Advances in Consumer Research
https://acr-journal.com/

Volume-2 | Issue-5 | Nov 2025

Original Researcher Article

Examining the Impact of personal Data Breaches on Consumer Trust and Privacy Protection Behavior in E-Commerce

[1]Dr. Hardeep singh, [2]Dr. Nikita Anand, [3]Professor Sukhvir Singh, [4]Dr. Nupur Angirish, [4]Dr. Nupur Angirish, [5]Dr.Pompi Das Sengupta and [6]Shahid Amin

[1]Professor, Department of Management Studies, Amritsar Group of Colleges, Amritsar, Punjab, India
[2]Assistant Professor, Department of Management and commerce, Trinity Institute of Professional Studies, Dwarka, Sector 9, New Delhi, India
[3]Professor, Department of Commerce, SGTB Khlasa college DU
[4]Associate Professor, GIDC Rajju Shroff ROFEL Institute of Management Studies, RSRU
[5]Assistant Dean, Associate professor School of Commerce and Management, Arka Jain University, Jharkhand
[6]Associate Professor, Department of Management, Institute of Technology and Management Gwalior, Madhya Pradesh

Received: 29/09/2025
Revised: 15/10/2025
Accepted:28/10/2025
Published:25/11/2025

ABSTRACT

E-commerce practices are under a microscope due to increasing worries about data privacy and security, especially as personal data breaches become more common. These breaches, as many incidents have shown, do more than just cause financial losses; they really hurt consumer trust—something businesses need to stay afloat in e-commerce. Companies now rely heavily on personal data to improve user experiences and boost sales. However, data breaches have become a major factor influencing what shoppers do online. This study looks at how these breaches change how consumers trust e-commerce sites and how this, in turn, affects their privacy habits.

Keywords: data breaches, consumer trust, privacy protection behavior, e-commerce, data security.

INTRODUCTION:

In today's e-commerce world, protecting data is more important than ever, especially with the rise in data breaches(Ho et al., 2023). These breaches don't just expose personal info; they hurt consumer trust, which is key for e-commerce to work. Studies show that losing trust after a breach can last a long time, changing how consumers act, especially when it comes to privacy (Singh et al., 2024). When e-commerce sites first interact with customers, they promise confidentiality and security. If they break that promise, it raises concerns about transaction safety (Singh et al., 2024). So, businesses need to understand that privacy violations have consequences beyond legal issues; they affect how consumers see them, leading to less trust and fewer purchases (Aragon et al., 2025). Awareness of privacy protection is a big factor in consumer trust and behavior in e-commerce (Alkis & Köse, 2022). When people face potential security threats, they are often more careful about their data and the platforms they use. Marketing plays a role in raising this awareness by sharing the measures taken to protect customer data, which can restore trust (Bauman & Bachmann, 2017). This tricky balance between security and consumer behavior mirrors broader trends in the digital market, where transparency and proactive communication can build trust (Bauman & Bachmann, 2017). Trust here isn't just a result of transactions; it drives engagement and loyalty in e-commerce (Bauman & Bachmann, 2017). Understanding the connections between data breaches, consumer trust, and protective actions is important for both researchers and businesses.

Building on the ideas about consumer trust in e-commerce, we need to create a theoretical structure to study personal data breaches. The Unified Theory of Acceptance and Use of Technology (UTAUT) has changed to fit e-shopping situations, bringing in things like trust, how risky it feels, and what other people think(Singh et al., 2024). Each of these things is super important in shaping what consumers think about online deals. Usually, trust is seen as the thing everything else is built on, because it has a direct effect on whether consumers will share their personal info and use e-commerce sites. Studies have shown that when people trust more, they feel like there's less risk, which makes them more likely to shop online without worrying too much (Singh et al., 2024). On the flip side, how risky things seem includes worries about data breaches, losing privacy, and maybe losing money. These worries can make people not want to use e-commerce services (Otieno, 2025).

When we talk about "hedonic motivation," it simply means how much you enjoy the shopping experience itself. That enjoyment can sometimes balance out the risks you see with data breaches (Lam, 2023) For example, if you love shopping online and get a lot of kicks out of it, you might be more likely to brush off the risks that are there. Also, if the service is top-notch – like if customer service is quick to help and data protection is strong – it can grow trust and make you feel safer (Strzelecki & Rizun, 2022). Using a solid theoretical model based on UTAUT stuff helps us really get what's going on with consumers when data breaches happen.

This look isn't just about trust and risk; it also sees how important having fun and social stuff are. As e-commerce keeps changing, making a safe and trustworthy space will be key for fighting the bad stuff that comes with personal data breaches and boosting how consumers protect their own privacy (Khan & Mohamadali, 2023).

One major problem is that current data protection methods often can't keep up with today's cyber threats, which leaves many vulnerabilities open. A data breach doesn't just put sensitive consumer information at risk; it also weakens trust in e-commerce, creating a situation where people hesitate to share their personal information online (Morić et al., 2024). According to one analysis, companies that have data breaches see a notable drop in customer loyalty and trust. About 65% of customers affected say they'll likely stop doing business with the company after such an incident (Strzelecki & Rizun, 2022) . Moreover, if security measures seem weak, it can lead to negative reviews; around 85% of individuals share their bad experiences, making the reputational damage worse (Zhang et al., 2022). This damage is made even worse by how often these breaches happen. One report showed that the number of compromised accounts reached an all-time high, leading to more doubt about online transactions (Makridis, 2021).

E-commerce platforms also face regulatory hurdles that add complexity to their operations. Data protection algorithms can be quite complicated and may not always align with important legal frameworks, like GDPR and CCPA. Not following these regulations can mean significant financial penalties, which can make it tough for smaller companies to compete (Pathak, 2024). Furthermore, companies that don't prioritize strong data protection might become targets for malicious actors. A good example is the breach at ManpowerGroup, where the data of over 144,000 people was compromised, showing the possible consequences of weak security (Gbadebo et al., 2024). Plus, e-commerce businesses always struggle to prove to consumers that their security measures are effective. Concern over risk can keep potential customers away from online platforms. Studies show that perceived risk negatively impacts consumer trust, meaning even the possibility of a breach can greatly affect whether people decide to make a purchase (Singh et al., 2024).

Many organizations are starting to invest in cybersecurity, but there's still a gap in public awareness about personal data breaches and what they mean. Research suggests that 52% of consumers think security is crucial when deciding what to buy, yet only a few really understand the measures in place to protect their data (Hassan, 2025). This situation gives e-commerce platforms a chance to not only improve their security but also educate consumers about what they're doing to keep data safe and secure. we need a better handle on how personal data breaches affect consumer trust when it comes to online shopping. One big hole in what we know is a lack of in-depth studies looking at exactly how the seriousness and type of a data breach change how much consumers trust, and how this differs across different groups of people. There are studies on consumer reactions to breaches, but they often don't dig into how things like age, gender, and social status change those reactions (Mayer et al., 2023). This means we might be missing a lot of the story. Also, a lot of studies don't think about how different cultures see data privacy and trust. Some cultures are way more sensitive about this stuff. So, focusing only on, say, Western countries means missing out on what's happening in places like Asia or Africa, where online shopping is blowing up (Zimu, 2023). Even though we know protecting personal data is important, there aren't many studies that follow consumers over time to see how their behavior changes after a breach. Most research looks at the immediate aftermath, but what about the long-term effects? Consumers might change how they protect their privacy way after the fact (Blascak & Toh, 2022; Ho et al., 2023; Turjeman & Feinberg, 2023).

Another issue? We need more studies that pull together ideas from psychology, marketing, and cybersecurity. This would give us a fuller picture of consumer trust and privacy protection. Sure, we've got insights from each of these fields, but we need frameworks that mix them all together. This would help us understand the tricky relationships between consumer trust, data protection, and whether people actually buy stuff online(Otieno, 2025). Right now, most frameworks stick to one field, which means we might miss the bigger picture of what drives consumer trust in online shopping. Also, we haven't really looked into how new tech like AI and blockchain changes how consumers feel about data security and trust. Lastly, studies tend to focus on numbers, but we're missing out on hearing from consumers themselves about their experiences with data breaches. Getting stories from consumers could give us really rich, detailed info that numbers alone can't. This would shed light on the personal side of trust and privacy (Strzelecki & Rizun, 2022). By filling these gaps, future research can help us better understand consumer trust in online shopping. It can also help businesses figure out how to protect consumer data and win back trust after a breach. Addressing these many different issues will not only improve our understanding of the topic but also help create real solutions that protect consumers in the ever-growing online marketplace (Pattnaik et al., 2022). While there's much research on data breaches, a specific area needing more attention involves how these breaches directly affect consumer trust in e-commerce. The novelty of this study is in its holistic view of how consumers' beliefs about data security impact their buying habits and platform engagement. This study is combination of trust-related ideas, and current risk perceptions.

By bringing together data from various parts of the e-commerce world, this research highlights the significant impact that data breaches have on shaping what consumers think and do. A key point is that there's a strong connection between trust and keeping customers, as data breaches can seriously damage the credibility of e-commerce platforms, leading to a notable increase in

negative feelings among consumers after such events (Lukito & Ikhsan, 2020). Therefore, this study gives e-commerce businesses practical advice, stressing the need for strong data protection plans and open communication to ease consumer worries about data security breaches. The trend analysis shows that consumer trust levels change in response to major breaches , so businesses should prioritize investing in IT to boost consumer confidence and strengthen privacy protection measures. This research also connects the impact of data breaches to broader social trends related to being aware of privacy and having trust in the digital world. Given that past research suggests consumers are more likely to rethink their relationships with brands that have experienced breaches, the message for businesses is clear: building trust needs to be a constant effort to prevent losing customers due to data incidents.

The insights from this research have the potential to spark major changes in the e-commerce sector. By emphasizing the need for measures that build trust and effective communication plans, organizations can lessen the negative effects of data breaches. By doing so, they not only protect their customer base but also position themselves well in the fast-changing digital marketplace, where data security and consumer trust are more important than ever. Ultimately, this study strengthens the call for solid practices in privacy protection and trust management, reflecting a crucial moment for businesses navigating the complex relationship between technology, consumer behavior, and regulations.

Objective of the study

The aim of this study is to shed light on the relationship between data breaches and how consumers view privacy and security. Largely, the main goal involves figuring out how personal data breaches change consumer trust in e-commerce companies. Another crucial goal is to analyze the specific privacy protection behaviors that consumers adopt after a breach, looking closely at changes in their online shopping habits and how they share personal data.

2. LITERATURE REVIEW

Considering the rise of data breaches in e-commerce, research shows it affects how much consumers trust companies and if they protect their privacy. Many studies emphasize how important consumer opinion is when reacting to these breaches (Hydari et al., 2024; Singh et al., 2024). For example, data breach victims often lose trust in the affected company; stats say around 65% feel this way (Hydari et al., 2024). This lack of trust worsens because 85% of consumers share bad experiences about data security, hurting a company's reputation (Masuch et al., 2021). Looking at psychological ideas like the Social Exchange Theory, you see that concerns about personal data use directly change what consumers think and do on e-commerce sites.

Also, the protection of personal data in e-commerce has become a hot topic academically and in practice. Rules like GDPR and CCPA have changed how companies handle and talk about data protection(Bettini et al., 2020). There's ongoing discussion about whether these rules really help rebuild consumer trust after breaches. Some studies suggest that while following the rules shows accountability, it doesn't completely fix lost trust(Miltgen & Smith, 2018). This points to the complex job of trust restoration; companies need solid security and clear communication to reassure consumers that their info is safe (Knight & Nurse, 2020).

Looking at recent findings, security features are becoming more important for consumer behavior in e-commerce. Visible security steps, like encryption and user authentication, act as reassurance and can improve a consumer's view of the brand, influencing their willingness to use e-commerce sites (Ologunebi & Taiwo, 2023). Plus, enjoying a service (hedonic value) and needing privacy are connected; companies need to carefully manage both (Ologunebi & Taiwo, 2023).

Basically, understanding the research on data breaches, consumer trust, and privacy protection reveals the complex relationship between these things in e-commerce. The common themes across studies emphasize that companies need strong security and a consumer-focused approach that values transparency, communication, and proactive action against data threats. These actions aren't just for following rules; they're also crucial for building long-term consumer relationships and staying competitive in a market that increasingly cares about privacy (Beke et al., 2021).

2.1 The Evolving Landscape of E-commerce and Data

E-commerce keeps changing, driven by new tech and what shoppers want, so how data is kept safe and how much people trust online stores are now linked even more closely. Since we're using online shopping more, it's super important that companies manage data well to keep customer info safe, which helps build trust (Sachdev & Sauber, 2023). But, data breaches happen way too often and are a big deal, which can break that trust, making shoppers think twice about buying online. Just to give you an idea, back in 2021, over 500 million records were exposed in data breaches (Singh et al., 2024). Because of stuff like this, people worry more about their personal info staying safe when they shop online. Companies get hurt when breaches happen, but it also makes everyone trust online stores less in general. Actually, research shows that lots of shoppers are less likely to buy online after a data breach, with maybe up to 80% saying they might not use a site if they don't think their data is safe (Zou et al., 2022). Because people are so concerned about their privacy, e-commerce businesses are changing how they handle security, like focusing on being open about what they do and trying to stop problems before they start, all to get shoppers to trust them again (Duarte et al., 2024).

2.2 Personal Data Breaches

Personal data breaches usually involve unauthorized access to sensitive personal information without

permission, potentially causing significant harm to individuals' financial stability and social standing (Hydari et al., 2024). The variety of personal data involved can include details like social security numbers, financial account information, passwords, and even health records. The increasing digitization of e-commerce interactions has led to a dramatic rise in the scale and frequency of personal data breaches, illustrating a key weakness in our information security systems (Weigl et al., 2023).

These breaches can occur through various means, such as hacking, phishing, or accidental disclosures, and they aren't just external threats; insiders can also cause breaches. Breaches might also occur through third-party vendors who manage data for businesses, emphasizing the need for careful vendor selection and management (Arroyabe et al., 2024). Often, when consumers find out their personal information has been exposed, they immediately distrust the responsible entities. Studies suggest that this lost trust can reduce consumer engagement and willingness to share personal information, hindering e-commerce growth (Singh et al., 2024).

2.3 Consumer Trust in Digital Environments

Consumer trust in digital spaces is super important, especially when you think about how data breaches mess with online shopping. It's all tied to whether people trust the website, ya know? When you're buying stuff online, you don't get to see things in person, so you really gotta trust that the site is safe and legit (Pham et al., 2020). And when there's a big data breach? People remember that, and it makes them way less likely to trust a site with their info (Ha et al., 2019). Basically, if consumer think their info is at risk, they're not gonna shop online as much or share their personal details.

Also, people really care about whether companies are doing a good job keeping their data safe. If they think a company's got their back, they're more likely to stick with them and buy from them again. But if they think a company's data security is weak, they might just head over to a competitor who seems more serious about protecting their info (Khoa & Huỳnh, 2022). Don't forget about how your friends and other people influence your decisions! If everyone's talking about how they don't trust a certain e-commerce site after a breach, that feeling can spread, and suddenly, a lot of people are skeptical about online shopping (Li et al., 2019). This can turn into a bad cycle where companies lose sales and can't afford to invest in better security, making the problem even worse (Liu et al., 2022).

For e-commerce to work, it's key to grasp the theories behind how people protect their privacy. That's how we can really look at how data breaches mess with consumer trust and the steps people take to stay safe (Cornière & Taylor, 2024). We can use different ideas from psychology and sociology to explain what's going on with privacy worries. This helps us understand both what customers do and how companies react to breaches.

2.4. Theories of Privacy Protection Behavior

The Privacy Calculus Theory basically says people weigh the good and bad before sharing info online. They think about things like getting personalized stuff or deals, but also the risk of identity theft (Tudoran, 2024). Then there's the Theory of Planned Behavior. It explains how our attitudes and what others think affect what we do about privacy. If you've had bad experiences with privacy before, you're probably going to be more careful and not trust e-commerce sites as much (Acquisti et al., 2020).

The Social Exchange Theory also matters. It says e-commerce should be fair for everyone. Breaches mess that up, and people lose trust and might not shop there again (Zou et al., 2022). But research does show that if companies are serious about privacy and handle breaches well, customers are more likely to stick around (Hydari et al., 2024). It's all about trust going both ways.

There's also the Privacy Paradox to think about. People say they care about privacy, but they don't always do things to protect it. For example, they might not read privacy policies(Ehrari et al., 2020). This can be an issue because companies might not bother improving privacy if they think customers don't really care that much.

All these theories show that understanding privacy is really complicated and tied to trust. It's about psychology, age, and what people think is fair. How people react to data breaches isn't just about what's happening right now, but also their history and what society expects (Ehrari et al., 2020). And to that point, there's even an infographic that details what happens when data breaches erode trust in companies -- it shows what happens to consumers too! As companies try to make their way through this digital world, they have to use these theories to manage privacy well. If they match what they do with what customers expect, they can build trust and stop data breaches from hurting their business (Draper et al., 2024).

3. METHODOLOGY

To really dig into what data breaches mean for how consumers trust e-commerce and what they do to protect themselves, a online survey of a good mix of online shoppers who've been hit by data breaches was conducted. The survey used a set of questions to put numbers to things like how risky they feel things are, how much they trust, and what they do to stay safe. These surveys help researchers collect information about people's attitudes towards data security, showing how breaches affect their trust in online shopping and if they're willing to keep using e-commerce sites. The existing scales were used to measure trust and privacy worries, making sure our measurements are solid. The descriptive statistics, was used to find connections between breaches and trust, and how these things change consumer behavior. This approach is in line with what you see in the literature

It's really important to have a carefully planned way to choose who participates and how we gather information

from them. The research involved a diverse group of people that represents the larger world of e-commerce consumers. We decided to include people with varying experience in e-commerce because we know that reactions to data breaches might be quite different between those who are new to online shopping and those who are more experienced. For example, people who often shop online might have different levels of trust compared to those who only do it sometimes. So, we need a wide range of participants to effectively capture these differences.

4. DATA ANALYSIS AND RESULTS

The results from this data analysis both highlights the immediate impact of personal data breaches, and clarify wider implications for privacy protection behavior in e-commerce too. The finding is that data breaches and consumer trust have a cyclic relationship. Eroded trust leads not only to diminished consumer engagement but also a more notable demand for tougher privacy protections in digital commerce.

The analysis highlights the wide-ranging effects of data breaches on how much consumers trust e-commerce and how they then act to protect their privacy. It's quite clear that trust takes a serious hit after a breach. A significant portion, around 65% according to the infographic detailing breach repercussions , say they trust the company less. This drop is directly linked to consumers being more careful about their privacy. Studies suggest people start using stronger privacy measures after a breach, often looking at how secure other platforms seem (Hydari et al., 2024). For instance, a hefty 80% said they'd ditch a vendor after a breach, showing how vital data security is for keeping customers (Özer et al., 2023). It also seems this distrust leads to people wanting more transparency in how their data is used, with many actively seeking out detailed privacy policies before buying anything online(Rizvanović et al., 2022).

4.1 Impact of Data Breaches on Consumer Trust

Figure 1: Impact of data breaches on Consumer Trust

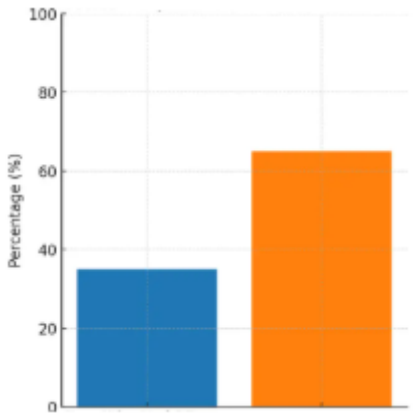

Figure 2: Consumer experience with data breaches

The figure 1 bar chart shows the percentages of consumers affected by data breaches, those who would stop shopping with a breached brand, those who find breached brands untrustworthy, and those who have taken protective actions against cyber incidents. The figure 2 bar chart highlights the consumer experience, showing that 35% have experienced a data breach while 65% have not.

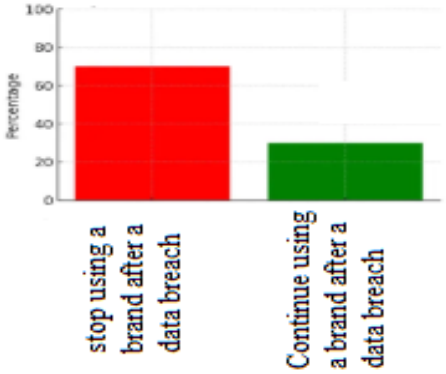

Figure 3: Impact of data beach on brand use

The figure 3 displays the impact of data breaches on consumer behavior. It reveals that 70% of consumers would stop using a brand after a data breach, while only 30% would continue. These findings emphasize the need for tailored strategies focused on enhancing consumer awareness and security perception, elements crucial to fortifying trust in the digital space

4.2 Factors Influencing Privacy Protection Behavior

Many factors influence privacy protection behavior, highlighting the complexity of consumer interactions in e-commerce, especially after data breaches. Increased awareness, social influences, perceived security, and demographic variations shape consumer attitudes and behaviors. Understanding this interplay provides insights for e-commerce platforms aiming to cultivate consumer trust and promote data protection, establishing a more sustainable and secure online retail environment.

Consumer reactions to data breaches aren't simple; they hinge on a few things. How responsible does the organization seem? How bad was the breach, really? And how well did they communicate about it? Studies suggest trust gets re-evaluated based on how open the company seems to be in its response. You see, firms that handle communication well during these crises usually suffer less damage to their reputation. For example, the data shows a whopping 65% of consumers lose trust after a breach. This really drives home the point about preventative steps, and, of course, how important clear communication is after it happens. Also, business process modeling offers some insights, perhaps. Adding strong security measures early on could lower the risks from data breaches, as noted in (Assen et al., 2024). So, if you want to rebuild trust, and succeed in the long run, you have to engage proactively and really focus on what consumers need.

Table 1: Factors influencing privacy protection behaviour

Factor	Description
Emotional Response	Consumers' emotional reactions, such as fear or anger, significantly influence their responses to data breaches. Fearful consumers are more sensitive to the size and scope of a breach, while angry consumers focus on the perpetrators. This distinction affects their subsequent actions and perceptions.
Type of Data Compromised	The nature of the compromised data plays a crucial role in consumer reactions. Breaches involving sensitive personal information, like Social Security numbers, are more likely to lead to identity theft and cause greater consumer distress.
Public Disclosure of Vulnerabilities	Increased public disclosure of vulnerabilities is associated with a higher frequency of data breaches. This transparency can lead to heightened consumer concern and erode trust in organizations' data security practices.
Consumer Perception Capabilities	Consumers' ability to perceive and understand online security risks influences their reactions. Those with weaker perception capabilities may not recognize potential risks, leading to inadequate protective measures and increased vulnerability.
Trust in Government Information	High trust in government information can enhance the positive effect of benefit perception on consumer behavior, making consumers more likely to engage in protective actions following a data breach.

4.3 Relationship between Trust and Behavior

The relationship between trust and consumer behavior, especially when it comes to personal data breaches, works in a cycle. Trust can lead to engagement, while breaches can lead to more protective actions. Plainly, trust isn't just key for keeping consumers loyal; it's also a crucial factor that affects protective behaviors in e-commerce (Higueras-Castillo et al., 2023). As organizations deal with tricky consumer expectations and evolving digital threats, it'll be vital to

acknowledge the importance of rebuilding trust after a breach and adapting to the resulting behavioral changes to keep consumer relationships strong and create a safe online shopping space. This cycle of trust and behavior, where consumers react to data security, highlights the need for constantly improving privacy protection. As a result, improving trust not only makes marketing more successful but also boosts consumer privacy and data security in e-commerce (Pham et al., 2020). Comprehending this trust-behavior connection in e-commerce gives businesses vital insights for thriving in a world where data vulnerabilities and consumer skepticism are growing.

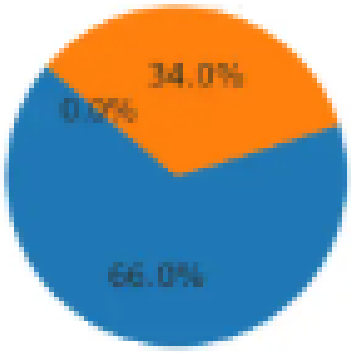

Figure 4: Trust levels after data breach

The pie chart in figure 4 emphasizes the majority of consumers, at 66%, who would not trust a company after a data breach, stressing the critical need for companies to maintain consumer trust.

4.4 DISCUSSION

It is clear that data breaches cause issues beyond just immediate money losses. They really affect how much consumers trust companies and how they act to protect their own privacy. A big thing to note is that trust goes down after a breach. Studies show about 65% of people who were affected don't trust the company as much anymore. This lack of trust, they say, changes what they buy and how they deal with that brand (Bada & Nurse, 2019). Also, around 80% of consumers might stop using a business after a breach, which shows it hurts loyalty in e-commerce (Cappellozza et al., 2021). Plus, it's super important for consumers to understand what a company is doing to protect their data. If companies don't explain their security plans well, people get worried and might switch to safer options.

The psychological side of consumer trust leads to how privacy worries change their behavior. The insights from the path model show how trust and risk work together to shape what users do. Trust is a really big deal for e-commerce success. Companies that really work on protecting data not only keep consumer info safe but also build the trust that keeps customers coming back. if companies are really clear about how they use data, people will see less risk in privacy breaches, which makes them more confident and willing to buy things online (Zou et al., 2022).

Ultimately, data breaches cause problems for companies right away, but the lasting effects on consumer trust and privacy habits are huge. By dealing with trust issues, raising awareness, and putting strong security in place, we can create a more secure consumer world. As companies try to make it in the digital market, they need to remember how deeply data breaches affect people. This can help them not only keep customers loyal but also stand out by being more trustworthy in the digital age. For sure, data security and consumer trust will keep changing, so we need to be ready to put consumer confidence first for e-commerce businesses to last and grow (Ahi et al., 2022).

5. IMPLICATIONS FOR E-COMMERCE PLATFORMS

The effects of personal data breaches go way beyond just losing money. They really hit consumer trust hard and change how people act to protect themselves when using e-commerce sites. It's super important for these sites to get what these breaches do and work to fix them. That way, they can keep good relationships with their customers and stay in business for the long haul. As online shopping changes, shoppers care more and more about companies that have strong privacy measures in place. So, e-commerce sites need to keep up by having really good data security plans. Using things like strong encryption and being open about how they use data can help people feel safer and maybe win back their trust after a breach (Liu et al., 2022). Also, giving customers easy ways to ask questions and share their worries about their data—like having customer service just for that—can make them think the service is better, which is key when dealing with a crisis (Knight & Nurse, 2020).

Using cool tech like artificial intelligence and machine learning can also help find possible security problems before breaches even happen. This kind of proactive move can seriously boost consumer trust because it shows you're serious about keeping their info safe (Kareem, 2024). Plus, when a data breach does happen, being clear and honest about it—telling everyone what happened and what you're doing to fix it—can lessen the damage to trust and keep your reputation from taking too big of a hit (Masuch et al., 2021). Managing public relations well during these times is crucial. Research says that talking to people quickly and clearly can stop

bad word-of-mouth from spreading, which really affects how people feel about the companies involved (Kuoppakangas et al., 2023).

6. LIMITATIONS OF THE STUDY

Research has shown self-reporting can be a bit off, as people tend to answer how they think they should rather than how they actually feel or act (Overton et al., 2021). Also, the survey only looked at a certain group, mainly younger, tech-savvy adults. That means what we found might not apply to everyone, especially older folks or those who don't use e-commerce as much. Focusing on just one data breach might miss the bigger picture, since people's reactions can change if they've dealt with multiple breaches or just feel generally unsafe online, as previous studies have pointed out.

Also, cultural factors like how people view privacy and security weren't really looked at, even though they can change how people react to breaches in different places. For example, studies indicate culture has a big impact on how people understand privacy rules and respond to breaches (Mersinas et al., 2024). And since tech is always changing, what we found might not stay relevant for long as e-commerce and cyber threats evolve. As consumer trust doesn't just react to breaches but is also influenced by ongoing changes in the digital world and new ways to protect data.

7. CONCLUSION

Drawing together the threads of this investigation into data breaches and their effects on consumer trust and privacy behaviors in e-commerce, we arrive at a complex conclusion. It highlights the need for strong security and increased consumer knowledge. As this research shows, data breaches deeply affect how consumers feel, often significantly hurting their trust in e-commerce platforms. When companies don't protect personal data well, consumers feel less secure, leading them to rethink their use of online services(Liu et al., 2022). This drop in trust shows up in various ways, most notably in a hesitance to share personal details, which then affects their willingness to shop online. This could potentially slow down e-commerce growth. Statistics on data breaches, for example, the growing number of people and records affected in recent years, also show how common these issues are (Liu et al., 2022). Such data complicates things for consumers, making them more careful and prompting them to demand better security from e-commerce sites.

Ultimately, the connection between data breaches, consumer trust, and privacy protection in e-commerce is intricate and multifaceted. The discussed findings point to the importance of keeping high data protection standards and ensuring clear communication between businesses and their customers. As e-commerce continues to change and grow, the effects of data breaches will likely remain a key issue. Further research is needed to understand their impact better and to create effective ways to lessen negative outcomes. It's evident that companies should invest in tech to fight breaches and include consumers in talks about data privacy to rebuild and keep trust. So, the duty falls on both consumers and businesses to foster an environment where trust can thrive. This balances innovation with protecting personal data, ensuring lasting growth and confidence in e-commerce. Such insights offer helpful direction for future research. This future research should focus on finding new solutions and adapting to how consumer behavior changes in response to data privacy concerns.

8. RECOMMENDATIONS FOR FUTURE RESEARCH

Considering the ongoing discussions about consumer trust and how people try to protect their privacy when personal data is compromised, it's important to map out some areas for future research. These studies could help us better understand what's happening in e-commerce. One key area is longitudinal studies. These would help us see the long-term effects of data breaches on how much consumers trust companies and how their behavior changes. We could learn how quickly trust drops after a breach and how long it takes to recover after a company takes steps to fix the problem. Existing research shows that using different demographic information can highlight different ways people react to breaches, so companies can create more specific privacy strategies(Zou et al., 2024). Also, comparing companies that have successfully rebuilt trust with those that haven't could help us understand the best ways to handle a crisis and keep consumers engaged.

Qualitative research is also necessary to really understand how consumers feel about data privacy and why they do what they do to protect it. Through interviews and focus groups, researchers could gather more detailed information about the emotional and psychological impact of data breaches (Acquisti et al., 2020). This type of research adds to the quantitative data and could help us create better models for predicting privacy behaviors in e-commerce. Additionally, we need to look at how new technologies like blockchain and AI can improve data protection. If consumers trust these technologies—and if they actually prevent data breaches—companies could find new ways to ensure privacy and increase user confidence in e-commerce platforms.

REFERENCE

1. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. Journal of Consumer Psychology, 30(4), 736. https://doi.org/10.1002/jcpy.1191
2. Ahi, A., Sinkovics, N., & Sinkovics, R. R. (2022). E-commerce Policy and the Global Economy: A Path to More Inclusive Development? Management International Review, 63(1), 27. https://doi.org/10.1007/s11575-022-00490-1

3. Alkis, A., & Köse, T. (2022). Privacy concerns in consumer E-commerce activities and response to social media advertising: Empirical evidence from Europe. Computers in Human Behavior, 137, 107412. https://doi.org/10.1016/j.chb.2022.107412
4. Aragon, K. A. P., Cabudoc, M. A. L., Remolin, A. B., & Zamora, Z. M. D. (2025). Analyzing the Impact of Privacy Concerns on Consumer Behavior. International Journal of Research and Innovation in Social Science, 920. https://doi.org/10.47772/ijriss.2024.8120077
5. Arroyabe, M. F., Arranz, C. F. A., Arroyabe, I. F. D., & Arróyabe, J. C. F. de. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. Technology in Society, 78, 102670. https://doi.org/10.1016/j.techsoc.2024.102670
6. Assen, J. von der, Hochuli, J., Grübl, T., & Stiller, B. (2024). The Danger Within: Insider Threat Modeling Using Business Process Models. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2406.01135
7. Bada, M., & Nurse, J. R. C. (2019). The social and psychological impact of cyberattacks. In Elsevier eBooks (p. 73). Elsevier BV. https://doi.org/10.1016/b978-0-12-816203-3.00004-6
8. Bauman, A., & Bachmann, R. (2017). Online Consumer Trust: Trends in Research. Journal of Technology Management & Innovation, 12(2), 68. https://doi.org/10.4067/s0718-27242017000200008
9. Beke, F. T., Eggers, F., Verhoef, P. C., & Wieringa, J. E. (2021). Consumers' privacy calculus: The PRICAL index development and validation. International Journal of Research in Marketing, 39(1), 20. https://doi.org/10.1016/j.ijresmar.2021.05.005
10. Bettini, C., Kanhere, S. S., Langheinrich, M., Misra, A., & Reinhardt, D. (2020). Is Privacy Regulation Slowing Down Research on Pervasive Computing? Computer, 53(6), 44. https://doi.org/10.1109/mc.2020.2968013
11. Blascak, N., & Toh, Y. L. (2022). Prior Fraud Exposure and Precautionary Credit Market Behavior. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4292240
12. Cappellozza, A., Moraes, G. H. S. M. de, Perez, G., & Simões, A. (2021). Antecedent factors of violation of information security rules. RAUSP Management Journal, 57(1), 85. https://doi.org/10.1108/rausp-02-2021-0022
13. Cornière, A. de, & Taylor, G. (2024). A Model of Information Security and Competition. Marketing Science. https://doi.org/10.1287/mksc.2023.0513
14. Draper, N. A., Hoffmann, C. P., Lutz, C., Ranzini, G., & Turow, J. (2024). Privacy resignation, apathy, and cynicism: Introduction to a special theme. Big Data & Society, 11(3). https://doi.org/10.1177/20539517241270663
15. Duarte, C. de A. L., Messias, I., & Oliveira, A. (2024). Technological Acceptance of E-Commerce by Generation Z in Portugal. Information, 15(7), 383. https://doi.org/10.3390/info15070383
16. Ehrari, H., Ulrich, F., & Andersen, H. B. (2020). Concerns and Trade-Offs in Information Technology Acceptance: The Balance between the Requirement for Privacy and the Desire for Safety. Communications of the Association for Information Systems, 47(1), 227. https://doi.org/10.17705/1cais.04711
17. Gbadebo, M. O., Salako, A. O., Selesi-Aina, O., Ogungbemi, O. S., Olateju, O. O., & Olaniyi, O. O. (2024). Augmenting Data Privacy Protocols and Enacting Regulatory Frameworks for Cryptocurrencies via Advanced Blockchain Methodologies and Artificial Intelligence. Journal of Engineering Research and Reports, 26(11), 7. https://doi.org/10.9734/jerr/2024/v26i111311
18. Ha, N. T., Nguyen, T. L. H., Nguyễn, T. P. L., & Nguye, T. D. (2019). The effect of trust on consumers' online purchase intention: An integration of TAM and TPB. Management Science Letters, 1451. https://doi.org/10.5267/j.msl.2019.5.006
19. Hassan, S. S. (2025). The Role of Prior Cybersecurity Knowledge in Promoting Safe Online Practices: A Study from Somaliland. Research Square (Research Square). https://doi.org/10.21203/rs.3.rs-7502598/v1
20. Higueras-Castillo, E., Alves, H., Liébana-Cabanillas, F., & Ramos, Á. F. V. (2023). The consumer intention to use e-commerce applications in the post-pandemic era: a predictive approach study using a CHAID tree-based algorithm. European Journal of Management and Business Economics. https://doi.org/10.1108/ejmbe-12-2022-0375

21. Ho, F. N., Ho-Dac, N. N., & Huang, J. S. (2023). The Effects of Privacy and Data Breaches on Consumers' Online Self-Disclosure, Protection Behavior, and Message Valence. SAGE Open, 13(3). https://doi.org/10.1177/21582440231181395
22. Hydari, M. Z., Liang, Y., & Telang, R. (2024). Sound and Fury, Signifying Nothing? Impact of Data Breach Disclosure Laws. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2406.15215
23. Kareem, K. M. (2024). The Intelligence Technology and Big Eye Secrets: Navigating the Complex World of Cybersecurity and Espionage. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4880998
24. Khan, I., & Mohamadali, N. A. B. (2023). Understanding the Role of Customer Trust in E-Commerce. International Journal of Computer Science and Information Technology, 15(4), 89. https://doi.org/10.5121/ijcsit.2023.15407
25. Khoa, B. T., & Huỳnh, T. T. (2022). How do customer anxiety levels impact relationship marketing in electronic commerce? Cogent Business & Management, 9(1). https://doi.org/10.1080/23311975.2022.2136928
26. Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. Computers & Security, 99, 102036. https://doi.org/10.1016/j.cose.2020.102036
27. Kuoppakangas, P., Hagman, S., Stenvall, J., & Kinder, T. (2023). Social Learning and Reputation Management in an Espionage Crisis. Corporate Reputation Review. https://doi.org/10.1057/s41299-023-00171-1
28. Lam, T. N. (2023). Key Factors Shaping Customers' Satisfaction and Reuse Intentions: An Extensive Systematic Review. TEM Journal, 2123. https://doi.org/10.18421/tem124-23
29. Li, S., Song, X., Lu, H., Linyi, Z., Shi, M., & Liu, F. (2019). Friend recommendation for cross marketing in online brand community based on intelligent attention allocation link prediction algorithm. Expert Systems with Applications, 139, 112839. https://doi.org/10.1016/j.eswa.2019.112839
30. Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce [Review of Cyber security threats: A never-ending challenge for e-commerce]. Frontiers in Psychology, 13. Frontiers Media. https://doi.org/10.3389/fpsyg.2022.927398
31. Lukito, S., & Ikhsan, R. B. (2020). Repurchase intention in e-commerce merchants: Practical evidence from college students. Management Science Letters, 3089. https://doi.org/10.5267/j.msl.2020.5.014
32. Makridis, C. (2021). Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. Journal of Cybersecurity, 7(1). https://doi.org/10.1093/cybsec/tyab021
33. Masuch, K., Greve, M., & Trang, S. (2021). What to do after a data breach? Examining apology and compensation as response strategies for health service providers. Electronic Markets, 31(4), 829. https://doi.org/10.1007/s12525-021-00490-3
34. Mayer, P., Zou, Y., Lowens, B., Dyer, H. A., Le, K., Schaub, F., & Aviv, A. J. (2023). Awareness, Intention, (In)Action: Individuals' Reactions to Data Breaches. ACM Transactions on Computer-Human Interaction, 30(5), 1. https://doi.org/10.1145/3589958
35. Mersinas, K., Bada, M., & Furnell, S. (2024). Cybersecurity Behavior Change: A conceptualization of Ethical Principles for Behavioral Interventions. Computers & Security, 148, 104025. https://doi.org/10.1016/j.cose.2024.104025
36. Miltgen, C. L., & Smith, H. J. (2018). Falsifying and withholding: exploring individuals' contextual privacy-related decision-making. Information & Management, 56(5), 696. https://doi.org/10.1016/j.im.2018.11.004
37. Morić, Z., Dakić, V., Djekic, D., & Regvart, D. (2024). Protection of Personal Data in the Context of E-Commerce. Journal of Cybersecurity and Privacy, 4(3), 731. https://doi.org/10.3390/jcp4030034
38. Ologunebi, J., & Taiwo, E. O. (2023). The Importance of SEO and SEM in improving brand visibility in E-commerce industry; A study of Decathlon, Amazon and ASOS. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4638890
39. Otieno, E. A. (2025). Data protection and privacy in e-commerce environment:

Systematic review. GSC Advanced Research and Reviews, 22(1), 238. https://doi.org/10.30574/gscarr.2025.22.1.0024

40. Overton, H., Kim, J. K., Zhang, N., & Huang, S. (2021). Examining consumer attitudes toward CSR and CSA messages. Public Relations Review, 47(4), 102095. https://doi.org/10.1016/j.pubrev.2021.102095
41. Özer, M., Köse, Y., Bastug, M. F., & Kucukkaya, G. (2023). The Shifting Landscape of Cybersecurity: The Impact of Remote Work and COVID-19 on Data Breach Trends. Research Square (Research Square). https://doi.org/10.21203/rs.3.rs-3630534/v1
42. Pathak, M. (2024). Smart Compliance: Smart Contracts for Financial Regulatory Compliance. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4715505
43. Pattnaik, N., Li, S., & Nurse, J. R. C. (2022). Perspectives of non-expert users on cyber security and privacy: An analysis of online discussions on twitter. Computers & Security, 125, 103008. https://doi.org/10.1016/j.cose.2022.103008
44. Pham, C. H., Vu, N. H., & Tran, G. T. H. (2020). The role of e-learning service quality and e-trust on e-loyalty. Management Science Letters, 2741. https://doi.org/10.5267/j.msl.2020.4.036
45. Rizvanović, B., Zutshi, A., Grilo, A., & Nodehi, T. (2022). Linking the potentials of extended digital marketing impact and start-up growth: Developing a macro-dynamic framework of start-up growth drivers supported by digital marketing. Technological Forecasting and Social Change, 186, 122128. https://doi.org/10.1016/j.techfore.2022.122128
46. Sachdev, H. J., & Sauber, M. H. (2023). Employee–customer identification: Effect on Chinese online shopping experience, trust, and loyalty. Cogent Business & Management, 10(3). https://doi.org/10.1080/23311975.2023.2275369
47. Singh, N., Misra, R., Quan, W., Radić, A., Lee, S.-M., & Han, H. (2024). An analysis of consumer's trusting beliefs towards the use of e-commerce platforms. Humanities and Social Sciences Communications, 11(1). https://doi.org/10.1057/s41599-024-03395-6
48. Strzelecki, A., & Rizun, M. (2022). Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping. Sustainability, 14(10), 5866. https://doi.org/10.3390/su14105866
49. Tudoran, A. A. (2024). Rethinking privacy in the Internet of Things: a comprehensive review of consumer studies and theories [Review of Rethinking privacy in the Internet of Things: a comprehensive review of consumer studies and theories]. Internet Research, 35(2), 514. Emerald Publishing Limited. https://doi.org/10.1108/intr-01-2023-0029
50. Turjeman, D., & Feinberg, F. M. (2023). When the Data Are Out: Measuring Behavioral Changes Following a Data Breach. Marketing Science, 43(2), 440. https://doi.org/10.1287/mksc.2019.0208
51. Weigl, L., Barbereau, T., & Fridgen, G. (2023). The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions. Government Information Quarterly, 40(4), 101873. https://doi.org/10.1016/j.giq.2023.101873
52. Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D. P., & Ghorbani, A. A. (2022). Data breach: analysis, countermeasures and challenges. International Journal of Information and Computer Security, 19, 402. https://doi.org/10.1504/ijics.2022.127169
53. Zimu, F. (2023). Exploring the Impact of Cultural Factors on Consumer Behavior in E-Commerce: A Cross-Cultural Analysis. Journal of Digitainability Realism & Mastery (DREAM), 2(3), 31. https://doi.org/10.56982/dream.v2i03.90
54. Zou, H., Qureshi, I., Fang, Y., Sun, H., Lim, K. H., Ramsey, E., & McCole, P. (2022). Investigating the nonlinear and conditional effects of trust—The new role of institutional contexts in online repurchase. Information Systems Journal, 33(3), 486. https://doi.org/10.1111/isj.12410
55. Zou, Y., Le, K., Mayer, P., Acquisti, A., Aviv, A. J., & Schaub, F. (2024). Nudging Users to Change Breached Passwords Using the Protection Motivation Theory. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2405.15308