International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

Drivers and Impediments of Computer Security and e-Business Success

Seiyaboh Zideigha[1], Wari Denyefa C.[2], Adoubara Kakandar[3]
[1]Department of Mathematics/Computer Science, Niger Delta University, Bayelsa State, Nigeria
[2, 3] Department of Computer Science, School of Applied Sciences/ Federal Polytechnic Ekowe, Bayelsa State, Nigeria

ABSTRACT

In today's economy, information is one of the most important assets of an organization, probably second only to human resources. Information has become important both as input and output. Hence computer security is of great concern to companies and businesses that want to implement e-business. The internet, which is the primary medium for conducting e-business, is by design an open non-secure medium. Since the original purpose of the internet was not for commercial purpose, it was designed to handle secure transactions and one of the most important issues in e-business is security. This paper explores factors that influence customer's perceptions of security which influence the success of e-business in Nigeria and also outlines and analyses computer security with regard to online businesses. This is followed by an evaluation of the current tools and practices for ensuring computer security in e-business. The demerits of the present practice are also presented.

Keywords: Computer Security; E-Business; Internet; Transaction; Access Control

I. INTRODUCTION

1.1 What is Computer Security?

The process by which the data stored in a computer system cannot be compromised or read by anybody without permission is what is termed security or computer security. Most computer system security measures include data encryption and passwords. The translation of data/information into a form that is garbled without an unraveling mechanism. A password or sometimes called passkey is a shrouded word or phrase that gives a customer access to a particular program or system (Beal, 2017).

The world of computers and e-business technology is going through an era of electronic terrorism. It is a major problem that is potentially dangerous that it threatens the proper functioning of the computer system in information age (Ayeni, 2004)

(Ifinedo, 2006) states that businesses in Nigeria can increase their market reach, enhance customer's services and reduce both marketing and distribution cost through computers connected to the internet. It is virtually true that in today's environment, most businesses, government agencies, and many individuals now have their own websites for their daily transactions via the internet. But the internet services is prompt to vulnerabilities to compromise various insecurities and thefts. Although the original purpose of the internet was to move files among computers and to enable easy remote access to computers. More than anything else, simplicity and easy usability were among the main motivation for designing the internet. This has led to a simple scalable network design that offers best effort service, in which the network does not guarantee anything, not even the delivery of the data (Mathy et al, 2000).

Security, both for the internet and web is essentially an afterthought. The rapid proliferation of new software and communication systems has led to a state in which users are not fully knowledgeable about computer software and systems architectures. This makes users oblivious to a number of vulnerabilities that can lead to inadvertent security breaches or those that can be maliciously exploited. As a result demand for secure web services grows. Thus there is a need for protecting computers on the internet. There are a number of ways computers could be attacked by hackers, crackers, and disgruntled insiders. Common threats include hacking,

cracking, masquerading, eavesdropping, spoofing, sniffing, Trojan horses, viruses, bombs, and denial of services arising from computer usage.

Once information is kept on the internet, the protection of data in computer systems begins to pose challenges to companies and organizations. It is clear that when such data involves a financial transaction, there should be computer reliability.

For businesses, the competition would be on the basis of availability of information (Ayeni, 2004). Therefore hacking or eavesdropping of information being communicated from one organization to another can be a serious threat to business because of the impediments it might encounter.

Nigeria is rated the fastest growing telecommunication country in Africa (Ayo et al, 2007). And it appears the country have a situation that presents tremendous opportunities for global commercialization but this cannot be realized without a reliable supporting computer security framework. Protecting online assets and network resource is extremely important.

II. SECURITY MEASURES AS AN IMPEDIMENT

Security measures are supposed to deny access to unauthorized users who try to break the protocol to access information; but because of poorly integrated and ad-hoc solution, security measures often interfere with an authorized user's normal job.

Vendors often implement security enhancement in response to specific customer demands. Such enhancements, made to existing systems, at a minimal cost often result in reducing convenience or poor performance. Vendors commonly adopt the attitude that a customer who wants security measures should be willing to live with the inconvenience.

Many users/customers take it upon themselves to fix security problems of their own system. Because of the limitation in the system, fixing security issues often entails restricting procedural control: limited access from remote terminals restricted physical access to local terminals. Multiple passwords or logins; frequent password changes, automatic disconnect after a period of inactive usage; and call-back devices. Some of these controls don't significantly increase security, however, they do raise the recognition that security is sore. Since clients and administrators don't see a way to manage this inconvenience, security is regularly utilized just if all else fails, when an issue has just happened or an unmistakable danger exists (Nigeria Computer Security Center, 1987; Jide & Bankole, 2006).

Information protection is a critical need in the economy. Therefore e-business needs expert and professionals to protect the value and usability of assets, the integrity, and continuity of operations.

2.1 Potential Security Attack Methods

The following describes potential security attack methods from an attacker or hacker

• Guessing passwords

This style of attack is manual or automated. Manual attacks are strenuous and only successful if the attacker knows something about the shopper. Automated attacks have a higher likelihood of success, because of the probability of guessing a user ID/Password. Tools exist that use all words in the dictionary to test user ID/Password combinations or attack a popular user ID/Password combinations.

• Using denial of service attacks

The denial of service attack is one of the examples of impacting site availability. It involves getting the server to perform a large number of mundane tasks, exceeding the capacity of the server to cope with any other task (Darshanand, 2005).

• Using unknown server bugs

The attacker analyzes the site to determine the type of software used on the site, what patches are used and then exploits the system without the patch (Darshanand, 2005).

• Using server roots exploits

Roots exploits refer to techniques that gain super user access to the server. The two main types of these attack are buffer overflow attack and executing scripts against a server (Darshanand, 2005).

III. COMPUTER SECURITY AS DRIVER TO E-BUSINESS

Before the issue of data security became widely known in the media, computer security was focused on the physical machine. Traditionally, computer facilities

have been physically protected for three reasons (National Computer Security Centre, 1987)

i. To prevent theft or damage to the hardware.
ii. To prevent theft or damage to the information.
iii. To prevent disruption of service.

However, computer security can be defined as a technological and managerial procedure applied to computer systems to ensure the availability, integrity, and confidentiality of the information managed by the computer (Afolorunso A. A., 2009). It means the protection of integrity, availability, and confidentiality of computer assets and services from associated threat and vulnerabilities. Today, these protections to e-business applications are doing more than ever to increase efficiency and improve the relationship with partners and customers. (So and Sculli, 2002) stated that in relation to trust and e-business technologies, consumers are concerned about their privacy and security.

As a result, computer security is a driver to:
• Increase enterprise effectiveness
• Enable competitive advantage
• Reliable and secure information
• Increase products/services sales and quality
• Increase profit
• Increase communication and customer relationship
• Increase enterprise reliability
• Increase confidence of trust

IV. METHODOLOGY

A. Method

A qualitative approach which is suggested by Strauss and Corbin (1990) was adopted here. Qualitative research is subjective in nature and involves examining and reflecting on meaning and perceptions of individuals in order to gain an understanding of social an organizational phenomenon. It assists the researcher in understanding the target phenomenon in depth and its natural settings. A total of 27 interviews were carried out in the city of Yenagoa; 16 with customers and 13 with managers and IT staff of small and medium size e-businesses. The questions that were used for asking customers were open and focused on exploring their perception of security (regarding deterrence to e-business) and how they would check to determine if a certain website and the ATM card system in Nigeria are secure or not. On the other hand, the questions posed by organizations focused on identifying their perception and viewpoint on customer's concerns with regard to security and what issues customer's needed to know for distinguishing between a secure website from a non-secure one. During the presentation of the results that emerge from the fieldwork, several quotations from the interview transcripts were provided (presented in italics during the results narrative)

B. Result/Findings

This section presents the findings regarding the perception from both customers and organizational (through the eyes of selected technical and managerial employees) perspectives.

• Customer Perspective
Customers answer with regard to how to check the security of a website and what criteria to consider when doing so can be categorized into those referring to tangible features and those referring to intangible features.

Tangible features are technological security features on the website that can be checked by users visiting the website, such as https, padlocks, security certificates and security symbols. Intangible features are those not seen on the website yet the user needs to understand or have knowledge of them.

They are affected by the society in terms of communication and the environment where the customer lives and what they hear from others as well as past experience, such as whether the website is well-known and reputable. The perception of the tangible features is constructed by informal word-of-mouth communication between people. Tangible features need to be understood and checked by the customer on a website rather than capture through social discourse between people; understanding is gained by having knowledge and experience of these features: for example, in the case of security certificates, a customer needs to know what it means to have one and how to find out the expiration of these certificates. Some customers indicated that tangible indicators meant very little to them and much less than the intangible indicators.

The following are some responses received from the customers in italics:

Some respondents indicated that the presence of details about security features on the website and information about the website policies, besides the interface design, would make them feel that it is more secure. Examples of the participants' responses are:

"I mean the website provides you information that makes you feel a sense that it is secure. Moving from one page to another until arriving at a confirmation page gives you a sense of security."

"A customer would trust a website if the website shows the customer a brief description of what security issues they should be aware of"

The following participant indicated the presence of a padlock on a website suggested security presence but does not rely solely on that indicator rather relies more on people's experience and commendation of the website:

"In fact, this depends on what people say, for example, I heard that the padlock at the bottom of the page means that this website is secure … but the main thing for me is what other people say because they have had experimentations with these websites before me."

Some respondents indicated that they do not transact business online because they believe the ATM card system in Nigeria is not secure:

"We hear that people can print and clone these ATM cards with any existing card number and with the correct PIN, the newly cloned card can be used to access the same account. This is totally unacceptable because just a single extra security layer is all that is required to shut down any ATM cards that are not printed by the originating banks"

When asked how to determine if a website is secured or not, several participants answered that if a site is well known then it must be secure:

"I think the issues here depends on the website. If the website is well known and rated by users, includes an actual address and telephone number then the site is secure … if I find a payment via WebPay, I can complete a transaction without any reluctance because the company is well known. The reputation of feedback on a website and the rating by customers and their experience proofs that the website is secure and credible."

In the last quotation, the participant highlighted the familiarity of an electronic payment service provider such as WebPay and the influence on security perception that the presence of such familiar service has. This was also asserted by another participant when he said

"I didn't hear anyone censure Amazon…you know why – because this website deals with the largest company in the world like WebPay. It undertakes the security of the website, these websites pay millions of naira for that."

The reputation of a website was also reported by other participants, who said it is based upon what customers view when considering buying online.

"I think there is no way to say if a website is secure or not. The only thing is the reputation of the company's website."

A few participant highlighted the significance of the website's existing known (and typically physical) identity, such as that of the banks and telecommunication companies in Nigeria. Participants appear not to use websites which are anonymous and have no real physical location:

"I trust only the bank…suppose anything happens, I can go to them and refer to them since they have a physical place. In fact, I have been a customer of this bank for a long time now so I discarded the fact that the bank would steal or trick me. There should be some information I should know as a customer to protect from fraud. For example, the first time I logged into a system (website) it forced me to change the password after six months. After a while, I was not able to log into the system because I had forgotten the password. After trying to log into the system for many times I was blocked and the system redirected me to visit my branch nearest to me to activate my password … all of these processes are in order to protect me. So they are concerned about security."

The last quotation also showed that providing a strong password is an indication of security:
"The company that respects its customers is well-known, implicitly provides the required conditions to complete the transaction in a secure way."

On other participant stated that: "I hear that there are many people purchasing over the internet and some buy and sell shares as well, so I think it is secure otherwise why would people buy and sell online."

To summarize, customers' viewpoint derived from the fieldwork fall into tangible and intangible indicators of security. On close inspection, it may appear that several of the intangible indicators appear to be identical.

• Organizational perspective
Some organizational perspectives are highlighted in italic which includes:

Some respondents indicated their impression in general about a customer's acceptance and engagement in e-commerce. For example, one participant believed that customers have a generally negative attitude towards online shopping and that there is no trust between customers and merchant:

"It is a shame that we have the highest level of ATM fraud in Nigeria when most (if not all) of the fraudulent activities can be checkmated or prevented. Truth be told, there is nowhere in the world where that experiences the embarrassing high level of ATM fraud. The implementation of this technology in Nigeria is characterized by ineptitude, lack of knowledgeable programmers and security experts who can guide and implement a secure transaction channel regardless of the level of education of the ATM card users.

… I suggest the way forward is:

Let the ATM payment gateway providers provide additional layers of security especially in the area of online transaction. Let the banks reduce the number of potential target cards by disabling the online usage feature by default and enable them based on the request."

With similar viewpoint this respondent expressed disappointment:

"In fact, by my experience with an e-commerce website, for several months, I arrived at an unbelievable fact that Nigerians don't believe or trust shopping online."

In contrast, however, another participant was optimistic by showing the achievement of her company and the degree of online acceptance from customers. The participant commented that customers nowadays are more aware and have a greater propensity to accept online trading given their experiences of using ATMs and the generally wider availability of credit cards

"We applied an electronic ticketing system on our site which was an important factor in enabling our business. As a result, it has become easy for customers to book a ticket and pay online from anywhere … people are accepting doing business online this day. There was a minor rejection at the first time but it was later accepted by our customers… really, we are surprised how people are ready to accept it."

She asserted that her company focuses on strong customer support to allay and respond to customer's concerns, by saying:

"The customer viewpoint is considered and we have a customer service center that is responsible for customer's inquiries, claims, and problems and we also take on their feedback which is important for us."

Another participant said ease of use of the website provides to an extent a feeling of security:

"The user's viewpoint is necessary for us, providing a website that is easy to deal with, friendly, motivates the customer to use it, which makes him feel secure to an extent…but it not exactly secure"

In another statement, the participant highlighted that a simple and true (i.e. product exactly matches what the customer expects) transaction with the customer makes him/her feel a sense of security which makes the customer want to return.

"In fact, the facilities, services, and security that we provide are not just talked but the fact that when a customer visits our website and obtains the product that he wants with the same specification, and this happens

without difficulty. It makes the customer want to come back. This is because they found sincerity in treatment. Now we have more than 10,000 active users who buy and sell on our website. These ones have tried and succeeded and found it is secure".

He continued by pointing out that the company's website also has a forum where buyers and sellers can chat, get to know each other, share opinions, provide suggestions, report transaction problems, recommends certain sellers and certain products, provide feedback and request support from the website. In addition, the website also provides a rating system which makes customers feel the website has a greater credibility.

"One of the important things that make customers feel that our website is secure and credible is the rating system which indicated positive and negative ranking for buyers and sellers, and the best buyers and sellers… we have a forum on our website. We have seen for example one customer asked a question and another customer told him to refer our company's policy, the clause number#. If a customer faces a challenge, we resolve it within 24 hours. The nature of our website is that it is easy to deal with. It also makes the customer happy and confident and in control"

He added that "we put on our website 'Secure 100%' we carry the responsibility for that"

In contrast, another participant stated that customer concerns are address solely by the services provided on the website. "The customer viewpoint is considered at service level; what he would like to see and what he wouldn't like".

Some of the technical staff involved in the development and maintenance of the company's website did not consider checking of tangible indicators as a sufficient mechanism for determining the security or otherwise of a website. This is first because the technical staff appeared to be unconvinced that the tangible indicators provide real security; websites are hacked despite the presence of these indicators, so customers could be led into a false sense of security by relying solely on them. Secondly, these indicators assure customers of the organization's trustworthiness. For example, by using security certificates as an indicator the website is guaranteed by a third party and thus the website is secure, but this is no assurance that it cannot be breached by hackers.

"It is difficult to say whether or not a website is secure even if you are a professional. Displaying 100% secure and using certificates just means you are not lying to your customers but it is not a guarantee that it cannot be hacked"

These indicators (e.g. security certificates) are thus not sufficient to assure that a website is completely secure. Here, the risk does not come from the website itself but might come from outside party (e.g. hackers). One participant maintained that there is no way to confirm whether or not a website is secure even when such websites are very well-known.

"Frankly, there is no way to judge that a certain website is secure, whether it Amazon or eBay … it is reputation and ease of use. The guarantee is the experiment and reputation"

From the interviews with organizational members, it was found that naïve customers are sometimes not aware of technological details such as the meaning of terms like https. Examples from participants also reported that understanding security is not an important thing for the customer and that the only concern is other people's experiences or reputation of the website.

"Some people don't care about security, they don't think whether it is secure or not. They are just concerned about what other people say about the website, if it is well known and credible then they will use it and trust it."

Another participant said "to say a website is secure 100% means nothing to the customer. I think the reputation of the website makes the customer feel it is secure. The main concern is about reputation"

Thus from an organizational perspective, customer looks for intangible indicators such as reputation, well-known company and the system of rating provided by previous customers of the website in order to assess whether or not a website is sufficiently trustworthy to engage in an online transaction.

V. CONCLUSION

Based on the findings, the conflict between some of the views of organizations as to what customer consider important and those views of the customers themselves can be clearly seen. The findings showed that some of the participating organizations indicated their acknowledgment of customer security concerns by stating them on the first page of the website that it was 100% secure.

On the other hand customer's responses have revealed that they do not intensively check tangible security features, being more interested in knowing the identity of the other party. They want to know whether they are dealing with a national company which is well known, famous and reputable. If these questions are answered affirmatively, then the customer feels secure.

Consequently, more effort is required by the organizations to seek strategies to make their websites better known and to boost reputation. But a question is raise if good reputation actually translates security? In essence, it can do so only if protection of customer's data is a responsibility of the company.

VI. REFERENCES

[1]. Alan, D.S. and William, T. R., (2002). "E-Lending: Foundations of Financial and Customer Marketing in an Informative Intensive Society", Journal of e-Business and Information Technology, Vol. 3, No. 1, pp. 5-19

[2]. A. Liska, The Practice of Network Security – Deployment Strategy for Production Environment. Prentice Hall PTR, Pearson Edcuation Inc., 2003

[3]. A. Strauss and J. Corbin, Basics of qualitative research: grounded theory procedures and techniques. SAGE Publication, London, 1990

[4]. A. Andreu, Professional Pen Testing for Web Applications, Wiley Publishing Inc., 2006

[5]. A. Dent and C. Mitchell, User's guide to cryptography and standards, Artech House, 2005

[6]. BA, S., Whinston, A.B. and Zhang, H. (1999), Building trust in the electronic market through an electronic incentive mechanism, Proceedings of the 20th International Conference on Information Systems, North Carolina, United States.

[7]. Beal, V. (2017) "Security: Computer Security" Retrieved from http//www.webopedia.com/TERM/S/security.html (April 14, 2017)

[8]. Bellovin, W.A., Fitchen, W.L. Mchugh, J. (2000). Windows of vulnerability: A case study analysis of computer, (December) 52 – 58.

[9]. Breidenbach, S. (ND), "How secure are you?", Available from: http://www.informationweek.com/800/prsecurity.htm, (April 19, 2007)

[10]. Carnegie Mellon University (Cert) (1999). "Deploying firewalls", Available from: https://www.cert.org/security-improvement/module/m08.html, (April 19, 2001)

[11]. Darshand, K. (2005). E-Commerce Security: Attacks and Preventive Strategies.

[12]. Eben, O. (2003). A systematic approach to e-Business security, University of New Brunswick, Fredericton, Canada.