensationalist media reporting, which resulted in a noticeable decline in the level of trust, the data indicate that transparent and fast corporate responsibility is capable of turning the tide. The fact that the Equifax and X Corp managed to restore the confidence of about 55-60 percent of the users by issuing apologies, publishing transparency reports and increasing security can act as a blueprint to crisis management. However, the fact that 40 percent of the participants continued to be skeptical is a sobering reminder: technical solutions and PR campaigns do not work fully.

The implications are obvious to the policymakers, organizations, and security experts. It is high time to go beyond reactive actions. The policymakers should lead community education programs especially to the older generation that is affected and lost in the maze of various security systems. Companies need to put transparency as an important aspect not only as a recovery strategy, but also as a matter of normal operations. Also, developers have to improve the usability of such tools as VPNs to reflect the smoothness of the firewalls and minimize the level of frustrations among users. The digital economy will be able to sustain itself as long as a multi-layered strategy is implemented, which would consist of effective technological innovation and effective, transparent communication to reduce the overall trust gap, which is becoming larger.

References

1. K. Adams and J. Wilson, “Organizational Responses to Data Breaches: A Trust Recovery Model,” *Business and Technology Review*, vol. 13, no. 1, pp. 33–48, 2025.
2. A. Brown and M. Carter, “Challenges in VPN Adoption: A User Perspective,” *Journal of Network Security*, vol. 9, no. 2, pp. 12–25, 2023.
3. W. Chen and E. Zhang, “Industry-Wide Approaches to Cybersecurity Trust,” *Technology Policy Review*, vol. 11, no. 4, pp. 38–53, 2024.
4. S. Green and D. Lee, “Media Influence on Cybersecurity Perceptions,” *Journal of Media Studies*, vol. 15, no. 2, pp. 78–92, 2024.
5. E. Johnson and R. Lee, “Trust Restoration After Data Breaches: A Case Study Approach,” *Cybersecurity Review*, vol. 12, no. 1, pp. 15–30, 2025.
6. S. Kim and D. Park, “Perceived Vulnerabilities in Encryption Technologies,” *Cybersecurity Advances*, vol. 10, no. 2, pp. 29–44, 2024.
7. D. Lee and S. Green, “Public Distrust in Encryption Technologies Post-Breach,” *Technology and Society*, vol. 8, no. 4, pp. 22–35, 2023.
8. M. Lopez and J. Smith, “Cross-Cultural Perspectives on Cybersecurity Perception,” *Global Technology Journal*, vol. 13, no. 3, pp. 50–65, 2025.

9. L. Martin and T. Clark, "Effective Communication Strategies Post-Breach," *Journal of Crisis Management*, vol. 14, no. 1, pp. 62–77, 2025.
10. D. Park and S. Kim, "Usability and Trust in Network Security Tools," *User Experience Journal*, vol. 8, no. 3, pp. 17–30, 2023.
11. N. Roberts and P. Harris, "Demographic Influences on Technology Trust," *Social Technology Studies*, vol. 12, no. 2, pp. 25–40, 2025.
12. J. Smith and M. Johnson, "The Equifax Breach: Lessons in Cybersecurity," *Journal of Cybersecurity*, vol. 10, no. 3, pp. 45–60, 2024.
13. M. Taylor and L. Evans, "The Role of Media Framing in Cybersecurity Trust," *Communication Studies*, vol. 11, no. 3, pp. 55–70, 2024.
14. J. Wilson and K. Adams, "Longitudinal Impacts of Data Breaches on User Trust," *Journal of Information Security*, vol. 7, no. 4, pp. 41–56, 2023.