INTERNATIONAL JOURNAL OF BUSINESS EDUCATION AND MANAGEMENT STUDIES (IJBEMS)
A Peer Reviewed (Refereed) International Journal
Impact Factor 4.308 | http://www.ijbems.com | ISSN:2941-9638
Vol. 9. Issue 1. 2023 (September)

SAFETY AND SECURITY POLICIES OF ONLINE STORES: BASIS FOR ENHANCEMENT OF RISK MANAGEMENT PROGRAMS

Ceazar Jose H. Leyba, MBA

AMA University School of Graduate Studies, Quezon City, Philippines
cjleyba555@gmail.com

Dr. Richard Oliver F. Cortez
AMA University School of Graduate Studies, Quezon City, Philippines
richardoliverc@gmail.com

ABSTRACT

Online shopping has undergone remarkable growth over the past decade due to the fact thatit is a more inexpensive and convenient form of purchase than traditional shopping. Initially, however, the move from one buying method to a more current one produced fear among customersregarding the following: exposure of personal information, online fraud, inconsistency between requested and desired product quality, unsuccessful shipping, etc. People purchase via the Internet for a variety of reasons, including the opportunity to buy anything at any time without physically visiting a store or the possibility to get the same goods at a cheaper price by comparing multiple websites simultaneously. The goal of the study was to identify the variables that influence consumers' willingness toengage in online purchasing. These were taken into consideration when devising tactics to boost levels of satisfaction and trust. It specifically attempted to achieve the following goals: 1.) To showthe business profiles of the online stores in terms of the following. 2.) To know the extent on which the online stores impose the above-mentioned safety and security policies as part of risk management. 3.) To determine the frequency of occurrence of the threats that hinder an effective risk management. 4.) To gather the remedies recommended by the online stores to improve risk management. 5.) To know the effectiveness of the above-mentioned recommendations as part of risk management. 6.) To enhance the risk management program coined by the researcher as “CJLEnhanced Risk Management Program”. In this study, the descriptive methodology was used. The main tool utilized to get data from the 150 respondents was a structured questionnaire. In order to supplement the responses provided on the survey questionnaires, interviews were conducted at random with the owners, IT personnel, or managers. The percentage, weighted mean, Likert scale, ranking, are the statistical tools used to present, analyze, and interpret the data. The following were the most important findings: 1.) The findings suggest that the implementation of secure log-in authentication, secured payment processing, and technical training for employees indicates a strong commitment to risk management. 2.) The findings showthat identity theft is the most frequent threat in online stores, followed by data breaches and payment processing issues. By implementing measures to prevent identity theft, such as secure login procedures and encryption of customer data, businesses can mitigate the risks associated with online transactions. 3.) The top three remedies recommended are the use of a good collection method, credit history checking of customers, and changing passwords regularly. These methods contribute significantly to risk management by protecting customer information and preventing unauthorized access. 4.) Changing passwords regularly, using good collection methods, and restricting access to data while enabling virus protection from reputable vendors are proven to beeffective in ensuring safety and security in online stores.

INTRODUCTION

Electronic marketing Online shopping has experienced tremendous growth over the past decade due to the fact that it is a more economical and convenient method of purchasing than traditional shopping. Initially, however, the transition from one purchase method to a more modern one created apprehension among customers regarding the following: exposure of personal information, online fraud, inconsistency between ordered and desired product quality, unsuccessful shipping, etc. People purchase via the Internet for a variety of reasons, including the ability to buy anything at any time without physically visiting a store or the ability to find the same product at a reduced price by comparing multiple websites simultaneously (Vasic et al., 2019).

The development of Internet technology has made online purchasing more popular than traditional methods. Therefore, the new technological development must accommodate the assurance of secure transactions (Tham et al., 2019). Customer satisfaction is directly linked to how safe an online purchase is. Still, this connection is not very strong. Most studies show that security has a big effect on customer satisfaction, but this find is a little bit different. A study done in South Africa found that most people do not want to shop online because they are afraid of scams, theft, credit card use, hackers, and dishonest salespeople. For these customers, security is something that goes without saying, so it does not make them feel too happy. But if this part was removed, it would make a big difference in how happy people were. Security is very important to get more customers, so online shops should work harder to make their sites safer. One way to make a website more trustworthy is to buy the appropriate certificate that will make the website safer. For example, a business that edits and proofreads English documents bought the VeriSign SSL Certificate, which is a certificate of the highest level of trust, and their sales went up by 27%. When an online business has a certificate, the address bar of their website is green and their web names start with https://. This shows that the website is safe and can be trusted (Vasic et al., 2019).

Online users should be aware of the risks associated with online transactions, just as they must take security precautions when purchasing in traditional stores. However, this is not the only privacy concern we should consider. Due to Data Privacy, we emphasize the significance of safeguarding privacy when shopping online. Web perils have expanded beyond malware and scams. Attackers are aware that the more a person engages in online activities, the greater the risk of revealing personal information, particularly when one is looking to make a purchase.

Now that data breaches, hacking, and identity theft are more prevalent, online consumers should take precautions against attacks that could compromise their privacy. There are a variety of methods that can be used to compromise a user's privacy, and an uninformed user will eventuallyencounter threats such as phishing, online scams, spam, Internet fraud, and malicious websites.

Today, online purchasing has become a dominant alternative shopping platform with which traditional retailing would have a difficult time competing. However, those who have never shopped online before may consider this platform to be hazardous. Therefore, consumers with little to no online purchasing experience are more risk-averse than those with more experience.

Inexperienced consumers may be attracted to functions such as consultation and guidance, caretaking and safeguarding, and hospitality when learning to transact on an e-commerce platform.These features are essential for introducing novices to online transactions by assisting them in overcoming obstacles caused by their inexperience (Naseri et al., 2021).

In addition, consumers will have a high level of digital trust in a brand or company when it demonstrates the ability to provide safety, privacy, security, dependability, and data ethics with its online programs or devices. Digital trust is essential because it distinguishes between reliable and unreliable services (Lim, 2021).

It is simpler and more profitable to obtain credit cards in the name of another person, run up large bills, and then vanish. It is known as identity theft, and it is a rapidly expanding crime. Bands of criminals would explicitly break into homes to steal checkbooks, credit card statements, receipts, and other financial mail. Seeking social security numbers, birth dates, locations of employment, and account numbers. Thousands of cases of identity fraud were reported annually (Schneier, 2017).

According to a survey, none of the respondents strongly concurred that the payment system for online shopping is highly secured. Only 15% of respondents concurred that the online paymentsystem is highly secure, while 27.5% disagreed. The majority of consumers believe that the payment mechanism for online shopping is not secure, which is a major concern. Typically, they prefer not to use their credit or debit card when purchasing online. Businesses should introduce new and enhanced technologies to build consumer confidence in the payment system (Rahman etal., 2018).

Users must be educated on the laws and policies governing customer data. Inform both the consumers and employees about the information security practices. Inform them on how to safeguard credit card information and what they should do to maintain the security of their own financial information. Highlight the organization's data security best practices and instruct them not to disclose sensitive information via email, text, or chat. Employees must also be trained on the steps required to safeguard customer information. Instruct them to adhere to mandated security protocols and policies in order to safeguard the business from potential legal ramifications (Danielson, 2023). Today's cybercriminals exploit an apparently endless supply of zero-day vulnerabilities using automated tools. Despite the broad availability of security and anti-fraud solutions, the fundamental architectures of traditional signature and policy-based solutions lack the intelligence and proactive adaptability required to effectively defend against advanced attacks. Due to the heightened threat environment of today, businesses can no longer afford to gamble. They must prepare to play a new game requiring sophisticated skill and strategy.

The Research Objectives

The researcher specifically intends to accomplish the following objectives:

1. To show the demographic profiles of the business respondents as to Nature of products sold, Size of the business, Number of years in operation, and Average gross sales.
2. To know the extent on which the online stores impose the safety and security policies as part of risk management.
3. To determine the frequency of occurrence of the threats that hinder an effective riskmanagement.
4. To gather the remedies recommended by the online stores to improve risk management.
5. To determine the effectiveness of the above-mentioned recommendations as part of risk management.
6. To gather the recommendations from the respondents on how to avoid the risks and improve customer satisfaction
7. To enhance the risk management program coined by the researcher as “CJL 24- point Management Program”

Selected Literature Review

The reviewed literature and studies emphasize raising store owners' awareness by teaching them the fundamentals of secure online behavior. Phishing and social engineering are older techniques that are still effective and should be made known to employees. On the software and hardware levels, more work is required to make the system resistant to malicious attacks associatedwith contactless payment transactions.

According to Eilhardt’s (2022) study, businesses were beset by fraud, chargebacks, and overall risk prior to the development of contactless payment systems. Today, business owners and consumers face credit card fraud involving the theft of card information. Or, even more questionable, utilize the stolen information to make fraudulent online purchases. Which ultimately leads to an increase in abuse cases and chargebacks, which harms businesses. Her article mentioned that business owners have access to a variety of fraud prevention tools to promote safeonline purchasing. Among the available programs for detecting fraud are those that combine machine learning algorithms with manual rules. These systems can compare the country where thecard was issued to the actual location of the user, analyze email addresses and purchase behavior, and process data in real time. Therefore, if you are going to take a variety of cashless payment methods, you should invest in fraud detection software to identify and eliminate business fraud risks.

According to the findings of a number of studies, it is necessary to take an exhaustive approach to both planning and carrying out the deployment of safe online payment alternatives on websites. This process begins with selecting a payment processor, continues with the elimination of system vulnerabilities through routine security audits, and concludes with the timely updating of all software that is used to run your website in order to protect the privacy and safety of your clients. There are measures that can be taken to safeguard one's online reputation from damage caused by fraud and also to increase the safety of financial transactions conducted online.

Studies done in the past, such as the one that was carried out by Tran and Nguyen (2020), have noted that business owners need to have a firm understanding of the nature of online transactions, which is that customers and businesses engage and transact primarily through the use of websites and interfaces. As a consequence of this, managers need to carry out duties with the primary intention of establishing trust and providing customers with a sense of security. To begin, online retailers should make every effort to grow their product portfolios on their websites. This can be accomplished by offering comprehensive information about businesses, products, purchasing rules, and a hotline number. This will increase customers' cognitive trust in the store. In addition, having a Facebook account or a profile on LinkedIn might be of great assistance in establishing massive trustworthiness. The study also stated that websites and interfaces need to be invested in and modernized in order to secure the safety of customers from hackers. This is particularly important when considering the encroachment of personal information or taking advantage of online shopping websites in order to make money or cause customers to lose money. The construction and promotion of the image of the company should always be maintained by the images, achievements, or benefits that bring customers honestly, and always take customer needs to set up the operational goal, as well as creating the sustainable development for future transactions for both parties. In addition, the image of the company should be constructed and promoted in a way that creates a win-win situation for both parties. In conclusion, in order to demonstrate improved operational performance, the completion and creativity of the sales form need to be demonstrated by recording any comments, ideas, or complaints received from customers.

Although it requires businesses to make some additional expenses, this method has become the industry standard for providing customers with safe and secure online payment options. This capability gives companies an advantage over rival websites in terms of competition for customers'attention and spending.

Customers and your company can be shielded from harm if you facilitate safe and secure online purchasing and offer a variety of encrypted online payment solutions. In addition, the use of these strategies presents the opportunity to optimize the sales funnel while simultaneously attracting newcustomers.

Other researchers have discussed the dangers posed by harmful attacks from malware and other third parties that can jeopardize the safety, security, and integrity of data. Techniques such as phishing and adware infections are included in these attacks, but they are not the only ones. Asa direct result of this, there have been multiple breaches of data, some of which have even damagedrespectable companies like Amazon and Google. Because of the prevalence of instances of fraud, individuals continue to exercise caution when considering whether or not they should switch to doing their shopping online. The majority of concerns are reasonable given that purchasing anything online entails the handling of financial transactions, while some are the result of a lack of adequate information. The security of online purchasing via ecommerce sites will be improvedif appropriate knowledge on cyber security concerns that can harm customers is provided, and theassociated awareness of end users will eliminate negative attitudes.

Nevertheless, despite the fact that previous research have been conducted, there are still a limited number of empirical studies on the influence of upgraded policies on safety and security as a basis for development of risk management programs. Research should be conducted focusingon aspects of the protection of online transactions that are not technological in nature.

In a nutshell, the bulk of the studies concentrate on safety and security, which is of the utmost significance in online stores because it serves to safeguard both the companies and the customers. There are many dangers that come with shopping online, including the possibility of having personal information stolen, falling victim to fraud, and even having their data compromised. Strong security measures should be used by firms in online stores in order to guarantee customers' safety and peace of mind. This involves the utilization of safe payment gateways that encrypt important consumer information in order to shield it from the possibility of cyberattacks. In addition, companies should frequently upgrade the software and systems they use in their operations in order to address any vulnerabilities that could appear.

Protecting the privacy of customers' personal information is an essential component of the safety and security offered by online retailers. To secure the personal information of their customers and prevent such information from falling into the wrong hands, businesses have a responsibility to comply with all applicable data protection laws and regulations, such as the General Data Protection Regulation (GDPR).

In addition, online retailers should adopt stringent authentication procedures in order to confirm the consumers' identities and prevent unauthorized access to user accounts. This can involve two-factor authentication, in which consumers are asked to submit an additional verification element, such as a code texted to their mobile device in addition to their password. This can be done in conjunction with traditional password-based authentication.

In addition, a study discusses how it is essential to educate clients about best practices for internet security in order to guarantee their safety online. Businesses have a responsibility to make available materials and information that teaches customers how to generate secure passwords, identify phishing efforts, and refrain from clicking on questionable links. Online retailers should routinely check their systems for any unexpected transactions in order to improve customers' sense of safety and security.

Theoretical Framework

The NIST defines the framework's core as a collection of cybersecurity activities, desired outcomes, and informative references pertinent to all critical infrastructure sectors. The Core presents industry standards, guidelines, and practices that enable communication of cybersecurity activities and mission objectives from the executive level to the implementation/operations level across the entire organization. The NIST CSF categories, or essential functions, contribute to the development of a solid business foundation and aid in identifying legal and regulatory requirements for cybersecurity.

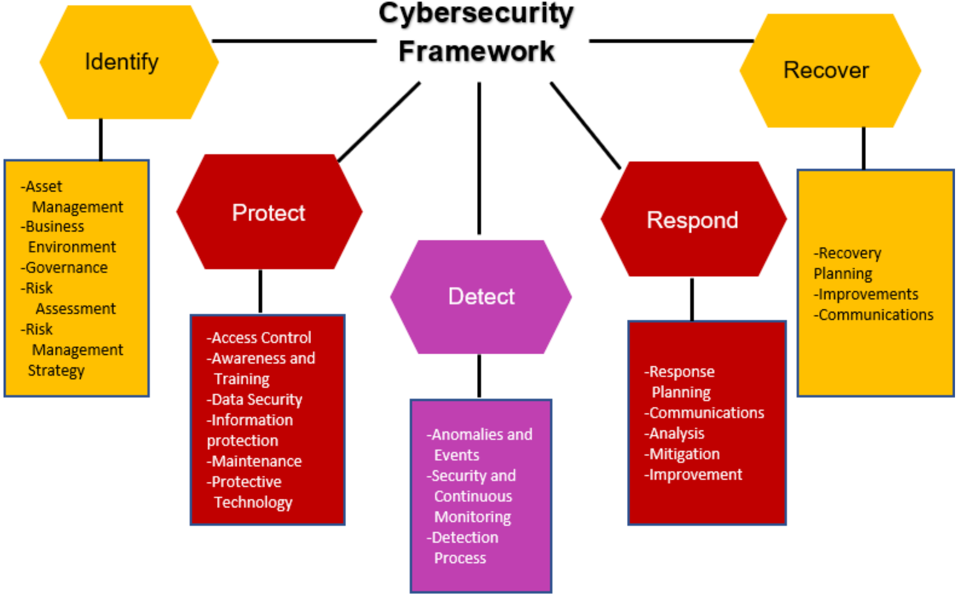

Figure 1. National Institute of Standards and Technology Framework

Identify

The NIST defines the Identify function, the first function of the framework, as requiring the development of organizational comprehension to manage cybersecurity risk to systems, assets,data, and capabilities. The emphasis is on the business and how it relates to cybersecurity risk, taking the available resources into account. This function provides the groundwork for future cybersecurity actions within your organization. Determining what environments exist, what hazards are associated with those environments, and how it relates to your business objectives is crucial to the Framework's success. Successful implementation of the Identify function enables organizations to comprehend all assets and environments outside the enterprise, define the current and desired states of controls to secure those assets, and devise a strategy to transition from the current to the desired state of security.

Protect

Protect is an essential function of the Framework Core because its purpose is to design and implement appropriate safeguards to ensure the delivery of critical infrastructure services. This Function facilitates the capacity to limit or contain the impact of a potential cybersecurity incident.

Where Identify primarily concentrates on baselines and monitoring. Protect is the proactive phase of the Framework. The Protect function encompasses categories such as access control and education and awareness. Multi-factor authentication practices to control access to assets and environments and employee training to reduce the risk of accidents and socially engineered vulnerabilities are examples of these categories and the Protect function as a whole. As data breaches become more prevalent, implementing the appropriate protocols and policies to reduce the risk.

Detect

The Detect function necessitates the formulation and execution of the necessary activities to identify the occurrence of a cybersecurity event. The Detect feature allows for the timely detection of cybersecurity events. The Detect function of the Framework Core is a crucial component of a robust cyber program; the quicker a cyber event is detected, the quicker its consequences can be mitigated. Detecting an intrusion or event can mean the difference between life and death for your business, making the Detect function of the Cybersecurity Framework essential for both security and business success. Implementing these standards, best practices, and solutions will assist you in scaling your program and mitigating cyber-security risk.

Respond

This function is defined as the creation and execution of appropriate actions in response to a detected cybersecurity incident. The Respond Function aids in mitigating the effects of a potential cyber security incident. It employs response planning, analysis, and mitigating activities to ensure that the cybersecurity program is continually enhanced. Adopting the Respond function necessitates the creation of an incident response plan, which ensures conformance with reporting requirements and their encrypted and secure transmission for a given location and industry. An excellent next step is to develop a mitigation strategy.

Recover

Recover is defined as the requirement to develop and implement the appropriate activitiesto maintain resilience plans and restore any degraded capabilities or services caused by a cybersecurity incident. The Recover Function facilitates a prompt return to normal operations to mitigate the effects of a cybersecurity incident. This function is important not only to the business and security team, but also to consumers and the market. Internally and externally, businesses are in much better positions if they recover quickly with grace and discretion. Aligning a recovery plan will aid in ensuring that, in the event of a data breach, the organization will be able to continuepursuing its goals and objectives and draw essential lessons.

Conceptual Framework

An important thing to be done during the process of coming up with an effective risk management program is knowing what are the most common safety and security being implemented by the online store owners. It is also vital to know the extent of imposition of these policies as well as the frequency of occurrence of the threats that hinder risk management. The research paradigm below shows what the conceptual frameworks wants to communicate. The researcher will apply the Input-Process-Output model in the study.

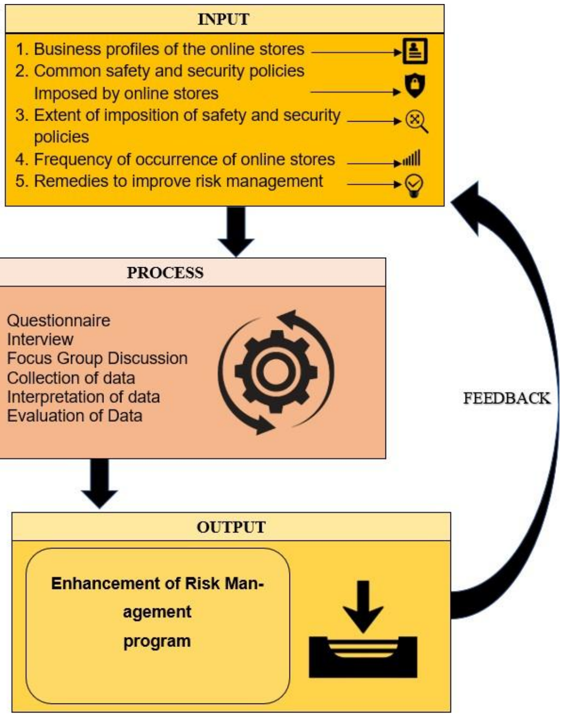
INPUT
1. Business profiles of the online stores
2. Common safety and security policies Imposed by online stores
3. Extent of imposition of safety and security policies
4. Frequency of occurrence of online stores
5. Remedies to improve risk management
PROCESS
1. Questionnaire
2. Interview
3. Focus Group Discussion
4. Collection of data
5. Interpretation of data
6. Evaluation of Data
FEEDBACK
OUTPUT
Enhancement of Risk Man-agement program

Figure 2. Paradigm of the Study

The Figure illustrates the paradigm of the study using the INPUT-PROCESS-OUTPUT scheme. The first box is labeled INPUT, consisted Business profiles of the online stores, Commonsafety and security policies imposed by online stores, Extent of imposition of safety and security policies, Frequency of occurrence of online stores, and the Remedies recommended to improve risk management

The second box is labeled PROCESS, consisted of the Evaluation of the common safety and security measures, and how to improve risk management through the utilization of the following Data gathering Instruments: 1.) Questionnaire 2.) Interview 3.) Focus group discussion, and 4.) Documentary analysis. Also included here is the application of statistical tools.

The Third box is the OUTPUT or the outcome which develops an enhancement of risk management program. The small box on the side is the FEEDBACK or information about reactionsto the recommendations that was gathered to be used as a basis for improvements of the risk management program.

METHODOLOGY

The research methods to be utilized for this study are discussed. This will cover the demographic and sampling method, a description of the respondents, a research instrument, the procedure for data collection, and statistical analysis of the data. The researcher will use the Descriptive Method, inferential, and Quantitative research designs to collect the necessary data because this method of research is a fact-finding study with adequate and precise interpretation of the results. It aims to determine "what exists" or what a phenomenon necessitates. Since the focusof this study is the safety and security policies for enhancing the risk management program of online stores in the city of Manila, the descriptive method of research is the most appropriate approach for drawing conclusions and making suggestions.

Respondents of the Study

The 102 online This investigation will target one hundred fifty online store owners in thecity of Manila. Since there are numerous online stores in Manila and it is impossible to collect datasimultaneously, the researcher chose cluster sampling.

The cluster sampling technique will be used in the study. It is a probability sampling technique usually used to study large populations geographically dispersed. In this study, 150 online store owners were recruited. Using the fishbowl technique, the researcher will list all the 16 areas in the city and put them in the bowl. The areas represent the clusters for the city of Manila. Among the 16 areas, the researcher randomly selected five areas that will be the focus of the study. Binondo, Malate, Sampaloc, Sta. Mesa, and Sta. Cruz are Five areas randomly selected. From here, online store owners from these areas were sent a letter requesting permission to conduct the study and questionnaires. Furthermore, participants were given a variety of methods for obtaining surveyapproval, such as messenger or email.

Data Gathering Instruments

The researcher combed through various works of literature and studies pertinent to the study as she prepared the instrument. The identified studies and writings served as the foundation for efficiently creating and drafting the instrument. Then, the researcher used the following tools to collect the necessary data:
.

Documentary analysis. The researcher will consult a vast amount of pertinent literatureand studies that aided in the analysis of data collected by other research instruments.

Questionnaire. The researcher will collect data through the use of a survey questionnaire. It intended to determine the safety and security of the online stores. The first section provides information on the respondent's nature of business, size of the business, years in operation, and average net income for the past 5 years. The second section provides information on the common safety and security policies imposed by online stores as part of risk management, the extent on which the online stores impose the safety and security policies, frequency of occurrence of the threats that hinder risk management, and the specific remedies recommended by the online storesto improve risk management. The collected information from the respondents was analyzed, arranged, and interpreted.

Interview. The researcher will conduct both unstructured and structured interviews. The structured type was conducted personally, but informally, to supplement the responses on the quantitative portion of the questionnaire and cast light on certain issues that were not adequately addressed by the interviewees. For the qualitative portion, respondents were asked about their specific recommendations to improve risk management in a structured interview. The interview was conducted as a methodical means of conversing with and listening to respondents, as well as a means of gathering information from them through conversation. The respondents were regardedas the primary source of data for the study because interrogating them allowed for the collection of data and the acquisition of information regarding their assessment of their own safety and security policies.

Statistical Tools

To assure validity, reliability, and interpretability, questionnaire data will be aggregated, tabulated, and statistically processed. The researcher employed the following statistical methods.

Frequency and Percentage Distribution. This will be used to determine the business profiles of the online stores, common safety and security policies imposed by the online stores. Percentage is defined as a number expressed as 100. It has been used to represent numbersfrom 0 to 1 and is used to compare things.

In this study, percentages will be applied to analyze responses to questions related to respondents' characteristics such as nature of business, years in operation, size of the business, average net income, as well as the common safety and security policies imposed by online stores.The value is the frequency of occurrence of each variable and the total value is the sum of the frequencies.

Weighted Mean. To know of to what extent do the online stores impose the safety and security policies as part of risk management as well as the frequency of occurrence of the threats that hinder an effective risk management, the weighted mean will be used used. The responses ofthe respondents were put into five categories and were provided with corresponding weight. Thenthe weights were multiplied by the number of replies in each group and were added and then divided from the total of the product.

Ranking. In this study, the percentile rank is to be used to rapidly determine how a particular score compares to other scores in a distribution of scores for business profiles and for the common safety and security policies imposed by online retailers. This type of inferential statistic is also used to compare the weighted mean of the extent of imposition of safety and security to the other scores in a score distribution. In statistics, percentile rank refers to the proportion of scores that are equal to or below a specified score. Similar to percentages, rankingsrange from 0 to 100. It is the data transformation that replaces numerical or ordinal values with their rank when sorting data.

Likert Scale. To be considered correct on the rating scale, the five-point Likert scale method of measuring to what extent do the online stores impose the above-mentioned safety and security policies as part of risk management. The scale was also used to determine the frequency of occurrence of the threats that hinder an effective risk management. Each statement has Five responses, which were classified under the degree of extent from “5” which means To a Great Extent down to “1” which means To No Extent.

The equivalent point given to each item showed the degree of extent of the safety policies or frequency of occurrence of the threats and viewed by the respondents to be obtained by estimating weighted average which became the verbal description.

RESULTS

Summary of Findings

This study was carried out in order to enhance a risk management program that can be used to improve the safety and security policy of the onl9ne stores. The descriptive method of research was used, as well as the survey technique. The questionnaire and structured and unstructured interviews, which were used at random to elicit additional insights from respondents, were the primary data collection tools.

The selected respondents from selected areas in the city of Manila evaluated all of the indicators. Because of some restrictions and limitations, the questionnaires were distributed online via a survey platform. The questionnaire responses were supplemented with interviews conducted via phone calls, video calls, and messenger chat. The researcher arrived at the following conclusions based on the data gathered.

1. On the Profile of the Business as to Nature of Products Sold

There were 47 businesses or 31% who belongs to the "Food Product" category, 45 businesses or 30% who belongs to the "Physical Product" category, 30 businesses or 20% who belongs to "Services" category, and the last in rank are the businesses who belong to the "Consultancy" category with 6 respondents or 4%.

2. On the Profile of the Business as to Size of the Business

There were 65 businesses or 43% who belongs to the "Micro" category, 53 businesses or 35% who belongs to the "Small" category, 22 businesses or 15% who belongs to the "Medium" category, while the last in rank are those "large" with 10 businesses or 7%.

3. On the Profile of the Business as to Number of Years in Operation

There were 48 businesses or 32% who belongs to the "7 years and above" category, 40 businesses or 27% who belongs to the "1-2 years" and "3-4 years" category, and 22 businesses or14% who belongs to the "5-6 years" category.

4. On the Profile of the Business as to Average Gross Sales

There were 90 businesses or 60% who belongs to the "P 500,000 and below" category, 28businesses or 18% who belongs to the "P 600,000 – P 1,000,000" category, and 16 businesses or 11% who belongs to the "P 2,000,000 - P 3,000,000" and "P 4,000,000 and above" category.

5. On the extent on which the online stores impose the above-mentioned safety and security policies as part of risk management.

The first Three in rank on imposition of the safety and security policies are as follows: **a.** “Secured log-in authentication” with weighted mean of 4.11 and is interpreted as ”To a Large extent” **b.** “Secured payment processing” with weighted mean of 4.07 and is interpreted as ”To a Large extent”, **c.** “Technical training for employees” with weighted mean of 4.06 and is interpreted as ”To a Large extent.

6. On the frequency of occurrence of the threats that hinder an effective risk management

The first Three in rank in the frequency of occurrence are: **a.** “Identity theft” with a weighted mean of 3.74 and is interpreted as ”Often”, **b.** “Data breaches” with a weighted mean of 3.49 and is interpreted as ”Sometimes”, and **c.** “Payment processing issues” and “Fraudulentcustomers” both with weighted mean of 3.48 and interpreted as ”Sometimes”.

4. On the remedies recommended by the online stores to improve risk management.

The first Three in rank are: **a.** “Use of good collection method” with 118 responses or 14%, **b.**” Credit history checking of customers” and “Changing of password regularly” both with115 respondents or 13%, **c.** “Restriction of access to data” with 105 respondents or 12%.

5. On the effectiveness of the above-mentioned recommendations as part of riskmanagement.

The first Three in rank are: **a.** “Changing of password regularly” with a weighted mean of 3.49 and is interpreted as ”Effective”, **b.** “Use of good collection method” with a weighted mean of 3.43 and is interpreted as ”Effective”, **c.** “Restriction of Access to data” and “Enable virus protection from reputable vendors ” both with weighted mean of 3.39 and are interpreted as ”Effective”.

DISCUSSION

Conclusion

Based on the summary of findings from the data gathered, the following conclusions are drawn:

In conclusion, this data analysis indicates that a significant number of online businesses fall under the categories of "Food Product" and "Physical Product," making up 31% and 30%, respectively. This implies that consumers are increasingly relying on online platforms for purchasing such products. However, the lower representation of businesses in the "Services" and "Consultancy" categories highlights that these sectors may require further development in terms of online presence. In terms of safety and security, it is essential for all online stores, regardless of category, to prioritize robust measures in order to ensure customer trust and protect their personaland financial information.

The distribution of businesses across different size categories in the online store industry, it is evident that a majority of them fall under the micro and small categories. While the number of medium and large businesses is comparatively lower, it is important to recognize that all online stores, regardless of their size, should prioritize safety and security measures to protect themselvesand their customers from potential threats. Regardless of the size of the business, implementing robust security protocols, encryption techniques, and secure payment gateways is essential for creating a trustworthy and secure online shopping environment.

It is evident that a significant number of online stores have been operating for several years, indicating a certain level of trust and reliability. However, it should be noted that this data alone does not guarantee the safety and security of these online stores. While longevity could be an indicator of credibility, it is essential for consumers to consider other factors such as secure payment options, encrypted websites, customer reviews, and privacy policies when making onlinepurchases. Ultimately, it is crucial for individuals to exercise caution and thorough research beforeengaging in any online transactions to ensure their safety and security.

The data suggests that the majority of online stores fall within the "P 500,000 and below" category. While this may indicate a thriving market, it also raises concerns about the safety and security of these smaller businesses. With limited resources, they may struggle to invest in robustcybersecurity measures, making them more vulnerable to online threats. On the other hand, the smaller proportion of businesses belonging to higher income categories, such as "P 2,000,000 - P3,000,000" and "P 4,000,000 and above," suggests a potential correlation between higher financialcapacity and a stronger focus on safety and security. Nonetheless, it is crucial for all online stores,regardless of their income category, to prioritize safety and security measures to protect their customers' data and ensure a trustworthy online shopping environment.

The findings suggest that online stores are taking significant measures to ensure safety and security for their customers. The implementation of secure log-in authentication, secured payment processing, and technical training for employees indicates a strong commitment to risk management. These policies are viewed as being in place to a large extent, providing customers with peace of mind while engaging in online transactions. Nevertheless, it is important for onlinestores to continually assess and update their safety and security measures to keep up with evolving threats and protect against potential breaches. By prioritizing the implementation of these policies, online stores can foster trust and confidence among their customer base and ultimately enhance the overall shopping experience in the digital realm.

The findings show that identity theft is the most frequent threat in online stores, followedby data breaches and payment processing issues. This highlights the need for effective risk management strategies to ensure the safety and security of online stores. By implementing measures to prevent identity theft, such as secure login procedures and encryption of customer data, businesses can mitigate the risks associated with online transactions. Additionally, addressingdata breaches and fraudulent customers through regular security audits and strong authentication protocols can further enhance the safety of online shopping experiences. Overall, prioritizing safety and security measures is crucial for maintaining customer trust and confidence in online stores.

It is evident from the responses that online stores prioritize various measures to enhancesafety and security. The top three remedies recommended are the use of a good collection method, credit history checking of customers, and changing passwords regularly. These methods contributesignificantly to risk management by protecting customer information and preventing unauthorized access. Additionally, restricting access to data is also recognized as an essential measure to ensure the safety and security of online stores. By implementing these recommended remedies, online stores can instill trust and confidence in their customers, guaranteeing them a secure shopping experience.

Changing passwords regularly, using good collection methods, and restricting access to data while enabling virus protection from reputable vendors are proven to be effective in ensuring safety and security in online stores. These measures, with weighted means ranging from 3.39 to 3.49, indicate a high level of effectiveness. By consistently changing passwords, users can minimize the risk of unauthorized access to their online accounts. Employing good collection methods ensures that customer data is handled securely, reducing the chances of data breaches. Restricting access to data limits the number of individuals who can potentially compromise sensitive information. Lastly, enabling virus protection from reputable vendors helps prevent malware and other malicious threats from infecting online stores and compromising customer information.

Recommendation

Based on the findings and conclusions, the online store owners have recommendations when it comes to the safety and security policies that will enhance risk management programs.

It is noticeable that the "Services" and "Consultancy" categories have lower representation in the online business landscape. This indicates that there might be a need for further development in terms of online presence for businesses in the "Services" and "Consultancy" sector.Regardless of the category, online stores may prioritize safety and security measures. Robust security measures may be implemented to mitigate any potential risks and ensure a safe and secureonline shopping experience for customers. Additionally, safety and security may be prioritized for all online businesses, irrespective of their category.

Businesses in the online store industry, regardless of their size, may prioritize safety andsecurity measures. It is important to recognize that the majority of online stores fall under the micro and small categories. Even though the number of medium and large businesses is comparatively lower, they may not neglect the importance of securing their online platforms. Implementing robust security protocols, encryption techniques, and secure payment gateways is essential for creating a trustworthy and secure online shopping environment. By implementing robust security protocols, encryption techniques, and secure payment gateways, businesses may create a trustworthy and secure online shopping environment.

It is important to understand that longevity alone does not guarantee the safety and security of these stores. Consumers may consider other crucial factors such as secure payment options, encrypted websites, customer reviews, and privacy policies. Longevity may not be the sole basis for trusting an online store. Checking customer reviews and ratings may offer insights into the reputation and reliability of an online store. Stores may transparent and comprehensive privacy policy to demonstrate the store's commitment to protecting customer information. Consumers may take the necessary precautions and consider multiple factors to ensure their safetyand security when making online purchases.

Online stores, regardless of their income category, prioritize safety and security measures to protect their customers' data and ensure a trustworthy online shopping environment. However, due to limited resources, smaller businesses may struggle to invest in robust cybersecurity measures, making them more vulnerable to online threats. They may allocate necessary resources to implement cybersecurity measures that protect against a wide array of online threats. By doing so, they can ensure the safety of their customers' data and foster a trustworthy online shopping environment.

It is important that online stores may continually assess and update their safety and security measures in order to keep up with evolving threats. As technology advances, so do the tactics used by cybercriminals. By prioritizing the implementation of these policies, online stores can ensure that they are prepared to effectively respond to new risks and protect against potential breaches in the future. They may build trust and confidence among their customer base. This not only safeguards customer information but also enhances the overall shopping experience in the digital realm.

There may be a need for effective risk management strategies to ensure the safety and security of online stores. By implementing measures to prevent identity theft, such as secure loginprocedures and encryption of customer data, businesses can mitigate the risks associated with online transactions. Additionally, they may address data breaches and fraudulent customers through regular security audits and strong authentication protocols can further enhance the safety of online shopping experiences. Overall, safety and security measures may be prioritized as these are crucial for maintaining customer trust and confidence in online stores.

It is clear that online stores may prioritize safety and security measures to protect customer information and prevent unauthorized access. Online stores may limit access to data, which is recognized as a fundamental measure in ensuring the safety and security of the platform. By implementing these recommended remedies, online stores can greatly enhance trust and confidence among customers, offering them a secure shopping experience. It is recommended that they prioritize these remedies and implement them promptly. By instilling trust and confidence, online stores may attract more customers and ultimately drive higher sales.

By consistently changing passwords, users may significantly reduce the risk of unauthorized access to their online accounts. They may employ good collection methods to handle customer data securely and minimize the chances of data breaches. Online stores may implement strong encryption and following best practices for data storage to protect their customers' sensitive information. They may limit the number of individuals with access to sensitive information to reduce the risk of internal threats and data leaks. Access may only be granted to trusted personnel who have a genuine need for it. Overall, through the implementation of these measures, online stores may significantly enhance safety and security.

REFERENCES

Amoroso, D. L., & Lim, R. A. (2015). Exploring the Personal InnovativenessConstruct: The Roles of Ease of Use, Satisfaction and Attitudes. *AsiaPacific Journal of Information Systems*, 25(4), 662–685. https://doi.org/10.14329/apjis.2015.25.4.662

Aziz, N. N. A., & Wahid, N. A. (2017). Understanding Customer Behaviour Towards Online Shopping. *In 2nd Business Management and ComputingResearch Colloquium* (pp.164-168). http://dx.doi.org/10.6007/IJARBSS/v8-9/4689

Aziz, N. N. A., & Wahid, N. A. (2018). Factors influencing online purchase intention among university students. *International Journal of AcademicResearch in Business and Social Sciences,* 8(7), 702– 717.

Aziz, N.N.A., Wahid, N.A.(2018). Why Consumers are Hesitant to Shop Online:The Major Concerns towards Online Shopping. . *International Journal ofAcademic Research in Business and Social Sciences,*

Batongbakal, Luisito Jr.(2021, April 17). How to Use GCash: *A Complete Beginner's*

Bilgihan, A. (2016). Gen Y customer loyalty in online shopping: An integratedmodel of trust, user experience and branding. Computers in Human Behavior, 61, 103–113.

Bringula, Rex P. (2016). *Reasons for Non-Engagement in Online Shopping :Evidence from the Philippines.* 12(2), 17–30. https://doi.org/10.4018/IJEBR.2016040102

Bringula, Rex Perez. (2016). *Taxonomy of Factors Influencing Non-Use ofOnline Shopping of Students. Modern Applied Science*, 10(4), 119. https://doi.org/10.5539/mas.v10n4p119

Campbell, Patrick (2021, April 18). Importance of pricing: why pricing is important for saas and beyond. https://www.priceintelligently.com/blog/bid/157964/two-reasons-why- pricing-is-the-most-important-aspect-of-your-business

Caramela, Sammi (2021, May 1*). Elevating Expectations: 6 Ways Product Quality Affects Your Brand.* https://www.business.com/articles/5-reasons-why-product-quality-matters/

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Raghav Rao, H. (2016). Online shopping intention in the context of data breach in onlineretail stores: An examination of older and younger adults. Decision Support Systems, 83, 47–56.

Cheema, Umair, Rizwan,M.R., Durrani, J.F (2016). The trend of online shoppingin 21st century: impact of enjoyment in tam model. *Asian Journal of Empirical Research 3(2):131-141*. http://aessweb.com/journal- detail.php?id=5004.

Darji, Prachi (2021, May 18). *5 Most Common Problems faced by Consumerswhile Shopping Online.* https://www.myadvo.in/blog/5-most-common- problems-faced-by-consumers-while-shopping-online

Devanesan, Joe (2021, April 21). *The Philippines is going cashless.* https://techwireasia.com/2020/07/digital-payments-are-finally-soaring-in-the-philippines/

Dhiranty, A., Suharjo, B., & Suprayitno, G. (2017). An Analysis on Customer Satisfaction, Trust and Loyalty Toward Online Shop (A case study Of tokopedia.com). *Indonesian Journal of Business and Entrepreneurship*,3(2), 101–110. https://doi.org/10.17358/IJBE.3.2.101

Dungo, Fehl (2021, May 12). *Best Online Shopping Sites in the Philippines YouMust Visit in 2021*. https://philpad.com/online-shopping-sites-philippines/

Ecommerce Trends That Are Powering Online Retail (2021).

Ethridge, D. E. (2004). *Research Methodology in Applied Economics*. JohnWiley & Sons.

Evans, N, Bosua, R. (2017). Exploring innovation in regional manufacturing SMEs: Small Enterprise Research

Faqih, K. M. S. (2016). An empirical analysis of factors predicting the behavioral intention to adopt Internet shopping technology among non-shoppers in a developing country context: Does gender matter? Journal of Retailing andConsumer Services, 30, 140–164

Forsythe, S.M. and Shi, B. (2013). Consumer Patronage and Risk Perceptions inInternet Shopping. *Journal of Business Research, 56, 867–875*.

Forwardhttps://www.bigcommerce.com/articles/ecommerce/ecommerce- trends/

Fox, W. & Bayat, M. S. (2017). *A Guide to Managing Research*. Cape Town

Gnanadhas, M.E., Sunitha, C.K (2016). Online Shopping: A Overview. https://www.researchgate.net/publication/264556861_Online_Shopping_-_An_Overview/link/53e782fc0cf25d674ea59e7e/download.

Guide. https://filipiknow.net/how-to-use-gcash/#What_is_GCash

Hargrave, Marshall (2021, March). Electronic Retailing (E-tailing). https://www.investopedia.com/terms/e/electronic-retailing-e-tailing.asp

https://www.investopedia.com/terms/s/stakeholder.asp

https://www.investopedia.com/terms/a/anova.asp

Hunt, Tian (2021) 5 Creative Advertising Trends Seen in 2021 .Https://www.outbrain.com/blog/creative-advertising-trends/

Jain, Anamika S. (2021, April). *Top 10 Benefits and Disadvantages of OnlineShopping.* https://toughnickel.com/frugal-living/Online-shopping-sites-benefits#:~:text=Better%20prices.,coupons%20and%20rebates%2C%20as%20well

Jayasubramanian, P., Sivasakthi, D., (2015). A Study on Customer SatisfactionToward Online Shopping. *International Journal of Applied Research*, 5,489–495.

Kartiwi, M., Hussin, H. (2018). Impact of external factors on determining E-commerce benefits among SMEs in Malaysia

Katawetawaraks, C.,Wang, Chang Lu (2015). Online Shopper Behavior: Influences of Online Shopping Decision*. Asian Journal of BusinessResearch Volume 1 Number 2.* https://swsu.ru/sbornik- statey/pdf/Online%20Shopper%20Behavior%20Influences.pdf

Koch, Julia, Frommeyer, Britta., Schewe, Gerhard (2020). Online ShoppingMotives during the COVID-19 Pandemic—Lessons from the Crisis. *Center for Management of Muenster University.* https://www.mdpi.com/2071-1050/12/24/10247/pdf

Lufkin, Bryan (2020) *The curious origins of online shopping.* https://www.bbc.com/worklife/article/20200722-the-curious-origins-of- online-shopping

Mittal, Tarun (2021, April 20). *Common problems faced by customers while shopping online*. https://yourstory.com/2017/04/common-problems-online-shopping

Moon, N., Sultana, S., Nur, F.N., Saifuzzaman, M. (2017) .A Literature Review ofthe Trend of Electronic Commerce in Bangladesh Perspective.

Musa, H., Mohamad, M. A., Khalid, F. A., Rahim, N. A., Najihah, N., Zamri, A.,Fakulti, Teknologi, P., & Teknousahawanan, D. (2015). *Factors Affecting Customer Satisfaction towards Online Shopping*. 1–17.

Nguyen, H. T. (2014). Factors affecting customer satisfaction and trust in an e- commerce setting: A case study of Muachung.vn in Vietnam. *AU-GSB e- Journal*, 7(1), 43–52. http://www.assumptionjournal.au.edu/index.php/AU-GSB/article/view/446

Online Shopping – Definition and Meaning. Market Business News https://marketbusinessnews.com/financial-glossary/online-shopping- definition-meaning/

Purthi, C. D., & Gupta, P. (2017). *The Impact of Online Shopping on Customer Satisfaction in Mr . Chander Deep Purthi* , (research scholar). 5(5), 1–11.

Rabo, J.,Ang, M.l (2018). Determinants of Customer Satisfaction in a Philippine Retail Chain. DLSU Research Congress Journal. https://www.dlsu.edu.ph/wp-content/uploads/pdf/conferences/research- congress-proceedings/2018/ebm-13.pdf

resources/customer-satisfaction

Shanthi, R., Kannaiah, Desti (2016) Consumers' Perception on Online Shopping. *Journal of Marketing and Consumer Research www.iiste.orgISSN 2422-8451 An International Peer-reviewed Journal Vol.13, 2015*https://researchonline.jcu.edu.au/39753/1/Dr.%20Desti%20Consumers%20percep

Shergill, Gurvinder S.(2015). Web-based shopping: Consumers' attitudes towards online shopping in New Zeal**and. *Journal of Electronic*** Commerce Research. https://www.researchgate.net/publication/228620838

Tabaei, Z., Fathian, M., & Gholamian, M. R. (2011). Effective Factors onElectronic Customers Satisfaction. *3rd International Conference onInformation and Financial Engineering Journal*, 12, 579–582.

Tagam, R. G., Fini, L., Toling, R. E., & Veri, M. G. C. (2016). *Consumer Perception and Purchase Behavior on Online Shopping Among Studentsin Mindanao University* .October, 0–14. https://doi.org/10.13140/RG.2.2.23011.35362

tion%20on%20Online%20Shopping.pdf

Todd, Peter A.,Jaryenpaa, Sirrka L., (2015). Consumer Reactions to ElectronicShopping on the World Wide Web. *International Journal of Electronic Commerce Volume 1, 1996 - Issue 2.* https://www.tandfonline.com/doi/abs/10.1080/10864415.1996.11518283

Tram, Ngoc (2021, May 18). *Shopping Online: Common Problems Faced ByCustomers.* https://www.magesolution.com/blog/shopping-online- problems-customers-faced/

What is Customer Satisfaction. Learn About Quality. https://asq.org/quality-

Yen, Nguyen (2021, April 11). *Buying things on the Internet.* https://ieltsonlinetests.com/writing-correction/buying-things-internet-corrected-essay