British Journal of Applied Science & Technology
18(2): 1-12, 2016; Article no.BJAST.30312
ISSN: 2231-0843, NLM ID: 101664541

SCIENCEDOMAIN *international*
www.sciencedomain.org

Experience in Social Engineering by eCommerce Platforms in Kenya

Lawrence Mwagoti Mwasambo[1*] and Christopher A. Moturi[1]

[1]School of Computing and Informatics, University of Nairobi, Kenya.

Authors' contributions

This work was carried out in collaboration between both authors. Author LMM designed the study, performed the statistical analysis, wrote the protocol, wrote the first draft of the manuscript and managed the literature searches. Author CAM managed the analyses of the study and literature searches. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJAST/2016/30312
Editor(s):
(1) Samir Kumar Bandyopadhyay, Department of Computer Science and Engineering, University of Calcutta, India.
Reviewers:
(1) Jose Ramon Coz Fernandez, Complutense University of Madrid, Spain.
(2) Tolga Mataracioglu, Tubitak Uekae, Turkey.
Complete Peer review History: http://www.sciencedomain.org/review-history/17113

Original Research Article

Received 1st November 2016
Accepted 28th November 2016
Published 3rd December 2016

ABSTRACT

eCommerce systems have been targeted by cyber criminals as they receive and use the money, rely on technology, outsourced services and use of payment technologies like mobile money and online banking channels to carry out their day-to-day transactions. This study sought to investigate social engineering and its mitigation in eCommerce platforms in Kenya. An existing Social Engineering Defensive Framework was adopted and its dimensions were used to create questionnaires and interview guides. The study used 30 out of the 34 pure-play eCommerce firms operating in Nairobi, Kenya. The results indicate that phishing/spear phishing as the leading threat followed by baiting/Trojan Horse, social media/fraudulent websites, search engine poisoning among others. Mitigation measures indicate organizations need to regularly check their website listing in hacking sites (such as pastebin.com and ghostbin.com) and periodically document and update new policies regarding social engineering and information security. This paper proposes social engineering mitigation best practices, emphasizing the need for organizations using the derived best practices and incorporating security culture.

**Corresponding author: E-mail: mwagoti@gmail.com;*

Keywords: Social engineering; social engineering threats; eCommerce platforms.

1. INTRODUCTION

Social engineering threats continue to increase attacks and propagating malicious programs. The pervasiveness and persistence of social engineering; use a combination of psychological and technical ploys has been shown in several studies [1-3]. A social engineering attack targets this weakness by using various manipulation techniques in order to elicit sensitive information. This includes luring computer users to execute the malware and combating any existing technical countermeasures has been shown in several studies. There are much newer and emerging attack types. The impact of these new types of social engineering attacks has been tested through an experimental study by [3]. [4] show various social engineering attacks and their leading human factors and discuss the defense methods in terms education, training, policy, and procedure.

The communications regulator in Kenya [5], whose mandate includes facilitating the development of e-commerce and its security frameworks, shows that the internet/data market has maintained an upward trend, with an internet penetration levels of 87.2 percent. The emergence of new markets such as eCommerce present the country a prime opportunity for the market to make a turnaround and begin to record growth as it provides physical delivery services for online transactions. The dawn of internet saw entrepreneurs all over the world capture the idea and infuse technological innovation to create new products, services and business models [6,7]. These include purely internet-based companies that conduct most of their businesses online. This trend has also been exhibited in Kenya, where many businesses are now adopting eCommerce due to eased shopping hence making it more convenience and thus more appealing to the large population which accesses internet services.

Considering that social engineering was the second top cyber security issue in Kenya in 2015 [8], we sought to understand social engineering and its mitigation in eCommerce platforms in Kenya. There is a reasonable sign of prevalence of these violations and the failure of organizations to terminate them hence threatening the integrity of eCommerce organizations and their customers.

2. RELATED WORK

2.1 Social Engineering Concept

Social engineering can be defined, in context of information security, as the manipulation of people to get them to unwittingly perform actions or to divulge information that causes harm (or increase the probability of causing future harm) to confidentiality, integrity and availability of organization's resources, including information, information systems or financial systems [9,10]. Social engineering is a non-technical method of intrusion hacker's use that relies heavily on human interaction and often involves tricking people into breaking normal security procedure. The successful or unsuccessful attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network. [11] provided a gap analysis based on the physiological techniques of persuasion knowledge, attitude bolstering and influencing decision making, and proposed guidelines on how to improve social engineering defense mechanism. Transformational leadership, attitude and normative beliefs play important roles in information security culture and intention to resist social engineering [12]. Human and cultural factors can be influenced to result in more positive behaviours and lead to more secure information environments (Parsons et al. [13]).

2.2 Social Engineering in Global Perspective

[14] through Internet Crime Complaint Centre regularly releases public alerts on the updates on internet crime schemes and provides internet crime prevention tips. Such scams include e-mail compromised through social engineering targeting businesses with foreign suppliers or businesses that regularly perform wire transfer payments. According to the data, business e-mail compromise continues to grow and targets businesses of all sizes. The scam has been reported in all 50 states and in 79 countries resulting businesses to a loss of $ 1.2 billion.

[15] while conducting phishing campaigns noted that phishing statistics went higher, with 23% of recipients of phishing messages opening them

and 11% clicking on the attachments as compared to previous year. A campaign of just 10 e-mails yields a greater than 90% chance that at least one person will become a victim. This trend shows how effective social engineering attacks are continuing to evolve. [16] found that social engineering become the number one attack technique in 2015. Attackers have shifted away from automated exploits and instead engage people to do their dirty work of infecting systems, stealing credentials and transferring funds. Across all sectors and in the attack of all sizes, threat perpetrators used social engineering to trick people into doing things that once depended on malicious code. Attackers use people in three progressively controlling ways: running attacker's code for them; handing over credentials to them or directly acting for them; and transferring funds to them [16].

[17] reported different notable social engineering attacks were: phishing against government entities of UK and US during tax season with a 400% spike in phishing emails targeting taxpayers which steal credentials, account numbers and other variants that scam users to pay taxes through an IRS look-alike site, 700,000 people lost power in Ukraine after phishing attacks shut down compromised supervisory control and data acquisition (SCADA) system servers and prevented them from rebooting, an unknown man walked out with 120,000 carats of diamonds worth about $28 million in 2007 by only using his charm and no technology and lastly a ransomware attack at Los Angeles-based hospital where a malware used resulted to multiple cases of network downtime and in turn the attackers demanded a large sum of money in exchange for regaining control over the network.

2.3 Social Engineering in Africa Perspective

Social engineering trend has not excluded Africa, with advance fee scam, which rises from various nations in Africa. [18] found that 51% scam emails originate from Nigeria and a further 34% originating from Cote d' Ivoire, Burkina Faso, Ghana, Senegal and other West African nations. The most famous phishing attack is the Nigerian scam also referred as "419 scam". [19] have presented a closer look at how 419 Nigerian scam operates as well as detailed examples of 419 scam campaigns, some of which last for years.

In 2015 the Integrated Financial Management Information Systems [20] passwords of a senior county staff in Kenya were stolen and used to make illegal payments. IFMIS is the national system that integrates budgeting, procurement, accounting, electronic funds transfer, auditing, asset management and financial reporting. There have been other well published fraudulent payments through the IFMIS. In December 2014 there was a phishing attack in over 5,000 Facebook users [8]. Occasionally, many mobile users in Kenya receive texts and calls from persons purporting to have sent money wrongfully to their number and hence demanding it back or purporting to have earlier agreed to some amount but seem to have forgotten the deal. Many M-Pesa (mobile money) shop operators and customers have fallen prey to this attack. Several people have complained of being fleeced while conducting online purchases in using different eCommerce platforms.

2.4 Social Engineering Attacks in eCommerce Platforms

[3] has presented new and emerging attack types, the level of awareness regarding these attack types and the impact these new attack types potentially have on users' ability to detect them. The social engineering attack types are categorized as: (a) Person-Person attack which involves direct or in-person interaction of the attacker with the victim and the attacker uses deceptive methods to take advantage of the victim's ignorant or his behavioral weakness and exploits the trust and they include pretexting, reverse social engineering and tailgating. (b) Person-Person via media where attack vector does not involve the physical presence of an attacker but leverages attacks using computers and mobile phones. The attacks are phishing, SMShing, cross-site request forgery, malware by email, malware by popups, Malware by search engine poisoning, malware by social networks and Vishing.

An analysis of eCommerce related security issues, their impact on eCommerce success, and the available integrated security strategies is presented in [21]. The survey indicates that attackers can attack different points during an eCommerce transaction such as tricking an online shopper, sniffing the network connection between an eCommerce website server and shoppers and lastly attacking website's server.

[22] discuss the inner working of hackers and crackers using psychology to manipulate people into giving them access or the information necessary to get access. [23] have analyzed the various methods used in phishing and present a fishbone diagram outlining the causes and methodologies used in phishing. To combat social engineering attacks requires organizations to plan a comprehensive information security program, and a shared social responsibility [1].

[24] reviews various approaches to phishing that is constantly growing and evolving threat to Internet-based commercial transactions while [25] propose the detection of phishing attacks using a machine learning approach. [26] while examining the role and value of information security awareness efforts in defending social engineering attacks proposed a multi-layered shield to mitigate various security risks and minimize damage to systems and data. [9] examine unintentional insider cases that derive from social engineering exploits in order to identify possible behavioral and technical patterns that can development mitigation strategies.

2.5 Social Engineering Frameworks

The study examined the following frameworks:

Social Engineering Personality Framework [27]: The framework is based on the relationship between personality traits of the Five Factor Model (Conscientiousness, extraversion, agreeable, openness and neuroticism) and the six principles of influence (authority, commitment & consistency, reciprocity, liking, social proof and scarcity) used by social engineers. The framework shows that specific personality traits of a victim increase or lessen the susceptibility to [28] principles of influence which are utilized to attack by a social engineer.

Social Engineering Defensive Framework [29]: This model outlines four basic phases for attack prevention. The phases are autonomous from one another and can be performed in a request that suits the need of the organizations. The phases are: determining exposure, evaluating defenses, educating employees and streamlining existing technology and policy.

Social Driven Vulnerability Assessment Framework [30]: The framework is a crucial element for holistic social engineering risk management, which actively uses SE 2.0 techniques to stimulate an attack against enterprises. It focuses on realistically simulating social engineering based attacks, assessing, assessing the technology-enabled breaks opened as an up host of the social engineering based vulnerability, ethically respecting the employee and complying with existing legislations, contextualizing the attacks at either enterprise and individual levels; analyzing and interpreting findings correctly and applying the results to find long-term solutions. The phases of the model are setup, passive social information mining, spear phishing attack simulation, technological attack simulation and awareness.

2.6 Conceptual Framework

The Social Engineering Defensive Framework was adopted [29]. The four phases of the framework are shown in Fig. 1.

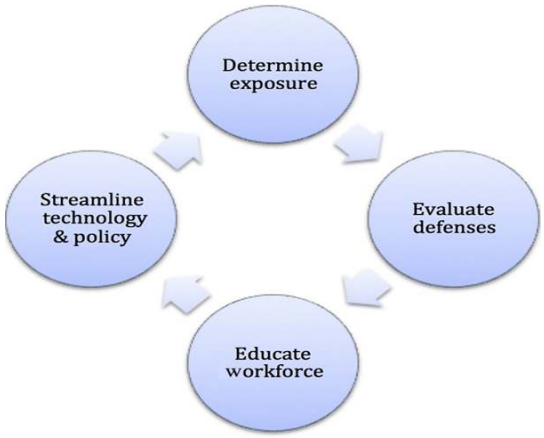

Fig. 1. Conceptual framework
(Source: Valerie Thomas, 2014)

a) **Determining exposure:** Focuses on seeing sites and other available resources as the attacker. Business needs to take a web exposure assessment which is a nonintrusive method of gathering client data in order to offer a readable delineation of what data is exposed to the internet or outside required areas.
b) **Evaluating defenses:** This was used to evaluate effectiveness of detection technology and appropriate response to attacks.
c) **Educating workforce:** Involved assessing how organization teaches employees and business partner on how attacks are executed and their impacts by breaking down attack scenarios depicting how each

bit of information is obtained and how it might be employed in attack by perpetrators.

d) **Streamlining existing technology:** This involved improving effecting defensive technologies which are likely in organizations by improving configuration changes, use of new technologies which have provided patches to identifiable vulnerabilities and creating policies to guide in case of social engineering.

3. RESEARCH METHODOLOGY

3.1 Research Design

The research took a survey approach achieved through interviews and questionnaires and respondent's opinion regarding social engineering in eCommerce platform. A pre-study of key eCommerce business was used to identify organizations that are conducting online business. The following characteristics were used to select the eCommerce businesses: Pure-play (Click only) eCommerce firm that still uses physical logistics that assist in delivering systems, owns an interactive website, uses either of the following eCommerce business models, B2B E-Commerce, B2C E-Commerce or C2C E-Commerce [7,31].

The target respondents were IT and Business Managers, but with more focus on IT managers as they are perceived to have a deeper understanding of the research subject. Business managers were interviewed while ICT managers were issued with questionnaires. The respondents were asked the following key questions: What are the different types of social engineering threats faced their eCommerce platform? What are the mitigation strategies to social engineering threats? Thematic analysis was conducted through qualitative data gathered through interviews. This assisted in creating and verifying social engineering best practices.

The research design facilitated testing of the following research hypothesis:

H0: Social engineering training will lead to reduced threats and attacks on eCommerce platforms.

HA: Social engineering, training will bear no issue in containing threats and attacks in eCommerce platform.

Hypothesis testing was based on independent sample testing of two predictors believe to have an effect on successful training employees and business partners on social engineering.

3.2 Data Collection and Analysis

This study used 30 out of the 34 pure-play eCommerce firms based in Nairobi, Kenya. Pure-play eCommerce use physical logistics that assist in delivering systems, owns an interactive website, and uses either of the following eCommerce business models, B2B, B2C or C2C [7,31]. Kenya has been home to major technological innovations and the origin of Africa's tech movement and is often referred to as Africa's Silicon Valley. Kenya is recognized as the pride of the global technological innovation sphere through the revolutionary M-Pesa, a mobile transfer service. Nairobi is a technology epicenter were all Kenyan innovation hubs are located and which have assisted in growing business ideas/innovations and in turn has accelerated technology businesses to grass root level [32]. Most of these firms used are well established and have been household names for several years now. These firms are key eCommerce players in the Tech Landscape.

The data collected was first checked for consistency and completeness then weighed to ascertain if it was fit for analysis. It was then grouped into various categories and entered into SPSS software package for analysis. Quantitative data were analyzed through descriptive statistics: mode, frequency counts and percentages to describe the dispersion. From the qualitative several subjects were built from the coded data, which were then culled out to acceptable few.

3.3 Validity and Reliability

The questionnaire was scrutinized by a senior researcher who critiqued the contents, design, and validity and corrected where issues were raised. The documents were submitted to four PhD candidates for verification. Test-retest method of assessing reliability was employed and the same instruments were distributed twice to the same group at separate times. With the study being perceived by the respondents to be sensitive in nature, 10 organizations were integrated into the test-retest reliability assessing. Final refinement of questionnaires was done and contact persons were distinguished.

4. RESULTS AND DISCUSSION

4.1 Demographics

The demographics of the respondents were as follow: 87.5% of the respondents were IT managers and 12.5 % Business Managers. Most of the organizations had operated between the ages of 1 to 5 years with 70.8 % followed by 6 to 10 years with 25% and lastly 11 to 15 years with 4.2%. This indicates that eC0mmerce organizations in Kenya are still in a formative stage, but still old enough to experience different social engineering attacks and threats. Respondents who are postgraduates formed the largest proportion (54.2%) and finally those who are university graduates (45.8%). The study sample had relatively high level of education and this indicated a serious chance of receiving a high grade of character data which could impact positively on understanding social engineering threats and impacts in Kenyan eCommerce platforms. The respondent organization mostly used pure play business approach (91.7%), (Conducting their business online) and click &mortar approach (8.3), (Selling online and have physical premises).

4.2 Social Engineering Attacks

The research sought to establish social engineering threats that eCommerce businesses are facing with the view to compare what has already been indicated from previous empirical studies. The respondents were asked to tell whether they have faced the threats while running their day-to-day actions. The research showed that Phishing is the biggest threats as most eCommerce businesses have faced the menace, indicated by 30.4 percent of responses and 10 percent of the cases tapped. Baiting/Trojan Horse and Social Media/ Fraudulent Websites had equal shares of 25.2 percent of responses and 50 percent of the cases recorded. Equally, SMShing and Diversion Theft had an equal share of 7.6 percent of response cases and 25 percent of events noted. Pretext/ Reverse social engineering had 11.4 percent of responses and 37.7 percent of cases noted, followed lastly by search engine poisoning with a case of 12.7 percent of responses and 41.7 percent of cases recorded. This was mostly attributed to the uniqueness of the attack and those who were using the search engine without the knowledge of how the attack is perpetrated and in turn fall victim easily. For instance, some respondents agreed to have severally times been redirected to a search engine similar to Google search, which was not legitimate. Table 1 illustrates.

The research included controlled phishing exercise to the target respondents, where spear phishing emails were sent to the target organization, which were not attached to any infectious payload or rootkit, but with a reverse TCP shell which spawned a command shell on the victim and send it back using Social Engineering Toolkit (SET); so as to demonstrate real life simulation and 95.8 percent clicked on the link attached to the spear phishing email. This re-enforces that many eCommerce platforms are highly susceptible to social engineering and that they need proper ways to contain the threats. The phishing exercise shows the organizations are vulnerable to social engineering attacks like Baiting/ Trojan Horse, where attackers can attach an infectious payload to the phishing email and when it's clicked, the payload will be downloaded and then used by an attacker to execute its intent ended purpose.

4.3 Hypotheses Testing

The research had a null H0 and alternative HA hypotheses that were tested by conducting an independent sample t-test on the independent and dependent variables.

Table 1. Social engineering threats frequencies

Social engineering threats	Responses percentage	Percent of cases
Phishing/ Spear phishing	30.4%	100%
Baiting/ Trojan horse	15.2%	50%
Pretexting/ Reverse social engineering (using voice)	11.5%	37.5%
Social Media/ Fraudulent websites	15.2%	50%
SMShing	7.6%	25%
Search engine poisoning	12.7%	41.7%
Diversion theft	7.6%	25%

H0: Social engineering training will lead to decreased attacks on eCommerce platforms in Kenya.

Test Variable for H0: Educating Workforce.

Grouping Variable: Type of eCommerce Approach.

An Independent-Sample *t*-test was calculated comparing the mean score of educating workforce to the mean score of E-commerce type. No significant difference was found (t (22) = 1.308, p> 0.5). The mean of eCommerce organizations which conduct click and mortar (sell online and have a physical premise) (m = 4.50, SD = 0.707) was not significantly different from the mean of organizations which conduct pure play (m = 4.79, SD = 0.263). [33] stated that reject the null hypothesis if the output value under sig. (Sometimes p or alpha) is equal to or smaller than .05 and fail to reject the null hypothesis if the output value is larger than .05. In this case, the research accepts the null hypotheses as for the p > 0.05 and reject the alternative hypothesis HA.

4.4 Dimensions of Social Engineering Defensive Framework

The results which test the dimensions of Social Engineering Defensive Framework have been summarized in Table 3.

4.4.1 Determining exposure

Caved in the extremely active growth of social engineering attack, threats, knowledge of what aspects concern an organization is a prerequisite for effectively protecting organizations against social engineering. Section determining exposure focused on the following important elements: periodically test and checking privacy and information security controls, to validate their effectiveness, how often do the organization conduct internet searches to locate and remove information that is in public domain or visible to the public, Conducting regular searches of information systems and physical storage to identify personally identifiable data outside approved areas and lastly checking if their websites are listed in hacking forums.

4.4.2 Evaluating defenses

Evaluating defenses is one key process that which will assist an organization to mirror and reflect what is going on and assist in establishing what is needed in order to seal any security loophole. The selected evaluating defenses quality were: Documenting personal data and other sensitive information maintained by the organizations on how its stores and held securely, conducting regular social engineering risk & evaluating privacy, specific authorization to accessing PII, separating of duties to ensure integrity of security checks & counterbalances, Implementing mitigation controls for detecting and unauthorized access control, Data Security controls, such as encryption and use of public key infrastructure and regular review and updating data destruction policies.

4.4.3 Educating workforce

Describing an attack can be informative but showing an attack has a far greater impact [29]. The most vulnerable link in data is the end-user. [34] explored the feasibility of predicting user susceptibility to deception-based attacks and observed that security training makes a noticeable difference in a user's ability to detect deception attempts. Since it is highly unlikely that social engineering attacks will ever be completely eliminated, the most important strategy to combat the attacks is to educate the workforce [35]. Mandatory social engineering and information security training on recurring basis, communicating and posting social engineering policies to customers and users from social engineering audited reports, clearly determine and making easily accessible reporting of social engineering complaints and privacy issues to relevant authorities, public or individuals.

4.4.4 Streamlining technology and policies

Innovation alone cannot avert social engineering assaults; it can minimize the effect of fruitful ones. Viable cautious advance likely exists in your environment, however, they could be enhanced with design modifications. Factors that attribute to streamlining technology and policies are: Employing of automated tools like intrusion detection systems and prevention and next-generation firewalls to monitor and report any anomalous activity, Use Data loss prevention solutions to track the movement and use of information within your system and prevent the unintentional disclosure of personal sensitive data, for both data at rest and data in motion and ensuring availability & recovery of data in case the loss happens.

Table 2. Group statistics and Independent sample test

Group statistics							
	Type of eCommerce the firm uses	**N**	**Mean**	**Std. deviation**	**Std. error mean**		
Educating workforce	Pure play	22	4.7879	.26318	.05611		
	click and mortar	2	4.5000	.70711	.50000		

Independent samples test										
		Levene's test for equality of variances		**t-test for equality of means**						
		F	**Sig.**	**t**	**df**	**Sig. (2-tailed)**	**Mean difference**	**Std. error difference**	**95% confidence interval of the difference**	
									Lower	**Upper**
Educating workforce	Equal variances assumed	10.524	.004	1.308	22	.204	.28788	.22014	-.16866	.74441
	Equal variances not assumed			.572	1.025	.667	.28788	.50314	-5.74360	6.31936

Table 3. Dimensions of social engineering defensive framework

Statements	**Not at all**	**Small extent**	**Moderate extent**	**Great extent**	**Very great extent**	**Mode**
	%	**%**	**%**	**%**	**%**	
Testing and checking privacy and information security controls	-	-	-	25	75	5
Conducting internet searches to locate and remove information in public domain	-	4.2	4.2	16.7	75	5
Searching information system and physical storage to identify PII outside approved areas	-	-	-	12.5	87.5	5
Checking organisation website listing in hacking forums	25	25	41.7	8.3	-	3
Document personal data and other sensitive information maintained by your organization	-	-	-	12.5	87.5	5
Social engineering risk assessment and evaluate privacy threats evaluation.	-	-	-	12.5	87.5	5
Authorized access to sensitive data and PII	-	-	16.7	33.3	50	5
Job Segregation to ensure integrity of security checks and counterbalances	-	-	20.8	50	29.2	4
Data migration controls	-	-	-	12.5	87.5	5
Data Security controls, such as encryption and use of public key infrastructure.	-	-	16.7	37.5	45.8	5

Statements	Not at all	Small extent	Moderate extent	Great extent	Very great extent	Mode
	%	%	%	%	%	
Reviewing and keeping up-to-date data destruction policies	-	-	12.5	4.2	83.3	5
Provide mandatory social engineering and information security training on a recurring basis to all employees and other staffs involved	-	-	-	33.3	66.7	5
Do you communicate and post social engineering policies to customers and users (For illustration, on the organization's website, or on a bulletin board at the office, through statements inserted in text files or emails) from social engineering audited reports.	-	-	-	20.8	79.2	5
Have you clearly determined and making easily accessible process for reporting privacy incidents and complaints (Depending on the nature of the issue, this may include reporting to the authorities, public and/or individuals)	-	-	4.2	8.3	87.5	5
Employ automated tools, like Intrusion detection/prevention systems, next generation firewalls, including perimetric protection, malware analysis, forensics, Log Analysis and Vulnerability analysis, to monitor and alert about suspicious or anomalous activity	-	-	-	12.5	87.5	5
Use Data loss prevention solutions to track the movement and use of information within your system and prevent the unintentional disclosure of personal sensitive data, for both data at rest and data in motion and ensuring availability & recovery of data in case the loss happens.	-	-	-	20.8	79.2	5
Conduct policy violations to determine if they are well utilized	-	-	-	16-.7	83.3	5
Periodically update and document new policies, regarding social Engineering threats noted and documented	-	-	-	12.5	87.5	5

(Source: Research data, 2016)

4.5 Best Practices

While many cyber security organizations urge the corporate world to use defense-in-depth, social engineering requires a layered and multifaceted defense strategy [36,37]. [13] have outlined factors that instill and maintain a culture where positive security behaviours are valued. These include usability challenges associated with information security, employee's education and awareness and incorporating behavioral training, influence of individual differences, personality traits and cognitive abilities, biases and organizational culture. Many researchers have classified and grouped social engineering mitigations in different categories, but they all lead to policy, audit and awareness training [10,18,38]. Alongside all this, this paper proposes the following social engineering mitigation best practices based on the analyzed research data:

1) Understand as an organization, what is safe to broadcast to the web or public and only necessary information should be communicated or availed to the masses and remove any personally identifiable information that is in the public domain.
2) Email addresses, information of high profile people, clients, business partners and persons of interest in the organizations should be kept secret.
3) Periodically test and check privacy and information protection command
4) Regularly check if the organization's website is listed in hacking forums like pastebin.com, ghostbin.com or anonpaste.com.
5) Document personal data and other sensitive information maintained by your establishment and ensure its stored securely and as per laws and regulations in place.
6) Regularly conduct social engineering risk assessment and evaluate threats to your organization, contractors, and business partners.
7) Ensure physical security to the organization information system and accessing the said systems should be through authorized personnel only. This can be enforced through the use of guards, biometrics, alarm systems and log files.
8) Implementing mitigation controls designed to prevent and detect unauthorized access, theft or abuse of PII and other sensitive data.
9) Encryption of sensitive data, in motion and at ease.
10) Regularly review and keep data destruction policies updated, to downplay risk of data breaches through unauthorized access to archived media or information processing systems that are no longer in use.
11) Providing mandatory social engineering training on a regular base.
12) Communicating and posting social engineering policies to employees, business partners, and customers, on the organization's website, emails and memos on the notice board in the organization.
13) Making easily accessible process for reporting social engineering incidents and complaints, to authorities, customers, business partners, and employees.
14) Using automated tools, like intrusion detection systems, next-generation firewalls including perimetric protection, malware analysis, forensics, Log Analysis and Vulnerability analysis to monitor and alert anomalous activity in the organization's network.

5. CONCLUSION

This research sought to demonstrate a well-defined reason for concerns and advances pertaining to social engineering in eCommerce platforms in Kenya [8]. The analysis of the quantitative data gathered and the identification of various issues that arose from qualitative data has informed the best practices. The analysis covered four dimensions, namely, determining exposure, evaluating defenses, educating the workforce, streamlining technology and policy and demographic areas like ownership of the eCommerce organisation. The results show that most eCommerce organizations in Kenya have been affected by social engineering and phishing as the leading social engineering threat with 100% of cases tapped followed by baiting/Trojan Horse and social media/ fraudulent websites each tying with 50%. Search engine poisoning, pretext/ reverse social engineering, and diversion, the theft had 41.7%, 37.5% and 25% of the events recorded. Mitigation measures from indicate organizations to be faring well but still they need to ensure their websites are regularly checked for listing in hacking sites or forums and ensure periodic update and documentation of new policies regarding social engineering and information security. This research offers best practices derived from the four phases of social

engineering defensive framework and was deemed essential after research analysis.

The research has led to strategies that would enhance successful mitigation of social engineering attacks and threats and hence it would ensure safe systems for customers, business proprietors, and their stakeholders. For policy makers and senior level managers, they need to ensure that apart from using the derived best practices, they ought to have the following in their arsenal for mitigating social engineering: Physical security of their business premises, having information security policies and procedure in place, which are up-to-date, securing the whole organization and incorporating security culture in an organization. The ultimate way to tackle social engineering is through creating awareness, this involves teaching and including desktop simulation of social engineering attacks and ensuring that social engineering mitigation tactics need to be updated time after time due to the evolving nature of social engineering by the creativity of the attacker.

For individuals protect themselves from social engineering, they should observe: not clicking on embedded email links and download attachments from unknown senders, Patch software's and operating schemes, use up to date antivirus software, pay attention to URLs and ensure are secured with Https before sending sensitive info, never provide personal info unless you're sure to do so, and lastly be weary of unknown phone calls and SMS asking for your personal data or employee information.

ACKNOWLEDGEMENTS

We acknowledge the participation of the eCommerce businesses in Kenya. We acknowledge the contribution of the following faculty members at the School of Computing and Informatics, University of Nairobi: Daniel Orwa, Peter Wagacha, and Samuel Ruhiu.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Abraham S, Chengalur-Smith I. An overview of social engineering malware: Trends, tactics, and implications. Technology in Society. 2010;32(3):183-196.
2. Mouton F, et al. Social engineering attack framework. In Information Security for South Africa; 2014. IEEE.
3. Ivaturi KR. Social engineering–emerging attacks, awareness and impact on online user attitudes and behaviours. ResearchSpace@ Auckland; 2014.
4. Luo XR, et al. Social engineering: The neglected human factor for managing information resources and technology: Emerging applications and theories. Emerging Applications and Theories. 2013; 151.
5. CAK, First Quater Sector Statistics Report for the Financial Year 2016/2016; 2015.
6. Hasan, Harris. Entrepreneurship and innovation in e-commerce. Journal of Achievements in Materials and Manufacturing Engineering. 2009;32(1):92-97.
7. Kabuba PK. E-commerce and performance of online businesses in Kenya. Univeristy of Nairobi: Nairobi; 2012.
8. Serianu. Kenya cyber security report 2015, in achieving enterprise cyber resilience Through situational awareness. Serianu ltd; 2015.
9. Greitzer FL, et al. Analysis of unintentional insider threats deriving from social engineering exploits in Security and Privacy Workshops (SPW). IEEE; 2014.
10. Kumar A, Chaudhary M, Kumar N. Social engineering threats and awareness: A survey. European Journal of Advances in Engineering and Technology. 2015;2(11): 15-19.
11. Schaab P, Beckers K, Pape S. A systematic gap analysis of social engineering defence mechanisms considering social psychology. In Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA); 2016. Lulu. com.
12. Flores WR, Ekstedt M. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers & Security. 2016;59:26-44.
13. Parsons K, et al. Human factors and information security: Individual, culture and security environment; 2010.
14. FBI. Business Email Compromise. Internet Crime Complaint Center (IC3); 2015.

15. Team VR. Data Breach Investigations Report; 2015.
16. Proof Point, The human factor report. 2016;1-28.
17. PwC, Anatomy of Social Engineering Attack, in Exploiting Human Behaviours; 2016.
18. Herley C. Why do nigerian scammers say they are from nigeria? In WEIS; 2012.
19. Isacenkova J, et al. Inside the scam jungle: A closer look at 419 scam email operations. In IEEE Security and Privacy Workshop; 2013. IEEE.
20. IFMIS. Integrated Financial Management Information System; 2016 [Cited 17/09/2016]; Available: http://www.ifmis.go.ke/
21. Matbouli H, Gao Q. An overview on web security threats and impact to e-commerce success. In Information Technology and e-Services (ICITeS), International Conference; 2012. IEEE.
22. Hasan M, Prajapati N, Vohara S. Case study on social engineering techniques for persuasion. arXiv preprint arXiv: 1006. 3848; 2010.
23. Weider DY, Nargundkar S, Tiruthani N. A phishing vulnerability analysis of web based systems. In Computers and Communications. ISCC; 2008. IEEE Symposium on. 2008. IEEE.
24. Banday MT, Qadri JA. Phishing-A growing threat to E-commerce. arXiv preprint arXiv: 1112.5732; 2011.
25. Basnet R, Mukkamala S, Sung AH. Detection of phishing attacks: A machine learning approach. In Soft Computing Applications in Industry. Springer. 2008; 373-383.
26. Ghafir I, et al. Social engineering attack strategies and defence approaches. In Future Internet of Things and Cloud (FiCloud), IEEE 4th International Conference; 2016. IEEE.
27. Uebelacker S, Quiel S. The social engineering personality framework, in 4th Workshop on Socio-Technical Aspects in Security and Trust (STAST). IEEE: Vienna, Austria. 2014;24-30.
28. Cialdini RB. Influence, in the psychology of persuation. HarperCollins e-books; 2009.
29. Gardner B, Thomas V. Building an information security awareness program: Defending against social engineering and technical threats. Elsevier; 2014.
30. Frumento E, Puricelli R. An innovative and comprehensive framework for social vulnerability assessment. Magdeburger Journal Zur Sicherheitsforschung. 2014;2: 493-505.
31. Schultz P. Behind the internet business models: An E-health industry case. Copenhagen Business School; 2009.
32. Moime D. Kenya, Africa's silicon valley. Epicentre of Innovation; 2016. Available:https://vc4a.com/blog/2016/04/25/kenya-africas-silicon-valley-epicentre-of-innovation/
33. Cronk BC. How to use SPSS statistics: A step-by-step guide to analysis and interpretation. Pyrczak Pub; 2012.
34. Heartfield R, Loukas G, Gan D. You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks. IEEE Access. 2016;4:6910-6928.
35. Atkins B, Huang W. A study of social engineering in online frauds. Open Journal of Social Sciences. 2013;1(03):23.
36. Abeywardana KY, Pfluegel E, Tunnicliffe MJ. A layered defense mechanism for a social engineering aware perimeter. In SAI Computing Conference (SAI); 2016. IEEE.
37. Janczewski LJ, Fu L. Social engineering-based attacks: Model and new zealand perspective. In Computer Science and Information Technology (IMCSIT), Proceedings of the 2010 International Multiconference; 2010. IEEE.
38. Chaudhry JA, Chaudhry SA, Rittenhouse RG. Phishing attacks and defenses. International Journal of Security and Its Applications. 2016;10(1):247-256.

© 2016 Mwasambo and Moturi; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Peer-review history:
The peer review history for this paper can be accessed here:
http://sciencedomain.org/review-history/17113