International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 5, ISSN No. 2455-2143, Pages 1-5
Published Online September 2019 in IJEAST (http://www.ijeast.com)

IDENTIFYING RISKS AND SECURITY MEASURES FOR E-COMMERCE ORGANIZATIONS

Md Haris Uddin Sharif, Ripon Datta, Mounicasri Valavala
University of the Cumberlands
Williamsburg, Kentucky, USA

Abstract—**The objective is to identify the Risk in each layer and how to mitigate the risk, for an e-commerce based company called (e-global). For this we have built the strategies in how to mitigate risk and gave solutions to the e-global. In this paper plan will be leveraged more about the security measures in the following content. Growth in the online shopping spend has increased more than the retail stores ever before; online stores have opportunity to sell the products Globally without moving anywhere and without creating building stores, market places for customers to come and buy their products. As everything sold online there is whole lot Customer personal data is online and this is a risk for the online shopper to protect the customer data and their privacy online and financial data. To Maintain all these key data of the online shoppers the system which e-global is not sufficient for fraudulence ongoing to the online companies. For this we have come up with better security measures and control in each layer to stop the online fraudulence and data theft.**

Keywords—**E-commerce Risk, Online Shopping Growth, Security Policy, Administrative Controls, Physical Controls, Technical Controls, Legal Legislations, and regulations for E-commerce.**

I. INTRODUCTION

Brand promoting in web-based business can possibly round up a gigantic piece of that online gathering of people when executed rightly. A product with demand can increase the customers shopping if the organizations maintain customers' confidence in shopping their site. E-commerce Company must have a solid security program in place to address and mitigate the company against risks and threats up to an acceptable level. We made a powerful security approach that covers every one of the requirements of the association [1]. The security strategy recognizes authoritative, physically, and specialized controls that must be set up to distinguish security hazards and create relief techniques to limit the impacts of these dangers.

II. SECURITY POLICIES

Security policies are guidelines for maintaining and implementing the overall security program of an organization. Organizational assets can be classified in a wide range. They can be critical databases, applications or products, clients, employees, physical assets, critical data and so on. The security policy is a well-written document that comprises rules for a company to protect this information and assets. This document also mentions the priorities of different assets so that they can be easily protected during a crisis. Thus, a security policy is a "living record," implying that the report is never completed and is consistently updated as the business changes [2]. Below are some of the policies which should be reviewed thoroughly.

A. Physical Security Policy –

The physical security policy deals with concerns like employee safety, the physical identification of employees, safety of the building, and so on. Some examples of such policies are. Ensuring building security by setting up surveillance cameras, logbooks, employee keycards, and tokens, and others [2]. Unused workstations shall be disconnected and/or removed, lock the doors of empty offices. Backup data should be safely secured off-site.

B. Personnel Policy –

This includes rules which the employees are expected to follow to maintain the integrity and security of business information, company systems, and equipment. Below are few examples. Employees shall not leave their workstations unlocked. Mandatory employee security awareness training programs. Communication policy about the appropriate use of devices and company equipment. Rules to prohibit unauthorized access and data misuse by employees. No personal devices allowed on company premises.

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 5, ISSN No. 2455-2143, Pages 1-5
Published Online September 2019 in IJEAST (http://www.ijeast.com)

C. Network Security Policy –

Some common examples are. Blocking any network traffic, the source of which is a blacklisted IP address. Developing and implementing firewall strategies. When implementing new security systems and equipment, a thorough proper testing procedure shall be established. The firewall security policy is a main subset of the network security policy. It can be considered that network security is measured at a conceptual level and firewall security policies are measured at a technical implementation level. It consists of strategies to filter incoming and outgoing network traffic. A bad implementation of this policy will accept malicious content and reject useful data.

Firewall policies can mention strategies to allow or deny traffic by default. As per the allow by default rule, all type of network traffic or packets can pass through the firewall, and unwanted ones are explicitly denied [3]. This type of policy is unsafe or insecure because new and unrecognized content will pass through the firewall. As per the deny by default rule all packets are denied through the firewall and only selected ones are allowed to pass explicitly. This kind of policy is considered safe by nature because unidentified threats will automatically be denied access. The firewall policies are well maintained by the usage and requirements of the organization [3]. The policy implemented so that it takes one microsecond or even less for the packet to pass through the firewall. Drop templates are identified to manage the traffic dropped by firewalls. Only secure e-mail access should be allowed through the firewalls.

III. ADMINISTRATIVE CONTROLS

When it comes to Administrative controls, this assumes the hugest part in actualizing and upgrading the general security of the associations. The reason they are huge is that they are straightforwardly identified with customers and employees of the association which influences the general execution of the organization, in this case, the e-global should have administrative controls are the process of developing and ensuring compliance with policy and procedures [4]. The first order of administrative policies includes company policies and standards.

Making e-commerce site on a Platform that uses the sophisticated programming language would be more secure than the open-source platforms, the platforms which are sophisticated would give better security with two-level authentications. Provide security training for employees on sending the email or text with customer information in any communication platforms this should secure and monitored. Checking tracking numbers for all the orders which are shipped to the customers, this will be helpful for the shipping companies. Setting up alerts on suspicious activities like when multiple transactions coming from the same IP address, same person and card name and recipient name is different than cardholder name strong Passwords and complex logins on the front ends make harder for hackers and protect customer's information [5]. Storing sensitive data like Credit card details and CVV codes of customers in the database and purge the old data and keep minimal data about the customer like phone number just for chargeback and refunds. Using the secure socket layer connection for online checkout this will safeguard customers data, it's important to use SSL certificates to authenticate the identities and URL green bar, and SSL security mark would build confidence in customer to use your site.

IV. PHYSICAL CONTROLS

Physical Controls of e-commerce industry has been an area dealing with significant volume of threats and loss in terms of assets and equipment. Flash drives, PCs, tablets carry data that could be lost or stolen in context of transportability and versatile access. In the beginning of e-commerce transactions-based industry, there were extensively concentrated servers PCs basically utilized by a couple of individuals and were anchored in showcase [6]. Today, work regions are stacked with PCs and versatile workstations that can virtually connect systems and exchange information. Securing data and physical equipment is becoming challenging with customers moving their PC's from workplaces. Destruction of physical property with attacks like distortion, vandalism, any unplanned disaster around equipment, robbery end up being "personality boggling and dynamic" [6].

With the advancements in portable equipment like flash drives, PCs, tablets, phones the scope of threats to these devices goes up as well. Around 74,000 workers, providers, and temporary experts were influenced by an information break in 2014 due to stolen PCs with decoded particular information (Scott, 2014). For this scenario, the impact of cost was not the primary concern. A past delegate announced a real claim against Coca-Cola proclaiming it was tactless in anchoring information. Conditions now like never before should be worried over "physical robbery of contraptions and hardware" [7]. Telephones including PDAs, PCs, and hard drives make day to day life very easy and carry most of our personal data, thus making them more vulnerable and are defenseless against burglary.

Stolen mobiles are not the only major way that attackers can hack into personal information. With the device in hand, an attacker can download information from stolen device onto an unsecured computer/device. This can be mitigated by avoiding scenarios where an attacker can easily have access to one's device, for example, never leave a device with personal information in a location where an unauthorized group/user can access it. Another problem scenario is when a flash drive with unknown source of data is downloaded to a user's workstation by the user unbeknownst to the risk. This could potentially bring malware/virus to the user's system or wipe

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 5, ISSN No. 2455-2143, Pages 1-5
Published Online September 2019 in IJEAST (http://www.ijeast.com)

out the whole system with bad data. This sort of occasion occurred at a U.S. Specialist of Defense base in the Middle East in 2008.

A delegate working at the base embedded a wrangled USB memory stick into the association's workstation. The tainting spread undetected in both unclassified and planned structures and sent information back to remote servers in different nations. (Lynn III, 2010). The physical controls of e-commerce are often taken for granted since they don't deal with any technical protocols or security encryptions. Although the policies are often adhered to, this still doesn't completely prevent vandalism and other forms of distortion of assets. Affiliations reliably base on particular and managerial controls and thus, splits may not be found immediately [7]. Aggressors can get into anchored zones by hacking and tend to find the opportunity to control access cards or softening up through entryways.

Barriers or preventive measures for these dangers can be summed up to physical impedance ID frameworks, ready structures, and man traps. Control cases that could help stop burglary are the utilization of RFID frameworks and association locks. "Physical security ensures individuals, information, prepare frameworks, work environments and sidekicks resources" [6]. Techniques that physical security ensures these favorable circumstances is through "site structure and design, characteristic sections, crisis reaction status, preparing, get the chance to control, interruption affirmation, and power and fire affirmation" [6]. Business insight or disaster recuperation plots are required to diminish business interference in the midst of appalling event, effect or naughtiness. Implementation of one security measure cannot cover for other gaps in the industry.

Access Control Cards - These are settling to a client and must be swiped keeping in mind the end goal to secure passage. The downside to access control cards is that they can be easily stolen and used without any assistance while being a major factor of cast to locate or revoke the access. Biometrics - Uses a physical trademark, for example, a stand-out check or retina to see a client. Because of the cost of executing this game-plan, " [6] and operator protection issues, biometrics has not been generally perceived yet. Biometrics - Uses a physical trademark, for instance, a one of a kind check or retina to perceive a customer. Due to the cost of executing this course of action, "[6] and agent insurance issues, biometrics has not been for the most part recognized yet.

Without solid physical security and IT organization can devour incalculable risks in aspects of firewalls, and impedance premonition frameworks just to have secret information stolen by a hacker or malicious program. Encryption of devices is another closer step to ensure security because it reduces the risks of data access by unauthorized users. To quote scenarios where personnel with high access rights has left his/her workstation unsecured include an unsecured PC left by a specialist containing PII was stolen. Physical security packs must finish a security program that modifies prosperity tries and thriving concerns [6]. Physical security ought to always utilize what is known as a "protect all around" [7] way to deal with strengthening security through various controls.

V. TECHNICAL CONTROLS

At whatever point the client starts an association it needs to experience a progression of system security layers, for example, Firewalls IDS/IPS, DMZ, Cryptography/Encryption conventions, Audit logs, Alarms, and cautions. A firewall is simply program or hardware device that filters the information coming through the Internet connection into your private network or computer system [10]. If an incoming packet of information is flagged by the filters, it is not allowed through. It is designed to prevent unauthorized access to or from a private computer network. The static and dynamic standards the firewall permits/obstructs the activity.

Security in Network Layer -

Any scheme that is developed for providing network security needs to be implemented at some layer in protocol stack as depicted in the table below.

Layer	Communication Protocols	Security Protocols
Application Layer	HTTP FTP SMTP	PGP. S/MIME, HTTPS
Transport Layer	TCP /UDP	SSL, TLS, SSH
Network Layer	IP	IPsec

Table 1: Network Layers and Respective Protocols [8]

An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communications network. The application layer abstraction is used in both of the standard models of computer networking: Internet Protocol Suite (TCP/IP) and the OSI model. We are utilizing DMZ to include an extra layer of security to an association neighborhood; the approaching customer demand can get to just what is uncovered in the DMZ, though whatever remains of the association organize is firewalled using interior firewalls [8]. On the off chance that the information is permitted through the firewall the information is then handled through Network-based IDPS (Intrusion discovery and avoidance framework) [9]. This will choose whether to permit or square the association given the information/activity examination. They screen the occasions and investigate the information for any unapproved movement, and if it identifies any it drops the information.

IDPS logs record exercises of regulatory access and individual access of records and approaching and cordial network to the IDPS framework. We are utilizing solid security/cryptography convention called Kerberos [9]. This convention utilizes solid cryptography with the goal that a customer can demonstrate its personality to a server and server to customer over any system association. The customer and server scramble the correspondence for the protection, and just

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 5, ISSN No. 2455-2143, Pages 1-5
Published Online September 2019 in IJEAST (http://www.ijeast.com)

the server can unscramble it. The confirmations takes a shot at the customer/server favor a customer produce ticket and demand the administration. The server gets the ticket and unscrambles it and if it coordinates at that point stipends access to the administration [4]. After the traffic flows, it goes through all the security layers the information currently gets handled by the switch, and it courses the information to its goal. We are utilizing review logs to archive the client login data, timestamps and source and goal.

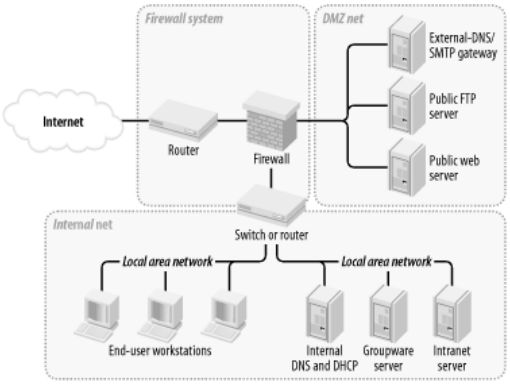

Figure 1: Network Structure [7]

As seen in the image above whenever the client initiates a connection, it must go through a series of logical/technical layers for securely transmitting and receiving of the data. This will prevent the unauthorized usage of the data. DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical sub network that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet. It confines the unapproved access of the information, and in addition on the off chance that somebody moves beyond through the DMZ they get experienced by the inner and outside firewalls which hinder the utilitarian necessities, including access controls, pattern designs, standards and channels, administrations, content limitations, and security and subtle confirmation elements [10]. A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through. It is designed to prevent unauthorized access to or from a private computer network [7].

VI. DISCUSSION

Every e-commerce legal and law terms conditions should outline that purchasers are going into an agreement to when they buy merchandise from your site. Outline the terms of conveyance, transportation, discounts and installments, prohibitions of risk, and terms of utilization for e-commerce business site. Moreover, e-commerce business legal and laws should be well explained for below issues.

Ecommerce Shipping and Delivery Policy, there are a few fundamentals that set an establishment for whatever remains of your delivery. Insights about fundamental transportation source/focus, for instance, where will you dispatch from? Do you have enough space? Guarantee your station is capable and your setup will get you in and out quickly. Which transporters will be used for transportation and conveyance? Do you use a close-by transporter or a national one? Shop around and guarantee you mastermind those rates. Rate number crunchers are the easiest way to deal with compose the right expenses for your shipments [11].

Consider realizing distinctive transportation rate other options to refuse tricking or undercharging customers who are close or to a great degree far off from you. The e-commerce site will have to mention how you speak with clients about shipments also automated messages don't have to debilitate. This will have what you incorporate with your shipments. Think about putting receipts, pack records, rules, or even altered notes in your cases. The web-based business may have how you encourage returns. Either join a name with your demand or be set up to send one when it's required. Influence your landing to approach clear and easy to find.

The important way to build trust with the client is refund policy while doing e-commerce business. It is insightful to be liberal in your refund arrangement, and client should get refund by promised time frame. We can request user to pay the cost of the profit as you're qualified for the product which you have anticipated [12]. Before going ahead with the pursue of any term by the user make sure the term and condition are set before buying of any the product with acknowledgment of the refund policy.

Protecting of Interests, the terms and conditions are fundamental for securing your business, and potentially your own, advantages when offering on the web. Now in the e-commerce market you could never experience question or challenges in the web-based business.

For standard e-commerce terms and conditions, every e-commerce business organization must have its standard e-commerce terms and condition that will be authored by state agency or local government agency will not violate any state laws and regulations. Standard Ecommerce Terms and Conditions must have explained details about information commensurate with latest consumer contract regulations, jurisdiction or choice of Law, Delivery Terms, liability limitations, what Happens and who pays for returns [13].

The law for all sites which is owned by the Owners of Ecommerce the data should be protected. When any user visits the business site, his information should safe and secure. (Ex. User identity and financial details. The organization must have online advertising compliance. E-commerce business website owner must think about the pertinent laws for internet promoting like conventional promoting for physical stores; online retailers should likewise conform to directions when publicizing on the web. The Federal Trade Commission (FTC)

controls for promoting are intended to ensure customers and to avert tricky and uncalled-for acts or practices.

VII. Conclusion And Future Work

E-commerce business organization has to details information for their client about how to collect taxes online. For e-commerce business owners will have to research how the state classifies a physical presence. In legal terms, it's called a "nexus," and each state defines nexus differently. The e-commerce site should have details about to handle customer financial data. Payment Card Industry (PCI) consistence is a term well-known to numerous individuals looking into web-based business directions. As an internet business webpage owner, one of the models you should think about is the Payment Card Industry (PCI), Data Security Standard (DSS) standard. All associations, including on the web retailers, must take after this standard when putting away, preparing and transmitting charge card information. The PCI Security Standards Council has established by various monetary organizations, including JCB International, MasterCard, and Visa that is in charge of the improvement and usage of security benchmarks for account information assurance. Through its PCI Security Standards that the association looks to improve installment account information security.

VIII. Reference

[1] Jennifer, S (2013) 15 Ways to Protect Your Ecommerce Site from Hacking and Fraud, CIO IDG. https://www.cio.com/article/2384809/e-commerce/15-ways-to-protect-your-ecommerce-site-from-hacking-and-fraud.html

[2] Paquet, C. (2013). Network Security Concepts and Policies, Cisco Press.

[3] Yadav, A. (2013), Network Design: Firewall, IDS//IPS, InfoSec Institute. Retrieved from

[4] Cohen, G. A. (2012). U.S. Patent Application No. 13/112,097.

[5] Infosec (APRIL 10, 2018)Firewalls, IDS, IPS, And The CISSP. http://resources.infosecinstitute.com/network-design-firewall-idsips/ - gref

[6] Harris, S. (2013). Physical and Environmental Security. In CISSP Exam Guide (6thed, pp. 427 502). USA McGraw-Hill.

[7] Zhang, F., Du, B., & Zhang, L. (2015). Scene classification via a gradient boosting random convolutional network framework. IEEE Transactions on Geoscience and Remote Sensing, 54(3), 1793-1802.

[8] Bradley, T. (2018). Introduction to Intrusion Detection Systems (IDS), Life wire.

[9] da Cruz, M. A., Rodrigues, J. J. P., Al-Muhtadi, J., Korotaev, V. V., & de Albuquerque, V. H. C. (2018). A reference model for internet of things middleware. IEEE Internet of Things Journal, 5(2), 871-883.

[10] Bradley, M. (2018). Durable solutions and the right of return for IDPs: Evolving interpretations. International Journal of Refugee Law, 30(2), 218-242.

[11] Walter, W., Morrison, I., Rieken, G., Thomas, M., & Toebben, S. (2014). U.S. Patent No. 8,825,854. Washington, DC: U.S. Patent and Trademark Office.

[12] Bradley,S. (2014). Physical Security. In Cehv8: Certified Ethical Hacker Version 8 Study Guide (pp. 393-409). Indianapolis, IN USA: Wiley

[13] Lynn III, W. J. (2010, September 30). Defending a New Domain. Retrieved from url: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

[14] Thea Earl [May 06, 2018] The Beginner's Guide to Ecommerce Shipping and Fulfillment. https://www.shopify.com/blog/14069585-the-beginners-guide-to-ecommerce-shipping-and-fulfillment