Data Security Concerns and Consumers' Trust in Online Business

Bilquis Ferdousi
School of Information Security and Applied Computing
Eastern Michigan University
Ypsilanti, MI 48197, USA
bferdous@emich.edu

Abstract

As online business is exploding in COVID pandemic world, the purpose of this research was to gain a deeper understanding of consumers' concerns of data security that affect their decision in online business practices. Research shows that data security concerns play a vital role in potential consumers' purchasing decision in online business. The study was based on extensive review of existing literature that focused on the need for consumers' increased information security measures and the importance of consumers' sustaining trust in online business.

Introduction

Technology is increasing at a faster pace than anything else in the world today, and because of that the traditional brick and mortar businesses are shifting the way they market toward their consumers, sell their goods and services online. In recent COVID pandemic world online business and services became essential, in some instances it's no more choice or option. The early evidence suggests the shift to online business is accelerating, consumers are buying more products in online. A number of small businesses, even if they are squarely situated in the brick and mortar business, are starting the online channel as a source of resilience in their business. Online business is one of those obvious industries that have attracted more venture capital during the pandemic. In COVID pandemic world the volatile economy may relies heavily on the online business and services.

In May 2020, The Census Bureau of the Department of Commerce announced that the estimate of U.S. retail e-commerce or online sales for the first quarter of 2020 was $160.3 billion, an increase of 2.4%from the fourth quarter of 2019. The first quarter of 2020 online estimate increased 14.8 from the first quarter of 2019. Online sales in the first quarter of 2020 accounted for 11.8% of total sales.

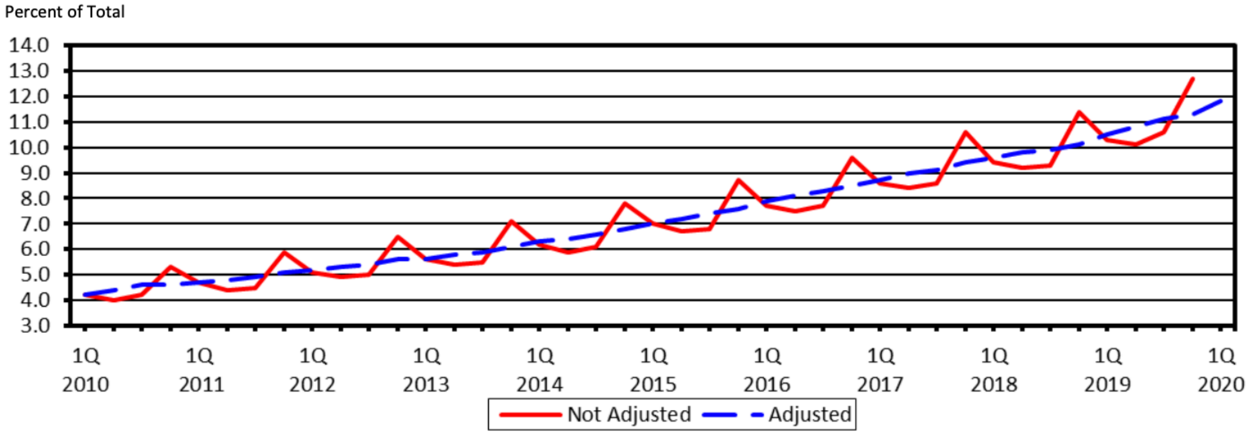

Figure 1: Estimated quarterly U.S. retail online sales as a percent of total quarterly retail sales: 1st quarter 2010 – 1st quarter 2020. Source: United States Census Bureau, U.S. Department of Commerce (2020).

Data Security Issue in Online Business

However, people are still concerned of how their personal and financial information or data is being used, shared, protected and secured in online business practices. There is always concern about online data security that significantly impact consumers on their development of trust in online business, which in turn, affects their decision to practice online businesses and services. Even though online business can be incredibly convenient and productive when utilized successfully, but there is a risk of data security. Research suggest that data security is one of the biggest barriers to online business (Limbu, Wolf, & Lunsford, 2011). Recent studies concluded that the primary factor hampering the success and further growth of online business is the lack of security (Kuruwitaarachchi et al., 2019).

Data security in online business is becoming more topical as the shift from traditional shopping and transactions move away from brick and mortar to click only business. Online business is rapidly growing in the global marketplace, and still, it comes with a risk that the data transactions can be compromised, which ultimately leads to financial loss for consumers while a damaged reputation for business corporations. Thus, the data security in online business transactions plays vital role in the ongoing success as well as the growth of online business (Kuruwitaarachchi et al., 2019).

The online business has reformed traditional brick and mortar business model, subjecting consumers in online transactions to greater risks in terms of their privacy and data security. The concern of the lack of their privacy and data security perceived by consumers is greater in online business than in the traditional business, thus, become is the main obstacle to the successful development of online business. Existing research findings shows that potential online consumers' concern over privacy and data security of their financial and personal information is an impediment to growth of Business to Consumer (B2C) model of e-commerce or online business. It appears that the two major critical factors for B2C model of e-commerce are consumers' privacy and data security concern that influence their willingness to purchase online or provide personal information for online service.

Existing literature shows that trust is a significant factor in consumers' online business decision. According to Alshibly (2015), data security is a vital factor that play the center role in developing consumers' trust in the online business. Consumers' intention to buy online is affected by their perceptions on data security, especially when it's related to sensitive financial and personal information. This suggests that trust in secured data transaction may increase consumers' willingness to purchase online, and that through taking data security into serious consideration the online business can be reached at the optimum level (Limbu et al., 2011).

For the development and growth of online business the most important factor is to build trust among consumers. The trust upon online business totally depend on the data security and privacy policy of the business website. To maintain privacy in the online business, a complete and secure data system is required. Consumers relatively feel more hesitation doing their online financial transaction or providing their personal information in online business than in the traditional business although online payment system is more convenient and easier (Muneer et al., 2018). Research findings shows that the lack of proper and complete measurement from the online business institutions also causes the breaches of data. According to a survey, 92% consumers believe that although online businesses are responsible to keep consumers' personal data private but practically the online businesses disclose the consumers' data to others (Muneer et al., 2018).

In this context, the purpose of this study was to:

1) Study the overview of online business data security.
2) Discuss the different security issues in online business.
3) Understand and analyze the purpose of security in online business.

Data Security

In general, online business or e-business is referred as buying and selling products via electronic channels, primarily the Internet, the global online market place. Online business also includes providing and receiving services online. Online business connects customers and vendors over the internet as they conduct business interactions (Kuruwitaarachchi et al., 2019). Existing literature suggested that data security is the most significant factor of consumers online business decision.

In online business context, data security refers to consumers' perceptions about the security of the online transactions of data as well as the protection of data from unauthorized access. Consumers' concern for data security can be categorized into financial security that relates to providing their financial information and non-financial security that relates to revealing their personal information. Current research suggests that consumers in online business have serious concerns about providing their financial and personal information during online business transactions. Thus, if customers' data negligently or purposefully compromised then that may trigger serious concerns among online consumers resulting in a negative perceived business practices leading to breaking of trust in online business (Limbu et al., 2011). Data security in online business is the protection of online data from unauthorized access, use, alteration, or destruction. Data security is one of the principals and continuing concerns that restrict consumers engaging with online business (Kuruwitaarachchi et al., 2019).

Elements of Data Security

Data security is usually defined as the composite of three attributes: Confidentiality, Integrity, and Availability (CIA) - the core principles of information security. These attributes were later complemented with further items such as reliability, safety, and maintainability when combining security with dependability (Heurix et al., 2015).

Confidentiality

Confidentiality refers to protecting information from being accessed by unauthorized people. The confidentiality of data and information is materialized in offering access to them only for authorized users (Popescul, 2011). The information can only be accessed by authorized people because if that information is not secured, the consumers will loss financially and the company or the organization involved in that business will eventually lose its reputation and business (Mir et al., 2011).

Integrity

Integrity can be defined as the dependability and trustworthiness of data or information. More specifically, it is the accuracy, consistency, and reliability of the data content, processes and systems. Integrity of data assures that the data has neither been tampered with nor been altered or damaged since the time of the last authorized access or read. Data integrity assure that the data must be kept in the correct and complete original form and must not be modified without an authorization, either accidentally or on purpose (Popescul, 2011). Data can be corrupted when it is available on an insecure network system. When data is modified by third party without an authorization, it loses its integrity. This unauthorized change made to the data, whether by human error or intentional tampering, compromises the reliability of data (Mir et al., 2011).

Availability

Availability of data assures that the data is always available whenever it is needed (Popescul, 2011). Availability means that the Information requested or required by the authorized users should always be available when requested. Availability is often the most important attribute in service-oriented online businesses that depend on information (Mir et al., 2011).

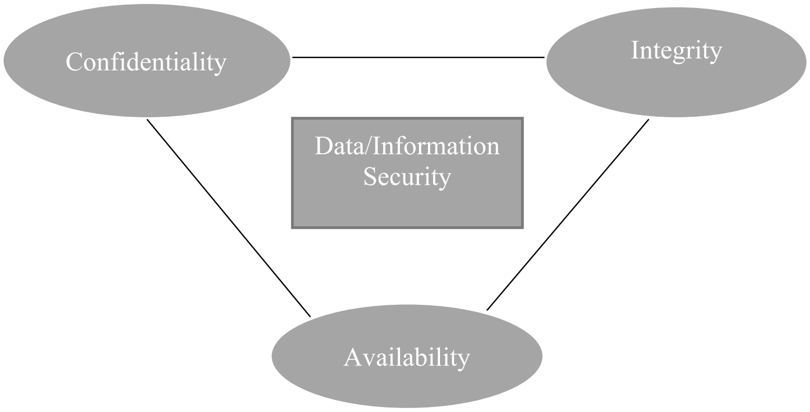

Figure 2: Classical CIA triad of data security

Trust in Online Business

Traditional or online, across the business industries, trust is important factor to develop and maintain business relationships with consumers. Trust, as the willingness to accept vulnerability to the actions of another, has been found to be particularly important in the situations with greater uncertainty, interdependence, and a fear of opportunism by others. Trust helps consumers to take the perceived risk in regards to financial transactions in online business and play critical role to consumers' sharing sensitive information as well as the adoption of new technology for business transaction (Martin, 2018).

In online business trust between business and consumers is more important because, unlike during the transactions in traditional brick and mortar business, the vender is not present in person during the business transaction. The consumers are not dealing with real person in online business, rather are just dealing with a user interface in front of their computer. It is much easier for a business entity to set up a website and an electronic payment processing system than a real-world storefront in online business. It is also cheaper, faster and more convenient. However, it is also much more difficult for consumers to determine the authenticity of the websites they are dealing with. This makes it very difficult for consumers to trust that the online businesses are who they claim to be. Developed trust can help consumers to reduce the uncertainty and complexity of transactions and relationships in online business where it is difficult to connect identities with actual individuals (Gupta & Dubey, 2016).

Trust is an individual's belief or expectation of others' ethical behaviors determined under important factors such as subjective norms, risk, confidence, and security (Krot & Lewicka, 2015). With a high level of risk and uncertainties of data security in the online business environment, trust is a critical factor, especially in successful online business transactions where financial and sensitive information involve. Consumers' trust has a significant influence on their online business decision in this situation. Existing literature shows that the trust is the most common factor that affect consumers' decision regarding purchasing online – an issue which considered one of the biggest hindrances in the growth of online business. Consumers' trust is especially significant in the online business environment to positively impact their attitudes toward online business that lead to their decision in purchase and/or service online.

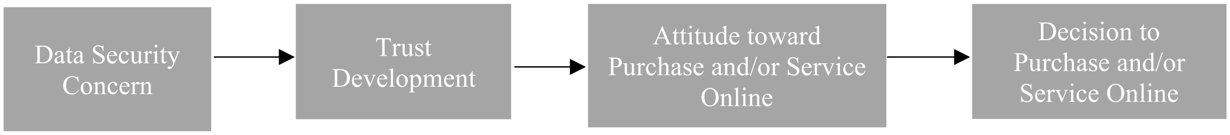
Data Security Concern
Trust Development
Attitude toward Purchase and/or Service Online
Decision to Purchase and/or Service Online

Figure 3: Trust development process of consumers' decision to business online

Conclusion

With advancement of emerging digital technology and tools, the online business or e-commerce has become very popular but with many data security challenges that are the concerning issues in online business. If these issues are not combatted, online consumers will refuse to do online business especially that requires financial transactions and personal data. The consumers' trust upon online business totally depend on the data security assurance of the online business site. To develop successful online business most important factor is to build trust among consumers. This study findings may provide valuable information for online marketing strategists assuring consumers' protecting their esteemed data.

References

Alharbi, M. I., Zyngier, S., Hodkinson, C. (2013). Privacy by design and customers' perceived privacy and security concerns in the success of e-commerce. *Journal of Enterprise Information Management, 26*(6), pp. 702-718.

Gupta, P. & Dubey, A. (2016). E-commerce- study of privacy, trust and security from consumer's perspective. *International Journal of Computer Science and Mobile Computing, 5*(6), pp. 224-232.

Heurix, J., Zimmermann, P., Neubauer, T., Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers & Security, 53*. Pp. 1-17.

Krot, K., & Lewicka, D. (2015). The Model of HRM-trust-commitment relationships. *Industrial Management & Data Systems, 115*(8).

Kuruwitaarachchi, N., Abeygunawardena, P.K.W., Rupasingha, L., & Udara, S.W.I. (2019). A systematic review of security in electronic commerce - threats and frameworks. *Global Journal of Computer Science and Technology: E-Network, Web & Security, 19*(1).

Limbu, B. Y., Wolf, M., & Lunsford, L. D. (2011). Consumers' perceptions of online ethics and its effects on satisfaction and loyalty, *Journal of Research in Interactive Marketing, 5*(1), pp. pp. 71-89.

Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online, *Journal of Business Research, 82*, pp. 103-116.

Muneer, A., Razzaq, S., & Farooq, Z. (2018). Data privacy issues and possible solutions in e-commerce. *Journal of Accounting and Marketing, 7*(3). DOI: 10.4172/2168-9601.1000294.

Mir, Q. S., Dar, M., Quadri, S M K., & Beig, M. B. (2011). Information availability: Components, threats and protection mechanisms. *Journal of Global Research in Computer Science,2*(3). Pp.21-26.

Popescul, D. (2011). The Confidentiality – Integrity – Accessibility triad into the knowledge security-A reassessment from the point of view of the knowledge contribution to innovation. *Proceedings of the 16th International Business Information Management Association Conference (Innovation and Knowledge Management, A Global Competitive Advantage)*, June 29-30, 2011, Kuala Lumpur, Malaysia, ISBN: 978-0-9821489-5-2, pp. 1338-1345.

United States Census Bureau, U.S. Department of Commerce. (2020). Quarterly retail e-commerce sales 1st quarter 2020. Retrieved from https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf

Biography

Bilquis Ferdousi is Associate Professor of Information Assurance & Cyber Defense, Information Technology in School of Information Security and Applied Computing at the Eastern Michigan University. She holds Ph.D. and Master's degree in Information Systems. She also has Master's degree in Sociology and Psychology. She has twenty years of experience as full-time faculty in computer technology programs - Information Assurance & Cyber Defense, Information Technology, and Information Systems. She developed many undergraduate and graduate curriculum in computer technology programs offered online, hybrid, and face-to-face methods. She also serves as program coordinator. Her current research focus mainly includes: Effect of psychological factors in new technology adoption, Human-computer interaction and usability of digital device, Use of mobile apps and emerging computer technology for interactive academic learning, Impact of advanced technology on privacy and data security, Social engineering in cyber security, Digital forensics analysis, Gender gaps and underrepresentation of minority groups in computer technology programs.