Texila International Journal of Management
Special Edition Dec 2019

A Study of the Awareness of Security and Safety Culture Among Employees Across Organizations

Article by Alexander D.K. Acquaye[1], Nestor Naabulee Nasage[2]
[1]PhD candidate, MBA, MASC, LLB, CPP, MISPON,
Principal – S.G. Technologies Accra Ghana,
[2]PhD Candidate, MBA, MSC, ODCC, ODCP, 1OD. LCM LEVEL 3, 4, 5 & 6 DIPLOMA UK,
Managing Consultant - Uni-Sky Holdings Limited Sunyani Ghana,
Lecturer- College for Community and Organizational Development Sunyani Ghana
E-mail: alex.acquaye@gmail.com[1], nasagenestor@yahoo.com[2]

Abstract

The security and safety culture of organizations requires care and nurturing. When a culture of security and protection is sustainable, it transforms the security of a unique event into a life cycle that generates safety returns forever. In any system, humans are always the weakest escape. A culture of security is primarily for humans, not for computers. Computers do exactly what we tell them to do. The challenge is with humans, who click on the things they receive in the email and think what someone tells them. Humans need a framework to understand what is right for security. The study investigated the knowledge of a safety culture among workers in organizations, using data from secondary sources. This study was evaluated in two points of view; First, it assessed how awareness of a safety culture was established among employees of organizations. Second, it assessed the importance of creating a culture of safety and security among workers in organizations. The study concluded that, organizations can create security and safety awareness culture through; education, building security community and policies, initiating security boot camp, motivation, security and safety mindfulness. The study also concluded that, security and safety awareness across organizations is important and a key determinant of ensuring; Long-term commercial viability of organizations, impenetrable processes of organizations, Safe operations of organizations' applications systems, Data protection, Protection of organizational functions from top to down, Increased organizational effectiveness and performance and building and maintaining a flexible network environment and hence staying away from information risks.

Keywords: *Awareness, Security and Safety, Culture, Organizations.*

Introduction

The security and safety culture of organizations requires care and nurturing (Hafey, 2017). Hafey (2017) claim that, it is not something that grows positively as a member. Hafey (2017) further argued that, you must invest in a culture of security and protection. A culture of sustainable security is greater than a single event. When a culture of security and protection is sustainable, it transforms the security of a unique event into a life cycle that generates safety returns forever (Hafey, 2017).

A culture of sustainable security has four key characteristics (Marzbali, Abdullah, Razak, & Tilaki, 2011). First, it is deliberate and vandalized. The main objective of a culture of security and protection is to promote change and improve security, so it must be a disorder for the organization and deliberation with a series of actions to promote change. Second, it is attractive and fun. People want to share a fun and challenging safety culture. Third, it is gratifying. For people to invest their time and effort, they must understand what they will get in return. Fourth, it provides a return on investment. The reason someone is safe is to improve supply and reduce weaknesses; We must redouble the effort invested (Marzbali et al., 2011).

A strong security and safety culture not only interacts with everyday actions, but also determines how security affects what your organization provides to others (Sasse, Brostoff, & Weirich, 2001). Sasse, Brostoff, and Weirich, (2001) claimed that, these offers may be products, services or solutions, but they must have a security application in all parts and a culture of sustainable security. They further claim that, it is not an annual event, but it is integrated into everything you do.

DOI: 10.21522/TIJMG.2015.SE.19.02.Art013
ISSN: 2520-310X

Why does the organization need a culture of security and protection? The main answer is something deep that we all know (Furnell & Clarke, 2005).

In any system, humans are always the weakest escape. A culture of security is primarily for humans, not for computers (Furnell & Clarke, 2005). Computers do exactly what we tell them to do (Martins & Elofe, 2002). Martins and Elofe, (2002), claim that, the challenge is with humans, who click on the things they receive in the email and think what someone tells them. Martins and Elofe (2002) further claim that, humans need a framework to understand what is right for security. In general, humans within your organization want to do the right thing: they just need to teach them (Martins & Elofe, 2002).

Fortunately, wherever an organization sits in the spectrum of security and safety culture, there are things that can be done to improve the culture (Martins & Elofe, 2002).

The purpose of this study is to investigate the knowledge of a safety culture among workers in organizations, using data from secondary sources. This study was evaluated in two points of view; First, it assessed how awareness of a safety culture was established among the employees of the organizations. Second, it assessed the importance of creating a culture of safety among workers in organizations.

Literature review

Simply put, a culture of security and protection is based on the old saying "knowing that they are enemies". If you know what you're facing, you can take action to protect yourself. A culture of safety is a culture that involves all participants in the organization; this can be extended to business partners and, in some cases, to customers; certainly, some aspects of a security culture may include customers, for example, educating customers about fraudulent emails can be considered part of a security culture Developed by your organization (Hofstede, Neuijen, Ohayv, & Sanders, 1990). Hofstede et al. (1990) claim that, Prefer a safety culture through the use of safety awareness training and positive attitude, driven from top to bottom, towards safety.

Some theories of security and safety management are analyzed below

The risk theory as a base for the theory of safety and security

Risk theory is a commonly used scientific field, based on the identification of threats, the identification of risks and the specification of how to overcome the risk (Sodiya, Onashoga, & Oladunjoye, 2007). They claim that, the essence of the danger lies in the objective existence of threats. The danger comes from the consciously controlled representation, or the chaotic and uncontrolled representation of each part of the complex. In the behavior of the elements, moments may arise when the elements, either intentionally or randomly, enter into a direct reaction (collision, effect). Many interactions are negative and have a devastating effect. This effect is proportional to the size and direction of the procedure (measure), where the individual reference objects participate in negative interactions. This negative reaction is called a "security incident" (Cichonski, Millar, Grance, & Scarfone, 2012).

The application of risk theory assesses threats (or negative actions) that affect the reference body and those that have a fairly significant effect (Kleindorfer & Saad, 2005). Kleindorfer and Saad (2005) claim that, the purpose of risk identification is to identify the worst possible impact of threats and develop measures to counter them. They further claim that, the proposed measures should prevent the effects of threats or prevent negative effects on the reference body. The purpose of the risk is to express the probability and extent of the negative impact on the reference body (Wiseman & Gomez-Mejia, 1998). Wiseman and Gomez-Mejia (1998) claim that, the risk can be quantified as well as qualitatively and its size has more variables.

There is currently no clearly defined and acceptable definition of risk. Typically, the risk is characterized by the magnitude of the negative impact or damage and the likelihood of being threatened (Klinke & Renn, 2002). Klinke and Renn (2002) claim that, the vulnerability emphasizes threats to the reference object. They also claim that, this parameter is involved in determining the probability of exposure. If you are not exposed to the threat of exposure, the probability of exposure, as well as the vulnerability, will be lower (Klinke & Renn, 2002). Risk management is used in many areas. These include project management, investment, economics, etc. It is always part of the management. The

objective of risk management is not to find a way to efficiently achieve the objective function of the reference object (Poolsappasit, Dewri, & Ray, 2011).

They further claim that, its objective is to determine the negative effect, which may affect the reference object, how the reference will be affected, how it behaves or how to minimize the effects. Risk management has an important position in security and protection (Poolsappasit et al., 2011). They again claim that, it focuses on minimizing damage or impact. Risk theory can be used as a methodology to identify possible adverse effects, which can damage the reference organism (Poolsappasit et al., 2011). As a result of this fact, risk management is used in many areas, where theoretical and important practical applications have been developed (Poolsappasit et al., 2011). Bedford, Cooke, and others, (2001), claim that, risk analysis methods have been developed and at present, we have many methods of risk analysis. These methods allow to determine the level of risk.

Depending on the approach and the nature of the application, different risk analysis methods can lead to different results, obtained during the analysis of a specific security problem (Bedford et al., 2001). Risk management prefers a repressive way to guarantee security or protection (Poolsappasit et al., 2011). Determine what risks and how the reference object should be prepared (Poolsappasit et al., 2011). Stoneburner, Goguen, and Feringa (2002) claim that, the disadvantage of risk management is that it does not know the causes of the threats.

They claim that, threats are taken as fact and focus only on what they can cause. Unacceptable risks are resolved with appropriate measures (Bedford et al., 2001). The solution comes as risk acceptance, risk retention, risk transfer and risk avoidance (Cummins & Weiss, 2009). Despite this inconvenience, risk theory creates the basis of security and protection theory (Beard, 2013). Beard (2013) claim that, the main contribution is the sophisticated methods of risk analysis. The risk theory applies well to the types of security or protection that protect the conditions of the reference object (physical security, information security, administrative security, etc.) (Beard, 2013). Beard (2013) claim that, the risk theory is less suitable for the types of security that govern the reference object (international security, home security, etc.). Beard (2013) further claim that, in these cases, it is about creating a safe and secure environment as a result of the adjustment.

The crisis theory and its relation to the theory of safety and security

The theory speculates that, the crisis is an important phenomenon, which has a negative influence on human society (Brown, 2019). Brown (2019) claim that, the negative effect is a common sign of security breach and crisis. Brown, (2019), again claim that, for security research, it is important to determine the reason and the nature of the security problems. Brown (2019) further claim that, in addition, we must examine the relationship between the theory of technological and physical security and the theory of crisis.

Crisis theory is a scientific discipline focused on the theoretical aspects of crisis research, mainly on the nature and causes of the crisis (Benbasat & Zmud, 2003). The fundamentals of crisis prevention and its management are based on crisis theory (Brown, 2019). The theory of the crisis has systems and a dynamic character (Brown, 2019). Brown (2019) claim that, the theory of the crisis is independent of a specific object of reference; It also investigates the basics of crisis creation and development. Crisis theory is the basis for the successful management of a crisis (Brown, 2019). Brown (2019) claim that, today, the crisis is understood as: time when the contradictions culminate, and / or as a complicated situation. These terms are similar. They are appropriate for the designation of a period of time when existential complications arise (Brown, 2019). The crisis is considered as a state or period in which the danger arises and, at the same time, the objective function of the reference object is threatened (Brown, 2019).

The crisis arises when there is a significant change in the conditions for the reference object (Brown, 2019). Brown (2019) argued that, the changing conditions occur due to the chaotic or uncoordinated behavior of each part of the system. During this period of time, the configuration of the conditions and the environment are changing. It could be caused by the lack of inputs, a failure in the power supply or production elements, or an electrical voltage escalation, etc; and each change requires an adequate reaction of the system to provide adaptation (Brown, 2019). Brown (2019) study clarify that, if changes are expected, the system can be prepared for them and then; you can also have a proper reaction. The

DOI: 10.21522/TIJMG.2015.SE.19.02.Art013
ISSN: 2520-310X

situation is different when a rapid change has a higher value than expected. Brown (2019) further clarify that, during this situation, the system may have an inappropriate reaction and, after that, complications or crises may arise.

Basically, the crisis is created due to: unexpected and large negative situation, unmanaged control, unexpected and large negative situation (Brown, 2019). Brown (2019) explained that, an unexpected situation is a situation that cannot be predicted. Complications are created by a large-scale negative event (for example, natural disasters, the sharp fall in the price of shares in the stock market, the large-scale attack of an unknown computer virus, etc.) (Brown, 2019). The system is not prepared for these changes, because they are not frequent and prevention is economically unbearable.

The system must be prepared for these negative situations. According to Brown (2019), Crisis management is based on minimizing the influence of the negative situation and also on the recovery of the system. Brown (2019) further states that, Crisis management is a special type of management created to manage and overcome the crisis. The activation of new forces and equipment is a basic measure of crisis (Brown, 2019).

The nature of the crisis that arises is based on unmanaged control. (Brown, 2019) explained in the theory that, the crisis usually includes periods (stages) of latent symptoms, acute, chronic and resolved / unresolved crisis. He claimed that in the stage of latent symptoms, the accumulation of unresolved problems occurs. If the management system is not updating or is not resolving the symptoms of the crisis, the crisis comes out. Brown (2019) claim in the acute stage, the problems culminate and unresolved problems also accumulate; the control system must begin to solve these problems slowly and then a breaking point of the situation is reached. This breakpoint is based on the capacity of the system, especially the control system. The crisis is eliminated if the system is able to activate and guarantee many resources for appropriate measures. Crisis management has also been activated (Brown, 2019). Crisis management must act quickly and be efficient enough to solve the crisis without damaging the elements of the complex (Brown, 2019). In crisis, we generally do not have enough relevant information. Therefore, crisis resolution must be made during an unclear situation and Knowledge and experience, obtained from previous crises, play a key role in handling complicated situations (Brown, 2019).

Decisions usually have irreversible implications and the systems have to be prepared for the crisis and must also make plans to eliminate the crisis situation (Brown, 2019). Brown (2019) state that, at the same time, they must resolve the crisis immediately at the stage of latent symptoms. This ensures the avoidance of crisis. Relations between crisis and security and protection Crisis theory and security and protection theory represent the common form (Brown, 2019).

Information security and safety related theory

Theories related to information security and safety are also reviewed below

Security policy theory

This theory aims to create an application and maintain an organization's information security needs through security policies (Ifinedo, 2012).

Risk management theory

Assess and analyze threats and vulnerabilities in the organization's information assets. It also includes the development and implementation of control measures and procedures to reduce risks (Clifford & Smith, 1995).

Control and audit theory

The theory suggests that the institution needed to establish control systems (in the form of a security strategy and standard) with periodic audit to measure the performance of control (Sunder & Cyert, 1997).

The theory also suggest that organization need establish control systems (in form of security strategy and standard) with periodic auditing to measure the performance of control (Sunder & Cyert, 1997).

Management system theory

The theory establishes and maintains a documented information security management system. This will include information security policies that combine the internal and external factors of an organization that are within the scope of policy, risk management and implementation (Rice, 2013).

Contingency theory

Information security is part of emergency management to prevent, detect and combat threats and vulnerabilities of the organization's internal and external capabilities (Donaldson, 2001).

Methodology

The study employed an exploratory research design which seeks to establish the awareness of security and safety culture among employees of organizations. The study makes use of secondary data to analyze into detail, how to create security and safety culture across organizations, as well as the importance of creating security and safety culture awareness across organizations.

Results Obtained from literature

The results obtained from secondary data are given below;

The importance of a security culture across the organization

Humans are complex creatures of habit, we do the things we do, in general, because that's how we always did (Jacob, 1977). The same can be said about the cultures in our society and even in the organizations we work for and in terms of long-term commercial viability, culture is everything, especially when it comes to information security (Argyris, 2017). Culture, good or bad, is the ultimate determinant of whether a company can build and maintain a flexible network environment and stay away from information risks (Hofstede, 2001).

A strong safety culture is both a mentality and a way of working and Once integrated in daily thinking and decision-making, can be an almost impenetrable process (Hofstede, 2001). On the contrary, an absent security culture will facilitate uncertainty and ultimately lead to security incidents that you cannot tolerate (Lord, 2012). This often happens because everyone literally works in silos; you know, the same people of us in the industry that we quickly announce are bad for security (Mitnick & Simon, 2011). Schön (2017) assert that, rather than being useful and doing what they can do to really improve security, these people often do better for their own interests, sometimes even to sabotage each other or work in general. Schön (2017) claim that, regardless of size or business, there are some organizations that simply click, and all seem to be moving in the same direction in terms of information security and privacy. However, where there may be a security defender, but his words fall on deaf ears. These cases do not usually end well.

Concepts and importance of information security and safety to organizations

In general, information security can be defined as protecting data owned by an organization or individual from threats and / or risks (Ifinedo, 2012). According to the Merriam-Webster Dictionary, security in general is the quality or security state, that is, to be free from harm. According to the Oxford Students Dictionary Advanced, in a more practical sense, security also takes steps to ensure the security of the country, people, valuable objects, etc. Sussman and Siegal (2003) considers security to be about preventing harmful consequences from deliberate and unjustified actions of others. Thus, the purpose of security is to build protection against the enemies of those who may harm, intentionally or otherwise. According to Thomson and Von Solms (2005) information security is the protection of information and its important elements, including systems and devices that use, store and transmit this information. Information security is a set of techniques, standards, policies and management practices that are applied to information to keep it safe (Thomson & Von Solms, 2005).

Information security performs four important functions of an organization that enable the safe operation of an application implemented on an organization's information technology (IT) systems, protecting the data collected and used by organizations, protecting the assets of the technology used in the organization, and finally protecting the organization's ability to operate (Ifinedo, 2012).

DOI: 10.21522/TIJMG.2015.SE.19.02.Art013
ISSN: 2520-310X

Information security also allows the safe operation of an application that is applied to an organization's information technology (IT) systems (Ifinedo, 2012). Ifinedo (2012) claim that, this is because to protect the data, the organization will apply or install the appropriate software that will secure data such as antivirus and other protected applications.

Therefore, information security is critical in any organization to protect applications that are implemented in organizations and to protect the data store on the computer as well. In addition to data protection, the installed application also needs protection because it can contribute to the loss or damage of information (Ifinedo, 2012).

Information security protects data collected and used by the organization (Ifinedo, 2012). If the information is left unprotected, anyone can access it and if the information falls into the wrong hands, it can destroy lives and bring down business and can also be used to harm (Ifinedo, 2012). Ifinedo (2012) clarify that, information security software will ensure that appropriate business information and legal requirements are protected by steps taken to protect enterprise data. In addition, the steps taken to protect enterprise information is a matter of maintaining privacy and will help prevent identity theft.

In an organization, information is an important business asset that is necessary for business and therefore needs appropriate protection (Posthumus & Von Solms, 2004). This is especially important in an increasingly interconnected work environment, where information is now exposed to a growing number and a variety of threats and vulnerabilities. Causing damage such as malicious code, computer hacking, and denial-of-service attacks is becoming more common, more ambitious, and more sophisticated (Posthumus & Von Solms, 2004). Therefore, through the application of information security in the organization, it can protect the assets of technology used in the enterprise.

With regard to the protection of the functions of the Organization, the General Directorate and the Information Technology Department are responsible for implementing information security that protects the Organization's ability to operate (Posthumus & Von Solms, 2004). Posthumus and Von Solms (2004) assert that, information is the most important element in an organization to do business. They further claim that, besides, the organization keeps the information of its customers, so it is important for them to protect the information and without information, the work cannot be run. By securing the information store; it can enable the organization to run the business as well. This is why information security is important in organizations.

Investigative framework

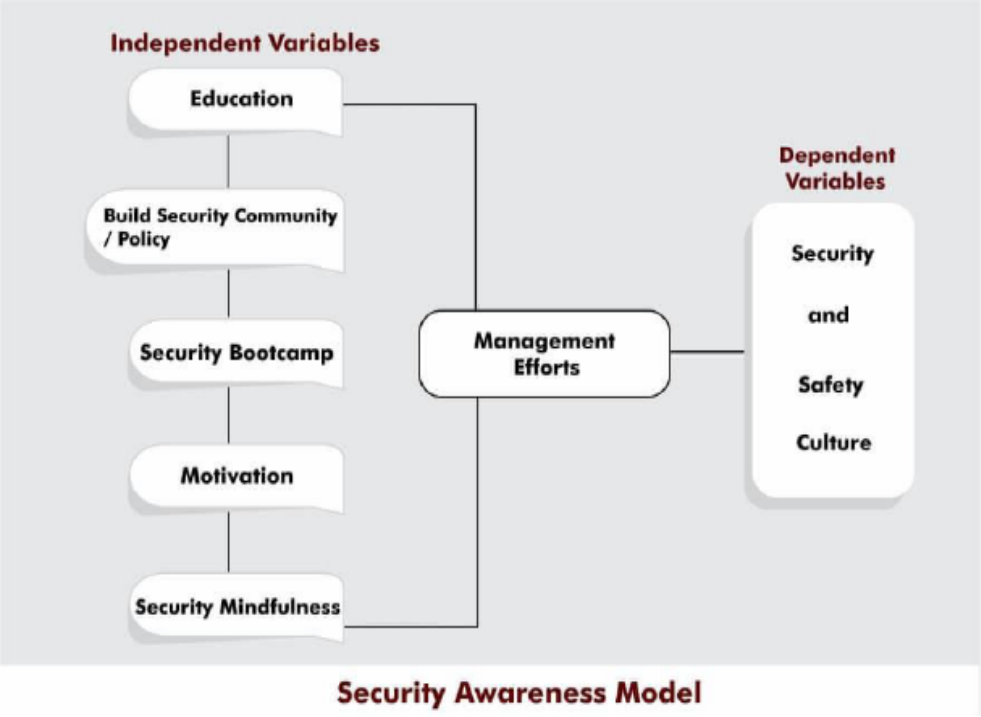

Figure 1

Researchers security and culture awareness model

The research frame work above described from left to right, the independent variables that management of organizations can adopt backed by strong efforts to ensure security and safety culture across all functions of the organization, from top to bottom.

Creating security and safety awareness culture across organizations

The below discussed the various ways and means of creating security and safety culture across organizations.

Education

Knowledge is power, cybercrime education and typical attack scenarios are an essential part of any security awareness training program (Christopher, Choo, & Dehghantanha, 2017). Christopher, Choo, and Dehghantanha (2017) assert that, Security must be strengthened and nurtured, and therefore the spirit of training should be conducted using a top-down approach. Management should be training advocates who are involved in the development of company policy and also, extend security and safety education to everyone who can be a threat to your organization - including all employees, contractors, entrepreneurs, consultants, third parties (such as suppliers) and even customers (Shaw, Chen, Harris, & Huang, 2009).

Many organizations see the security department as responsible for security. A culture of sustainable security requires everyone in the organization and everyone should feel safe (Solana, 2003). Solana (2003) clarify that, this is a culture of security for all and thus, Security belongs to everyone, from executive staff to lobby ambassadors. Solana (2003) further claim that, everyone has a part of the company's security solution and security culture.

At Uber, Samantha Davison, director of the Uber Security Program claim in their website (www.uber.com) that, “we try to change the security stories of our employees, by creating programs that address the needs of the region, management and role, our employees understand that security is part of their story and our culture.” This is an example of a company that truly believes that security belongs to everyone and puts security in everything they do.

You can achieve an “all-in” mentality by integrating the highest levels of security into your vision and mission (Quinn & Spreitzer, 1997). Quinn and Spreitzer (1997) explain that, People look at these things to understand what they should focus on and update vision or organizational objective to clarify that security and safety are not negotiable. Solana (2003) talk of the importance of security from the highest levels. This means not only people who have security in their nickname (CISO, CSO), but also from other C-level executives down to individual managers.

Build security and safety community/ policy

Security and safety is everyone's problem and either of us can become the weakest link in an organization's cybersecurity defenses; the finger that clicks on the malware package, the one who reveals his password as a legitimate site (Singer & Friedman, 2014). Singer and Friedman (2014) claim that, a holistic view must be taken where everyone recognizes the role they play in corporate culture and the impact that they can have personally on security. Singer and Friedman (2014) came out that, Understanding security issues throughout the organization, from a clean office policy to developers, understands the importance of securing security and encryption records.

Arrey (2019) asserts that, if you don't have a secure development lifecycle, get one now. Arrey (2019) clarify that, the Safe Development Life Cycle (SDL) is the foundation of a sustainable security and safety culture. SDL is the process and activities that your organization agrees to implement for each program or system version (Arrey, 2019). Arrey (2019) further clarify that, it includes things like security requirements, threat modeling and security testing activities. Arrey (2019) again claim that, SDL answers how your safety culture is secured and that, it is a culture of sustainable safety and security at work. Clients from different sectors are beginning to demand the crazy idea that organizations have SDL and follow-up and if you do not have an SDL at this point, Microsoft has released most of the details about its SDL for free and any industrial SDLs are attributed to Microsoft (Arrey, 2019).

DOI: 10.21522/TIJMG.2015.SE.19.02.Art013
ISSN: 2520-310X

There is a reasonable place for SDL to live in the product safety office and If you don't have a product security office, think carefully about investing in one (Arrey, 2019). This office is within engineering and provides central resources for deploying parts of your security culture. Although we don't want the entire organization to turn off security from the product safety office, think of it as a consultant to teach engineering about the depths of safety (Arrey, 2019). Arrey, (2019), assert that, the security community is the backbone of a sustainable security culture and the community provides interpersonal communication across the organization. Arrey (2019) further clarify that, the security community helps bring everyone together against the common problem and removes the mentality of "We are against them."

The safety community is achieved by understanding the different levels of security interests within the organization: defenders, safety science, and sponsors and Security advocates are those people who have a passion at home to make things safe thus these are the leaders within your community (Arrey, 2019). The security he understands is not emotional but he realizes that he needs to contribute to making security better. Annan (2005) claim that, sponsors are from the administration who help shape the security direction. He further asserts that, bring all these people together in a special interest group that focuses on security. The security community can appear as an individual interface and weekly or monthly meetings to discuss the latest security issues, It can become an annual conference, where the best and brightest of the organization have the opportunity to share their knowledge and skills on the big stage (Annan, 2005). Fennell, (2010), claim that, for too long, people associate safety with boring training or anyone who says no all the time. Fennell (2010) went further to say that, to promote a culture of sustainable security, build fun and participate in all parts of the process. If you have a specific security training, make sure that it is not a boring sound on a PowerPoint presentation and If you get involved in your community through events, don't be afraid to laugh and frustrate about some (Fennell, 2010).

Security boot camp

Security awareness training and simulation exercises provide a first-hand firsthand experience necessary to learn and understand where the risks lie (Blanchard, 2006). A safety training camp can be created that uses a combination of formal classroom-based training, with realistic simulation exercises that train people to detect security problems (Blanchard, 2006). Security camps should cover all aspects of security from phishing and online security to desktop security to physical security (Camp, 2009). Phishing simulations should be performed regularly, but also randomly, to create more natural scenarios (Blanchard, 2006). People are your best asset, and they can also be one of the greatest assets.

Puhakainen and Siponen (2010) assert that, Security awareness is the process of teaching your entire team basic lessons about security. They further claim that, you must adjust each person's ability to judge threats before they are asked to understand the depth of the threats. Security awareness got bad rap because of the mechanisms used to deliver it and Posters and personal reviews can be boring, but they should not (Puhakainen & Siponen, 2010). Add some creativity to your awareness efforts.

On top of public awareness is the need for application security and safety knowledge and Safety awareness app for developers and testers within the organization (Siponen, 2000). Siponen (2000) claim that, in your organization, they may sit in the field of information technology, or may be an engineering job. Siponen (2000) again claim that, AppSec Awareness recognizes the most advanced lessons employees need to know to build safe products and services. Consciousness is an ongoing activity, so you never succeed in solving a good crisis and bad things will happen to your organization, and often it will be horrible

Motivation

Training on security awareness and the culture it instills are measurable and if you include tests and other measurement activities, make them fun and give rewards for doing a good job (Puhakainen & Siponen, 2010). Create a system that rewards and promotes safety best practices, but on the contrary, poor results are not used by the individual as punishment so instead, focus on how to improve the program - after all, we are all different, and different learning styles fit different types of people (Kohn, 1999). Look for opportunities to celebrate success. When someone passes a mandatory security awareness program and successfully completes it, give them a high score or five more important things

(Peltier, 2010). A simple $ 100 cash reward is a great incentive for people, and will cause them to remember the safety lesson that saved money (Merchant & der Stede, 2007). Merchant and der Stede (2007), claim that, people will also quickly tell five of their colleagues that they have received money for learning, and they will jump in training quickly. Merchant and der Stede, (2007), further assert that, if you're giving up the idea of giving away $ 100 per employee, stop being too cheap and calculate the cost. The return on investment in preventing a single data breach significantly exceeds the $ 100 spent. The other aspect of the reward is security progress. Peltie (2010) claim that, management should Provide opportunities for team members to grow into a dedicated security role through progress. Make security a professional choice within your organization and put your money where your mouth is, If you say security is important, prove it by providing growth potential for those with a passion for security (Peltier, 2010).

Klein and Rice (2014) claim that management should Provide staff with the opportunity to earn an advanced degree in security. Klein and Rice (2014) further claim that, many universities now offer a master's degree in cybersecurity. If you can't find a place nearby, create your own account and again, put your money in your place and take care of the first group of students (Klein & Rice, 2014).

Security mindfulness

Employees should feel empowered after receiving training and knowledge to help play their role in preventing a security breach (Coopey, 1995). A culture of safety is a state of mind, and if done properly, it can become part of the lifestyle of an organization, along with general everyday work (Glendon & Stanton, 2000). But we must always remember that a culture of security is part of an ongoing process. Cybercriminals rarely sit on their laurels and develop new and more sophisticated technologies to deceive us (Singer & Friedman, 2014). All elements of a culture of security need to be cultivated as part of an ongoing process and training should be repeated regularly, keeping the random side to simulate phishing (Singer & Friedman, 2014). Becoming a mindfulness security will make the security work normalized.

Employees are one of the first lines of defense when it comes to effective cybersecurity, thus you can say they act as "human firewalls" (Singer & Friedman, 2014). Singer and Friedma (2014) claim that management can implement great systems and policies - for example, everyone should know that you don't click suspicious links or download unfamiliar files. But in the absence of a supportive culture, this protection collapses.

As we often hear, it doesn't take a single password to break an organization, therefore, the development of a security culture is critical (Singer & Friedman, 2014). To achieve this, Focus on encouraging employee participation in security. Herath and Rao (2009) claim that management should follow the correct steps and your security culture will form on its own. Herath and Rao, (2009) came out the following basic ideas below

1. Start hiring - ask candidates before hiring to get an idea of how they handle security.
2. Start from the top - a culture of safety starts from the top, with the CEO or president of the company. This person should design good security practices and talk honestly about it at every opportunity.
3. Each manager is a leader - as with the CEO, each manager must live and design good security practices.
4. Workforce Survey - Ask employees periodically about their knowledge, views and security practices. Then analyze and act on the results to improve the security situation of the organization.
5. Against Manpower Training - educate your workforce. Conduct refresher courses at least once a year. We can't expect staff to follow good practices if they don't know what those are.
6. Make Security a Campaign - Like participating in a community issue that uses posters, updates and gatherings, we must do the same to enhance employee security engagement.
7. Rewarding Good Practices - When employees do the right thing, reward them. In some cases, material rewards are appropriate, but the reward can be something as simple as public praise.

DOI: 10.21522/TIJMG.2015.SE.19.02.Art013
ISSN: 2520-310X

Summary of results

The below gives the summary of the results.

Table 1. Summary of how to create security and safety awareness across organizations

Determinant /Variable (Security and Safety Awareness)	**Results Obtained**
Education	A key significant determinant of security awareness across organizations.
Building security community and policies	Building security community and strong policies for security and safety culture awareness is very significant in creating security awareness across organizations.
Initiating security Boot camp	Initiating security Boot camp such as Security awareness training and simulation exercises is significant at providing a first-hand firsthand experience necessary to learn and understand where the risks lie, and hence creating security and safety awareness across organizations.
Motivation	Create a system that rewards and promotes safety best practices is a significant determinate of the awareness of security and safety culture across organizations.
Security and safety mindfulness	Security mindfulness in everyday operations and decision making is of significance in creating security awareness across organizations.

Source. from Literature

Table 2. Summary of the importance of creating security and safety culture across organizations.

Determinant /Variable (importance of creating security and safety awareness)	**Results**
Long-term commercial viability	Security and safety culture are significant in ensuring a long-term commercial viability of organizations.
Impenetrable processes	Security and safety culture awareness ensures impenetrable processes of organizations.
Safe operations of applications.	Security and safety culture across organizations allows the safe operation of an application that is applied to an organization's information technology (IT) systems.
Data protection	Security and safety culture across organizations ensures information security and data protection in the organization.
Protection of organizational functions.	Security and safety culture awareness across organizations is of significance in protecting all organization functions from top to down.
Increased organizational effectiveness and performance.	Creating security and safety culture awareness is of significance in ensuring organizational effectiveness and performance.
Build and maintain a flexible network environment and stay away from information risks.	Security and safety culture, good or bad, is the ultimate determinant of whether a company can build and maintain a flexible network environment and stay away from information risks.

Source. from Literature

Discussion of results

The results of the study are discussed below

How to create security and safety awareness culture across organizations?

The study revealed that, organizations can create security and safety awareness culture through; Education, Building security community and policies, Initiating security Boot camp, Motivation and Security and safety mindfulness. Creating security culture through education confirms Christopher, Choo, and Dehghantanha (2017) study that, Knowledge is power, cybercrime education and typical attack scenarios are an essential part of any security awareness training program Christopher, Choo, and Dehghantanha (2017) assert that, Security must be strengthened and nurtured, and therefore the spirit of training should be conducted using a top-down approach. Management should be training advocates who are involved in the development of company policy and also, extend security and safety education to everyone who can be a threat to your organization - including all employees, contractors, entrepreneurs, consultants, third parties (such as suppliers) and even customers (Shaw, Chen, Harris, & Huang, 2009).

The study also confirms Singer and Friedman (2014) study about building security community and policy that, a holistic view must be taken where everyone recognizes the role they play in corporate culture and the impact that they can have personally on security. Singer and Friedman (2014) came out that, understanding security issues throughout the organization, from a clean office policy to developers, understands the importance of securing security and encryption records. Arrey (2019) also asserts that, if you don't have a secure development lifecycle, get one now. Arrey, (2019), clarify that, the Safe Development Life Cycle (SDL) is the foundation of a sustainable security and safety culture. SDL is the process and activities that your organization agrees to implement for each program or system version (Arrey, 2019). Arrey (2019) further clarify that, it includes things like security requirements, threat modeling and security testing activities. Arrey (2019) again claim that, SDL answers how your safety culture is secured and that, it is a culture of sustainable safety and security at work.

Again, the study confirm that, Security camps should cover all aspects of security from phishing and online security to desktop security to physical security (Camp, 2009). Phishing simulations should be performed regularly, but also randomly, to create more natural scenarios (Blanchard, 2006). People are your best asset, and they can also be one of the greatest assets.

The study confirms Kohn (1999) study that, organizations should create a system that rewards and promotes safety best practices, but on the contrary, poor results are not used by the individual as punishment so instead, focus on how to improve the program - after all, we are all different, and different learning styles fit different types of people (Kohn, 1999). Look for opportunities to celebrate success. When someone passes a mandatory security awareness program and successfully completes it, give them a high score or five more important things (Peltier, 2010).

Employees should feel empowered after receiving training and knowledge to help play their role in preventing a security breach (Coopey, 1995). A culture of safety is a state of mind, and if done properly, it can become part of the lifestyle of an organization, along with general everyday work (Glendon & Stanton, 2000). All elements of a culture of security need to be cultivated as part of an ongoing process and training should be repeated regularly, keeping the random side to simulate phishing (Singer & Friedman, 2014). Becoming a mindfulness security will make the security work normalized. These studies confirm the present study that security mindfulness is significant in creating security and safety awareness across organizations.

Importance of creating security and safety culture awareness across organizations.

The study went further to reveal that, security and safety awareness across organizations is important and a key determinant of ensuring; Long-term commercial viability of organizations, Impenetrable processes of organizations, Safe operations of organizations' applications systems, Data protection, Protection of organizational functions from top to down, Increased organizational effectiveness and performance and building and maintaining a flexible network environment and hence staying away from information risks.

DOI: 10.21522/TIJMG.2015.SE.19.02.Art013
ISSN: 2520-310X

Humans are complex creatures of habit, we do the things we do, in general, because that's how we always did (Jacob, 1977). The same can be said about the cultures in our society and even in the organizations we work for and in terms of long-term commercial viability, culture is everything, especially when it comes to information security (Argyris, 2017). Culture, good or bad, is the ultimate determinant of whether a company can build and maintain a flexible network environment and stay away from information risks (Hofstede, 2001).

A strong safety culture is both a mentality and a way of working and Once integrated in daily thinking and decision-making, can be an almost impenetrable process (Hofstede, 2001). On the contrary, an absent security culture will facilitate uncertainty and ultimately lead to security incidents that you cannot tolerate (Lord, 2012). This often happens because everyone literally works in silos; you know, the same people of us in the industry that we quickly announce are bad for security (Mitnick & Simon, 2011). Schön (2017) assert that, rather than being useful and doing what they can do to really improve security, these people often do better for their own interests, sometimes even to sabotage each other or work in general.

Information security also allows the safe operation of an application that is applied to an organization's information technology (IT) systems (Ifinedo, 2012). Ifinedo (2012) claim that, this is because to protect the data, the organization will apply or install the appropriate software that will secure data such as antivirus and other protected applications. Therefore, information security is critical in any organization to protect applications that are implemented in organizations and to protect the data store on the computer as well. In addition to data protection, the installed application also needs protection because it can contribute to the loss or damage of information (Ifinedo, 2012).

Information security protects data collected and used by the organization (Ifinedo, 2012). If the information is left unprotected, anyone can access it and if the information falls into the wrong hands, it can destroy lives and bring down business and can also be used to harm (Ifinedo, 2012). Ifinedo (2012) clarify that, information security software will ensure that appropriate business information and legal requirements are protected by steps taken to protect enterprise data. In addition, the steps taken to protect enterprise information is a matter of maintaining privacy and will help prevent identity theft.

With regard to the protection of the functions of the Organization, the General Directorate and the Information Technology Department are responsible for implementing information security that protects the Organization's ability to operate (Posthumus & Von Solms, 2004). Posthumus and Von Solms (2004) assert that, information is the most important element in an organization to do business. They further claim that, besides, the organization keeps the information of its customers, so it is important for them to protect the information and without information, the work cannot be run. By securing the information store; it can enable the organization to run the business as well. This is why information security is important in organizations.

Conclusion

From the study, it can be concluded that, organizations can create security and safety awareness culture through; Education, Building security community and policies, Initiating security Boot camp, Motivation and Security and safety mindfulness.

It can also be concluded that, security and safety awareness across organizations is important and a key determinant of ensuring; Long-term commercial viability of organizations, Impenetrable processes of organizations, Safe operations of organizations' applications systems, Data protection, Protection of organizational functions from top to down, Increased organizational effectiveness and performance and building and maintaining a flexible network environment and hence staying away from information risks.

Acknowledgement

All thanks to God for giving us this incredible strength, perseverance, courage and the ability to complete this paper. Even though any educational hustle and bustle is a lonely figure, but it requires the help and support of others and encourages them to succeed. "What could the eagle climb without conquering?" TAU, we owe it to those who have been frank, not defenders and very supportive in difficult times.

References

[1]. Annan, K. A. (2005). In larger freedom: towards development, security and human rights for all: report of the Secretary-General. United Nations Publications.
[2]. Argyris, C. (2017). Integrating the Individual and the Organization. Routledge.
[3]. Arrey, D. A. (2019). Exploring the Integration of Security into Software Development Life Cycle (SDLC) Methodology. Colorado Technical University.
[4]. Beard, R. (2013). Risk theory: the stochastic basis of insurance (Vol. 20). Springer Science & Business Media.
[5]. Bedford, T., Cooke, R., & others. (2001). Probabilistic risk analysis: foundations and methods. Cambridge University Press.
[6]. Benbasat, I., & Zmud, R. W. (2003). The identity crisis within the IS discipline: Defining and communicating the discipline's core properties. MIS Quarterly, 183–194.
[7]. Blanchard, P. N. (2006). Effective Training, Systems, Strategies, and Practices, 4/e. Pearson Education India.
[8]. Brown, N. J. (2019). Crisis management.
[9]. Camp, L. J. (2009). Mental models of privacy and security. IEEE Technology and Society Magazine, 28(3), 37–46.
[10]. Christopher, L., Choo, K.-K., & Dehghantanha, A. (2017). Honeypots for employee information security awareness and education training: a conceptual EASY training model. In Contemporary Digital Forensic Investigations of Cloud and Mobile Applications (pp. 111–129). Elsevier.
[11]. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. NIST Special Publication, 800(61), 1–147.
[12]. Clifford, W., & Smith, J. (1995). Corporate risk management: theory and practice. The Journal of Derivates, 30, 21, 31.
[13]. Coopey, J. (1995). The learning organization, power, politics and ideology introduction. Management Learning, 26(2), 193–213.
[14]. Cummins, J. D., & Weiss, M. A. (2009). Convergence of insurance and financial markets: Hybrid and securitized risk-transfer solutions. Journal of Risk and Insurance, 76(3), 493–545.
[15]. Donaldson, L. (2001). The contingency theory of organizations. Sage.
[16]. Fennell, M. (2010). Training skills. The Oxford Guide to Surviving as a CBT Therapist, 371–405.
[17]. Furnell, S., & Clarke, N. (2005). Organizational security culture: Embedding security awareness, education, and training. Proceedings of the IFIP TC11 WG, 11, 67–74.
[18]. Glendon, A. I., & Stanton, N. A. (2000). Perspectives on safety culture. Safety Science, 34(1–3), 193–214.
[19]. Hafey, R. (2017). Lean safety: Transforming your safety culture with lean management. Productivity Press.
[20]. Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154–165.
[21]. Hofstede, G. (2001). Culture's consequences: Comparing values, behaviors, institutions and organizations across nations. Sage publications.
[22]. Hofstede, G., Neuijen, B., Ohayv, D. D., & Sanders, G. (1990). Measuring organizational cultures: A qualitative and quantitative study across twenty cases. Administrative Science Quarterly, 286–316.
[23]. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83–95.
[24]. Jacob, F. (1977). Evolution and tinkering. Science, 196(4295), 1161–1166.
[25]. Klein, J. I., & Rice, C. (2014). US education reform and national security. Council on Foreign Relations.
[26]. Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. Production and Operations Management, 14(1), 53–68.
[27]. Klinke, A., & Renn, O. (2002). A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies 1. Risk Analysis: An International Journal, 22(6), 1071–1094.
[28]. Kohn, A. (1999). Punished by Rewards: The Trouble with Gold Stars, Incentive Plans, A's, Praise, and Other Bribes. Houghton Mifflin Harcourt.
[29]. Lord, K. M. (2012). Perils and Promise of Global Transparency, the: Why the Information Revolution May Not Lead to Security, Democracy, or Peace. Suny Press.
[30]. Martins, A., & Elofe, J. (2002). Information security culture. In Security in the information society (pp. 203–214). Springer.

DOI: 10.21522/TIJMG.2015.SE.19.02.Art013
ISSN: 2520-310X

[31]. Marzbali, M. H., Abdullah, A., Razak, N. A., & Tilaki, M. J. M. (2011). A review of the effectiveness of crime prevention by design approaches towards sustainable development. Journal of Sustainable Development, 4(1), 160.
[32]. Merchant, K. A., & der Stede, W. A. (2007). Management control systems: performance measurement, evaluation and incentives. Pearson Education.
[33]. Mitnick, K. D., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. John Wiley & Sons.
[34]. Peltier, T. R. (2010). Information security risk analysis. Auerbach publications.
[35]. Poolsappasit, N., Dewri, R., & Ray, I. (2011). Dynamic security risk management using bayesian attack graphs. IEEE Transactions on Dependable and Secure Computing, 9(1), 61–74.
[36]. Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), 638–646.
[37]. Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. MIS Quarterly, 757–778.
[38]. Quinn, R. E., & Spreitzer, G. M. (1997). The road to empowerment: Seven questions every leader should consider. Organizational Dynamics, 26(2), 37–49.
[39]. Rice, A. L. (2013). The enterprise and its environment: A system theory of management organization. Routledge.
[40]. Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the ﷺweakest linkﷺa human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122–131.
[41]. Schön, D. A. (2017). The reflective practitioner: How professionals think in action. Routledge.
[42]. Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92–100.
[43]. Singer, P. W., & Friedman, A. (2014). Cybersecurity: What everyone needs to know. OUP USA.
[44]. Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31–41.
[45]. Sodiya, A. S., Onashoga, S. A., & Oladunjoye, B. A. (2007). Threat modeling using fuzzy logic paradigm. Informing Science: International Journal of an Emerging Transdiscipline, 4(1), 53–61.
[46]. Solana, J. (2003). A secure Europe in a better world: European security strategy. Içinde Klaus Schilder ve Tobias Hauschild, Der., Civilian Perspective or Security Strategy.
[47]. Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems.
[48]. Sunder, S., & Cyert, R. M. (1997). Theory of accounting and control. South-Western College Pub.
[49]. Sussman, S. W., & Siegal, W. S. (2003). Informational influence in organizations: An integrated approach to knowledge adoption. Information Systems Research, 14(1), 47–65.
[50]. Thomson, K.-L., & Von Solms, R. (2005). Information security obedience: a definition. Computers & Security, 24(1), 69–75.
[51]. Wiseman, R. M., & Gomez-Mejia, L. R. (1998). A behavioral agency model of managerial risk taking. Academy of Management Review, 23(1), 133–153.