sustainability

MDPI

Article

E-Customer Security as a Social Value in the Sphere of Sustainability

Arnold Pabian [1,*], Barbara Pabian [2,*] and Beata Reformat [2]

[1] Department of Management, Czestochowa University of Technology, 42-201 Czestochowa, Poland
[2] Department of Management, University of Economics in Katowice, 40-287 Katowice, Poland; beata.reformat@ue.katowice.pl
* Correspondence: arnold.p@wp.pl (A.P.); barbara.pabian@ue.katowice.pl (B.P.)

Received: 25 November 2020; Accepted: 15 December 2020; Published: 18 December 2020

Abstract: Customer security in the e-commerce sector is not, but should be, approached in terms of sustainability, because it is a social problem concerning more than 2 billion people worldwide and over 20 million shopping sites. New techniques and technologies are implemented in this sector not only by e-sellers, but also by cybercriminals, which significantly lowers the level of its security. The purpose of the paper is to present, on the basis of own research, the main e-commerce threats from the perspective of the customer and the seller, and to indicate the possibility of their elimination, which should contribute to sustainable development. The threats from the e-customer's perspective were identified by considering individual phases of online purchase. In the case of e-shops, the threats were analyzed in a personnel—computer hardware—software structure. As conducted research shows, the threats for e-customers are located in three main areas: security of the means of payment, security of personal data and payment cards, and security of purchased goods. The security of the e-customer largely depends on the security of the e-store in which the purchase is made. Research has shown that e-stores are not fully secure, which mainly results from negligence and the lack of knowledge in the sphere of cybersecurity.

Keywords: sustainable development; social threats; security; e-commerce; e-customer; e-shop

1. Introduction

E-commerce is a rapidly growing area of business activity. It is predicted that in 2020 global e-commerce sales will exceed USD 4.2 trillion in the world [1]. The number of people shopping online will reach 2.05 billion, which represents 26.28% of the total number of people living on our planet [2]. The number of e-commerce sites will significantly exceed 20 million [3]. E-commerce is based on more and more modern techniques and technologies that contribute to better customer service and more efficient operation of e-stores. They include: Progressive Web Application (PWA), Accelerated Mobile Pages (AMP), voice commerce, artificial intelligence, and robotic warehouses [4]. Criminals also use more and more modern techniques and technologies, threatening the security of e-commerce.

E-commerce security refers to the state in which online sale participants (buyers and sellers) are not subject to any threats that could cause any harm to them. Security is a social category. The threat to security is, therefore, a social threat. The main goal of activity in the area of sustainable development is to eliminate not only ecological but also social threats. According to S. Jeanrenaud and J. Jeanrenaud, ecological and social threats are environmental and social challenges [5]. Therefore, the threat to e-commerce security should be included in the list of social threats from the perspective of sustainable development. The threat to security in the e-commerce sector is becoming a growing problem as more and more people buy and sell products and services via the Internet. Two billion people shopping online and twenty million shopping sites with millions of employees represent a huge number of

buyers and sellers that are not fully secure. In this case, it is not only about cybersecurity, but also about its classic types, e.g., the failure to deliver the purchased goods to the customer or the delivery of damaged or defective goods.

The conditionings presented above lead to the formulation of the following research problems: what are the threats to buyers and sellers in the e-commerce sector from the perspective of sustainable development? How to increase the security of online buyers and sellers contributing to sustainable development?

The purpose of the paper is to present, on the basis of own research, the main threats of e-commerce from the perspective of the customer and the seller, which due to the scope of their impact and the damage caused have a social nature and should be included in sustainable development programs. The threats from the e-customer's perspective were identified by considering individual phases of online purchase. In the case of e-shops, the threats were considered in the personnel—computer hardware—software structure. Considering the security of both sides to the purchase transaction is necessary because security of the e-customers not only depends on their knowledge and behavior, but also on the concern for the security of the e-shop. The paper also indicates activities that can significantly contribute to the elimination of identified threats, which will certainly contribute to sustainable development.

The article consists of five parts. After the introduction, a literature review has been carried out showing that e-commerce security is not considered in an aspect of sustainable development, although the risks of online shopping security are becoming a very serious social problem due to the huge and still growing number of e-consumers, e-commerce stores, and e-transactions. Then, the research methodology has been described, which the authors of this article used to conduct in-depth interviews on e-commerce security. The results of this study are presented in the section entitled Empirical Results. The final part of the article contains conclusions resulting from the research, debatable issues, and suggestions for further research directions related to the subject of this article.

2. Literature Review

The literature on sustainability indicates and discusses many various threats that have a negative impact on our planet and the societies inhabiting it. They are divided into ecological and social threats. The first part of the literature review verifies whether the threats to e-commerce security are reflected in the literature on sustainability. The focus is on reviewing social risks, while ignoring environmental risks, because e-commerce security is social, rather than environmental. Sally Jeanrenaud and Jean-Paul Jeanrenaud equate social threats with the challenges of sustainable development, while indicating the following key social challenges: population dynamics, poverty and inequality, exploitation, and well-being [5]. Mikael Ottosson and Anders Parment perceive consumption as a serious threat. According to them, consumption gives rise to economic, social, and environmental problems [6]. Nikos Avlonas and George P. Nassos associate the increase in consumption with the increase in global population growth. As a result, problems such as lack of food (food), lack of water, as well as diseases caused by environmental pollution arise [7]. Gregory T. Haugen discusses the issues of immigration and migration, health, mortality, and fertility in terms of world population growth [8]. According to Jerry A. Carbo and Viet T. Dao and Steven J. Haase and M. Blake Hargrove and Ian M. Langella, the factors influencing the destruction of the people, include poverty and inequality, destruction to consumers, destruction of communities, destruction of creativity, and destruction of democracy [9]. As this review shows, threats to e-commerce security are not discussed in the literature on sustainability. This fact is also confirmed by the review of other works in the field of sustainability by such authors as Robert Brinkmann [10], Steven Cohen [11], Marc J. Epstein and Adriana Rejc Buhovac [12], Erling Holden and Kristin Linnerud and David Banister and Valeria Jana Schwanitz and August Wierling [13], Daniel S. Fogel [14], Michael Lenox, Aaron Chatterji [15], and Leslie Paul Thiele [16].

Authors of works on sustainability often refer to the following social threats: social diseases, exploitation, poverty and deprivation, unemployment, and consumerism. These are briefly discussed below.

Social diseases are divided into direct (which can be prevented by maintaining proper lifestyle and hygiene) and indirect (which people have no influence on). Direct social diseases are the result of lack of physical activity, poorly balanced diet (rich in sugars, animal fats, salt, highly processed products, and stimulants), as well as stress, addiction, or workaholism. Indirect social illnesses develop as a result of harmful factors such as smog, soil and water pollution, noise, ionizing radiation, and other pathogenic agents. The most common social diseases are: obesity, diabetes, diarrhea, constipation, stomach and duodenal ulcers, heartburn, hemorrhoids, allergies, respiratory tract diseases, cancer, and mental illnesses. This list should be expanded by addictions, such as alcoholism, drug addiction, anorexia, and bulimia, as well as depression, affective diseases, personality disorders, and neuroses. All these diseases are spreading globally. Although they are not contagious, they lead to disability and in over 80% to premature death [17].

Exploitation takes different forms. There are 21 million victims of forced labor worldwide resulting from human trafficking, slavery, bonded labor, and prostitution. They generate USD 150 billion in illegal profits [5]. Forcing children to work is also a form of exploitation. According to the International Labour Organization (ILO), 168 million children worldwide are engaged as child laborers and more than half of these are engaged in hazardous work. According to the Department of Labor, there are nearly 140 products from 75 countries listed as products produced by child labor. These products are used throughout the globe including in developed countries [9].

The number of people who live below the international poverty line (less than $1.9 per day) worldwide has reached 783 million. The areas of greatest poverty are located in South Asia and sub-Saharan Africa. The consequences of poverty include hunger, malnutrition, limited access to education and other services, and often also social discrimination and exclusion [18]. Poverty significantly affects children. According to UNICEF data, by 2030 as many as 167 million children will live in poverty [19].

The International Labor Organization estimates that 188 million of the 5.7 billion people in the world who are of working age (over 15 years old) will be unemployed by 2020. A further 165 million can only count on a few hours' employment per week, which will not provide them with a decent standard of living as a result of too low wages [20]. Unemployment has negative social, psychological, and economic consequences.

Consumerism involves a lifestyle in which happiness is achieved by purchasing all kinds of products and services without moderation. As these purchases far exceed the needs of individuals, a part of them are never used. At the heart of consumerism is the conviction that possession of objects reflects social status and improves the quality of life. Consumerism often takes the form of shopaholism, i.e., an obsession with shopping. This is a social problem that often requires treatment after consultation with a psychologist or a psychiatrist.

The issue of e-commerce security is discussed in scientific literature from outside the area of sustainability. It is broad and multithreaded. Below there is a brief overview of research initiatives undertaken in this area in recent years.

Review of the literature shows that customer security is one of the most important research areas regarding e-commerce. According to Abdul Halim Barkatullah, Djumadi development of e-commerce has reformed traditional commerce subjecting consumers in e-commerce transactions to greater risk while offering them only a weak bargaining position when it comes to their rights. This situation prompted this author to analyze self-regulation as an effective means for providing legal protection and consumer security in e-commerce transactions [21].

In many cases, e-customer security is considered from a narrow perspective, through the prism of a category of threats. Protection of the privacy of e-consumers is such a popular, often described, category of threats. Gabriele Pizzi and Daniele Scarpi analyzed privacy risks when using new retail

technologies. They propose that privacy in a retail environment should be perceived as reliant on retailer and technology related factors as well as consumers' personality traits [22]. Ruwan Bandara and Mario Fernando and Shahriar Akter focused on the problem of the privacy paradox. It refers to the fact that e-customers are concerned about their privacy, but usually do not take appropriate precautions to protect this privacy. The lack of caution consists, among others, in disclosing personal data [23]. Using communication privacy management theory, Ali Balapour and Hamid Reza Nikkhah and Rajiv Sabherwal examined the effects of privacy-related perceptions, such as privacy risk and the effectiveness of privacy policies, on the security perceptions of mobile app users [24]. The factors influencing the intention to buy online, and the associated risk is an important problem discussed in the scientific literature. Livoo B. Hong and Hoon S. Cha have concluded from their research that performance, psychological, social, and online payment risks negatively affect purchase intention. Reduction of risks will first improve consumer trust, and then increase consumer's intention to buy online [25]. Ing-LongWu and Mai-LunChiu and Kuei-WanChen showed that perceived risk has a negative effect on perceived usefulness and consumer satisfaction [26]. According to Anne-Sophie Riegger, Jan F. Klein, Katrin Merfeld, and Sven Henkel smart technologies provide traditional retailers with new opportunities of introducing amenities to e-commerce. However, their introduction faces certain barriers. They found, among others, four barriers to consumer acceptance of technology-enabled personalization (exploitation, interaction misfit, privacy, and lack of confidence) [27]. Spyridon Samonas and Gurpreet Dhillon and Ahlam Almusharraf attempted to capture the convergence and divergence of stakeholder perceptions with regards to security policy. For this purpose, they collected data from the employees of the e-commerce company [28].

Researchers also work on the security of data that is sent and collected in the e-commerce sector. Don Bush explained how data breaches lead to fraud. The breaches happen because the data stolen is valuable. Don Bush explained how data breaches lead to fraud [29]. Clare Sullivan conducted a comparative analysis of two major international data transfer schemes in existence today—the European Union model (the General Data Protection Regulation) and the Asia-Pacific Economic Cooperation Cross Border Privacy Rules system, in the context of the Internet of Things [30]. Darius Stitilis and Marius Laurinaitis took up the problem of treatment of biometrically processed personal data. The application of biometric technologies has become almost commonplace. They can help to raise the security level and make identification and authentication procedures easy, fast, and convenient [31].

Using the application also poses threats to e-commerce. Dezi Wu and Gregory D. Moody and Juan Zhang and Paul Benjamin Lowry note that App users typically have a poor understanding of information security. They examined how security perceptions of apps were formed and how these perceptions influenced users' intentions to continue using apps [32].

Various types of reports are also the source of information on e-commerce security. Some of them present data on the problems faced by Internet users shopping online. The information provided at the address could be an example [33]. The creators of this data do not go into detail about the security problems of e-customers, do not develop these issues, and do not try to organize it from the point of view of explicit and hidden concerns of e-customers. Despite these drawbacks, the reports are a valuable source of information on various aspects of the e-commerce sector. They also deal with the issues of security of e-shops.

Critical analysis of the literature on e-commerce security leads to the following conclusions: 1. e-commerce security is not considered through the prism of sustainable development, although the risks of online shopping security are becoming a very serious social problem due to the huge and still growing number of e-consumers, e-shops, and e-transactions; 2. e-commerce security threats are mainly considered from the perspective of cybersecurity, with less attention to threats that are not related to IT techniques and technologies; 3. there are no approaches aiming to identify a full possible spectrum of threats to security of e-customers and e-shops; and 4. threats to security strongly felt by e-customers, while ignoring or paying less attention to less experienced threats or unaware threats are mainly identified. The paper aims to fill the gaps indicated above.

3. Research Method

The research conducted by the authors of this paper concerned e-commerce security from the perspective of both the e-customer and e-shop. This security is the lower the more threats there are on the side of the buyer and seller. The objectives of the study were as follows:

- identification of a wide range of threats on the part of the customer who purchases on the Internet,
- identifying which types of threats are strongly felt by e-customers and which they are not aware of,
- determination of threats to the functioning of the e-store that are related to the security of customers,
- indication of the ways to eliminate threats, which should contribute to sustainable development.

To make the identification of threats structured and fairly complete, it was made on the basis of two systems. In the case of e-customers, the threats were identified in the structure of successive phases of purchase. These phases are as follows: connecting to the purchasing website, getting acquainted with the product offer, purchasing the product, waiting for the product, actions after the purchase. Threats on the side of the e-shop were considered in the following structure: e-shop staff, computer hardware and software.

The threats on the e-customer side were defined on the basis of 50 in-depth consumer interviews. The interviewed people were aged 18 to 70. There were 56% of women and 44% of men among them.

The study used the individual in-depth interview as a research method. The research tool was the scenario of an interview with the respondents. According to the scenario, the interview was as follows: (i) introducing oneself to the respondent; (ii) thanking respondent for participating in the interview; (iii) informing how long the interview will last; (iv) informing the respondent what we want to know; and (v) asking general and then specific open questions.

It was assumed that the threats strongly felt by e-customers are those that they specify and list after asking the questions: "What threats do you feel when shopping online?" and "What are you afraid of when shopping online?". The objective of the study was also to identify weakly perceived threats, as well as those that they are not fully aware of. The respondents did not mention them after asking the above questions. In order to identify the type of threat, in the further part of the interview, leading questions were used, e.g.,: "What other threats do you feel when shopping online?", "Do you feel any threats when you read the online store's offer?", "Are you not afraid that the product purchased online will not be original (it will be a counterfeit of the original product)?"

The interviews revealed not only the emotional and motivational behavior patterns of respondents regarding online shopping from the perspective of their security, but also made it possible to reach not fully recognized concerns related to such purchases.

People invited to the individual in-depth interview corresponded to the demographic variables established by the moderator and resulting from the definition of the target group for the e-commerce sector (gender, age, education, place of residence). The interview participants were recruited in terms of meeting the following criterion: making purchases via the Internet. The interview participants were approached using the snowball sampling method, which consisted in the nonrandom selection of respondents for research. After the completion of each subsequent interview, the moderator asked the respondent to indicate a friend who could be interviewed on the subject of the scenario. This method turned out to be very useful because people are reluctant to participate in such interviews and are distrustful of unfamiliar interlocutors. Due to the ongoing pandemic caused by the COVID-19 coronavirus, the classic in-depth interview in the "face-to-face" version has been replaced by a telephone interview. This form of communication provided the respondents with full freedom of expression and conversation in such a way as to achieve the objectives of the study.

The analysis of data obtained as a result of conducted in-depth interviews covered three stages of activities. The first one was to rewrite the interviews into separate files. In the second stage, sets of categories were built based on the research objective, according to which the information obtained in the interviews was selected. The third stage consisted in comparing the distinguished categories with the interviews conducted in order to find a common ground. The inference was inductive.

Since the security of the e-customer depends not only on his knowledge and behavior, but also depends on the concern for the security of the e-shop in which he purchases, the threats posed by online sellers were also addressed. These threats were identified on the basis of secondary sources and interviews conducted with 20 IT specialists. The focus was mainly on e-shop cybersecurity, as it has the greatest impact on the security of e-customers.

As in the previous case, the individual in-depth interview was used as a research method and as a research tool in the form of an interview scenario. The only difference was that face-to-face interviews were conducted while maintaining the security measures applied in connection with the COVID-19 coronavirus pandemic (adequate distance was maintained between interlocutors and masks were used).

4. Empirical Results

In the first part of empirical results we discuss the security of e-commerce customers, while in the second part the security of e-stores.

The conducted survey shows that threats to e-commerce customers are located in three main areas, presented in Table 1. E-commerce customers attach the greatest importance to the security of their money, purchased goods, personal data, and payment cards.

Table 1. The areas in e-commerce that are most at risk from the clients' perspective.

Customer Security When Shopping Online		
Security of means of payment	Security of personal data and payment cards	Security of the purchased goods

Source: own case study.

To investigate the problem of e-customer security in detail, this security has been analyzed from the perspective of individual purchase phases. Table 2 presents the risks in various phases of online purchase.

Table 2. Threats experienced by customers in various phases of making an online purchase.

No	Phases of Making an Online Purchase	Threats in Individual Phases of Online Shopping
1	Connecting to the shopping service	1.1. Fake shopping sites
2	Getting to know the product offer	2.1. False information on the website 2.2. No relevant information 2.3. Fake product photos 2.4. Complicated service operation
3	Product purchase	3.1. Fraudulent payment transactions 3.2. Malicious applications 3.3. Phishing
4	Waiting for the product	4.1. No shipment of goods 4.2. Wrong item shipped 4.3. Lost parcel 4.4. Delayed delivery date 4.5. Product damaged during shipment 4.6. Not original product 4.7. Factory defective product
5	Post-purchase actions (return of goods, complaints, etc.)	5.1. Refusal to accept the goods 5.2. Refusal to exchange goods 5.3. Refusal to refund 5.4. Dismissal of the complaint

Source: own case study.

As Table 2 shows, cybersecurity is not the only problem of e-commerce customers. Out of 19 security threats listed in Table 2 in individual purchase phases, only 6 can be associated with cybercrime (1.1, 2.1, 2.3, 3.1, 3.2, 3.3). We do not include in this group the risk consisting in missing essential information (2.2), while assuming that such a lack is caused by the seller's negligence, as well as the threat resulting from complicated service operation (2.4). The opinion about the complex service of the website usually results from the lack of sufficient IT knowledge on the customer side. Among the threats not related to cybersecurity and listed in Table 2, as many as nine (2.2, 4.1, 4.2, 4.6, 4.7, 5.1, 5.2, 5.3, 5.4) relate to the seller's actions, including their reliability and honesty. Risks 4.3, 4.4, and 4.5 are related to the suppliers of the goods, which are usually courier companies or the post office.

The threats related to online shopping are experienced by both those who do, and those who do not, do such shopping. Thirty-two percent of the people surveyed do not shop online. The reasons they indicate are presented in Figure 1. Attention should be paid to such prosaic reasons as the lack of the Internet or the lack of knowledge regarding the use of shopping websites. Most of the respondents who do not shop online prefer traditional forms. The interviews showed that direct physical contact with the goods is important to them. They want to touch the goods, see them from all sides, see how they function, and try them on. Attention was also paid to such important aspects of shopping in shops, shopping arcades, and shopping centers as: leaving the house, being among other people, window-shopping, or going for coffee while shopping. Concerns of this group of respondents related to cybersecurity concern such threats as: money theft and theft of personal data.

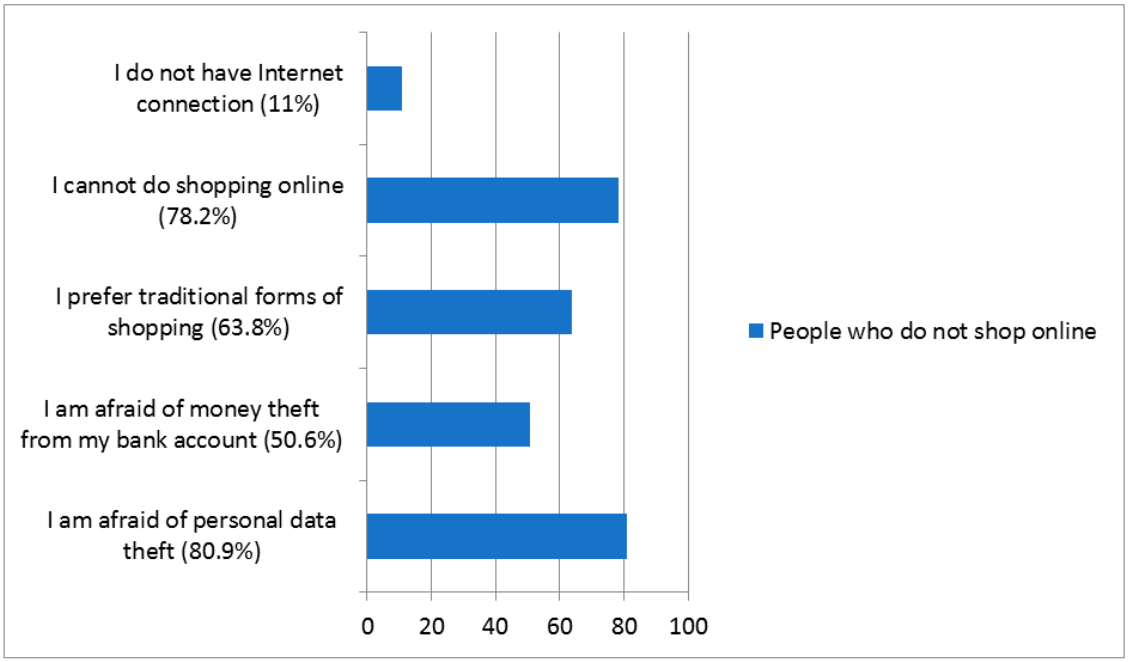

Figure 1. Reasons for not shopping online. Source: own case study.

Most of the respondents (68%) shop online. Figure 2 shows the security threats of this type of shopping that are most strongly felt. The respondents mentioned them first during the interview. As Figure 2 shows, most concerns are not related to the cybersecurity, but goods and their distribution. Most respondents are worried that the purchased goods will not meet their expectations (74.6). The phishing of personal data (14.3%), which is a manifestation of cybercrime, was one of the last places on the list of threats. Other risks, listed in Table 2, are poorly felt by the respondents or the respondents are completely unaware of them. The respondents did not mention them when they were asked the questions of: "What threats do you feel when shopping online?" "What are you afraid of when shopping online?" In order to identify weakly perceived threats, in the further part of the interview, the respondents were asked the following leading questions: "What other threats do you

feel when shopping online?", "Do you feel any threats when you look at the offer of online stores?", "Are there any threats in the sphere of customer contacts with the seller after the purchase?" In this case, the respondent listed specific threats occurring in the sphere indicated by the researcher. The weakly felt threats include: shipment of the wrong product, missing shipment, refusal to accept, exchange, or return the product. The survey also revealed that the respondents are not aware of certain risks. This was revealed by questions in which respondents listed a specific type of risk. Here is an example of such a question: "Are you not afraid that the product purchased online will not be original (it will be a counterfeit of the original product)?", "Are you not afraid that as a result of too complicated service of the website you will make mistakes negatively affecting the purchase (e.g., the price reduction resulting from the promotion will not be taken into account during the payment)?" The answers to such questions often included the following phrases: "I actually did not realize it", "I didn't think about it before", "It is worth remembering". The respondents were not aware of the following risks: the possibility of receiving a nonoriginal product, lack of essential information on the website of the online store regarding their rights, as well as the seller's obligations and complicated operation of the website, which could lead to errors and mistakes made by customers who do not have sufficient IT knowledge.

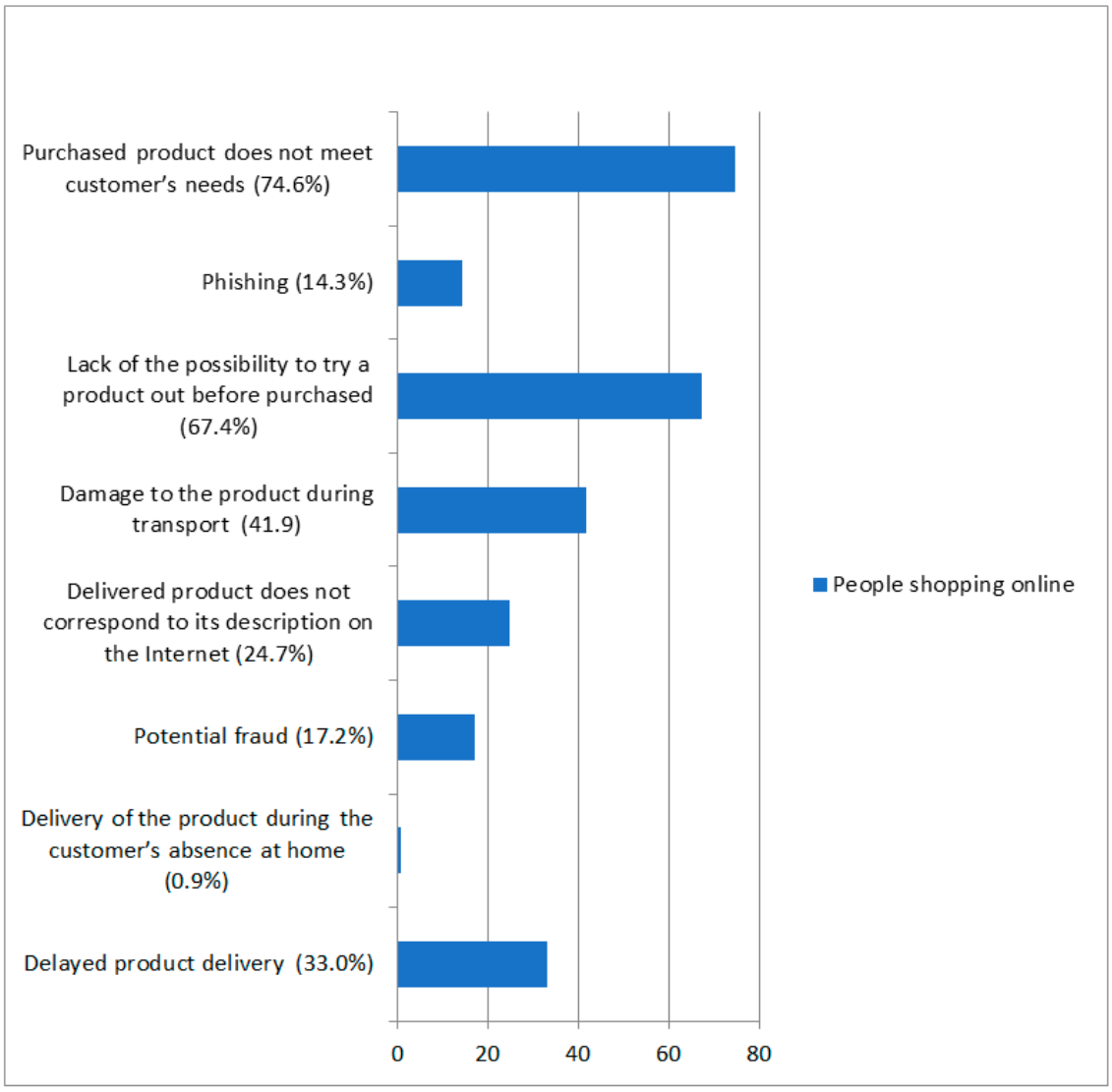

Figure 2. Concerns of customers shopping online. Source: own case study.

The security of e-customers on the e-commerce market can be significantly increased by implementing the following measures: investing more funds in the fight against cybercrime, conducting extensive information campaigns on the risks occurring during online shopping and ways to avoid them, while allocating more funds to educating the public in the field of IT.

Not only external organizations, but also the customer himself can increase his security while making online purchases. The most important activities that he can perform to increase this security include: education in the field of computer science (self-education, participation in courses), getting acquainted with opinions posted on the Internet about e-shops and courier companies, choosing reliable e-shops, selection of reliable courier companies, selection of a secure form of payment for the goods, payment for the goods after their delivery. Including e-commerce security in sustainable development programs would mean allocating some funds from its budget for this security.

The security of the e-customer largely depends on the security of the e-store in which they make purchases. Now the analyses will focus on e-commerce security from the perspective of online retailers. The security of e-shops is a profoundly serious problem because there are over 20 million e-commerce websites in the world [3]. Most e-commerce businesses in Poland trade in physical goods. Only 10% of stores sell virtual goods, e.g., digital music, e-books [34].

Cyber attacks are the main threat to the functioning of e-stores. They take various forms (payment fraud, phishing, Distributed Denial of Service (DDoS), spoofing—Domain Name System (DNS), IP address (IP), Address Resolution Protocol (ARP). Hacker attacks on e-stores and their customers cause a lot of damage, including financial damage. In 2018, they led to financial losses of over $600 billion worldwide. Soon that number will exceed one trillion dollars [35].

E-commerce is an incredibly attractive source of income for criminals. Most e-shops have huge databases. They contain customer personal data, credit card data, transaction histories, as well as information on the operating systems and computer hardware they use. With such knowledge, cybercriminals cannot only steal bank accounts, but also blackmail, demand ransom, and destroy electronic systems of both customers and e-shops.

Payment fraud is one of the most common forms of cybercrime in the e-commerce sector. Fraud most often occurs in connection with transactions made with payment cards on the Internet. As much as 95% of the surveyed Polish companies enable their customers to make payments with a credit or debit card. Eighteen percent of companies declare that they have dealt with fraud in the last 12 months. The industries that are exceptionally threatened by payment fraud in Poland include: digital goods and services, computer games, tourist services, and luxury goods [36]. Payment fraud causes significant financial losses: the shop owner loses the goods that have been taken over by the fraudster, must return the money to the aggrieved customer, it deteriorates his image and causes unfair competition because the fraudulent goods are placed on the secondary market and are usually offered at low prices.

On the basis of own research and extensive literature studies, the authors of this paper identified the main reasons for the emergence of threats to the operation of online stores. They are listed in Table 3 in the structure: e-shop staff—hardware—software.

Table 3. The causes of emergence of threats to the functioning of stores on the Internet.

No.	E-Store Elements	Reasons for the Emergence of Threats
1	Staff	• Lack of cybersecurity specialists among the staff • Lack of training and self-education on cybersecurity • Unsecured or poorly secured employee access to sensitive data • Failure to follow the application and server access procedures
2	IT equipment	• Outdated computer hardware • Inadequately secured access to computer hardware

Table 3. *Cont.*

No.	E-Store Elements	Reasons for the Emergence of Threats
3	Software	• Lack of software detecting cyber attacks • Lack of sophisticated antivirus systems • Lack of software or failure to perform penetration testing to detect gaps in the infrastructure • Missing data backup or its inadequate protection • Lack of additional security for critical systems, e.g., two-factor authentication (2FA) • No software updating

Source: own case study.

The further part of the article describes more important reasons for the emergence of threats, listed in Table 3, and presents solutions that contribute to their elimination.

One of the important aspects of caring for cybersecurity of an online store is employment of a person responsible for this area or the use of outsourcing solutions. According to the TestArmy report, there is a person responsible for cybersecurity in the internal structures of about 60% of Polish companies [34]. Hiring a specialist for cybersecurity is usually not enough to successfully fight fraud. It needs to be equipped with appropriate instruments necessary in this fight. Transaction filtering software or systems based on artificial intelligence can be such an instrument. Such systems automatically analyze data concerning the transaction participant and on the basis of this data they make predictions whether a given operation is a phishing attempt or not. They do not need human intervention in the event of changes in the fraudsters' behavior. Thanks to continuous learning, they adapt to changes by themselves.

Analysis of post security violation incidents is a necessary action in the event of any cyber attack on e-shops. Its purpose is to explain how the criminal has breached security and what legal and financial consequences this may cause. As a result, an e-shop can be secured better, and similar attacks can be avoided in the future.

Risk analysis, thanks to which potential threats are identified and the size of possible losses is estimated is another important process. This is related to performing security audits of the store's website, e.g., penetration tests. In 40% of companies, the security audit is performed irregularly, while in 60% it was not executed [34].

The ability to restore lost data (data back-up) is another activity in the sphere of cybersecurity. Research shows that only 20% of stores are not afraid of losing data because they have its current copy in another location. In 33.33% of cases, the data in the online store comes from other systems or is exported to other systems and can be restored with little effort. The security of e-shop employees' access to sensitive data is especially important. In this case, it is mainly about access via private phones, laptops, tablets, and other devices, which employees can use both outside the e-shop, as well as in its premises. Still relatively few Polish companies use additional security measures for critical systems, such as two-factor authentication (2FA). The standard is to use conventional methods of protection against attacks, such as antivirus programs, Secure Sockets Layer (SSL) certificate, data encryption on the server side, password manager, and training for employees [34].

The level of security is increased by strict compliance with the application and server access procedures. Only authorized people should have such access. Installation of antivirus programs on the computers of those employees who need to connect to company systems is also important. Access to these systems should be protected with strong passwords and two-factor authentication. It is also advisable to organize training courses for employees in order to expand their knowledge and skills regarding cybersecurity.

Other important activities increasing the security of the e-shop and its customers include:

- creating strong passwords, changing them frequently and securing them properly (it is recommended to use a password manager),
- application of special protection (the highest level of security) in relation to: credit card numbers, access data and personal data,
- software update,
- investing in equipment (replacing old with new) and ensuring its security.

Interviews conducted by the authors of this article with 20 IT specialists confirmed the usefulness of the above-mentioned tools and methods ensuring cybersecurity.

In the field of cybersecurity, the surveyed IT engineers attributed a lot of importance to: creating strong passwords, defining strict data access procedures, making backup copies, updating software, and educating employees. They highlighted some specific aspects of using these tools. Backup copies should be well secured, e.g., locked in armored cabinets. A software update usually includes additional functionalities. They may deteriorate the performance of functionalities that have been used so far. Training in the field of cybersecurity should be conducted regularly by carefully selected companies and cover both users and IT staff.

IT specialists were slightly less optimistic about such security methods as: keeping data on different servers, using multifactor authentication, and performing security audits. Servers should be protected against unauthorized access. Using own properly secured servers is the safest. It has been found that not all systems require multifactor authentication. None of the surveyed IT specialists found the performance of security audits especially important. The opinions that they are important or moderately important prevailed. Attention was also paid to the test environment, which should create fictitious, not real, data. Investing in modern IT infrastructure is another important requirement influencing cybersecurity.

5. Conclusions and Discussion

E-commerce security is a serious social problem, recognized as one of the threats that qualify for elimination under sustainable development. This problem is intensifying together with the increasing number of online buying customers and the increasing number of e-sellers. Today, the security issue concerns over 2 billion people worldwide who shop online and have over 20 million e-commerce sites at their disposal. The security of e-commerce should, therefore, be included in sustainable development programs along with the allocation of funds for increasing the security of e-customers and e-stores.

According to the survey, threats to e-commerce customers are located in three main areas: security of means of payment, security of personal data and payment cards, and security of purchased goods. The risks associated with online shopping are felt by both those who do and those who do not do such shopping. People who do not shop online are afraid of theft of money and theft of personal data. However, it is not only this kind of fear that prevents them from shopping online. More prosaic reasons include: lack of Internet, lack of knowledge about the use of shopping websites, and the preference for traditional forms of purchase.

The threats faced by people shopping online can be divided into: strongly felt, poorly felt, and unconscious. Most e-customers are concerned that the purchased product will not meet their expectations, which may be caused by the inability to try the product before the purchase or the discrepancy between the delivered product and its description on the Internet (product photos and its text description). Strongly felt risks also apply to the delivery of the purchased product (damage to the product during delivery, delayed delivery, delivery when the customer is away from home). In this group of threats, the risk of data phishing or potential fraud is secondary. On the other hand, the weakly perceptible threats include: shipment of the wrong goods, loss of the shipment, refusal to accept, exchange or return the goods. The threats that the respondents were not aware of (lack of important information on the website of the online store regarding their rights, as well as the seller's obligations, complicated handling of the purchasing website, which could lead to errors and mistakes

made by customers who do not have sufficient IT knowledge, receipt of a nonoriginal product) were also identified.

The security of e-customers on the e-commerce market can be significantly increased by investing more funds in the fight against cybercrime, by conducting extensive information campaigns on threats, and allocating more funds to educating the public in the field of IT.

The security of the e-customer largely depends on the security of the e-store in which they make purchases. Research shows that e-stores are not completely secure. They exhibit different activities in the field of cybersecurity. Such activities as backup, use of antivirus programs, software updates, compliance with application and server access procedures, and personal data protection are common and appreciated in the field of cybersecurity. On the other hand, e-stores are less involved in performing security audits and risk analyses. Investing in cybersecurity is also not a priority. Moreover, a significant number of companies do not employ specialists in this field. There is little use of artificial intelligence in this area.

The e-client does not have detailed knowledge about the resources and activities of the e-shop in which they purchased the goods and the company that will deliver the goods. Therefore, they do not know whether sellers and suppliers of purchased goods care about the security of their customers, and how they eliminate threats. In order to gain customer trust, e-shops and suppliers of goods should increase the security of their services and clearly communicate to customers whether and why their activities are secure.

Sustainable development aims to counteract environmental threats as well as social threats. The group of social threats that are at the center of sustainability interest is not precisely defined. The literature on sustainability most often indicates such social threats as social diseases, exploitation, impoverishment and poverty, unemployment, and consumerism. Are these all types of social threats that should be analyzed within the concept of sustainable development? Certainly not. There are many more of these threats, and some of them, become global and are more and more dangerous with the development of civilization. E-commerce threats are an example of these. The beginnings of e-commerce date back to the 1980s. Previously, there were no e-commerce security issues, as this sector did not exist. Today, 40 years later, more than 2 billion e-customers and more than 20 million shopping sites worldwide are affected by this problem. The problem is constantly growing as the number of online buyers and sellers is constantly increasing. Therefore, it becomes necessary to verify and organize the set of social threats that sustainable development deals with. Certainly, this collection should be extended by other threats of significant importance today, including threats related to e-commerce.

The precise definition of the set of social threats is complicated by the fact that some of their types are also related to ecology. For example, air pollution causes damage to the environment, which is recognized as an environmental problem, and worsens human health, which is recognized as a social problem. This problem can be solved by replacing ecological and social threats with a wider division, including ecological, ecological-social, and social threats.

Along with the increasing number of social threats, the number of goals and scope of activities in the field of sustainable development increase. It should also be accompanied by an increase in funds for the implementation of programs aimed at eliminating these threats.

In the opinion of the authors of this article, further research directions related to its subject should concern the following problems:

- ordering the set of social threats from the perspective of sustainable development,
- identifying new types of social threats resulting from the development of technology, examples of which are e-commerce threats,
- the mechanism of the emergence and evolution of e-commerce threats, including the shaping of their life cycles,
- social consequences of e-commerce threats affecting sustainable development,

- preventing the emergence of e-commerce threats and looking for more and more perfect ways to ensure the security of e-customers and e-stores.

Including e-commerce security in sustainable development strategies and programs will expand the interest of governments and international organizations in this problem, as well as increase the amount of funds that will be allocated to improving the security of e-customers and e-shops.

Author Contributions: Conceptualization, A.P.; Data curation, B.P.; Formal analysis, A.P.; Funding acquisition, B.P. and B.R.; Investigation, A.P. and B.R.; Methodology, B.P.; Project administration, B.P.; Resources, B.P.; Supervision, A.P.; Validation, A.P.; Visualization, B.R.; Writing—review & editing, A.P. and B.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. What is the Future of Ecommerce? 10 Insights on the Evolution of an Industry. Available online: https://www.shopify.com/enterprise/the-future-of-ecommerce (accessed on 15 February 2020).
2. OBERLO. How Many People Shop Online in 2020. Available online: https://www.oberlo.com/statistics/how-many-people-shop-online (accessed on 20 April 2020).
3. Milenkovic, J. How Many eCommerce Sites Are There in 2020? Available online: https://kommandotech.com/statistics/how-many-ecommerce-sites-are-there (accessed on 29 April 2020).
4. Rozwój Rynku E-Commerce na Świecie w 2020 r. Available online: https://www.ideo.pl/e-commerce/wiedza/ecommerce-trendy-2020,85.html (accessed on 25 April 2020).
5. Jeanrenaud, S.; Jeanrenaud, J.P. Challenging: An overview of our one planet predicament. In *Sustainable Business. A one Planet Approach*; Jeanrenaud, S., Jeanrenaud, J.P., Gosling, J., Eds.; John Wiley and Sons Ltd.: Hoboken, NJ, USA, 2017; Volume 9–10, pp. 18–19.
6. Ottosson, M.; Parment, A. *Sustainable Marketing: How Social, Environmental and Economic Considerations can Contribute towards Sustainable Companies and Markets*; Studentlitteratur: Lund, Sweden, 2015; Volume 27.
7. Avlonas, N.; Nassos, G.P. *Practical Sustainability Strategies. How to Gain A Competitive Advantage*; John Wiley and Sons Inc.: Hoboken, NJ, USA, 2014; pp. 3–15.
8. Haugan, G.T. *Sustainable Program Management*; Informa UK Limited: London, UK, 2013; pp. 43–99.
9. Carbo, J.; Dao, V.; Haase, S.J.; Hargrove, M.B.; Langella, I. *Social Sustainability for Business*; Informa UK Limited: London, UK, 2017; pp. 11–19, 68.
10. Munier, N. *Introduction to Sustainability*; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 2005; pp. 1–285.
11. Cohen, S. *Sustainability Management: Lessons from and for New York City, America, and the Planet*; Columbia University Press: New York, NY, USA, 2011.
12. Making Sustainability Work: Best Practices in Managing and Measuring Corporate Social Environmental and Economic Impacts. *Manag. Environ. Qual. Int. J.* **2008**, *19*, 18–273. [CrossRef]
13. Holden, E.; Linnerud, K.; Banister, D.; Schwanitz, V.J.; Wierling, A. *The Imperatives of Sustainable Development*; Informa UK Limited: London, UK, 2017; pp. 10–245.
14. Fogel, D.S. *Strategic Sustainability. A Natural Environmental Lens an Organizations and Management*; Routledge Taylor & Francis Group: New York, NY, USA, 2016; pp. 3–319.
15. Lenox, M.; Chatterji, A. *Can Business Save the Earth? Innovating our Way to Sustainability*; Stanford University Press: Palo Alto, CA, USA, 2018; pp. 1–174.
16. Thiele, L.P. *Sustainability*; Polity Press: Cambridge, UK, 2016; pp. 14–204.
17. Hen, E. Choroby Cywilizacyjne Przyczyny i Leczenie. Available online: https://www.medonet.pl/zdrowie,choroby-cywilizacyjne-przyczyny-i-leczenie,artykul,1735188.html (accessed on 8 December 2020).
18. Cele Zrównoważonego Rozwoju. UNIC Warsaw. Available online: http:www.un.org.pl/ce11# (accessed on 8 December 2020).
19. Alarmujące Dane UNICEF-u. Do 2030 r. 167 mln Dzieci Będzie Żyło w Ubóstwie. Available online: https://businessinsider.com.pl/finanse/raport-unicef-na-temat-ubostwa-wsrod-dzieci/rnrbm9c (accessed on 8 December 2020).

20. MOP: 2,5 mln Bezrobotnych Więcej na Świecie. Szokujące. Available online: https://www.money.pl/gospodarka/mop-25-mln-bezrobotnych-wiecej-na-swiecie-szokujace-6470438699955841a.html (accessed on 8 December 2020).
21. Barkatullah, A.H. Djumadi Does self-regulation provide legal protection and security to e-commerce consumers? *Electron. Commer. Res. Appl.* **2018**, *30*, 94–101. [CrossRef]
22. Pizzi, G.; Scarpi, D. Privacy threats with retail technologies: A consumer perspective. *J. Retail. Consum. Serv.* **2020**, *56*, 102160. [CrossRef]
23. Bandara, R.; Fernando, M.; Akter, S. Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *J. Retail. Consum. Serv.* **2020**, *52*, 101947. [CrossRef]
24. Balapour, A.; Nikkhah, H.R.; Sabherwal, R. Mobile application security: Role of perceived privacy as the predictor of security perceptions. *Int. J. Inf. Manag.* **2020**, *52*, 102063. [CrossRef]
25. Hong, I.B.; Cha, H.S. The mediating role of consumer trust in an online merchant in predicting purchase intention. *Int. J. Inf. Manag.* **2013**, *33*, 927–939. [CrossRef]
26. Wu, I.-L.; Chiu, M.-L.; Chen, K.-W. Defining the determinants of online impulse buying through a shopping process of integrating perceived risk, expectation-confirmation model, and flow theory issues. *Int. J. Inf. Manag.* **2020**, *52*, 102099. [CrossRef]
27. Riegger, A.-S.; Klein, J.F.; Merfeld, K.; Henkel, S. Technology-enabled personalization in retail stores: Understanding drivers and barriers. *J. Bus. Res.* **2021**, *123*, 140–155. [CrossRef]
28. Samonas, S.; Dhillon, G.; Almusharraf, A. Stakeholder perceptions of information security policy: Analysing personal constructs. *Int. J. Inf. Manag.* **2020**, *50*, 144–154. [CrossRef]
29. Bush, D. How data breaches lead to fraud. *Netw. Secur.* **2016**, *2016*, 11–13. [CrossRef]
30. Sullivan, C. EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of persona data in the IoT era. *Comput. Law Secur. Rev.* **2019**, *35*, 380–397. [CrossRef]
31. Stitilis, D.; Laurinatis, M. Treatment of biometrically processed personal data: Problem of union practice under UE personal data protection law. *Comput. Law Secur. Rev.* **2017**, *33*, 618–628. [CrossRef]
32. Wu, D.; Moody, G.D.; Zhang, J.; Lowry, P.B. Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention. *Inf. Manag.* **2020**, *57*, 103235. [CrossRef]
33. Berger, J. Ponad 90% Polskich Internautów Robi Zakupy w Sieci—Raport Trusted Shops. Available online: https://business.trustedshops.pl/blog/zakupy-polakow-w-sieci-raport-trusted-shops/ (accessed on 7 August 2020).
34. Bałut, D. Raport TestArmy Stan Cyberbezpieczeństwa Polskiej Branży E-commerce. Available online: https://testarmy.com/app/uploads/2018/09/raport_testarmy__stan_cyberbezpiecze__stwa_polskiej_bran__y_e-commerce_2018-1.pdf (accessed on 23 June 2020).
35. Redakcja Orange.pl Największe Ataki Hakerskie w Historii. Available online: https://www.orange.pl/poradnik/twoj-internet/najwieksze-ataki-hakerskie-w-historii/ (accessed on 4 February 2020).
36. Bezpieczny Handel w Internecie. Pierwsze Badanie Zjawiska Oszustw Płatniczych w Polskim E-Commerce. EY Building a Better Working World. Available online: https://www.ey.com/Publication/vwLUAssets/Bezpieczny_handel_w_internecie/$File/EY-Raport-Bezpieczny-handel-w-internecie.pdf (accessed on 23 June 2020).