International Journal of Business and ICT
Edited in association with the American Society of Competitiveness
March - June 2017, Vol.3, No.1-2
ISSN: 2412-9917 www.IJBICT.com

The Effects of Breach of Information on Guests and Properties in the Hospitality Industry and Solutions

Alaa Gado Kana Ph.D
Adjunct Faculty, National University, College of Letters and Sciences
11255 North Torrey Pines Rd, La Jolla, CA 92037, U.S.A.
E-mail:alaa_kana@yahoo.com

Abstract:*This article is about the effects of breaches of information and personal data for guests and customers in the hospitality industry. The hospitality industry properties like any other businesses lends great importance to protect the personal information of their customers and guests. Also, they significantly value impacts on management and customers and the guests themselves in sometime in terms of providing the privacy, safety and security. A lot of customers and guests have believed that their information and personal data are in safe of danger but that is not true. While most hospitality properties managements considered that information and data extremely important and adopt best ways to maintain them, we see at the same time exposure of a lot of properties and establishments around the world to various types of violations. At the conclusion we prove some solutions to the issue.*

***Keywords*:** Dumpster diving, Juice Jacking, Mousejack Attack, Phishing, Shoulder Surfing, Pertrxing, Piggybacking, tailgating, baiting, EMV.

I. Introduction

Everyone knows that the main objective for hospitality properties is to provide a pleasant stay to their guests and satisfy and exceed their needs and wishes by offering them unique services also for the rest of customers and guests who attend the property outlets. But at the same time it is imperative for the management of those properties to have great responsibility towards their guest and customers in finding the best ways to ensure safety of their personal data and information and keep it secret due the great importance to both sides. Any leak like hacking or violation of their data and information will affects and cause a bad psychological and material impact on the guests, customers and management in same time.

II. The Importance of the Personally Identifiable Information

Protected information represents the greatest amount of liability and financial risk to the hospitality properties, and these protected data and information must not be shared with unauthorized individuals or the public. Protected information include personally identifiable information (PII), card holder information, financial information, and protected health information (PHI). Protected information is subject to strict processes and technological controls.

In spite of that a lot of specialists agree that technological development and programs had an important role in the properties of the hospitality industry through its dramatically and effective contribution in facilitating the management procedures of data and information, at the same time it did not prevents or reduces the size of the risk that face the hospitality properties like violations and breaches especially those related to the data and information security and privacy [9]. For example, in recent years many hospitality properties in the United States saw a lot of breaches and violations in this regard:

- In June of the year 2005, the credit cards processing unites in the United States allowed to the credit and debit cards to broke almost 40 million credit card numbers, effecting Visa, Master Card, and American Express credit cards. And later turned out that the reason for this was because the network used for the credit cards were not in conformity with the security standards.
- In July of the year (2007) an employee in checks Services Company stole worth of 8.5 million from the company's records, which included the theft private credit card statements, bank statements, and personal data. He has been accused of fraud and was found guilty and sentenced to a prison for 57 months, imposing a fine amounted of $ (3.2) million US dollars on him.
- In the month of May of the year (2010) chain hotels with more than 30 properties faced piracy and rob of more than 700 personal data guests files, and it turned out that the hackers were able to use that information and data for a few months after the theft. The value of the damages estimated by hundreds of thousands of dollars.
- In the month of November of the year (2011), an hotel auditor was accused of stealing data and information for (237) credit cards belong to hotel's guests and customers, and then he sold it to someone who in turn purchased the precious needs amounted more than 840 thousand American dollar[12].

Unfortunately, to this day a lot of hospitality properties did not raise to the level required to update their plans and programs especially those related to the risk management to face and address the risks related to the personal information and financial data management although of aware of those properties the negative impacts on the company's financial stability and its success. The impact was so negatively on the property reputation.

III. Information and Data Sources in Hospitality Industry

As part of those operations, the hospitality properties management reserves enormous information base and great personal information for its guests and customers, in addition to the lack of obstacles and barriers to access to such data or impenetrable as a result of lack of interest in some of these managements in some cases by the security and confidentiality of such data and information. It is worth mentioning that most of the information and data sources are the customers and guests themselves, through several forms including:

- When guests and customers submitting their personal information and data for making room reservation through internet (Online) or when they reserve a tables in the restaurant, bar, ballroom ... etc.
- Guests and customers' bills which charged to the rooms as a result of ordering or purchasing services and products in the hospitality property outlets such as restaurant, bar, coffee shop…etc.
- When Guests and customer subscription in points or rewards programs for the hospitality industry properties and outlets, such as hotels, restaurants…etc., which is called (Member Rewards), this program requires giving them periodic discounts and other benefits due to their use of products and services.
- Guest and customer submitting their information and data when they visit (concierge office/desk) [13].

IV. Hospitality Industry: Targeted Industry

Hotels and restaurants considered today part of an important and vital installation in hospitality industry. In fact, statistics indicate that both are considered the largest sectors at risk and significantly for various types of electronic violations those related to credit card and so on. In particular, the global security report issued by (Trustwave) in the month February of 2010 refers to that hacker who was dramatically targeting hospitality industry properties. The report pointed out that the (38%) of those breakthroughs were in hotels and resorts and (98%) of them targeting the guests and customers and credit card numbers [2].

Today a lot of hackers use various modern techniques to obtain the maximum amount of individuals' personal data and information. They steal their identities and money or sell their personal information to third parties, and unfortunately those hackers considered it a lucrative market to them through the collection and re collection of those data. In same time some bad people and criminals may exploit it to hunt down and steal a person's identity and impersonating capacity or to help in some criminal acts which increased recently [6].

That most data and information that are exposed to penetration continuously in hospitality properties is one or more of the customers and guests personal information related to the financial statements so the information or personal data is a legal concept, not a technical, and are defined as information that can distinguish a person from another. Or, it could be said it's that information that is used for the purpose of expression of individual identity or to track someone's identity. Also it can be seen that data consider unknown to conceal the identity of someone. In this regard, in (1990) the identity of 87% of the US population was uniquely gotten through gender, post code, full date of birth [7].

The personal information under the (National Institute of Standards and Technology) means any information or data about individuals with any agency or entity. And these information include full name, personal number or social security number, date and place of birth, mother's name, personal address or home address, e-mail, or identification card number or digital card, passport number, vehicle registration papers and car number, driver's license data, fingers printing, individual hand writing, the genetic information, the person's phone numbers such as work phone number or a home phone number or cellular device number, user name and password to log in to a computer or PIN number, and vital records. Or, it includes any other information that can be linked or associated with the individual, such as health, educational, financial information, or those related to work and employment [1]. There is also information used less to distinguish the individual identity because it is common traits among humans, and in any case they are part of the personal information they share with other information to identify the individual, the most important are first and last name, country, city, age, gender, school name, workplace, grades, salary, job, and criminal record.

While the financial statements include those relating to credit card numbers and bank account numbers.

On the other hand many experts in the hospitality industry saw that the main reason why the hospitality industry properties is an easy target for many hackers than other industries because the size of the daily and repeated operations derived from the use of guests to the outlets of these facilities, and repeat use of their personal data and credit cards when they buying products and services.

V. Definition of Breaches or Hacking

The process of data and information violation called piracy or the so-called in English (Hacker) that means any penetration which unauthorized access to person's network information and data or his/her personal accounts, or personal computer by someone else.
A common example is the infiltration of e-mail and a breach of the company or a person. The practice or the process of finding and release this information called (Doxing). Some other specialists individuals from outside the property do this type of theft, called today (Breach), which is of course different from (Hack). It means to see or steal data and information that are protected by a person or unauthorized entity and always result to identity theft or other types of fraud. Both processes their sentences in most countries to reach arrest, especially if had caused harm to someone.

VI. The Costs of Information and Data Breach

Like other businesses, the hospitality properties are also exposed from time to time to the various types of breaches and the global security report (Trust wave). For the year (2013), it has pointed that (9%) of all information and data breaches has been in the field of hospitality, making it the third most tertiary industry vulnerable in this area.
The big negative impact that hospitality properties suffered reflected it exposed in expenses and additional costs as a result of those breaches or violations and those costs could be turn into massive losses of the company. Those costs include costs and various expenses that are paid to matters relating to the dangers and complaints procedures and claims and the costs of monitoring customers and guests credit card services who have been busting their information to reduce the size of the potential civil suits. This is in addition to other costs such as those related to hiring a team of public relations as in big hospitality companies to help control the damage caused by these violations and maintain the reputation of the company from collapse. Or that costs related to the creation of the main reasons for the occurrence of these violations and restore the data and information that were lost. In addition, the complaints and claims related to know the reasons for failure in not available, the reasonable safeguards to protect personal and financial data, in addition to the losses in lost revenues from prospective customers who choose to competitors as a result of those violations [11].
The hospitality property management considered is engaged directly about informing customers and guests who are affected in case any breach happen to their information and data. In this regard, in the United States a clear laws has been enactment in (46) state related to informing in case any personal or financial information exposed to suspicious actions like lost or stealing. Furthermore, protection in the case of individuals personal data affected from other states for certain violations so the management must compatible with the laws of that state, and that compliance with those laws can be costly and take long time because it requires a search in the privacy laws of each potential guest place of residence affected, as long as many hotels and restaurants welcome customers and guests within the United States and abroad. The informing requirements and associated costs take special dimension and big importance.
The possibility of controlling these costs can be reduced significantly if hospitality facility management has a good plan early. Studies suggest that the direct average cost of these intrusions vary from one study to another but they share in one common thing that it is very expensive. According to a (Ponemon) Institute report for the year (2011), the average cost of

data breaches for the year (2009) have reached (6.75) million per incident and (204) dollars for each individual record. According to the (Symantec Corp) company for the year (2013) and (Ponemon) Institute, the average cost of data breaches reached 136 dollars per record [3]. In addition, these breakthroughs cause losing customers and guests trust in hospitality properties such as hotels, restaurants, etc. and distort its reputation at a time many properties consider that its capital is invaluable and extremely difficult to compensate.

VII. Types of Violations in the Hospitality Facilities

The importance of information and data security in the hospitality industry has increased in recent years with the increase of bookings types via the World Wide Web with the increasing ways of collecting data available by as a means of social communication, telephone applications and booking sites engines. Also, the personal information and data concept has become spread and wide dramatically such as information technology and became it is very easy to collect that information by breaching and violating the internet networks security and the internet browser.

There is A concept that large hospitality properties need to protect their information and data from penetration, and of course this is wrong and untrue concept, as statistics indicate that in the year (2012) and according to (Verizon) report that two thirds of the (855) of the investigation into the companies incidents cases happened from (11-100) employees, with a subscription to many hospitality companies. In any case, there are no hospitality company exceptions from penetration. Independent and small companies are vulnerable to penetration greater than others because it is small and has systems easy to penetrate [8].

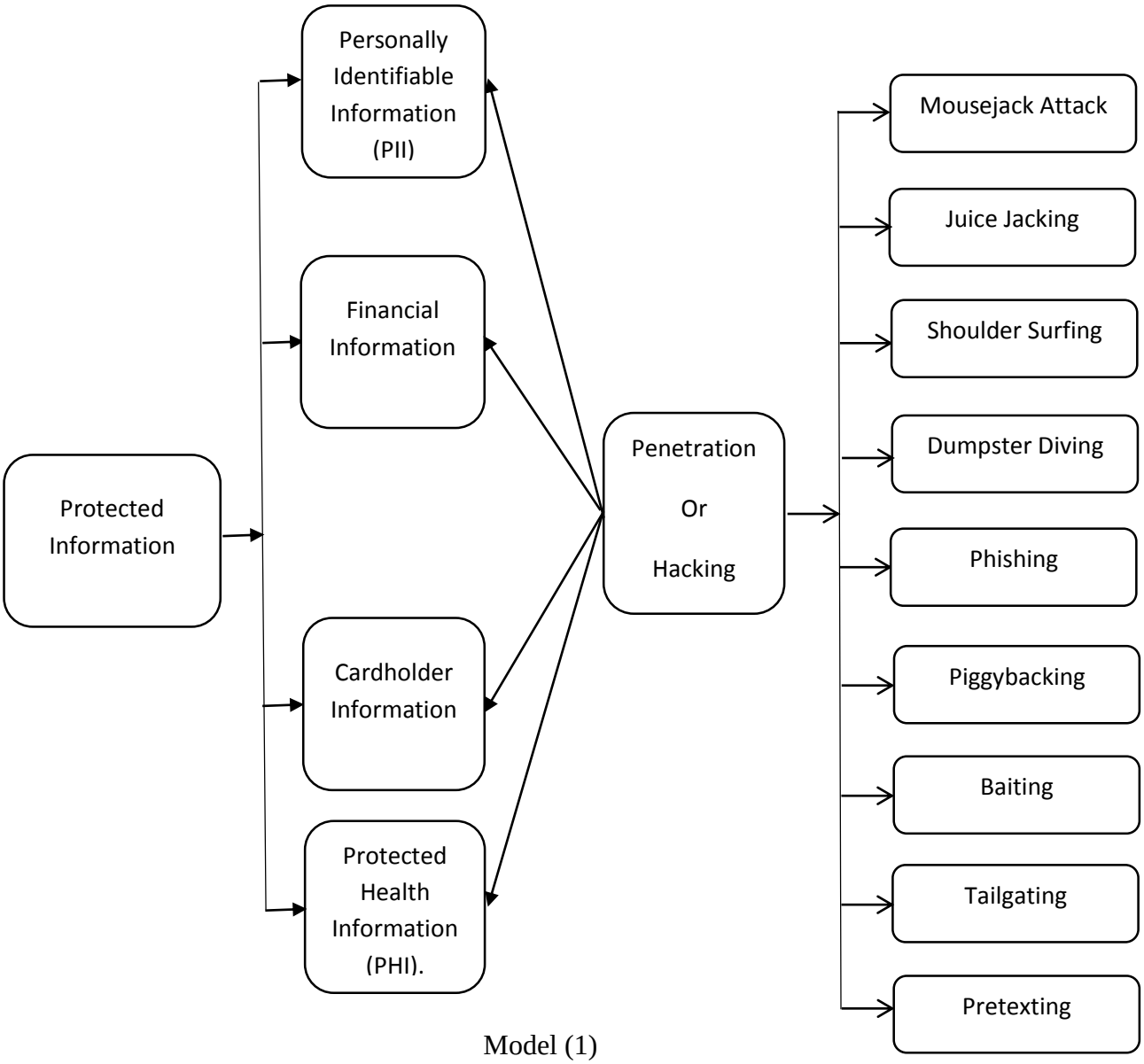
The main features of hospitality properties is that they are characterized by higher operational and especially in peak periods, making it as an industry vulnerable more than others for the operations mentioned above. Stealing guest and customers statements by people from inside or outside the hospitality property meant here not only by some people or unskilled employees but by some other individuals from outside the property and the specialists in this type of theft. For example, in hotels, which are consider one of the most important hospitality properties, most guest and customers exposed to breakthrough their personal data and information starting from the registration procedures (Checking in) and when housekeeping cleaning the rooms through other hotel outlets when guest using services and ending by departure (checking out). All those places shares guests data and information, so hundreds or even thousands of them are exposed. This applies to the rest of other hospitality properties [13].

On the other hand a study for (Trustwave Spider Labs) found that same thing applies to the food and beverage outlets as well, and the machines of these outlets are also vulnerable to penetration in addition to failing to disclose such breaches only after a long period of occurrence. As the study revealed that these hackers are not discovered when they break food and beverage outlets devices for (173.5) day and on the size of the high transaction and delayed disclosure of those breakthroughs as time can destroys a lot of those business [8]. And the penetration ways is varied from hackers to another's and from hospitality property to another, as model (1) below:

- When guest or customer leave or throw any documents or papers that contain data or information in the trash can, especially the ones that contain information or personal data such as name, address, account number etc. Or, when she/he don't ask about the bill like when taken a cup of coffee and then inform the server he don't need the bill or receipt, or the

server or the guest throw it waste basket, and then after a few moments someone pull the receipt from the waste basket and get the guest personal information. This kind of information theft is called (Dumpster diving).

- Another type of information and data theft is called (Juice Jacking), which mean stealing guest personal data from their cell device by someone while their cells on charging in a public area in the property like near the reception, bar, restaurant or in business center ... etc.
- When a lot of guests using their electronic devices in public areas in hospitality property like reception, lounges, or in some cases, in meeting or conferences rooms, exposing guests to penetrate their information or their own data, which is called (Mousejack Attack).



Model (1)
Kinds of penetration in the hospitality properties

- When guests using their devices near a stranger person or when there is someone near them, especially when they are checking their e-mails or when they access their personal information, and even when on social communication, putting their knowledge and their personal data on risk. This is called (Shoulder Surfing). This is also happens when guest attending a conference somewhere within the hotel corridors and noted that there is someone in elegant suit nearby. The guest assuming that he/she is also attending same meetings or conference sessions and continues
checking his/her e-mails or letters without paying attention to the seriousness of the matter.
-The other type of guest's information and data penetration called (Phishing), and it's a process that hunt the e-mails, and it's dramatically widespread phenomenon. In some cases, the message would be attached to the supplements so called (Attachments), and when the message is opened or when the guest click on unknown links the guest or even the employee sometimes will be a victim of what called (Malware) or called (Ransomware). One of a simple example is when guest received a phantom link in a letter by e-mail informing him that there is an incorrect cash movement in his bank account or an important message ... etc., and will click on the link, which then asks to put user name and PIN so the link start stealing guest's personal data and information [12].
-Our guest PII in risk and vulnerable at every place that a person visits the property like at checking in, point of sale etc... For example, it's very easy to steal guest information and data on reception office itself especially when the receptionist spoke to the guest and called him by own name or notified the guest to his room number aloud in front of those present in the reception area.
-When customers and guests using their credit card in hospitality property outlets such as when they are in the bar or in the restaurant, or when they purchasing some needs from the gift shop, which required using credit cards. At that time the guests' personal data will be vulnerable to theft by those devices (Credit Card reader) or through other methods such as (Malware). One study reported that more than 65% of the computers data in the hospitality industry was by hardware sales centers (2015 Trust wave Global Security Report) [12].
-When housekeepers leave guest room door opened while they are cleaning the hotel room or hospitality property, and unauthorized persons enter the room; or, when housekeepers open room door to someone without verifying his identity when he lost his room key.
-Improperly sliding guest bill underneath his room door, and pulled by another person, which displays the guest to steal his information and data.
-By using Personally Identifiable Information to make request seem legitimate so more information is divulged, this is called (Pertrxing).
-When authorized personnel convincing an agent in the property to let him enter a secure area, which is called (Piggybacking).
-When someone following an authorized person into a secure area without their permission which is called (Tailgating).
-When someone leaving USB drives in random places or sending them to unsuspecting recipients, when inserted into computers property. They install a virus which is called (Baiting).
-When intrusive software that allow unauthorized access to a computer or network, which is called (Malware).

VIII. The Best Methods to Protect Data Security in Hospitality Industry

The basics of management in the hospitality properties is to enhance and continuously protecting the security of guests data and information, and this helps to build trust with them dramatically and makes them feel safe and at the same time enhances the property reputation. Therefore, it is necessary to educate and raise the awareness of employees, customers and guests about the importance of the security of their data and information and communicate with them about the information and data privacy because it's very important. This matter is responsibility of all employees at the facility starting with the manager and through supervisors and ending with the workers [5].

On the other hand and to reduce the customers and guests' information credit cards penetration incidences and to prevent stealing their data, the credit cards companies in the United States created a new and modern technology to protect customers credit card called (EMV) or (Europay, MasterCard, and Visa) that will help protect against credit card fraud and theft. This technique summed up by putting a small computer chip in the card credit, making it safer, before the payment transactions in the old credit cards were formerly required swiped the card by the user or employee in the credit card reader device to obtaining the funds. Since all the user data in the black bar at the back of the card, which makes it easy for hackers to use different cards to obtain the users data, the new technology let the users put the new card in the machine. This process called (Dynamic Authentication). After the completion of the transaction the user pull or withdraw the card and there will be no card code in the machine which that means it is a faithful way to do the financial dealings [10].

The hospitality property management pay attention to the following procedures that limit the guest information and data penetration and most important:

- Hospitality property be aware of the privacy laws and notification requirements relating to guests and customer data.
- Be sure the hospitality properties managements use the compatible devices that fit with the credit and debit cards.
- Keep track the information and personal data and get to know all the parties that have access to this data, and perform the audit regarding the employees who have the ability to access the personal data.
- Make personal data and information security a written policy in the workplace.
- The necessity of securing all data and information on the hotel devices and computers. They must be protected by a private code to access, in addition to following the best procedures and hard arrangement to protect the information and data security through updating the protection programs belonging to the property computers periodically and in a regular basis.
- Recent studies indicate that lost or stolen mobile devices are the most common reason for information and data violations and breaches, so it is necessary to pay attention when using laptops, smart phones and do not allow to plug any unknown devices like external hard disks and Flash Memory (USB) devices to any of property computers under any circumstances. Doing so infects the computers with malicious software that could compromise the computer and possibly compromise protected and confidential information, and will be a strong threat to the hospitality proprieties.
- Hospitality properties may provide services to third-party vendors which require guest information and data, if so required the sellers must sign agreements to protect property from any breach of the data process may involve personal information.

- It is important to property to have an insurance coverage to mitigate losses when it occur, and to consult with the insurance company when their data is at risk and find the best solutions.
-The hospitality property should have the ability to hire or contract with consultants or experts in dealing with any kind of intrusions or violations property may be exposed, and in this regard there are also private parties that provide their services for this kind of problem.
-It is possible to get assistance and benefit from other sectors like banking sector and place it in the hospitality business, especially those related protection of the financial and information statements.
-Save all the paperwork related to credit card authorizations that related to guest payment in a safe place and locked always in order to preserve the confidentiality of the guest personal information.

IX. The Role of Employees in Guest's Information and Data Protection

The employees play a huge and important role in reducing the intrusion or violation that could be happened and this is reflected clearly through their participation in or during their performance of their daily work through the following steps:
-The necessity to have all employees trained properly by the property management and to deal properly with all positions that are related to recording guest information and data. Also at the same time the data security policies includes management agreements to allow them to reach and quick the guest data and information in case any inquiries from management or guests themselves.
-All guest information must be in the property computers, and it's very important to ensure that all guest personal identity is matched with the credit card provided before issuing the room key to the guest.
-Training employees to respect the confidentiality of guest personal information by not revealing or permitting any information or data relating to anyone either by phone, fax, etc.., where often a lot of employees in the property receiving a lot of phone calls in various work shifts from unknown people where their purpose is to obtain guests' personal information.
- The employees should never follow the caller's instructions. Computer criminals often pretend to be others in an attempt to gain unauthorized access to system and information. These criminals often have information about the property and mention employee names in their attempt to gain their trust. Following instructions of an unverified caller can lead to computer compromises that put protected and confidential information at risk.
-Be sure that the agent do not repeat loudly guests' information and data or room numbers in registration procedures or checking in process in front of other the people. It is recommendable to inform the guest's room number in a low voice or writing it on a piece of paper or on the cover of the room key.
- Do not give any key or allow unknown persons to enter the guest rooms under guest's friends or relatives. It is necessity to check the personal identities of those people and register their names with the security presence.
-The guests must have high awareness and understanding about using open network or make any financial transactions throw open network area and unsecured properly, and should be always cautious when they are using their devices in a public area (without wire). Today, lots of companies provide what is called (Patches) to protect these devices from possible types of attack.

- Customers and guests must not throw any bills that containing information or personal data in the trash, preferably shredded by paper shredder machine to avoid the information theft.
-Advice customers and guests to avoid charging their cellphones or devices in public areas in the hospitality property, and need to keep their devices charged always.
- All employees must pay attention continuously when they opened their work emails, or when they access to the guest personal information, and make sure there is no stranger or someone near them can peek or theft certain data. The same thing applies to customers and guests as well.
-When there is any doubt about any letter by email, the guest and even the employee must not click the hyperlink and never replay to the email because a hacker site attempt to get the agent or guest login information. Hackers use emotions to push them into doing something pretending to help them. They frequently use words with a sense of urgency that something bad will happen. Also, both must be cautious when opening any attachments, and avoid pressure of the unknown links. Otherwise, the employee or the guest himself will be a victim of what is called (Malware) and / or called (Ransomware). According to the U.S. Department of Justice report, in the past ten years victims in the United States have paid more than $57 million to hackers as a result of ransomware. This is a phishing attempt to get them to enter their login information to access property information [12].
-On the housekeepers, they must be attentive to not allow any non-authorized personnel to enter the guest rooms. It is important to keep room door closed when they finished cleaning the room. They must ask the guest to use own door key to enter his/her room and do not request from housekeeper to open door for them. If the guest room key does not work or the guest has no key, the employee advice him to go to the front desk to get a new key. In emergency cases, the guest room can be opened by hotel security after making sure of the identity of the room holder by confirming it from front desk.
- Slide the guest bill underneath the room door properly by push it inside the room completely to avoid stolen by others.

X. Conclusion

The financial stability and continued success of the hospitality properties is very important and both are based on the proactive approach of information and data's security risk management, so the weak and slothful procedures or existence a security gaps could lead to guest's information and data breaches and violation, in addition financial and reputation loss.
The maintaining process of the confidentiality and security of the personal information has become the priority of all managements in hospitality industry. They start using the appropriate measures to protect the personal information of their customers and guests and preventable from of unauthorized access or violation. They do that by complying with all applicable information security, privacy and data protection laws, and contractual obligation globally. They must provide continues training and awareness programs, policies, procedures, and hospitality brand names standards to ensure information security and privacy compliance to reduce the size of the gap that could have negative impacts on the hospitality property [4].
Today, a lot of developed countries including the United States attach to this issue great importance. This is manifested clearly through the enactment of many laws and regulations that restrict these operations to protect customers in various sectors from exposure to such practices of stealing information and data. At the same time, a lot of managements of hospitality properties make sure to follow up on this issue by devoting a lot of time and

resources in processing and protecting data and related information in order to provide the best services to their guests and customers to increase their loyalty.

Reference

[1] Brandley, Aaron. "Online Website Security: What is PII?, N.p., 01 August 2016. Web. 03 Sept. 2016.http://www.onlinewebsitesecurity.com/tag/personally-identifiable-information.
[2] Cole, Robert. "When Will Hotels Get Serious About Protecting Guest Information?" RockCheetah. RockCheetah, 26 June 2013. Web. 06 Feb. 2017.http://rockcheetah.com/blog/security/when-hotels-serious-protecting-guest-information/.
[3] Gregory, Jennifer Goforth. "How Hospitality Can Brace Against Breaches." Hospitality Technology: Technology Resource for Restaurant/Lodging Executives. N.p., n.d. 06 August 2013, Web. 05 Sept. 2016. http://hospitalitytechnology.edgl.com/news/how-hospitality-can-brace-against-breaches-87650.
[4] Haley, Mark G. "Magazine." Hospitality Upgrade.01 Oct. 2012. Web. 15 Feb. 2017. http://www.hospitalityupgrade.com/_magazine/magazine_Detail.asp?ID=763.
[5] Malhotra, Arvind, and Claudia Kubowicz Malhotra. "Evaluating Customer Information Breaches as Service Failures: An Event Study Approach." Journal of Service Research 14.1 (2011): 44-59. Web 07 Feb.2017. http://journals.sagepub.com/doi/pdf/10.1177/1094670510383409.
[6] Marion, Roger H. "Magazine." Hospitality Upgrade. N.p., 01 June 2013. Web. 06 Feb. 2017. http://www.hospitalityupgrade.com/_magazine/MagazineArticles/Protecting-Guest-Data-is-no-Picnic.asp.
[7] McCallister, Erika & Grance,Tim & Scarfone ,Karen; U.S. Department of Commerce, National Institute of Standards and Technology, Special Publication, 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Recommendations of the National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.
[8] Montera, Nick. "Hospitality Industry Risks: Data Privacy and Security - Insurance | Employee Benefits | Surety – Parker, Smith & Feek."Insurance Employee Benefits Surety Parker Smith Feek. N.p., 05 July 2016. Web. 03 Sept. 2016. http://www.psfinc.com/articles/hospitality-industry-risks-data-privacy-and-security.
[9] Olsen, M. D., and D. J. Connolly. "Experience-based Travel: How Technology Is Changing the Hospitality Industry." Cornell Hotel and Restaurant Administration Quarterly 41.1 (2000): 30-40. Web. 07 Feb.2017. http://journals.sagepub.com/doi/pdf/10.1177/001088040004100121.
[10] Palagonila, Gamelah. "Unique Cyber and Privacy Risks of the Hospitality Industry." Willis Towers Watson Wire. 29 Sept. 2015. Web. 15 Feb. 2017. http://blog.willis.com/2015/09/cyber-and-privacy-risk-advisory-hospitality-industry-spotlight/.
[11] Thompson, Van. "Confidentiality in the Hospitality Industry."Confidentiality in the Hospitality Industry | Chron.com. Chron, n.d. Web. 15 Feb. 2017. http://smallbusiness.chron.com/confidentiality-hospitality-industry-75152.html.
[12] Venzapeak, https://www.venzapeak.com/davidsonhotels/enterprise/student/mycourses.php.
[13] Winder, Jason, and Greg Levine. "HOSPITALITY INDUSTRY PRIVACY." WASHINGTON DC | BOULDER CO. N.p., 06 Apr. 2016. Web. 12 Jan. 2017. https://aerstone.com/wp-content/uploads/2016/04/Aerstone-Whitepaper-Hospitality-Industry-Privacy.pdf.

Author

Alaa Gado Kana is a professor and instructor at National University and San Diego State University, respectively. Dr. Kana has been working for San Diego Hilton Gaslamp Quarter since 2008, and has been working in the hotel management field since 1985. Dr. Kana's career also consists of lecturing at several universities in Iraq, Jordan, and United States. Furthermore, he was assigned as a member of the Board of Directors and General Manager of Baghdad Hotel in Iraq. In addition, Dr. Kana is the author of four books that address hospitality management. Dr. Kana has also published many research articles related to the management field. For more information, please visit the following website:
www.alaakana.com