Mapping and Modeling Kenya's Hospitality Industry Cyber Security Factors: Case of Selected Hotels in the North Rift

Article · January 2019

CITATIONS
0

READS
20

1 author:

Lamek Ronoh
Rongo University
4 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Mara Research Journal of Computer Science & Information Security
Vol. 1, No. 1, November 2016, Pages 132 - 140, ISSN 2518-8453

Mapping and Modeling Kenya's Hospitality Industry Cyber Security Factors: Case of Selected Hotels in the North Rift

Lamek Ronoh
School of Computer Science and Bioinformatics
Department of Information Technology Security
Kabarak University, Private Bag 20157, Kabarak, Kenya
Email: ronohlamek@gmail.com

Received: November 19, 2016
Published: November 25, 2016

Abstract

This study investigated by modeling cyber-security factors affecting tourism and hospitality industry in Kenya. More specifically, three selected state of the art hotels in the North Rift that were then used for the study. The objective of the study was to explore cyber vulnerabilities in the tourism industry using three indicators; namely, the nature of the incident/threat, the impact of the incident/threat and the response to the incident/threat. These three indicators were inspired by a conceptual framework for cyber vulnerabilities in the tourism industry as proposed by Pizam and Mansfeld (2006). Correctional research design was employed in this study and notably the multiple regression model was used to predict cyber vulnerabilities using the aforementioned indicators in the tourism industry. Data was collected using questionnaires from the selected hotels. The collected data was coded, analyzed and the results generated were presented using the multiple regression analysis parameters comprising of model summary having the r2, regression coefficients and ANOVA. From the three aforementioned indicators (independent variables), hypotheses were formulated to test and establish the intensity of cyber vulnerabilities of the selected hotels. The ANOVA results formed the basis of rejecting or accepting the null hypotheses. The research results showed that the response to a threat or incident is a major indicator in understanding the cyber threats afflicting the hospitality industry in Kenya's North Rift selected state of the art hotels. In essence, the findings indicated that a better understanding of the nature of a threat, the lesser the impact of an incident and ultimately the better the response will be. The findings of the study is anticipated to be used by both the future researchers in related discipline as well as the tourism industry fraternity especially the Information technology personnel in making decisions relating to cyber security.

Keywords: Cyber-security, hospitality industry, multiple regression, model

1. INTRODUCTION

It is no doubt that information technology has become a convenient tool that every stakeholder or player in the tourism and hospitality industry cannot hesitate to embrace in this ever dynamic and competitive sector. In addition, technologies and applications continue to be developed at lightning speed because business owners want to provide their guests with ultra-convenience services and amenities. Due to Kenya's positioning as a strategic tourism and business destination, the country attracts hundreds of thousands of global visitors every year. To ensure they can cater for diverse global visitor, most of the organizations have invested in the use of technology to efficiently seamlessly collect, process and store huge amounts of customer and payment data. Most of these organizations have not invested in information security best practices, consequently making them highly vulnerable to cyber-threat in the country (Kigen et al., 2015).

In Kenya, for example, hospitality business accounts for 38% of all data security breaches. When compared to 19% for financial services and 14% for retail businesses, this statistic is both alarming and revealing. What factors account for the dramatic increases in this sector? Why is this industry suddenly so vulnerable to attack? What can we do about it? (Orthus White Paper, 2010). The hospitality industry is an attractive target for criminals who want to steal a valuable asset: personal data. However, the damage caused by a data breach extends beyond theft. It can include, among other things, the impact on a company's reputation and lost consumer confidence (Karpuk & Kelly, 2015).

Hotels and restaurants have historically always been targets for fraud; the industry's prevalent use of point-of-sale systems, complex supply chains, transient nature of guests, high volume of transactions and loyalty programmes and, marketing and reservation databases makes hospitality businesses a key target for hackers and criminals (Pitmans, 2013). However, the celebrations in the industry tones down because of pervasive ways of the cyber criminals who are persistent and always advanced in finding vulnerabilities of gaining access to various industry's assets and clients' information.

1.1 Statement of the Problem

The inevitable increase of embracing IT and internet in the hospitality and tourism industry in Kenya to provide better services and products to its diverse global customers has exposed them to numerous levels of cybercrimes in their daily operations. In essence, the evident increase in the sophistication of cyber criminals has a significant impact that can threaten individual hotels, destination brands or the entire tourism and hospitality industry as a whole. Hence, this study sought to investigate the cyber vulnerabilities in Kenya's tourism and hospitality industry using the predictor independent variables namely the nature and impact of the incident or threat as well as the response to the incident or threats.

1.2 Objectives of the study

The Specific objective of the study was to establish whether the nature and impact of the incident or threat as well as the response to the incident have a significant effect on cyber vulnerabilities in the tourism industry for the selected hotels in the North Rift in Kenya.

1.3 Research hypotheses

The hypothesis for the study was stated as follows:

H_{01}: The nature of the incident or threat has no significant effect on cyber vulnerabilities in the tourism industry for the selected hotels in the North Rift in Kenya.

H_{02}: The impact of the incident or threat has no significant effect on cyber vulnerabilities in the tourism industry for the selected hotels in the North Rift in Kenya.

H_{03}: The response to the incident or threat has no significant effect on cyber vulnerabilities in the tourism industry for the selected hotels in the North rift in Kenya.

1.4 Conceptual Framework

This study was guided by the authors' conceptual framework shown in Fig. 1.

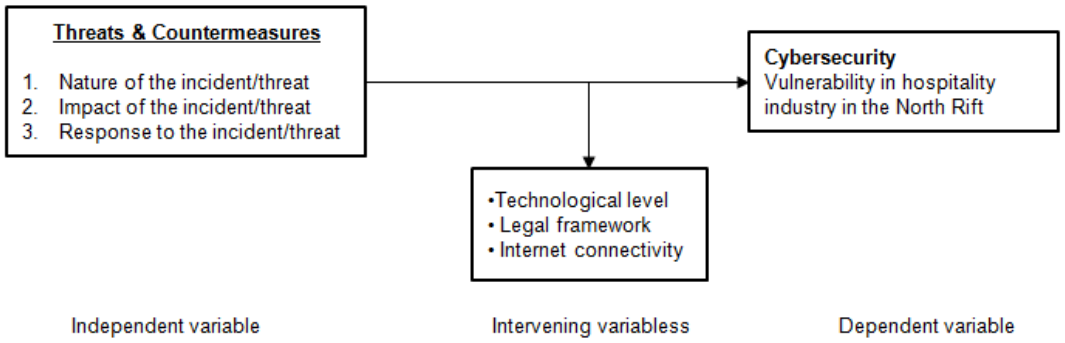

Fig. 1: Conceptual framework
Source: Pizam and Mansfeld (2006)

2. LITERATURE REVIEW

The threat from cyber-crime is a global problem that has grown exponentially over the last few years. Its impact is felt by all businesses, but with large volumes of valuable customer information, the hospitality and leisure sector has particular risks and issues to consider (Piper, 2013). In a rejoinder, two veteran insurers Fobert and Chase (2014) observed that while new threats are always emerging, hospitality firms should deploy robust data safeguards and procedures to mitigate the cyber exposures. These include assessing procedures for how the data is collected as well as where and how it is stored. If a third party stores the information, it is crucial to understand their security policy, procedures and the need to evaluate their insurance coverage.

Cyber risk has become a leading issue for many organizations as awareness in the era of cloud computing, social media, corporate Bring Your Own Devise (BOYD) policies, big data, and state-sponsored espionage which in itself has grown over the last couple of years. In an increasingly punitive legal and regulatory environment, and in the face of more frequent contractual insurance requirements specifying cyber liability, forward-thinking companies are taking proactive steps to explore and transfer cyber risk to third party organizations (AON, 2015).

One of the primary reasons that the industry is fast becoming a favourite target for hackers is the vast amount of credit card data it processes, transmits and stores across their networks on daily basis. Hotels specifically with their need to conduct charge backs or maintain customer data in their systems, amass a huge amount of sensitive credit card data across their networks. 67% of the respondents had experienced data breaches in the last 12 months. Of the respondents breached, 72% were identified as (PCI DSS) Level 4 Merchants. Of the breaches reported 58% were attributed to external attacks and 42% were attributed to internal attacks. Key loggers and memory sticks were the used to remove data in over 50% of the internal attacks identified. The theft of hardcopy (credit card) data was identified in over 15% of the breaches reported. The compromise of point of sale (PoS) devices was identified in 28% of the reported breaches. The unauthorised remote access to data bases was identified in 47% of external attacks. (Orthus Whitepaper, 2011).

PCI compliance for the hospitality industry is much different than other industries. Not only are hotels one of the largest targets for security breaches, but they also have unique situations that credit card companies don't necessarily understand. So an open form of communication between the industry and the credit card brands is crucial to improving security at each property. 40 percent of all breaches are from the hospitality industry. So someone needed to step up and begin the steps towards addressing the problems that the industry experiences (Walterscheidt, 2010). Olding and Turner (2007), for example, observed that a

suitable framework that will form the basis for an investigation is required in order to explore, understand and respond to the cyber vulnerabilities that are faced by the tourism industry in Australia.

2.1 Review of previous related research

Olding and Turner (2007) carried a survey on cyber security vulnerabilities in hospitality industry in Tasmanian Island of Australia. They based their research on the framework proposed by Pizam and Mansfeld (2006) and, came up with macro-level conceptual framework. At Micro-level, the aforementioned macro-level framework can be used to examine cyber vulnerabilities to the tourism industry by revolving around three main parameters; namely, the nature of threat, impact of threat and the appropriated response taken against the threat. This concept is illustrated in Fig. 2.

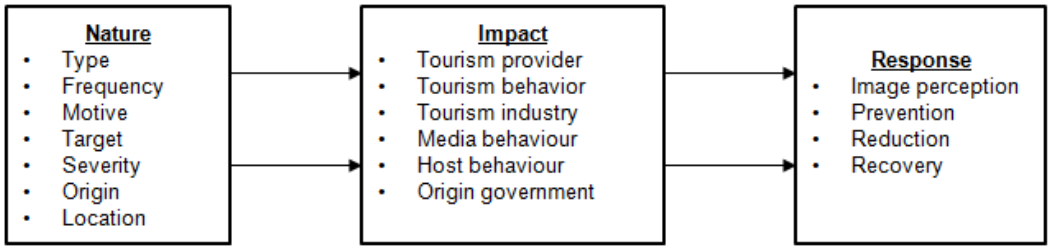

Fig. 2: Micro-level conceptual framework
Source: Olding and Turner (2007)

The weakness of this research, however, ended by the investigators only coming up with a framework for understanding the threats and vulnerabilities in hospitality industry. It does not effectively pinpoint the real-time nature of threats and their associated impact and how to respond or deal with such emerging threats.

Kefgen and Wolff (2015) highlighted four key pertinent areas that the hospitality industry should employ towards limiting exposures and liability. They advised that the initial step is to focus on developing a robust internal risk management plan; followed by an activity of carrying out annual risk assessment and insurance; thirdly, to check on franchise agreements, which addresses concerns such as data security, cyber-insurance, breach notification and Payment Card Industry (PCI) compliance and, lastly is for the sector to prepare itself on how to cope and come to terms with the ramification of cyber-attack realities. However, these authors failed to identify the key cyber threats to watch and how to mitigate or prevent them.

Palagonia (2015) highlighted incident response planning to be more important for the hospitality industry than for others and that a layered approach to security, compliance and risk management is necessary in order to mitigate direct and indirect threats and potential loss. The aforementioned measures are in addition to Europay, Mastercard and Visa card (EMV) adoption, point-to-point encryption (P2PE), tokenization, third-party vendor management, together with established best practices, can help prevent data breaches, minimize financial losses and may also aide in meeting PCI Data Security Standard compliance requirements.

According to the online article Tripwire (2016) which advised that the ideal approach to cybersecurity issues in hospitality and retail industry is the need to continuously keep on monitoring organizations' resources, prioritizing real time alerts and making sure that you are achieving the PCI compliance. However, the article failed to clearly isolate the most appropriate monitoring and real time alert resources to be adopted by the hospitality industry.

3. RESEARCH DESIGN AND METHODOLOGY

Correlational and survey research design was employed in this study. This design was chosen by the researcher because it allows for the simultaneous measure of the three variables in predicting the cyber vulnerabilities in the tourism and hospitality industry. A correlational research design is the measurement of two or more factors to determine or estimate the extent to which the values for the factors are related or change in an identifiable pattern. Correlational designs are used when many variables are measured simultaneously but unlike in an experiment, none of them are manipulated. When we use correlational designs, we can't look for cause-effect relationships, because we haven't manipulated any of the variables and also, because the variables have been measured at the same point in time. When it is difficult to control for other possible factors that could be causing changes in behaviour, we can use the correlational research design to determine the extent to which two factors are related, not the extent to which one factor causes changes in another factor.

4. DATA ANALYSIS

In quest of bringing out the presence or absence of the relationship between variables, the researcher employed the multiple regression equation to model the three factors(variables) using the following model,

$$Y=\beta_0+\beta_1x_1+\beta_2x_2+\beta_3x_3+\varepsilon_{ij}.$$

where:

Y is the dependent or criterion variable (cyber vulnerability)

β_0 is the constant value,

X_1, X_2 and X_3 are the independent variables; nature of incident/threat, impact of incident/threat and response to the incident/threat respectively.

β_1, β_2 **and** $\beta_3$are the regression coefficients and,

ε_{ij} is the error component with mean of zero because normality will be assumed.

The data was analyzed using SPSS programme version 23.0 and besides presenting the findings using the aforementioned inferential statistics, descriptive statistics was also succinctly employed.

5. FINDINGS AND DISCUSSIONS

The findings indicated that there is wave of increasingly sophisticated cyber attacks to the hospitality industry in hotels in as revealed by the selected hotels in the Kenya's North Rift. The results indicated that all the hotels selected for the study had experienced data breaches in the last one year. Of the respondents breached, 59% were identified as malware infection, 27% were online fraud and a whopping 84% were credit card breaches. In particular, of the breaches reported 93% were attributed to external attacks and 7% were attributed to internal attacks. Key loggers and memory sticks were used to remove data in over 50% of the internal attacks identified. The compromise of point of sale (PoS) devices was undertaken using the malicious software and this accounted for 34%. The unauthorised remote access to data bases was identified in 27% of external attacks. The study further revealed that the industry is insufficiently investing in cyber security countermeasures.

It's against this backdrop that the aforementioned attacks in the hospitality industry ought to be mapped and modeled, so as to guide the stakeholders to explore and mitigate on the cyber vulnerabilities in this very important industry. The study mapped and modeled these indicators as the nature of the incident/threat, the impact of the incident/threat and the response to the incident/threat. Nevertheless, the three parameters were statistically mapped and modeled using multiple regression model to explain the

relationships and how the industry can concisely understand the phenomena although mainly, information technology solutions will ultimately be applied as a counter-measure to the cyber-attacks mentioned elsewhere in this study. Thus, regarding the inferential statistics findings yielded the multiple regressions results discussed shown in Table 1.

Table 1: Model Summary

Model Summary[b]				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	.999[a]	.999	.995	.25210
a. Predictors: (Constant), Response, Impact, Response				
b. Dependent Variable: CybeSec_Vulnerability				

The 'R square' is the square of R and is also known as the 'coefficient of determination'. It tells us what proportion (or percentage) of the variation (sample) in the dependent variable can be attributed to the independent variable(s). In Table 1 above, the results shows that 99.9% of the cybersecurity vulnerabilities in the tourism industry in the North Rift tend to be accounted for by the variation of the independent variables. Thus, the findings indicate that there is a perfect correlation between cybersecurity vulnerabilities (dependent variable) and independent variables namely the nature of threat/incident, impact of threat/incident and response to the threat/incident, see Table 2.

Table 2: Regression coefficients

Coefficients[a]						
		Unstandardized Coefficients		**Standardized Coefficients**		
Model		**B**	**Std. Error**	**Beta**	**t**	**Sig.**
1	(Constant)	-88.740	4.431		-20.028	.032
	Nature	3.647	.173	5.715	21.114	.030
	Impact	3.721	.154	5.860	24.230	.026
	Response	-.165	.064	-.157	-2.555	.011
a. Dependent Variable: CybeSec_Vulnerability						

Stepwise selection method was adopted in the analysis where each independent variable was entered in sequence and its value assessed. This method was based on the criteria that if adding the independent variable contributes to the model then it is retained, but all other variables in the model are again re-tested to see if they are still contributing to the success of the model. If they no longer contribute significantly they are removed. Thus, this method was to ensure that we end up with the smallest possible set of predictor variables included in the model. In this case, all the three independent variables contribute to the success of the model.

Hence, after the computation, the multiple regression model mentioned above yielded the multiple regression equation shown below:

$$Y= \mathbf{-88.740 +- 3.647Nature+ 3.721Impact- 0.165\ Response}$$

5.1 Analysis Of Variance (ANOVA)

The researcher carried further analysis to ascertain the variability of relationships between the dependent and independent variables. The analysis of variance (ANOVA) tests whether the model is significantly better at predicting the outcome than using the mean as a 'best guess'. Specifically, the F-ratio represents the ratio of improvement in prediction that results from fitting the model (labeled 'Regression' in Table 3) relative to inaccuracy that still exists in the model (labeled 'Residual') in Table 3). If improvement due to fitting the regression model is much greater than the inaccuracy within the model, then the value of F will be greater than 1. In essence, Table 3 reports an ANOVA test, which assessed the overall significance of our model.

Table 3: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	17.267	28	.617	2.520	.004(a)
	Residual	9.300	38	.245		
	Total	**26.567**	**66**			

Since the *p*-value, ***p*=0.004<0.05**, we **reject** the three aforementioned hypotheses, at 5% level of significance and conclude that indeed at least some of the independent variables namely the nature of the threat/incident, impact of the threat/incident and response to the threat/incident at least have some significance on cyber security vulnerability of hospitality industry in the selected state of the art hotels in Kenya's North Rift.

6. CONCLUSION AND RECOMMENDATION

This paper modeled the correlational pattern existence of cyber security vulnerabilities afflicting the state of the art hotels in Kenya's North Rift.

As mentioned elsewhere in this paper, the model based on Pizam and Mansfel (2006) examined the nature of the cyber threats by looking at the potential threats and vulnerabilities that exist and attempted to classify them. Such threats were either specific target attacks such as Man in the Middle (MITM) or common threats/incidence such as an infection by virus like Trojan horse among others. The second part of the model, studied the impact of the threat of cyber attack by isolating severity of the attack on the information system or customers data itself. Lastly, researcher looked at the way the response team reacts to an incident or threat having known its nature and impact. The modeling and mapping was guided by Olding and Turner (2007) conceptual framework who suggested that the response to an incident or threat can either be proactive, reactive or mitigation.

In essence, the findings indicated that a better understanding of the nature of a threat, the lesser the impact of an incident and ultimately the better the response will be. It is quite imperative to know that in hospitality industry, when a reputation of a given destination is negatively affected, needless to say that the customers will have to think twice on which facilities to use with trusted information security promised.

6.1 Recommendations

- The stakeholders to embrace the model highlighted in this paper and thereafter expound and address each item of the model using information technology best practices solutions
- The tourism and hospitality industry should be taught on how to employ and effect the defense in-depth mechanism and use of Security information and event management (SIEM)
- The tourism and hospitality industry ought to prepare a sophisticated incident response team
- It is always important to study all nature of threats including APTs (Advanced Persistent Threats) and understand their nature of attack, impact of attack and how to appropriately respond to it using appropriate tools.
- Proactive response is better than reactive or mitigation
- The industry should carry out routine information technology monitoring and audit on the information systems on continuos basis.
- The industry should seriously think of embracing and adopting information security standards best practices such as Payment Card Industry Data Security Standard (PCI DSS) in conjuction with implementation of ISO 27002 an information security standard.

7. REFERENCES

AON Risk Solutions (2015, April 4). Hospitality Cyber Risk and Solutions. Financial Services Group.

Fobert, J., & Chase, W, B. (2014). Hospitality Risks: Keeping Pace With Emerging Exposures. Retrieved from http://www.acegroup.com/us-en/assets/ace_hospitality_wp.pdf

Karpuk, V, K., & Kelly, M. (2015, April 8). The Evolving Cyber Security Regulatory Environment. Hospitality Technology. Retrieved from http://hospitalitytechnology.edgl.com/news/The-Evolving-Cyber-Security-Regulatory-Environment103908

Kefgen, K., & Wolff, S, K. (2015). Cybersecurity: A Hospitality Industry Reality. AETHOS Consulting Group.

Kigen, M,P et al. (2015). Kenya Cyber Security Report. Achieving enterprise Cyber Resilience Through Situational Awareness. Serianu Limited.

Olding, A., & Turner, P. (2007). Cyber vulnerabilities and the tourism industry: developing a conceptual framework. ACIS 2007 Proceedings, 116.

Orthus White paper (2011). Hospitality Sector: New Target for Cyber Crime? Orthus Businesses as usual, Guaranteed.

Palagonia, P.(2015). Unique Cyber and Privacy Risks of the Hospitality Industry. Retrieved on April 12th, 2016 from http://blog.willis.com/2015/09/cyber-and-privacy-risk-advisory-hospitality-industry-spotlight/

Piper, DLA. (2013, February 20). Hospitality and Leisure: Cybersecurity - the new frontline. Retrieved from https:// www.dlapiper.com/~/media/Files/Insights/ publications/2013/02/Hospitality/Files/hospitalityandleisurecybersecurity/FileAttachment/hospitalityandleisurecybersecurity.pdf

Pitmans (2013). Do not disturb: Managing Data Protection and Cyber Security in the Hospitality Sector. Retrieved on April 7th , 2016 from http://www.pitmans.com/news/article/do-not-disturb- managing-data-protection-and-cyber-security-in-the-hospitality

Pizam, A., & Mansfeld, Y. (2006). Toward a theory of tourism security. Tourism, security and safety: From theory to practice, 1-28.

Tripwire (2016). Retail and Hospitality Cyber Threat Defense. Retrieved from http://www.tripwire.com/it-industry/retail-and-hospitality/ on 7th April, 2016 at 2:40 pm

Walterscheidt, K. (2010). PCI Compliance and Hospitality Industry. The Bottom line. The Journal of Hospitality Financial and Technology Professionals. Retrieved on April 14th, 2016 from https://www.hftp.org/i/downloads/The_Bottomline_Articles.pdf

Cite this article:

Ronoh, L. (2016). Mapping and Modeling Kenya's Hospitality Industry Cyber Security Factors: Case of Selected Hotels in the North Rift. *Mara Res. J. Comput. Sci. Inf. Secur.* Vol. 1, No. 1, Pages 132 - 140, ISSN 2518-8453