iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** II **Month of publication:** February 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

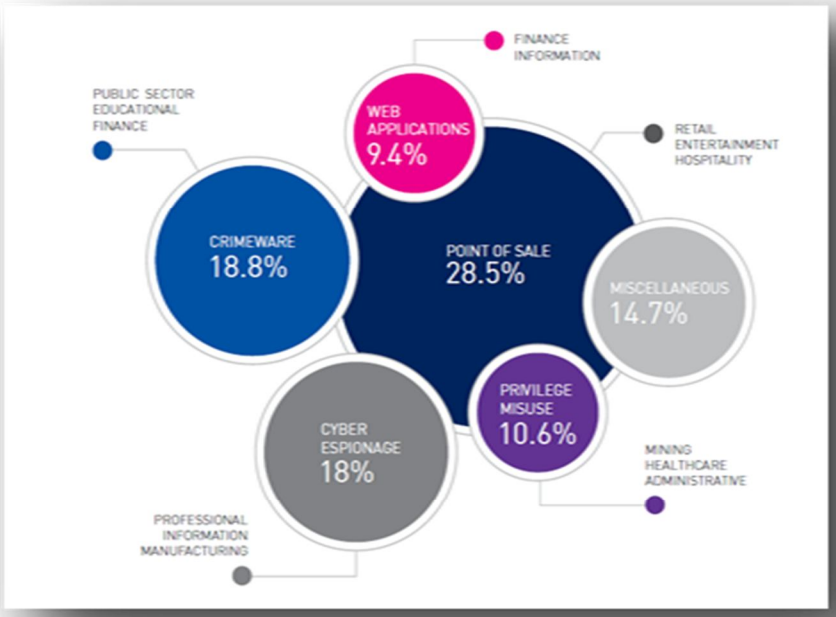
International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

Cyber Security Attacks in Hotel

Mrs. Malarvizhi. D[1], S.Nandhini[2], K.Sruthi[3], A.Veneshia Kathrine[4], S. R. Prateeksha[5]
[1]*Assistant Professor,* [2, 3] *III-BCA-A,* [4]*III-BCA-A,* [5]*III-BCA-A, Department of BCA & M. Sc. SS Sri Krishna Arts And Science College, Kuniamuthur, Coimbatore-08*

Abstract: ***to secure the computer networks. The research is completely qualitative while the case study and interviews have done in five random hotels in Reno, Nevada, USA.***
Keywords: Internet of Things, Cyber-attack, Security threats.

What is cyber security?
As with any technological advance throughout history,there will always be those that exploit them for their own gain,whenever new opportunities are created.



I. INTRODUCTION

"Modern societies have become increasingly dependent on Information and Communication Technologies that offer both opportunities and challenges with respect to improvements in the
quality of life of people and the communities in which they live". Technology in hospitality industry is driven by the increasing transaction volumes, complex reporting requirement, and international communication needs. Information technology (IT) can improve almost all areas of hospitality industry, such as guest services, reservations, food and beverage management, sales, food service catering, maintenance, security, and hospitality accounting.To protect the public trust and to prevent copycat hackers to hack into an organization's computer system, most of the organizations try not to reveal the data breaches and cyber attacks against their computer systems.

A. Cyber Risks and Cyber Attack Prevention Methods

We should know that none of the security software, antivirus, and other tools can % 100 guarantees to prevent hotels and any other business from cyber attacks (Accenture operations,n.d.). On the other hand, securing and limiting the system too much may cause other problems

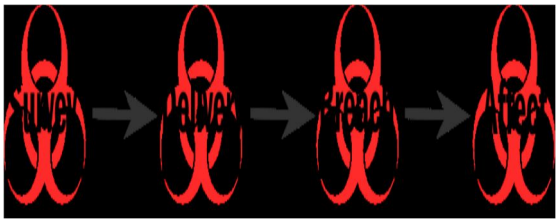
such as preventing the customers to access the information they might need; thus, hotels and other organizations should manage the risk in cyber defense which according to (Accenture operations, n.d.) requires a meaningful and understandable operational model which causes

balance in security implementation and operation as well as using the newest technology for cyber defense excellence, there are three steps available, which are: 1. Prepare and protect 2. Defend and detect and 3. Respond and recover.

1) *Prepare And Protect:* this step will give us a big view of the security performance in support of businesses. It makes us aware of the threat intelligence existence and will make us ready to manage our business vulnerability. In this between, experts will need to have forward thinking capabilities to help scale activities and on the other hand IT strategies will be designed based on great understanding of assets, data sets, technical and business functions.
2) *Defend And Detect:* in this step which is very critical, the forward thinking capabilities should effectively help the scale activities so that operational monitoring and controlling capabilities be able to analyze the security in an advance level which focuses on visualization to understand and identify the anomalies and suspicious activities
3) *Respond And Recover:* in the last step which focuses on intelligent incident response, some active defense strategies will be take into action which requires the security incidence management. This step is the art of the platforms to catch the hackers and attackers or any other threat to the business.
4) *Common Cyber Attacks - Stages and Patterns:* Regardless of whether an attack is targeted or un-targeted, or commodity or tools,attacks have a number of stages. Some of these will meet their goal whilst others may or may not be blocked. An attack, particularly if it is carried out by a persistent adversary, may consist of repeat stages. The attacker is effectively probleming your defences for weaknesses that, if exploitable, will take them closer to their ultimate goal. Understanding these stages will help you to better defend ourself.

B. Stages Of An Attack

The stages of an attack have adopted a simplifing model model that describes the four main stages present in most cyber attacks:
Survey - investigating and analysing available information about the target in order to identify potential vulnerabilities
Delivery - getting to the point in a system where a vulnerability can be exploited
Breach - exploiting the vulnerability/vulnerabilities to gain some form of unauthorized access
Affect - carrying out activities within a system that achieve the attacker's goal.



C. Purpose and Motivation of Attack

Government websites, financial systems, news and media websites, military networks, as well as public infrastructure systems are the main targets for cyber-attacks. The value of these targets is difficult to estimate, and estimation often varies between attacker and defender. Attack motives range from identity theft, intellectual property theft, and financial fraud, to critical infrastructure attacks. It is quite difficult to list what motivates hackers to attack systems. For instance, stealing credit card information has become a hackers hobby nowadays, and electronic terrorism organizations attack government systems in order to make politics, religion interest.

D. Attacks

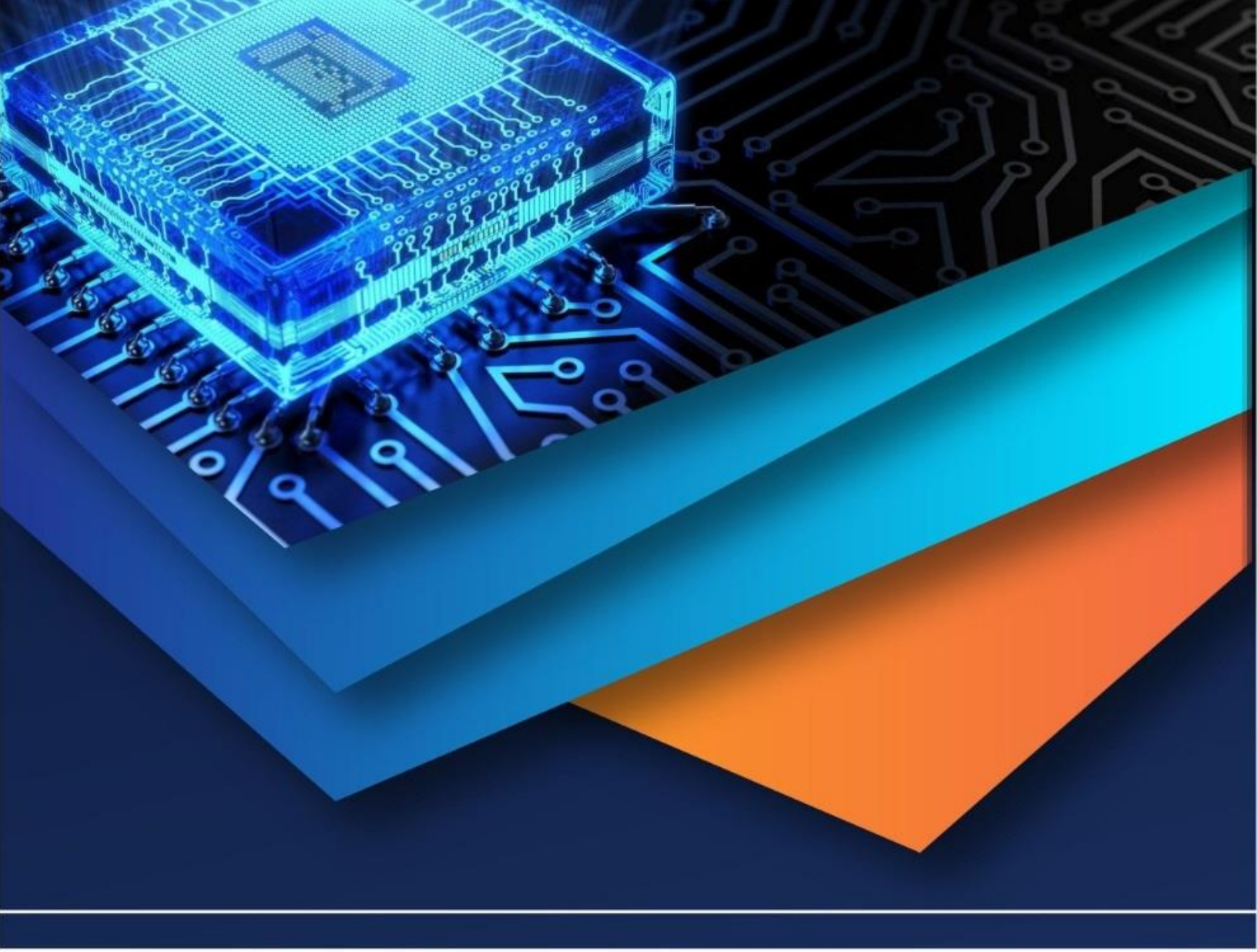
Attacks are actions taken to harm a system or disrupt normal operations by exploiting weakness using both techniques and tools. Attackers launch attacks to achieve goals either for personal satisfaction or recompense. The measurement of the effort to be expended by an attacker, expressed in terms of their expertise, resources and motivation is called attack cost.

II. CONCLUSION

The Cyber security attacks in hotels study tries to explain the importance of the cyber security in hospitality industry. It also discusses about the tools and techniques to prevent cyber attacks. The findings and results of this study after interview with the front desk employees, guests and IT manager/ Assistant of GM in five different hotels that were chosen randomly, shows that not all the hotels in Reno, Nevada has IT manager or someone who dedicates to computer system and networks. Even some of the hotels do not have contracted with any specific IT company to refer when the face any challenge or problem and they call random IT professionals from different companies to fix their computers' problem.

REFERENCES

[1] A, B. (2015). Evaluating Database Security and Cyber Attacks: A Relational Approach. TheJournal of Internet Banking and Commerce, 20(2)
[2] S. Andrew "Internet of things, smart spaces, and next generation networking," Springer, LNCS, vol. 7469, p. 464, 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY