International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

Information Security Policy Framework to Mitigate Data Breach Due to Human Factors in Physical Locations

Kwesi Hughes-Lartey [1,2*], Zhen Qin [1,3,4*], Francis E. Botchey [1,2], Sarah Dsane-Nsor [2,5]

[1] School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China;

[2] Computer Science Department, Koforidua Technical University, Koforidua EN-112-2188, Ghana, Ghana;

[3] Institute of Electronic and Information Engineering UESTC in Guangdong, Dongguan 523808, China;

[4] Network and Data Security Key Laboratory of Sichuan Province, Chengdu 610054, China;

[5] Computer Science Department, University of Cape Town, Cape Town 7701, South Africa;

***Abstract*—Information Security policy is probably the most important tool that can be used to protected an organization's information and computer resources. However, mostly entities concentrate on the technology and leave out the human aspect of it. Furthermore, these policies do not have anything to do with the physical locations both internal and external. Cyber attacker now takes advantage of human factors and the lack of policy for physical locations to launch their attacks on seemingly strong information security system rendered weak by human behavior and their susceptibility in some physical locations. In this paper, three physical location policy frameworks in relation to human factors are proposed. A linear regression of human factors and data breach incidents associated with physical locations is performed to validated the existing loophole in a strong information security due to their negligence. The results show that vehicles, offices and public places are physical locations that are statistically and significantly associated with data breach incidents due to human factors.**

Keywords—Data Breach; HIPAA; Human Behavior; Information Security; Policy Framework; Physical Locations;

I. INTRODUCTION

The primary way by which organizations conduct operations today is the use of Information Systems (Info Sys.). This provides a platform for data gathering data processing, data storing and making data available for future access[1]. These system often require some kind of Information Security (Info Sec.), which most organizations implement at the technological level and ignoring or oblivious to human factors [2], [3]. To deal with the threats that organizations face as a result of using Info Sys, there has to be a good Info Sec policy which must be generally be high-level, technology neutral, assesses risks, well defined procedures, directions, penalties and countermeasures when policy is transgressed. Info Sec policies are critical to the protection of an organization's info Sys. The policies are created to just to address the problems of keeping up with the increase rate of technological changes, leaving out the human factor problems [1].

To successfully build any Info Sec policy, the focal point must be people. People play a critical role in security systems more than any other thing. Info Sec is not immune to the vital role of people in ensuring its success [4]. Over the years, there have been major advances in information technology and information systems. however, it has not translated to the type of security assurance organizations desire due to the people factor or human factors[5]. Human factors are suspected to be at play in 80% to 90% of information security incidents in organizations [4] [6]. Human factors and technological factors should be considered to be on the same side when it comes to providing a secure security system. Attackers are well aware of this kind of interdependence between technology and people, and are therefore prepared to invest resources such as time and money to exploit human weak points in an organization's Info [2]. An Information Security Management System(ISMS) is a prerequisite to ensuring security, and to achieve the goal of ISMS, a robust security framework that does not only ensures technical mechanism such as authentication and cryptography of essential parts, but also people must be at the core of its design, implementation, and operation[7].

Therefore, consideration of non-technological factors and technological ones is important to promote a safe system. Human factors are the most vulnerable points of an Info Sec system. Factors such as personal gain, irrational behavior can negatively affect the functioning of a good Info Sec system. For example, if an organization has a policy that requires complex passwords from employees, it is obvious that the passwords may be written down i.e., writing on sticky notes and sticking them to the monitors or somewhere on workstations. This practice will most definitely open the flood gate for attackers into the organization. So human factors should be addressed at the design stage of the security system, in line with management policy. Human factors must be addressed at the early stage of system design and in line with ISMS requirements.

Info Sec studies generally focus on the effects of Info Sec with less consideration of security threats quantification, human issues, and clear specification of requirements which could assist senior management to make decisions on resource allocations and deal effectively with security threats[4][8]. Therefore, organizations remain without a clear rationale on specifications of how to achieve Info Sec goals and objectives in regards to human factors, which should have been considered from the early stage of the design process [3]

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

Human factor problems are further deepened when data is breached because the device got lost or stolen, from physical locations such as the premises of the organization, employee's home, employee or organization's vehicle and public places such as car parks, restaurants etc. When devices are lost or stolen, they present a new type of threat to both the individual who uses the device and the organization they work for \cite{tu2014understanding}. The Loss and theft of these devices is a growing risk that is yet to be addressed in detail by the Info Sec community[9].

As the aim of this paper, we propose an Info Sec policy framework for human factors with respect to physical locations and then we examine the statistical significance of physical locations in relation to device loss or theft that leads to data breach.

II. RELATED WORK

Many researches regarding Info Sec concentrated on the technology, indeed most of these studies propose different types frameworks with a technological 'accent' leaving out the critical human factors [8].

A. Corporate Culture

Schein [10]postulates how corporate culture in an essential part of Info Sec framework and how it exist on three different levels. These levels are artifacts, espoused values and shared tacit assumptions. Artifacts are considered to be the day-to-day behavior of employees in the organization that are not only visible but also measurable. Espoused values are the written documents that reflects the organization's formal values, such as its policy statements or vision. Shared tacit assumptions which are the true drivers of employee behavior affects Info Sec and are formed as a result of a joint learning experience based on successful past behavior. This is what Schein [10] classifies as the underlying beliefs and values of the employee. Niekerk et al [11] proposed that the establishment and maintenance of corporate sub-culture of Info Sec will underpin the successful protection of information assets. The whole idea is to ensure that there is a change in employee behavior and it will be necessary to 'borrow' methodologies and theories from behavioral sciences.

B. Human Factors

Hughes-Lartey et al [2] proposed a human factor and technology framework for Info Sec that was aimed at either preventing or reducing data breach incidents in an organization. The study focused largely on human factors and particularly so due to the fact that most researches in Info Sec are mainly technologically driven, ignoring the human aspects of it. Their framework was underpinned by the work of [12], providing a better understanding of human factors at the top level of management, when consideration was being made for an Info Sec framework. Again Hughes-Lartey et al ranked the susceptibility of devices, storages and software, termed as data locations. The rankings showed that laptops where the most susceptible data locations with underlying human factors. However, the study does not consider physical locations as a variable and its implication to data location susceptibility.

There are many Info Sec frameworks that are targeted at solving human problems, but they cover little or do not cover human factors and more especially threats associated with physical locations and human problems [3], [4], [13]. Alavi et al [14] provides a framework for understanding things and the forces that promote a better Info Sec posture. Alhogail et al [8] proposed a conceptualization of Info Sec culture framework that strives to provide a base for organizations to have an effective Info Sec culture and Liginlal et al [15] concluded from an empirical study for human error management framework in dealing with privacy breaches that human errors constituted a high percentage of the errors during information processing and this has an implication for Info Sec.

III. PROPOSED FRAMEWORK

Passwords provide us with some form of digital security by preventing unauthorized user from gaining access to portable computer devices such as the laptop. But it does not do much in preventing the device itself from being stolen or getting lost, thus compromising the data on it. A report by the Federal Bureau of Investigations (FBI) showed that portable computer devices are stolen in the United States of America every 53 seconds [16]. In this section, three organizational policy frameworks for portable computer devices in four physical locations, vehicles, offices, receptions and public places.

A. Vehicles

Fig. 1 shows a framework that can be adopted by organizations in their Info Sec policy framework in helping their employees have a 'desired' user awareness of the steps one can take in ensuring that portable devices in their possession are protected from loss or theft when they carry these devices in their vehicles.

- Lock the Doors

An unlocked vehicle will obviously be an open invitation for a device kept in a vehicle to be stolen. There as part on a comprehensive Info Sec policy framework, organization must take it upon itself in training or educating employees on keeping devices in vehicles. One such important aspect of that training is the importance of having the doors lock. Even if the vehicle in parked in front on one's home or in a place considered to be 'safe' [17]

- Passwords

Even though passwords cannot protect portable computer devices from being stolen as explained at the beginning of this section, they yet still provide some kind of protection in the event that are stolen. Thus making it difficult for the unauthorized person from getting access to the data on it [16]. It is not just important for organization to create the awareness of protecting devices with passwords, but there must also be adequate education on the general guidelines in choosing a strong password to make it difficult for the data on stolen and lost devices to be accessed [17].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

- Register Devices

A mitigating step against loss and theft of devices that should be part of an organization's Info sec policy framework in protecting portable computer devices in vehicles is the registration of these devices. Registering organizational computer devices and its software is yet another great anti-theft measure. By doing so, computer manufacturers and software developers can easily help track and track missing organizational devices or an employee's device with organizational data on it. Locating them becomes possible the 'thief' tries to get the device fixed or upgraded, given that the stolen devices is reported as stolen or lost early enough [16], [17].

- Don't Leave in Plain Sight

Portable device or portable computer devices should not be left in plain sight in the vehicle even if the doors are locked. This can motivate the 'thief' to smash the windows of the vehicle or find another of opening the doors of the vehicle in order to steal the device in plain sight [17].The best place to keep such items in a vehicle is explained in subsection 'Keep Device in the boot' of this section.

- Don't Put in Descriptive Case

Another way protecting portable computer devices is the encouragement of employees not to put the devices in a descriptive case. For example, putting a laptop in a laptop bag in a vehicle, especially in plain sight will make would be thieves guess what may be in it. The case should not point its content [18] Units

- Mark Devices

For the purposes of easy identification when a stolen device is found, organizations must have a policy where devices are marked. The marking should entail inscription of the organization's name on the device or attaching an asset tag unique to it only. The contact information of the organization can be engraved on the device or inside the device, like the battery compartment of a laptop. Nevertheless, care should be taken, and the right tools should be used in order not to damage the device[16].

- Keep Device in the Boot

The best place to keep portable computer devices is in the boot of a locked vehicle. First and foremost this is advantageous for the particular purpose of it being out of sight[16].

- Tracking Solutions

This is a scenario that is more like preparing for the future, in the event that a portable computer device is stolen from one's vehicle. The devices should be fitted with a tracker before it is stolen. This will help in monitoring and laying the groundwork for easy recovery when theft of loss takes place. Online services like Ztrace and Lojack allow users to disable their computers, erase information, prevent unauthorized access to files, delete information and pin point its location remotely. These services are also affordable and at completely worth it[16].

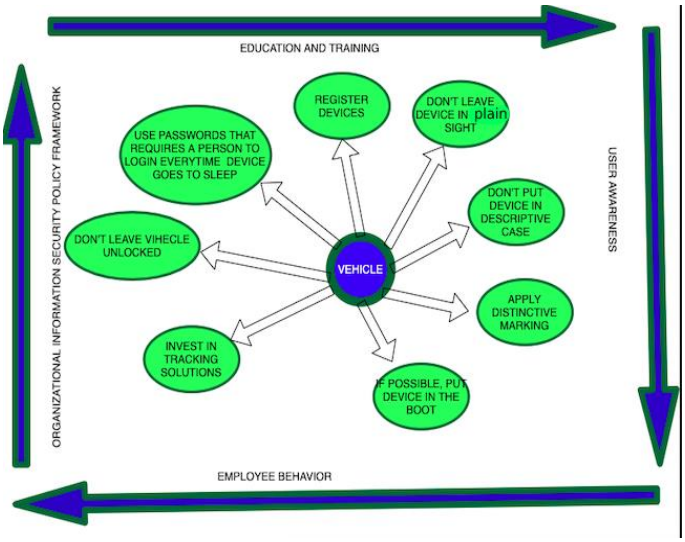

Fig. 1. Information Security Policy Framework For Devices in Vehicles

B. Office/Reception Desk

An Info Sec policy framework to protect against lost and theft of devices in an organization's offices or its front desk, as shown in Fig. 2.

- Security Cables and Cupboards

Organizations need to develop an Info Sec policy framework that requires that if an employee has to leave a portable device (i.e., laptop) temporarily unattended in the office or front desk, meeting room, even for a short while, then a security cable or similar device should be to attached firmly to a desk or similar heavy furniture. While not absolutely secure these locks do deter casual thieves[17]. Lock portable devices away out of sight when employees are not using it, preferably in a strong cupboard, filing cabinet or safe[18].

- Password

Passwords provide some kind of protection in the event that are stolen and this will make it difficult for the unauthorized person from getting access to the data on it[16] as explained in the second bullet of subsection A of this section.

- Register Device

Organizations need to keep note of make, model, and serial number of their computer devices, the portable one. This information should be on a hard-copy. Information Technology Services (ITS) already has this information. So organizations having it, will immediately help in the event a computer device is lost or stolen can greatly assist the police in timely retrieval, even as the incident is reported by the organization to the ITS Help Desk immediately [17]. Hence, device registration is important as explained in the third bullet of subsection A of this section

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

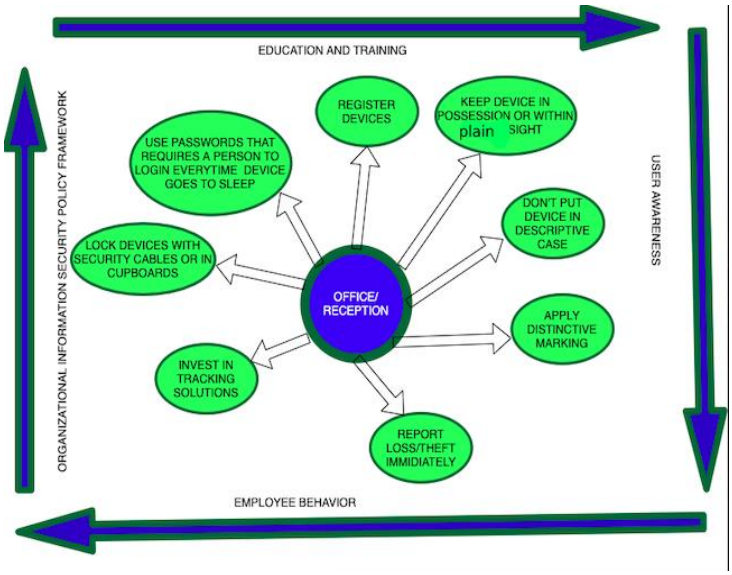

Fig. 2. Information Security Policy FramewoOffices/Reception Desks

- Keep in Plain Sight

User awareness of keeping portable computer devices in plain sight is critical to maintaining security. When devices are not in secure locations and are not in plain sight, it makes it easier for a 'thief' or an attacker the steal or gain unauthorized access to the device. Keep portable computer devices in the employees possession or in sight must be a constant thing[16]

- Don't Put in Descriptive Case

Thieves sometimes identify items by the cases they are put in. Organizations can discourage employees from putting devices descriptive case to avoid easy identification as explained in the fifth bullet of subsection A of this section

- Mark Devices

As explained in the sixth bullet of subsection A of this section.

- Report Loss/Theft

There should be a reporting system that allows employees to report incidents of loss or theft of computer devices on the organization's premises. An immediate or early reporting could be critical to blocking unauthorized access to the stolen device and to retrieving the lost or stolen device [17].

- Tracking Solutions

Tracking solutions are pro-active measures that can be taken by organizations against theft and loss of devices as explained in eighth bullet of subsection A of this section.

C. Public Places

Organizational policy framework for Info Sec in public places, is similar to the aforementioned, however, they are additional steps that employees must be aware of, in order to be protected. Fig. 3 shows some of the major issue's employees must understand to reduce the risk of a breach.

- Keep Device in plain Sight

User awareness is critical for employees to understand simple security behavior such as keeping portable device in their possession and within sight at all times no matter what, as explained in fourth bullet of subsection B of this section.

- Passwords

Passwords as explained in bullet two in subsection A of this section, are important in protecting device from unauthorized persons. Portable computer devices must be password protected. The password should not be associated with the employee or the organization. It should be complex enough comprising of alpha numeric values and symbol, mixing them in lower and upper case. However, the password should also be simple enough to remember[19].

- Set Short Screen Time

When using a computer and you leave it for a while without touching it or any activity, the screen will switch off after a certain length of time. When it does, it can also lock the device automatically. That period between the inactivity of the device and it locking is an opportunity for a thief or a hacker. They could take it and because it is unlocked, they can use it [18].

- Turn of Bluetooth and WiFi

According to Waddilove [18] If Bluetooth is turned on, a portable computer device will try to connect to other Bluetooth devices and they will try to connect to the device. Even though a confirmation is required for a complete connection, one can accidentally or mistakenly hit the Accept button on the screen. A hacker might also try to send photos or other files via Bluetooth and so user awareness must be created to never accept connections in a public place. You never know whether viruses, spyware, Trojans or other malware is being transferred to the device.

When one is in public places, the WiFi in your portable computer device will try to connect to the networks it finds. There are a lot of Wi-Fi networks around you in the high street, shopping malls, cafes, hotels and so on. Each time a device connects with a wireless network, it provides a little information about it. It can also be used to track your location too. This kind of awareness is needed by employees [18].

There is also the issue of fake WiFi hotspots which are easy to set up and it doesn't take much in the way of hardware. A hacker will create one in a public place with no security code required and when someone needs internet access, they will check whether there are any free WiFi hotspots around them, and when the find one they will connect

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

creating an exposure. They can now inspect the traffic and discover emails, usernames, maybe even passwords.

A hacker might even set the name of their free WiFi to one you are familiar with, like McDonalds, Starbucks, Costa or some other common cafe, restaurants, pubs or hotels with free WiFi. You think you are connecting to a free WiFi, but really it is the hackers. Thus, organizations should educate their employees to beware of fake WiFi in public places [18], [20].

Use VPN, Secure Https and Incognito Windows

There are instances where, in a public place and employee might want to use a genuine public WiFi, such as to access email, the internet, social networks and so on. The policy should be such that to use a WiFi in public places, use a virtual private network (VPN). A VPN, which is a way of encrypting internet traffic. When a VPN is enabled, everything between the device and the VPN server is encrypted, so even if someone could intercept your internet activities, they could not tell what you were doing. A VPN makes the internet private and much more secure when using public WiFi [17].

The use of Hypertext Transfer Protocol Secure (HTTPS) must be encourage by organizations and should be part of device usage policy. The major advantage HTTPS is that it does not just provide security but also trust. It protects users against what is known as man-in-the-middle (MitM) attacks that can be set into motion from compromised or insecure networks. Hackers use such techniques to steal sensitive information from devices being used by unsuspecting people[12].

When an individual browses the Internet in incognito window or mode, it increases their privacy and security. Incognito window is nothing but an online privacy feature that prevents a person's browsing history from being stored. When browsing the web is done in a regular window, the browser stores the URLs of every pages visited and retains that information even after the window is closed down. Nevertheless, it doesn't completely prevent a person from being tracked, since all it does is prevent information about websites you've visited from being saved[18]

- Tracking Solutions

To facilitate retrieval after loss or theft of device, organizations must invest in tracking solutions for their devices and indeed employee devices, if they are allowed to process and store sensitive information on them as explained in the eighth bullet of subsection A of this section.

IV. METHODOLOGY

Data is collected by or through Health Insurance Portability and Accountability Act, which is a USA law designed to provide privacy standards to protect patients' medical records, including health information given to hospitals, doctors, health plans, and other health care providers[21].

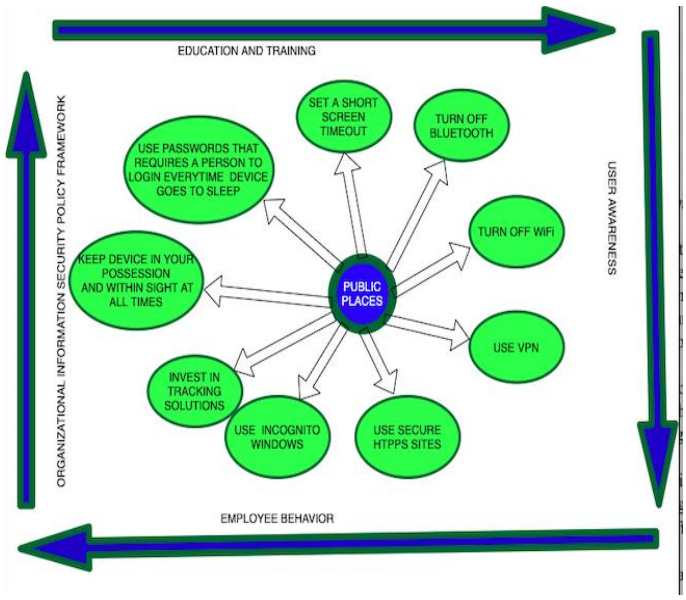

Fig. 3. Information Security Policy Framework For Devices in Public Places

The dataset contains more than 1600 recorded cases of data breach incidents. The breach incident record, specifies the location of the breach, name of the covered entity (CE), the State the entity is located in, the number of individuals affected, date of submission of the breach, type of the breach, business associate present and the description of the breach from October 2009 to November 2017. For the particular purpose of forecasting how human factors can lead to data breach incidents against an organization in a particular physical location (Vehicle, Office, Reception, Home, and Public Places), the study only selects a number of parameters; date of submission of the breach, the physical location where breach took place or associated with, and the description. The descriptive parameter indicates how the breach occurred.

It was observed that some of the records had missing values in all the columns except date of submission of breach (year). Thus, such records were removed and not considered. Data cleaning was performed in a manner that would support quantitative analysis. Furthermore, the descriptive column, which is a string format was changed to the binary values 0 and 1. This was done record by record, case by case and where there was evidence that the underlying cause of the breach was directly due to human error or behavior (human factor), a score of 1 was assigned otherwise 0.

For example, an investigation provided in the description field indicates that a breach that took place in 2009 in the Office for Civil Rights (OCR) was made possible because of underlying human factors, and so a score of 1 will be assigned to that physical location for the year 2009. This process is performed for each of the records on data breach incidents.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

After cleaning the dataset, data is extracted according to the data breach on a physical location, the year the breach happened, and whether human factors were associated with it for that particular year.

The study presumes that even though undetected and unreported data breach incidences may have some bearings on the findings, we are confident that the reported data breach cases typify data breach incidences on the stated physical locations in general.

Analysis of variance (ANOVA) for linear regression is adopted for the analysis of the study, where Pearson's r is implored. This will measure the linear relationship between two continuous variables. The regression line used is, DATA = FIT + RESIDUAL, that is:

$$(y_i - \overline{y}) = (\hat{y} - \overline{y}) + (y_i - \hat{y}_i) \quad (1)$$

where the first term is the total variation in the dependent variable(s) *y* from the dataset, the second term is the variation in the mean observation, while the third term is the residual value. Then square each of the given terms in Equation (1) and add them over all the observations *n*, which gives the equation:

$$\sum (y_i - \overline{y})^2 = \sum (\hat{y}_i - \overline{y})^2 + \sum (y_i - \hat{y}_i)^2 \quad (2)$$

Equation (2) can be rewritten as SST = SSE + SSM, where SST is the notation for the total sums of square, SSE error sums of square and SSM is the model sums of squares. The sum of the samples is equal to the ratio of the model's sums of square, r^2 = SSM/SST. With this, there is a formalization that the interpretation r^2 which explains the fraction of the variability in the data that is explained by the regression model. The variance s^2_y is given by:

$$\frac{\sum (y_i - \overline{y})^2}{n-1} = \frac{SST}{DFT} \quad (3)$$

where DFT is the total degree of freedom.

$$MSM = \sum \frac{(\hat{y} - \overline{y})^2}{1} = \frac{SSM}{DFM} \quad (4)$$

where DFM is a model degree of freedom.

In Equation (4) the mean square model (MSM) applies because the regression model has one explanatory variable *x*. The corresponding mean square error (MSE) is the estimate of the variance of the population of the regression line (σ^2) .

$$\sum \frac{(y_i - \hat{y}_i)^2}{n-2} = \frac{SSE}{DFE} = MSE \quad (5)$$

The ANOVA calculations for the regression are shown in Table 1

$$r_{jk} = \frac{s_{jk}}{s_j s_k} = \frac{\sum_{i=1}^{n} (x_{ij} - \overline{x}_j)(x_{ik} - \overline{x}_k)}{\sqrt{\sum_{i=1}^{n} (x_{ij} - \overline{x}_j)^2} \sqrt{\sum_{i=1}^{n} (x_{ik} - \overline{x}_k)^2}} \quad (6)$$

Equation (6) is used to compute the correlation matrix of all the dependent variables. It is a Pearson correlation matrix between the variables x_j and x_k.

A. *Characterization of Data Breach Incidents on Physical Locations*

The study characterizes the different types of physical location where the incident occurred or associated with, using the location type as described in the reported dataset. All the physical locations described below have protected health information (ePHI), store ePHI, and have data location breach incidents associated with them:

- Home: as a physical location is the abode of an employee where a data location (computer device, software, or data store) breached is associated with.
- Vehicle: as a physical location is the vehicle of an employee or the organization where a data location breached is associated with.
- Office: as a physical location is the premises of an organization where a data location breached is associated with, except the reception and car park given their unique characteristics of high association with visitors.
- Reception: as a physical location is the front desk of an organization where a data location breached is associated with.
- Public Places: as a physical location is any public place (outside the organization) such as car parks, restaurants, cafes, hotels, etc., where an organization's data location breached is associated with.

V. RESULTS

A. *Yearly Distributions*

Fig. 4 shows the general yearly distribution of data breach incidents with underlying human factor (HF) problems in five physical locations, and the overall breach incidents associated with human factor problems. In 2009, the overall number of breach incidents associated with human factors was 81, and those that took place in Vehicles were 43, 9 at Receptions, 27 in Offices, 6 at homes, and 5 at Public Places. In 2010, the number of breach incidents associated with human factors increased to 113. The number of these incidents also increased to 51, 40, and 10 in Vehicles, Offices, and Homes respectively. No such incident was recorded at Receptions, while Public Places had the same number as the previous year. In 2011, the overall breach incidents associated with human factors decreased to 79. A decrease was also observed in incidents that took place in Vehicles and Offices, being 48 and 22 accordingly. However, there was an increase in these incidents in Homes and Public Places, which recorded 12 and 6 cases respectively. A continuous increase in the number of breach incidents associated

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

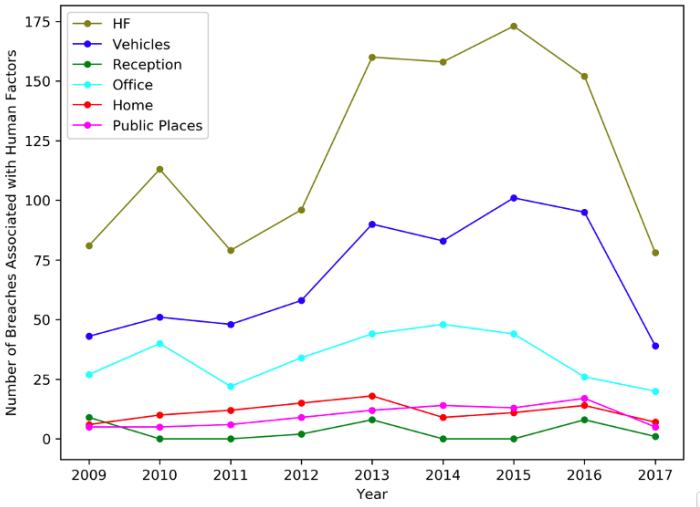

Fig. 4. Yearly Distribution of Breach Incidents Associated with Physical Locations

with human factors was observed from the year 2012 to 2013. The same trend is observed in Vehicles, Receptions, Offices, Homes, and Public places. Human factors saw 96 incidents in 2012 and 160 incidents in 2013. 58 incidents in Vehicles were recorded in 2012 and 90 incidents in 2013. In 2012, 2 incidents at Reception Desks were observed, and 8 incidents were recorded in 2013. Breach incidents recorded in 2012 in Offices, Homes, and Public places were 34, 15, and 9 respectively, and in 2013 the observations were 44, 18, and 12 in Offices, Homes, and Public Places accordingly. The number of incidents recorded in 2014, observed a slight decline for Human factors, Vehicles, Reception Desks, and Homes. Registering 158, 83, 0, and 9 respectively and an increase in incidents in Offices and Public Places, registering 48 and 14 accordingly. The observations for 2015 were 173, 101, 0, 44, 11, and 13 incidents for Human factors, Vehicles, Reception Desks, Offices, Homes, and Public Place in that order. A continuous decrease was recorded in 2016 and 2017 for Human factors, Vehicles, Reception Desks, Offices, Homes, and Public places. 2016 respectively and 78, 39, 1, 20, 7, and 5 incidents observed in 2017 in the aforementioned order. Each physical location and human factor breaches peaked in different years. Breach incidents at Reception Desks peaked in 2009. Incidents in Homes peaked in 2013 and Offices had their peak in 2014. Human factors and vehicles peaked in 2015 while incidents on Public Place peaked in 2016.

B. Predictions

Table 1 shows the results of a linear regression (ANOVA) experiment performed on the dataset, and the following can be predicted from the experiment where HF is the independent variable and physical locations are the dependent variables.

HF can statistically and significantly predict breach incidents in Vehicles, giving an F statistic that is equal to 92.212, and a distribution of [1,7). The probability of observing the value being greater or equal to 92.212 is less than 0.01. HF does not statistically and significantly predict Reception. The F statistic is equal to 0.048, with a distribution of [1,7) and the probability of observing the value greater or equal to 0.048 is greater than 0.05. HF can statistically and significantly predict Offices, the F statistic is equal to 9.480, with a distribution of [1.7) and the probability of observing the value greater or equal to 9.480 is less than 0.05. Just as with Receptions, HF could not statistically and significantly predict breach incidents in Homes. The F statistic is equal to 1.617, with a distribution of [1,7), and the probability of observing the value greater or equal to 1.617 to be greater than 0.05. HF can predict Public Places statistically and significantly. The F statistic is equal to 20.194, with a distribution of [1,7) and the probability of observing the value greater or equal to 20.194 is less than 0.01.

C. Variations

In table 2, a determination of the proportion of the variation in physical locations, which are the dependent variables explained by HF, the independent variable is shown.

TABLE 1. ANOVA: REGRESSION OF DATA BREACH INCIDENTS ASSOCIATED WITH HUMAN FACTORS IN PHYSICAL LOCATIONS

Dependent Variable	Sum of Squares		df	Mean Square	F	Sig
Vehicle	Regression	4442.950	1	4442.950	92.212	0.000b
	Residual	337.272	7	48.182		
	Total	4780.222	8			
Reception	Regression	0.866	1	0.866	0.048	0.833b
	Residual	126.022	7	18.003		
	Total	126.889	8			
Office	Regression	509.026	1	509.026	9.480	0.018b
	Residual	375.863	7	53.695		
	Total	884.889	8			
Home	Regression	22.521	1	22.521	1.617	0.244b
	Residual	97.479	7	13.926		
	Total	120.000	8			
Public Places	Regression	124.920	1	124.920	20.194	0.003b
	Residual	43.302	7	6.186		
	Total	168.222	8			

b. Predictors: (Constant), HF

TABLE 2. MODEL SUMMARY: DATA BREACH INCIDENTS ASSOCIATED WITH HUMAN FACTORS IN PHYSICAL LOCATIONS

					Change Statistics		
Dependent Variable	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**	**R Square Change**	**F Change**	**df1**
Vehicle	0.964a	0.929	0.919	6.941	0.929	92.212	1
Reception	0.083a	0.007	-0.135	4.243	0.007	0.048	1
Office	0.758a	0.575	0.515	7.328	0.575	9.480	1
Home	0.433a	0.188	0.072	3.732	0.188	1.617	1
Public Places	0.862a	0.743	0.706	2.487	0.743	20.194	1

[a.] Predictors: (Constant), HF

HF accounted for 91.9% of the explained variability in the physical location of the Vehicle.

The variability explained by HF in Receptions is very low. It is negligible because it is negative, -13.5%. Unlike Receptions, HF accounted for 51.5% of the explained variability in the physical location Office. It also accounted for 7.2% of the explained variability in the physical location Home, which is very low. HF accounted for 70.6% of the explained variability in the physical location Public Place.

D. Relationship between Breached Data Locations Concerning Human Factors and Physical Locations

Table 3 depicts the relationships between breached data locations with underlying human factors and physical locations. In the analysis human factor is the independent variable and the physical locations are the dependent variable. The relationships are such that the equation predicted $Vehicle = -4.774 + 0.597X(X = HF)$, indicating that an increase or change in breached data locations with respect to human factors, the average change in the mean of physical location (Vehicle) associated with it is 0.597. The relationship between data breaches with underlying human factors and the physical location it took place (Reception) predicted $Reception = 2.101 + 0.008X(X = HF)$. This indicates that when there an increase or change in data location breaches are associated with human factors, the average change in the mean of physical location (Reception) where it took place is 0.008

E. Strength of the Prediction

A computation of a Pearson correlation coefficient is shown in Fig. 5 to evaluate the strength of the relationship between HF (the independent variable) and the dependent variables (physical locations) when a breach occurred by human factors. The results of this evaluation, establishes a strong positive correlation of 0.862 between HF and the physical location public place. A moderate positive correlation of 0.043 is observed between HF and the physical location home. The strength of the correlation between HF and the physical location office is 0.758, which is considered as a strong positive correlation. Meanwhile, there is very little or weak positive correlation between HF and the physical location reception of 0.083. The correlation between HF and the physical location vehicle is strong positive, 0.96.

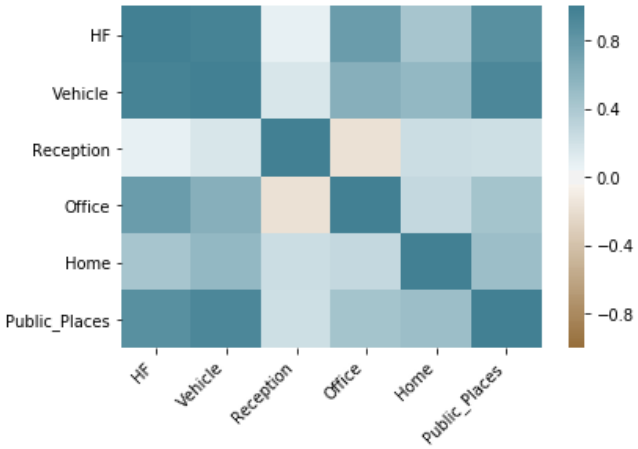

Fig. 5. Correlation of Human factors and Physical Locations Concerning Data Breach Incidents

TABLE 3. COEFFICIENT OF DATA BREACH INCIDENTS ASSOCIATED WITH HUMAN FACTORS IN PHYSICAL LOCATIONS

		Unstandardized	Coefficients	Standardized Coefficients		
Dependent Variable	**independent variable**	**B**	**Std. Error**	**Beta**	**t**	**Sig.**
Vehicle	(Constant)	-4.774	7.880		-0.606	0.564
	HF	0.597	0.062	0.964	9.603	0.000
Reception	(Constant)	2.101	4.817		0.436	0.676
	HF	0.008	0.038	0.083	0.219	0.833
Office	(Constant)	9.407	8.318		1.131	0.295
	HF	0.202	0.066	0.758	3.079	0.018
Home	(Constant)	6.184	4.236		1.460	0.188
	HF	0.043	0.033	0.433	1.272	0.244
Public Places	(Constant)	-2.573	2.823		-0.911	0.392
	HF	0.100	0.022	0.862	4.494	0.003

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

VI. DISCUSSION

The results in section 5 are an indication that Physical locations should be considered as critical factor in analyzing human factors in Information Security breach incidents. Statistically the findings are significant at 0.01 and 0.05 for the office, vehicle and public places, and statistically insignificant for homes and reception desks at 0.5 and above 0.5, as depicted in Table 4. Organizations need to come up with Info Sec policy frameworks amid at regular training and education of employees to increase their user awareness, which will in turn shape the 'behavior' to one that reduces or minimizes Info Sec incidents resulting from what they do in a physical location.

A. Information Security Policy Framework

Info Sec policy framework must be seen by organizations as a tool that can be used by management to understand the difference between employee behavior that are permitted and those prohibited and also laying out the consequences in therms if sanctions when a prohibited behavior occurs [22]. Organizations must understand that the main objective of Info Sec policy framework is to provide for management with support and direction in line with the standards and the business goals. It must be clear that every Info Sec policy framework contributes significantly to health of an Info Sys for an organization, which protects its information [23]. This will ensure that there is consistency between the organization's Info Sec policy framework and the standards of the organization stands assured and for this to be possible, it is vital that the human resource department is involved in the Info Sec policy framework development life cycle [24]. Organizations need to explicitly value the several steps needed to develop security policies, otherwise they risk developing a poorly thought-out Info Sec policy that is incomplete, irrelevant and absolutely redundant. This will involve more than a mere policy framework formation and implementation, if it has to fully support users [25].

B. Education and Training

The significance of Info Sec education and training in an organization can never be overemphasized due the human factor threats that the lack of it possess. The employees of an organization, irrespective of the size and form of the organization must be Info Sec conscious so as to make informed security decisions that could prove to be critical and crucial of the organizations. They must see these security decisions as a duty. Even though it can be argued that employees and for that matter human factors are not the only weak link in an organization's Info Sec, it is one of the most crucial part that is often ignored in the attempt to develop a secure system for both information and computing resources. Employees are a part of an Info Sec system and must thus be part of the solution through regular education and training [26]

C. User Awareness

A direct product of Info Sec education and training is user awareness. Most often organizations concentrate on the expansion of advanced security technology and provide regular 'professional' training for their Information Technology staffs, who per their profession require very little training to increase their security awareness, while the normal user is ignored, making them a weak link in a very strong Info Sec for the organization. Because of this problem, cyber attackers, today, are putting in significant efforts in research, resources and the development of advanced hacking tools that can be used to breach an organization's Info Sys.This problem is further exacerbated by the proliferation of the internet and portable user-friendly devices and the limited user awareness in terms of security among users. Therefore, this makes it even more attractive for cyber attackers to attack them or attack through them [26], [27].

TABLE 4. SIGNIFICANCE LEVEL OF RESULTS

0.01	0.05	0.1	0.5	Above 0.5
Vehicle =0.000	Office=0.018			Reception =0.833
Public Places=0.003			Home =0.244	

D. Human Behavior

A good info Sec policy framework will have education and training in it, which will in term underpin user awareness leading to an acceptable and security behavior from employees. Human behavior is the target of the aforementioned subsections. Perhaps the greatest and toughest threat to Info Sec lies not just in the technological security parameters but also in the carelessness and malicious actions or behavior of employees or internal users and other trusted constituents with easy access to the organization's information and computer resources. Users must also be recognized as endpoints of computer networks and as such they can also be 'hacked' if there are no security compliant behavior. Info Sec policy framework must take in account the general personality traits and attitudes and must be willing to sanction and reward bad and good security behavior respectively[28], [29],[30].

VII. CONCLUSION

In this study, we have proposed three Info Sec policy framework that can be adopted by organization to mitigate data breach incidents that area associated with certain physical locations. The findings of our experiments have added to the body of knowledge that physical locations also place a major role when it comes to security glitches with underlying human factors. In other words, human behavior is a key component if security will be breached in a specific physical location. the results also show that vehicles, offices and public place are physical location that employees cannot afford to be careless as it could lead to security breach. Every good Info Sec must take into consideration physical locations and human factors and form a policy framework that reduces the risk they pose. The limitation of this paper is that, it does not consider the susceptibility of specific data locations in a specific physical

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 04, April-2021

location with respect to human factors. Future studies will have to explore the categories of human behavior that are both directly and indirectly associated with data locations and physical locations.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China (No.61672135), the Frontier Science and Technology Innovation Projects of National Key R&D Program (No.2019QY1405), the Sichuan Science and Technology Innovation Platform and Talent Plan (No.20JCQN0256), and the Fundamental Research Funds for the Central Universities (No.2672018ZYGX2018J057).

REFERENCES

[1] J. Rees, S. Bandyopadhyay, and E. H. Spafford, "Pfires: A policy framework for information security," *Commun. ACM*, vol. 46, no. 7, pp. 101–106, 2003.

[2] K. Hughes-Lartey, Z. Qin, F. E. Botchey, and S. Dsane-Nsor, "An Assessment of data location vulnerability for human factors using linear regression and collaborative filtering," *Inf.*, vol. 11, no. 9, pp. 1–20, 2020.

[3] K. Hughes-Lartey, M. Li, F. E. Botchey, and Z. Qin, "Human factor, a critical weak point in the information security of an organization's Internet of things," *Heliyon*, vol. 7, no. 3, p. e06522, 2021.

[4] D. Suchbegriffe, "A Framework for Human Factors in Information Security A Framework for Human Factors in Information Security," no. May, pp. 1–7, 2012.

[5] M. G. Martinsons and P. K. C. Chong, "The Influence of Human Factors and Specialist Involvement on Information Systems Success," *Hum. Relations*, vol. 52, no. 1, pp. 123–152, 1999.

[6] B. Schneier, *Schneier on security*. John Wiley & Sons, 2009.

[7] M. Alotaibi, S. Furnell, and N. Clarke, "Information security policies: A review of challenges and influencing factors," *2016 11th Int. Conf. Internet Technol. Secur. Trans. ICITST 2016*, pp. 352–358, 2017.

[8] A. Alhogail, A. Mirza, and S. H. Bakry, "A comprehensive human factor framework for information security in organizations," *J. Theor. Appl. Inf. Technol.*, vol. 78, no. 2, pp. 201–211, 2015.

[9] Z. Tu, O. Turel, Y. Yuan, and N. Archer, "Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination," *Inf. Manag.*, vol. 52, no. 4, pp. 506–517, 2015.

[10] E. H. Schein, *The corporate culture survival guide*, vol. 158. John Wiley & Sons, 2009.

[11] J. Van Niekerk and R. Von Solms, "A holistic framework for the fostering of an information security sub-culture in organizations.," in *Issa*, 2005, vol. 1, no. 13.

[12] W. Ren, J. Yuan, L. Jiang, and T. Zhao, "Technical Framework Research on Critical Information Infrastructure Cybersecurity Classified Protection," in *2016 4th International Conference on Machinery, Materials and Information Technology Applications*, 2017.

[13] A. E. Speed, B. L. Woo, C. G. Kouhestani, J. J. Stubbs, and G. C. Birch, "Human Factors in Security," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2018-Octob, pp. 1–5, 2018.

[14] R. Alavi, S. Islam, and H. Mouratidis, "A conceptual framework to analyze human factors of Information Security Management System (ISMS) in organizations," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8533 LNCS, pp. 297–305, 2014.

[15] D. Liginlal, I. Sim, and L. Khansa, "How significant is human error as a cause of privacy breaches ? An empirical study and a framework for error management," *Comput. Secur.*, vol. 28, no. 3–4, pp. 215–228, 2009.

[16] O. S. Olamide, "5 Anti-theft and Recovery Measures for Laptops." https://www.dignited.com/34339/top-anti-theft-measures-for-your-laptop/. Accessed: 2021-02-25.

[17] Macalester, "Laptop Protection and Usage." https://www.macalester.edu/its/policies/laptop-protection/. Accessed: 2021-02-25.

[18] R. Waddilove, "9 ways to secure your phone in public and avoid hackers and thieves." http://www.rawinfopages.com/apps/index.php/android/370-ways-to-secure-your-phone-in-public/. Accessed: 2021-02-25.

[19] J. T. Force and T. Initiative, "Security and privacy controls for federal information systems and organizations," *NIST Spec. Publ.*, vol. 800, no. 53, pp. 8–13, 2013.

[20] C. Colwill, "Human factors in information security: The insider threat - Who can you trust these days?," *Information Security Technical Report*, vol. 14, no. 4. pp. 186–196, 2009.

[21] Micheal Molloy, "Dataset---{K}aggle{,}." "https://www.kaggle.com/forgotyourpassword/hipaa-data-breaches", 2020. [Online; accessed 22-June-2020].

[22] H. Chen and W. Li, "Understanding Organization Employee's Information Security Omission Behavior: an Integrated Model of Social norm and Deterrence.," in *PACIS*, 2014, p. 280.

[23] B. Standard, "Code of practice for information security management," *BS 7799 1995*, 1995.

[24] S. B. Maynard, A. B. Ruighaver, and A. Ahmad, "Stakeholders in security policy development," 2011.

[25] S. V Flowerday and T. Tuyikeze, "Information security policy development and implementation: The what, how and who," *Comput. Secur.*, vol. 61, pp. 169–183, 2016.

[26] E. Amankwa, M. Loock, and E. Kritzinger, "A conceptual analysis of information security education, information security training and information security awareness definitions," in *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, 2014, pp. 248–252.

[27] F. A. Aloul, "The need for effective information security awareness," *J. Adv. Inf. Technol.*, vol. 3, no. 3, pp. 176–183, 2012.

[28] J. Shropshire, M. Warkentin, A. C. Johnston, and M. B. Schmidt, "Personality and IT security: An application of the five-factor model," *Assoc. Inf. Syst. - 12th Am. Conf. Inf. Syst. AMCIS 2006*, vol. 6, pp. 210–216, 2006.

[29] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Comput. Secur.*, vol. 49, pp. 177–191, 2015.

[30] J. Shropshire, M. Warkentin, A. Johnston, and M. Schmidt, "Personality and IT security: An application of the five-factor model," *AMCIS 2006 Proc.*, p. 415, 2006.