Cybersecurity Education for Awareness and Compliance

Ismini Vasileiou
University of Plymouth, UK

Steven Furnell
University of Plymouth, UK

A volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

IGI Global
DISSEMINATOR OF KNOWLEDGE

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Vasileiou, Ismini, 1980- editor. | Furnell, Steven, 1970- editor.
Title: Cybersecurity education for awareness and compliance / Ismini Vasileiou and Steven Furnell, editors.
Description: Hershey, PA : Information Science Reference, [2019] | Includes bibliographical references.
Identifiers: LCCN 2018036338| ISBN 9781522578475 (h/c) | ISBN 9781522578482 (eISBN)
Subjects: LCSH: Business enterprises--Computer networks--Security measures. | Information technology--Security measures. | Employees--Training of. | Employee rules.
Classification: LCC HD30.38 .C93 2019 | DDC 658.3/124--dc23 LC record available at https://lccn.loc.gov/2018036338

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.

Chapter 3
The Role of Education and Awareness in Tackling Insider Threats

Shaun Joseph Smyth
Ulster University, UK

Kevin Curran
Ulster University, UK

Nigel McKelvey
Letterkenny Institute of Technology, Ireland

ABSTRACT

Insider threats present a major concern for organizations worldwide. As organizations need to provide employees with authority to access data to enable them to complete their daily tasks, they leave themselves open to insider attacks. This chapter looks at those who fall into the category which can be referred to as insiders and highlights the activity of outsourcing which is employed by many organizations and defines the term insider threat while pointing out what differentiates an accidental threat from a malicious threat. The discussion also considers various methods of dealing with insider threats before highlighting the role education and awareness plays in the process, the importance of tailoring awareness programs, and what the future holds for insider threats within organizations.

INTRODUCTION

In the early 1990s the United States saw a drive in the growth of business because of telecommunications networks and the Internet. Despite this growth, the dependency placed upon these networks placed the U.S. in a precarious position as it also increased their vulnerability to cyber exploitation and by the end of the twentieth century the U.S. had become the most vulnerable nation to cyber-attacks aiming to disrupt or interfere with essential services (McConnell, 2002).

DOI: 10.4018/978-1-5225-7847-5.ch003

Organizations, worldwide regardless of their size or form have all accepted that an increase in the development of their existing services is essential if they are to improve and gain a much-needed advantage over their fellow competitors. In their quest to achieve this goal organizations understand that a greater dependence is placed upon the need for information technology (IT) for them to compete successfully in the world of modern-day business (Abawajy, 2014). Businesses are already connected with the bulk of transactions taking place in an electronic format the consequence of which is a constant rise in the quantity of both personal and sensitive data produced and later collected. Sensitive data is looked upon as one of the many assets of any organization as many appreciate its significance, considering it to be the lifeblood of the processes and procedures which take place within their business (Sarkar, 2010). As many of today's organizations compete in lively and fast-moving environments which are constantly developing, they produce a large volume of sensitive data in a bid to achieve their goals which include lower prices, higher quality of products and services and a rapid development. However, the provision of new opportunities coupled with the globalization of activities in both businesses and organizations combined with the swift growth of ICT has given rise to a new problem in the form of threats (Stavrou et al. 2014).

Organizations can find themselves on the receiving end of threats as their information security is susceptible to dangers from a wide variety of sources which present in many different formats varying from the less complicated spam emails to the more structured and complex form of attack such as malwares (malicious software) which can steal or contaminate data and ultimately produce enough damage to leave systems in a condition where they are inoperable (Abawajy, 2014).

One such threat includes that caused as a direct result of online social networking (OSN) which has recently experienced a sudden rise. Certain employees within organizations are accountable for information and are later responsible for the leakage of this same information to outside parties. Careless use of social media has a harmful influence on organizations placing networks and systems at risk of malware which can result in many negative issues including copyright and defamation issues, reduced productivity which significantly affect the organization's reputation and future income (Molok et al. 2011).

Modern-day information systems are challenged by a wide range of threats and even though attacks which are started from outside such as viruses and hacking receiving much publicity the insider threat however, presents a considerably higher level of danger (Theoharidou et al. 2005). This view is shared by Baracaldo and Joshi (2012), McCormac et al. (2012), and Warkentin and Willison (2009) who all point out that Insider attacks are still one of the most dangerous threats organizations can face today.

The insider threat comes from the trusted organizational member and they can cause the greatest harm as they have access to the organization's greatest asset 'information'. Those individuals employed within an organization have the capability to either damage or destroy sensitive information using uncomplicated noncompliance of security policies, negligence, the absence of motivation in the protection of sensitive data, careless actions within the workplace or insufficient training. Including reduced productivity and revenue such actions result in the failure to protect the confidentiality of the organization, its associates, customers and ultimately the reputation of the organization's information system. This problem is often referred to as the 'endpoint security problem' as the employee is the last point of contact or endpoint of the information system (IS) and its network. It is often said that the weakest link or greatest security problem within a network lies between the keyboard and the chair (Warkentin, and Willison, 2009).

Organizations are faced with an ever-growing task in relation to computer security and face persistent attacks from both external and internal sources as there are many different threats which are all keen to breach organizational security defenses with a noticeable increase in the vulnerability to threats posed by the insider because of the worryingly high increase in the possession of privileged access to the network which they enjoy and require to carry out their jobs (Nurse et al. 2014; Martinez-Moyano et al.2008).

This view is also expressed by Claycomb and Nicoll (2012) as they highlight that insider threats are both a constant and ever-increasing problem. The insider attack presents a much greater risk to organizations, the main reason for this however is not solely due to the advantage which the insider currently enjoys by already holding secure access to the network but it is also due to the fact that the majority of network security procedures direct their attention to the prevention of external attacks from those who are outside the network perimeter the consequence of which is a reduction in the importance assigned to the safeguarding of network components against malicious access internally from within the actual network itself from management/employees who already have network access and certain privileges inside the network itself (Nurse et al.2014; McCormac et al. 2012). Martinez-Moyano et al (2008) also emphasize that the growing dependence of organizations on technological infrastructures has placed organizations in a position where they are exposed to an increased vulnerability from insider threats.

The rest of this chapter looks at those individuals who can be classed as insiders and offers a definition for the term 'insider threat' looking at their frequency of occurrence and the different causes. The practice of non-compliance within the workplace is examined highlighting some reported breaches of security by organizational employees and the reported damage caused to those organizations due to the practice of insider threats. Also covered within this chapter are the roles which both education and awareness can play in dealing with the growing problem of the insider threat within an organizational setting including the possibility of reducing the issue or eradicating it completely as organizations now place more emphasis on external threats and their prevention than they do on the insider threat which can be equally if not more dangerous to an organization.

BACKGROUND

The cost incurred to businesses worldwide due to security breaches and computer viruses has been a total of $1.6 trillion a year and 39,363 human years of productivity (Ula and Fuadi, 2017). This highlights the importance placed in the ability for organizations to protect their assets and why the security of information is such a major concern in organizations. The potential for attacks from hackers is such a worry that many are forced to employ services in a bid to protect against viruses and malware and the likelihood of an attack from an outsider. However, although protection from external attacks is an important concern it is also essential not to dismiss the possibility of attacks which occur closer to home as much evidence suggests that internal breaches have been the cause of many significant, costly attacks and security incidences in both government and organizational sectors (Sarkar, 2010). A similar view is shared by Chinchani et al. (2005) as they highlight that many organizations concentrate solely on external attacks as techniques and tools are now available to help in finding and fixing such weaknesses, unlike the internal threat which is not yet fully understood, difficult to calculate and there is an absence of available tools and techniques which are able to help with such a situation.

Insider attacks are a well-recognized problem with the threat they offer being acknowledged as far back as the 1980s (Chinchani et al. 2005). However, for years organizations have wrestled with this internal issue of defending themselves from individuals which they should trust in the day-to-day running of their business. Such individuals are referred to as 'insiders' which include employees, freelance workers, consultants and others who have the privilege of having access to vital areas within an organization which ultimately enables them to access important organizational information. Individuals in such positions however may exploit the trust bestowed upon them for their own personal gain and pose as a serious threat to confidentiality within the organization, the organization's significant assets and ultimately the organization's reputation (Liu et al. 2008).

Insiders worldwide are accountable for many such incidents with reports of insider threats by those granted the privilege of access to information within organizations where they have been employed. Many such incidents however, go unreported to protect the reputation and good name of the organization yet many still make the headlines such as the following:

- Over a period of months in 1996 two credit union employees working together altered credit reports for monetary gain. Both employees had authorization as part of their normal duties to update information received by the company however these two individuals misused their authorization by removing negative credit indicators and adding fabricated indicators of positive credit in exchange for money. The total amount of fraud because of these activities surpassed $215,000 however, the risk associated with the credit union as a result was immense (Randazzo et al. 2005).
- Sarkar (2010) highlights how the UK government hit the headlines in 2008 when a Home Office contractor lost a USB stick which held details of all 84,000 prisoners within Wales and England resulting in the end of a £1.5 million contract with a management consultancy firm.
- An international financial services company fell victim to a logic bomb in 2002 deleting 10 billion files in the company and affecting servers of over 1300 companies throughout the United States. The company suffered losses totaling $3million needed to repair damage and recreate the deleted files. Investigations later revealed that the logic bomb was planted by a frustrated employee who quit the company over a dispute regarding the amount of his annual bonus (Randazzo et al. 2005).

The incentive to work on insider threats varies from country to country as the U.S. interest appears to be centered more around events which cause damage to national security such as the case of Robert Hanssen, an FBI insider who was arrested in 2001 for stealing and selling secrets to the Russians and more recently, the case of Bradley Manning an American soldier and insider who revealed many confidential U.S. government documents. When compared to the $7billion fraud committed against the French bank Societe Generale by one of its own traders, Jerome Kerviel the difference is obvious (Hunker and Probst, 2011).

WHO ARE INSIDERS?

A reliable definition of an insider is difficult to obtain and as such it hampers the detection of threats from this group of individuals. The assumption of a perimeter around an organization such that those within the perimeter can referred to as insiders is not practical with the increase in mobile computing and outsourcing (Bishop and Gates, 2008). Similarly, an insider can have wireless connectivity and have a physical presence far away from an organization while likewise individuals can be physically present within an organization but have no authorization to use the computation infrastructure (Chinchani et al. 2005). Despite the arguments which surround an insider's physical location, many descriptions of what constitutes an insider are however offered. One such definition includes that proposed by Magklaras and Furnell (2005) who explain that the insider is an individual who has legitimately been given the ability to access one or several elements of the IT infrastructure using one or more authentication mechanisms. It is the use of the word legitimately which differentiates between the insider who enjoys a certain level of trust and advantages in comparison to the external hacker who must spend extra time and effort in obtaining a point of entry to the computer system an advantage which the insider already enjoys. As Sarkar (2010) highlights the insider can be an employee who has the required privileges such as keys, log on details for the network and suitable network access to enable them to fulfil his/her duties in their place of work on a day-to-day basis. This is a view which is shared by Greitzer et al. (2008) who define the insider as a person who is now or was on some earlier occasion granted the authority to access the organization's information system, data or network and such authorization is indicative of a high level of trust in that individual.

Hayden (1999) who also explains that insiders who can be employees, contractors or service providers or somebody with valid access to a system however, stresses that the issue of trust is an important factor regarding insiders as the more privileges they enjoy on the system, the greater will be their level of knowledge and access on the system and ultimately, they pose a higher potential threat.

Probst et al. (2010) describe an insider as the following:

- An insider is an individual who has rightful access to resources.
- An insider is an individual or company which the organization trust.
- An insider is the user of a system who can use their privileges for the wrong purpose.
- An insider is an individual who despite having authorized access may use this benefit to damage or remove organizational assets or help outsiders in carrying out such acts.

Probst et al. also highlight how the following definition for an insider has been proposed:

An insider is a person that has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization's structure. (Probst et al. 2010)

Despite this proposed definition of insiders, there are however, insiders which are not necessarily always friendly in nature helping organizations in their day-to-day functions as some may present as threats posing a danger to organizations and their resources namely their private data/information (Park and Ho, 2004). In defining the insider Anderson (1999) looks at the intent of the insider classifying them into three categories which include Normal – Abnormal – Malevolent. Anderson (1999) explains each of these three categories further highlighting the intent of each of three insider types as follows:

- **Normal:** This category of insider is likely to carry out insider activity which is unlikely to present a threat.
- **Abnormal:** The insider activity by this group may consist of routine errors which may cause issues in a weak system causing private information to be accidentally revealed
- **Malevolent:** This includes insider activity which presents a threat as it is carried out with mischievous intent.

McConnell (2002) highlights that everybody connected to the Internet is a possible insider within an organization and ordinarily in an environment which is non-computing the authority to access information is based upon distinct roles which relates to users and the access privileges they have. However, within the modern computing environment roles often change and, in many instances, are less well-defined.

The greatest threat to computer security is symbolized by insiders as these individuals understand fully the commercial side of their organization and the workings of the computer system and they possess confidentiality and the legitimate access to the network which enables them to carry out insider attacks (Nguyen et al. 2003)

THE INSIDER THREAT

The subject of the insider threat is not a new issue as documented reports of this problem date as far back as the 1980s (Chinchani et al. 2005) and as Miller and Maxim (2015) stress it is the responsibility of organizations to face up to the fact that insider threats pose a significant threat and are increasing in difficulty. The task of achieving a conclusive definition for the insider threat is both challenging and complex as so many varied opinions on this subject exist (Humphreys, 2008). Despite this fact there are however, many different definitions presented on this subject some of which including the following:

Cappelli et al. define the insider threat as:

Individuals who were, or previously had been, authorized to use the information systems they eventually employed to perpetrate harm. (Cappelli et al. 2004)

Bishop and Gates explain how the insider threat can be defined with respect of these two primitive actions:

1. violation of a security policy using legitimate access violation of a security policy using legitimate access

2. violation of an access control policy by obtaining unauthorized access (Bishop and Gates, 2008)

Finally, the definition offered by Greitzer et al. differs again as they say:

The insider threat is manifested when human behavior departs from compliance with established policies, regardless of whether it results from malice or a disregard for security policies. (Greitzer et al. 2008)

Greitzer and Frincke (2010) also highlight that despite the vast amount of research which has been carried out on the insider threat, especially in the studies of both the psychology and motivation of insiders, the prediction of insider attacks however still proves exceedingly difficult. The insider threat has commanded a serious amount of attention and it is referred to as the most difficult security problem to deal with because the insider has information which is unknown to outside hackers and as a result, they are able to inflict serious damage (Hunker and Probst, 2011). Internal attacks take place when authorized individuals including trusted employees within an organization execute specific actions in the organization abusing the trust and privileges, they have thus causing harm to the organization (Baracaldo and Joshi, 2012; Chinchani et al. 2005; Greitzer et al. 2008; Blackwell, 2009). As Greitzer et al. (2008) point out insider threats begin when the behavior of humans deviates from compliance with established policies whether it is a result of malicious intent or just a complete disregard for security policies

Trying to escape such threats from insiders is a frightening task as it is essential that employees receive privileges to enable them to carry out their jobs in an efficient manner. However, the provision of too many privileges to an employee can have detrimental effects if they are misused in either an intentional or unintentional fashion (Baracaldo and Joshi, 2012). Greitzer and Frincke (2010) claim that only a small number of employees take part in the type of behavior which could be described as that of an insider threat as the rest of the working population is made up of individuals who are classed as both honest and hard-working. Worryingly however, they also highlight that a report by the U.S. Department of Defense in 1997 confirmed that 87% of those intruders into the Department of Defense which were recognized included either employees or others who were internal to that organization.

The main motivational factor behind many insider attacks is pure and simple financial gain as highlighted by Cappelli et al. (2004) as they claim that carrying out insider attacks for any other purpose is simply not worth the risk. Financial gain can be achieved through different formats depending on the type of organization in which the insider threat takes place. In financial establishments such as banks, the value lies in customer account records and company accounts which give a direct route to funds while other types of organizations such as software companies do not offer such immediate financial rewards as the real value lies in the branded software code (Chinchani et al. 2005). Monetary losses incurred because of insider attacks range in value from five hundred dollars to tens of million dollars with approximately 75% of organizations experiencing a negative impact to their business and 28% reporting a negative influence on their reputations (Baracaldo and Joshi, 2012). All commercial sectors are troubled by the insider threat for several reasons including the following:

- Personal gain and profit (scams, fraud or theft of information and other assets).
- Taking part in reckless behavior whether it was intended to cause harm or not.
- Malicious damage/sabotage which was intended to inflict harm.

Martinez-Moyano et al. (2008) clarifies that data analysis carried out by CERT/CC (coordination center for the computer emergency response team) stresses that the three different insider threats which organizations face include 1) Long term, 2) Sabotage, 3) Espionage or information threat. Franqueira et al. (2010) also highlights that other classifications of the insider threat concentrate solely on the intentions of the insider and likewise organizes them into three separate categories which include the following:

- Theft of information also referred to as espionage when individuals steal private or personal from the organization.
- IT sabotage which occurs when somebody damages the organization or any individual within it.
- Finally, the third category refers to fraud which occurs when someone acquires unwarranted services or property from the organization.

Franqueira et al. (2010) point out however, that there is a connection between these three classifications as impersonators are in a better position to execute fraud while trespassers or those who carry out a lawful action in an illegal or improper manner are in a better place for the execution of sabotage and espionage. According to Greitzer and Frincke (2008) there are many different types of crimes associated with insider threats include Espionage, Sabotage, Terrorism, Embezzlement, Extortion, Bribery and Corruption. Even though insider threats have a higher success rate, they occur less often than outsider attacks as displayed in table 1. They pose a greater risk than their counterparts and have an immediate advantage by having legitimate access to the system (Chinchani et al. 2005).

MALICIOUS/ACCIDENTAL THREATS

The very mention of an insider threat invokes the image of an unhappy employee who is planning to take revenge or a malicious employee who is looking to achieve financial gain. Every organization is afflicted by employees who unintentionally put their employers and the organization itself in danger. Such insider threats however, are not deliberate and take place due to basic unfamiliarity or inexperience (Sarkar, 2010). All insider threats are not the same, as highlighted by Miller and Maxim (2015). There are several different types of insider threats which include the malicious insiders who are current or former employees or even trusted partners of the organization who abuse their positions and their legitimate access to the organization's network system/data making decisions fully aware that their actions will cause damage to the organization and have a full understanding that their actions will have a negative effect on the organization they attack. Such actions include - but are not restricted to - theft of information, fraud and sabotage. In comparison to this there are the insiders who are exploited by outside groups and influenced into carrying out actions which they see as reasonable but will result in damage to the organization. Finally, there is the category of insiders who, despite having privileges, are careless in security responses or cause a security breach through incorrect handling of the organization's main asset, 'information' on the network (Miller and Maxim, 2015; Cole, 2015; Glasser and Lindauer, 2013). Since few employees take part in insider threat activities the task of predicting insider attacks is made more difficult and experts have realized that a character who is despondent in his or her place of work and current job situation signifies the characteristics displayed by a would-be insider threat (Greitzer and Frincke, 2010).

Sarkar (2010) highlights that the largest security threat comes from those individuals with extended privileges and authorized access as great emphasis is placed on the importance of understanding the psychology of those individuals who are involved in insider activity, both malicious and non-malicious. Hunker and Probst (2011) list that there are psychosocial signs which highlight that an individual has the potential to be a malicious insider, some of which include the following:

- Disgruntled
- Accepting feedback
- Anger management

Table 1. Percentage of Insider attacks against outsider attacks

Year	2004	2005	2006	2007	2008	2010
Insider Attacks	29%	20%	32%	31%	34%	27%
Outsider Attacks	71%	80%	68%	69%	66%	73%

(Zawalge et al. 2013)

- Disengagement
- Disregard for authority
- Performance issues

The detection of malicious insiders presents an enormous task as Azaria et al. (2014) explain that initially the quantity of malicious insiders who have been exposed inside any given organization is normally very small, normally only amounting to a mere handful over the space of a decade thus creating an imbalanced data set of more than 99.9% honest users and less than 0.1% of malicious insiders which is not ideal for machine learning algorithms as they naturally assume data is balanced and the use of imbalanced data usually results in high accuracy for the majority class. Azaria et al. (2014) are also keen to point out that detection of malicious insiders is hindered further due to the lack of a publicly available data set for the insider threat as many companies are unwilling to share such data to protect their reputation.

Colwill (2009) emphasizes that the insider threat is constantly present revealing itself in many different formats and that the malicious insider can cause more harm to an organization as it has more advantages than the outside attacker. Colwill (2009) also highlights that those individuals who carry out malicious insider actions have a casual experience or mechanism which influences their motivation and ultimately leads to betrayal. Such experiences can be classified into three main sources which include:

- Rising, intensified or unaddressed dissatisfaction with their role or worth within an organization.
- Recruitment by unfriendly outside individuals or groups.
- The penetration of a malicious threat actor to a trusted position.

Neumann (2010) points out that despite the vast amount of attention which the intentional malicious misuse achieves it would however be considered irresponsible to overlook the acceptable accidental misuse as there is a likelihood that once this type of activity is accepted it could encourage malicious misuse later.

OUTSOURCING

Worldwide communications offer the chance to outsource tasks which were previously carried out within the organization in the home country to sites almost anywhere in the world. Such moves can involve transporting organizational activities to areas which have a favorable taxation structure which is more profitable with lower labor and set-up costs involving companies abroad which offer services at prices which are inexpensive and can deliver skills which are in limited supply. As a result, the move by organizations to outsourcing has become such an attractive proposition that the practice of outsourcing has become universal throughout the public and private sectors (Jones and Colwill, 2008). The quantity of third-party employees who are granted the privilege of long-term access to company systems and information comparable to that of full-time employees is increasing rapidly and as such the position of large volumes of outsider third party personnel is changed to insiders creating confusion over the difference between full-time company employees and third-party personnel (Jones and Colwill, 2008; Munshi et al. 2012).

While the subcontracting and outsourcing of certain tasks offers many benefits such as leading to improvements in efficiency, monetary gains, cheaper labor costs and other potential advantages it does however present the issue of the movement of organizational boundaries where security defenses could have been placed (Gollmann, 2011). As the growing tendency within organizations favors the use of mobile computing, working from home and outsourcing it also increases the probability of insider attacks. Outsourcing increases the possibility of confidential data being breached as information is moved beyond the organization's control and this data is made available to these third parties (Ophoff et al. 2014).

Despite the obvious difficulty of organizations ensuring that the confidential information they share while outsourcing stays confidential and no data breaches occur, outsourcing is however, not without its own difficulties. As highlighted by Colwill (2009) who firstly explains that the language differences can present issues such as misinterpretation misunderstanding at all stages and secondly outsourcing approaches can create further complications as many permanent staff witness roles being outsourced leading to feelings of alienation within the organization and employees are fearful of job security in case their roles within the organization are next in line for outsourcing. Colwill (2009) also highlights that provision of effective education in outsourced locations to the same level as it can be delivered within an organization is difficult due to the numbers of employees hired each month and due their physical location.

With many companies outsourcing many functions to external service providers, possibly in other countries allowing them to avail of the financial benefits, technical issues such as auditing the part of a business process which is being outsourced become difficult. Data protection and collection laws vary from country to country and outsourcing the task of auditing itself can be challenging as protection of the valuable confidential data already collected is of supreme importance and data should be as anonymous as possible so that it does not relate back to a particular individual revealing only the required data which the auditor needs to get results but prevents them from access to data they do not require and as a results prevents them from drawing unwanted conclusions from the data they have access to (Probst et al. 2010).

STOPPING INSIDER THREATS

An extensive and successful insider threat mitigation approach must include the motivational factors and behavior of humans beside organizational factors such as policies, procedures, hiring, training practices and technical weaknesses along with the best practices for avoidance or the early detection of unauthorized insider activity (Greitzer et al. 2008). Most mitigation strategies concentrate on how incidents are performed, detected and how the insider's identification is revealed. Even though such methods are successful in stopping insiders and their activity this occurs only when significant damage has already happened. Monitoring networks, email accounts and the log in activity of employees and their everyday work pattern may find irregularities here or there without causing suspicion. However, by the time these irregularities begin to add up and it is time to act on these findings it is in many cases too late as the insider has already acted and the damage has already been performed (Puleo, 2006).

As organizations develop, they become reliant on information technology with growing importance placed upon information security which was initially viewed as a technology problem which could be tackled using complex hardware and software solutions. However, the increasing number of security breaches has since disproved this theory, proving that it is in fact mainly a people problem as failure by the end users to recognize and follow the technological controls creates a concern as systems are compromised as a result (Yayla. 2011). With the issue of the insider threat growing in difficulty Sarkar

(2010) also highlights that technical solutions are not adequate for this issue as insider threats are essentially a people issue while Whitman (2003) emphasizes that technologists often ignore the human solutions opting instead for technology solutions when in fact it is essential that the human factor must firstly be discussed and incorporate technology for support when needed to achieve the required human behaviors. Colwill (2009) highlights that there is no disputing that the least technical controls for the prevention of insider attacks should include the following:

1. Encryption;
2. Access control;
3. Smallest possible privilege;
4. The use of monitoring, auditing and reporting

Colwill (2009) also points out that standard security policies and procedures are needed, and organizations must enforce said policies showing clearly what is expected of their employees. One method employed is the strict enforcement of company policies and excluding the personal use of any company assets within the workplace. As Colwill (2009) however, highlights that for such a measure to be successful it would need networks to be closed to all but essential business applications thus avoiding access to websites which are not work related and prevent time wasting and the risk of malware infections.

One method of detecting insider misbehavior is to adopt the use of monitoring as a suitable system can substantially reduce the potential of insider attacks and give an alert for the presence any suspicious behavior on the system so that the user's privileges can be restricted and prevent a possible insider attack (Baracaldo and Joshi, 2012). Even though research revealed that 70% of fraud is an insider issue 90% of security controls and monitoring are still focused on the external threat (Colwill, 2009). However, Greitzer and Frincke (2010) point out that although monitoring employees is an important activity in the fight against the prevention of possible insider threats they also highlight that employees could take offence when they learn that the very organization they work hard for each day is monitoring their very activity as only a minority of employees actually engage in insider activity which could possibly harm the organization.

As Flynn, et al. (2003) however, points out the use of monitoring should not just limit itself to individuals within the organization as the growing trend is leaning towards an increase in a mobile workforce who have the potential to cause an insider threat through the malicious use of the many mobile devices which this section of the workforce employ has also increased the potential for malicious use. Organizations need to be aware of the functionality of these mobile devices and in some cases the use of privately-owned mobile devices can be prohibited completely as they could be used to seize sensitive information and remote access to privileged data should be limited to a certain number and keep a log of when users use remote access for further inspection.

The Implementation of strong passwords is strongly recommended as is the practice of precise account management policies (Greitzer and Frincke, 2010; Randazzo et al. 2005). Even though the practice of good password management is strongly recommended within organizations, Randazzo et al. (2005) point out however that active practices such as compulsory password protection and change policies and the use of password-protected screen savers should be encouraged as this reduces the opportunity of insiders carrying out an attack using a fellow employee's computer or account. The importance of effective password practice is also highlighted by Cappelli et al. (2009) who explain that however vigilant an organization is in trying to prevent insider threats, if there is a possibility that their computer accounts can be compromised then the opportunity to side-step manual and automated controls exists and for this reason, password management practices and policies should apply to all employees to ensure that all the activity on any account is attributed to the account holder and only the account holder. If for any reason an employee's employment, consulting or contracting contract needs to be stopped then the immediate deactivation should take place of all their computer accounts, authorization on the system, remote access and privileges within the organization (Randazzo et al. 2005; Flynn et al. 2003)

Organizations should apply separate policies which privileged users should sign as they can cause the most harm having the greatest access to systems, networks and applications and they can log into the system as another user and have greater technical ability. Organizations should also employ techniques which only enable online activity to be attributed to one single employee thus disabling the privileged user from carrying out online activity under the guise of another employee. As with other employees if the privileged user's contract had to be ended then the organization should disable their access to the system at once to prevent an insider attack from a former employee (Flynn et al. 2003).

Organizations should investigate methods by which employees feel they can report suspicious behavior. Occurrences such as the sharing of passwords, trying to access information which an employee does not need to fulfil their duties or trying to gain access to unauthorized information or showing a complete disregard for the organization's safety policies and noncompliance with policies which are in place to protect the organization and the information it safeguards. Encouraging employees to engage in this type of practice will alert security personnel to the noncompliance with policies, thus providing them with the opportunity to investigate the issue before it becomes a major problem (Randazzo et al. 2005).

EDUCATION AND AWARENESS

In many organizations, the bulk of their security budget and time is devoted to placing defenses at the system boundary to protect the information and assets stored from outsiders including thieves and hackers who were engaged in the practice of economic espionage and other illegal activities. The everchanging environment has resulted in major technological advances offering employees the ability to make the most of the opportunity to communicate with the organization's network while still enjoying better mobility and this growth in remote working, home working and the decision to include outsourcing further complicates the issue with an increase in the number of personnel who have access to insider privileges resulting in organizations being exposed to an increased number of insider threats (Jones and Colwill, 2008). Appropriate employee education is a significant contributor to improving the durability of an organization and essential for the effective management of insider threats (Eggenschwiler et al. 2016). In the world of cybercrime Insiders have become one of the most extensively mentioned offenders as numbers increased with the past decade alone seeing a steady rise in the volume of attacks which have been reported as a direct result of insider activity (Eggenschwiler et al. 2016).

Technical solutions can offer valuable protection against security threats in the form of technology which offers a method for both the regulation and control of access to information and helps with the monitoring and detection of malicious activity. They are however unable to deliver a complete solution to the problem as it is the working environment and the human element which deliver the true foundations for success as the activities of cyber criminals takes on many different formats. It is for this very reason that the practice of user awareness and ongoing education are both recognized activities considered crucial in the mitigation of cyber threats (Colwill, 2009; Choo, 2011). Colwill (2009) also points out that the greatest non-technical methods accessible for both human issues and security are possibly education, training and awareness. Eggenschwiler et al. (2016) also emphasize the importance of educational measures, employee training and awareness campaigns highlighting the crucial part they play in the quest for insider threat recovery as they stress that encouragement of relevant education for employees within organizations is essential as the practice of such behavior not only contributes greatly to the strength of an organization but it is vital as it contributes considerably to the provision of an effective insider threat management.

Probst et al. (2010) highlight that employing the use of suitable training and awareness-building education will inspire the preferred security culture which an organization is looking for, while Furnell and Clarke (2005) emphasize that both awareness and understanding of security are prerequisites for the establishment of an effective security culture within an organization. Hunker and Probst (2011) highlight the importance of staff security awareness as they emphasize that it should be regarded as an essential factor for any comprehensive plan and the three levels of user awareness which should exist include the following:

- **Perception:** The user can detect treats in the environment.
- **Understanding:** The user can combine information from different sensors, understand them and the resulting knowledge allowing them decrease risks in the environment.
- **Prediction:** The user can predict future attacks and alter their own behavior to reduce or remove the risk completely.

The roles of awareness, training and education are also recognized by Whitman (2003) who highlights that one of the essential roles performed by an organization's security should be the implementation of a security education, training and awareness (SETA) program. Such programs seek to inform employees of the significance of security and its application in the day-to-day operation of an organization and by pairing this education program with a successful awareness program the desired result can be achieved, namely that employees will be able to recall the information provided, remembering organizational security and be conscious of this security as they deal with important information as they carry out their daily tasks in the workplace.

It is through the implementation or non-implementation of security countermeasures such as technology for monitoring purposes and SETA programs that organizations can prove their level of commitment to security. The awareness of employees along with the identification of the level of commitment shown by organizations will ultimately influence behavioral intent (Aurigemma and Panko, 2012). Siponen (2000) points out that information security awareness refers to a state where employees are aware and truly committed to the organization's security mission and although increased awareness should in theory decrease user related faults and improve the effectiveness of security techniques and procedures. This however is not always the case as in many instances despite creating security awareness amongst employees the true effectiveness of information security techniques and procedures is however lost as many end-users either misuse, misunderstand or simply do not employ the end-user security guidelines. Siponen et al. (2006) highlights that since the main threat to IS (information system) security is created by employees, alternative measures need to be adopted to deal with this issue as it is not enough for employees to be aware of IS security principles but there is a need for them to learn the IS procedures. The use of training sessions, presentations, newsletters, emails and screen savers in the promotion of IS security awareness in organizations is strongly supported as is the use of posters, brochures and newsletters in increasing the IS security messages within organizations. Kyobe (2005) emphasizes the importance of both education and awareness, highlighting that in order to achieve a better understanding of both security principles and application of technology policies in an organization it is fundamental to educate, train and generate security awareness.

Jones and Colwill, (2008) point out that security and awareness programs should be utilized to generate a better understanding of threats which exist both from insiders and outsiders emphasizing the methods employed to gain information or data access including malicious attacks and the direct consequences which can be suffered by an organization as a direct result of failure of controls. Such programs may also have an influence in creating a better level of trust between the employee and their employer as they offer the employee a better understanding and reason for the security policies and protocols which have been put in place as highlighted by Jones and Colwill (2008) and (Colwill, 2009). Employing such training updates also helps increase staff awareness of the organization's security cultural values and an improved staff awareness should realize a reduction in the probability of accidental breaches and a rise in the volume of malicious activity which is detected and reported (Jones and Colwill, 2008). A similar opinion is shared by Anderson (1999) who claims that in many cases the simple employment of measures such as security awareness, education, detection and reaction measures will often help with the insider problem which plagues many organizations.

TAILORING AWARENESS PROGRAMS

The recommendation for organizations whether large or small is the implementation of a security, education, training and awareness program to achieve an effective insider threat management. Although many ideas within cybersecurity awareness are common worldwide each organization should however tailor the training programs appropriately to specifically deal with the policies and meet the needs of their own organization (Cone et al. 2007). Each employee is an individual and when commencing an awareness program within an organization this should be taken into consideration as their different personalities will govern how they deal with compliance in relation to cybersecurity policies and when dealing with SETA programs a one size fits all approach should not be adopted as it is recommended that organizations instead provide a cybersecurity training and influential messages which are modified accordingly to meet the distinctive elements of each employee's personalities (Mc Bride et al. 2012).

Third parties are usually present at some point within processes as outsourcing is commonplace within many of today's organizations and as such, they may need education which is equivalent to that of the organization's full-time employees. It is important to offer solutions which not only develop but also preserve trust and relationships over time with the focus fixed on education and the creation of a better attention to security and support for employees and third parties. Delivering an effective education also presents a difficult hurdle which must be conquered, and ongoing education and awareness should support changes to meet the needs of employees especially in outsourced environments as providers are constantly increasing in numbers and many new employees are hired each month (Colwill, 2009). While the continuation of ongoing awareness programs is necessary especially in settings which have large turnovers of staff, Colwill (2009) expresses that finding out the success of programs in such areas can however prove difficult.

FUTURE RESEARCH DIRECTIONS

The insider threat is a problem which has the potential to cause significant damage, has been increasing in frequency in earlier years and it is a problem which is expected to grow in years to come. Many organizations are not fully aware of the seriousness of the problem that the insider threat poses, and it is essential that the future needs to ensure that all organizations are fully aware of the situation and apply company-wide policies to guarantee that all assets stay protected from the risks that they are constantly facing (Humphreys, 2008). With the increased number of organizations outsourcing tasks it is necessary that those carrying out outsourced tasks are receiving efficient education and awareness training like that of full-time insider employees as those in outsourced environments are regarded in many cases as insiders as they are offered the same privileges and access to information to enable them to carry out their duties.

Cone et al. (2007) highlights that an organization which receives effective security awareness training can greatly improve the confidence an organization has in their information although keeping the attention of a trainee for a satisfactory time span which is long enough to convey the required information is a challenge especially when the targeted audience view the topic as unexciting. New methods of delivering information in awareness training exercises are needed in the future and one such method which engages the target audience is the use of video games as they are involving and keep the attention of those for whom it is designed for (Cone et al. 2007).

Previous studies have concentrated on insider attacks which have already occurred and reactive issues such as what happens post insider attack and as Azaria et al. (2014) points out the detection of past attacks is not a serious problem and interest should be placed on what type of attack will be used in the future if the situation should arise where insider threats are prevented completely. Sarkar (2010) highlights that many professionals refer to the insider threat as a time bomb and the belief is that insider threats are more extensive than the figures which are recorded as many organizations do not divulge figures on the frequency of breaches and how often they occur as it could ultimately damage the reputation of the organization.

CONCLUSION

While awareness and education can both prepare the groundwork, the actual alteration in the behavior of individuals however, involves ceasing the practice of old habits and forming new ones through targeted training. To obtain the greatest benefit this needs to involve more than simply repeating security policies and veer towards building understanding along with development of knowledge of circumstances which cause security risks and the behaviors and reactions which are needed (Colwill, 2009). The insider threat is a well-established security issue and without adequate techniques, there is little that can be done to counteract the problem of the insider threat (Chinchani et al. 2005) and Hunker and Probst (2011) point out that the insider is already present within the system in some shape or form. The threat from insiders physically exists and is increasing in size and according to Miller and Maxim (2015) it is the duty of organizations to come to the reality that the insider threat could strike at any time and they should adopt a more aggressive standpoint in fighting the insider threat and avoid ‘the run for cover’ attitude.

The issue of the insider threat is an exclusive dilemma which can never be completely eradicated (Miller and Maxim, 2015; Sarkar, 2010; Hunker and Probst, 2011; Chinchani et al. 2005) and it can only be managed by employing mitigation strategies although due to the complexity of employees, contractors, suppliers, consultants outsourcing and the mobility of workforces this is an ongoing challenge for organizations (Sarkar, 2010). The worrying aspect is that although employees should be made aware of the difference between acceptable and unacceptable behavior in the workplace and from firms surveyed only 20% propose to increase awareness in the future and only 40% now offer constant awareness training to employees (Colwill, 2009).

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. doi:10.1080/0144929X.2012.708787

Anderson, R. H. (1999). *Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems (No. RAND-CF-151-OSD)*. Rand Corp.

Aurigemma, S., & Panko, R. (2012). January. A composite framework for behavioral compliance with information security policies. In *45th Hawaii International Conference on System Science (HICSS)* (pp. 3248-3257). IEEE.

Azaria, A., Richardson, A., Kraus, S., & Subrahmanian, V. S. (2014). Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data. *IEEE Transactions on Computational Social Systems*, *1*(2), 135–155. doi:10.1109/TCSS.2014.2377811

Baracaldo, N., & Joshi, J. (2012). A trust-and-risk aware RBAC framework: tackling insider threat. In *Proceedings of the 17th ACM symposium on Access Control Models and Technologies* (pp. 167-176). ACM. 10.1145/2295136.2295168

Bishop, M., & Gates, C. (2008). Defining the insider threat. In *Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead* (p. 15). ACM.

Blackwell, C. (2009). A security architecture to protect against the insider threat from damage, fraud and theft. In *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies* (p. 45). ACM. 10.1145/1558607.1558659

Cappelli, D., Moore, A., Trzeciak, R., & Shimeall, T. J. (2009). *Common sense guide to prevention and detection of insider threats 3rd edition–version 3.1*. Published by CERT, Software Engineering Institute, Carnegie Mellon University. Retrieved from http://www. cert. org

Chinchani, R., Iyer, A., Ngo, H. Q., & Upadhyaya, S. (2005). Towards a theory of insider threat assessment. In *Proceedings. International Conference on Dependable Systems and Networks, 2005 (DSN 2005)* (pp. 108-117). IEEE. 10.1109/DSN.2005.94

Choo, K. K. R. (2011). *Cyber threat landscape faced by financial and insurance industry. Trends & issues in crime and criminal justice No. 408*. Canberra: Australian Institute of Criminology.

Claycomb, W. R., & Nicoll, A. (2012). Insider threats to cloud computing: Directions for new research challenges. In *IEEE 36th Annual Computer Software and Applications Conference (COMPSAC)* (pp. 387-394). IEEE.

Cole, E. (2015). *Insider threats and the need for fast and directed response*. SANS Institute InfoSec Reading Room, Tech. Rep.

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? *Information Security Technical Report*, *14*(4), 186–196. doi:10.1016/j.istr.2010.04.004

Cone, B.D., Irvine, C.E., Thompson, M.F., & Nguyen, T.D. (2007). A video game for cyber security training and awareness. *Computers & Security, 26*(1), 63-72.

Eggenschwiler, J., Agrafiotis, I., & Nurse, J. R. (2016). Insider threat response and recovery strategies in financial services firms. *Computer Fraud & Security*, *2016*(11), 12–19. doi:10.1016/S1361-3723(16)30091-4

Flynn, L., Huth, C., Trzeciak, R., Buttles, P., & Nations, A. (2013). *Best Practices Against Insider Threats in All Nations. Technical Note CMU/SEI-2013-TN-023*. Software Engineering Institute.

Franqueira, V. N., van Cleeff, A., van Eck, P., & Wieringa, R. (2010). External insider threat: A real security challenge in enterprise value webs. In *International Conference on Availability, Reliability, and Security 2010 (ARES'10)* (pp. 446-453). IEEE. 10.1109/ARES.2010.40

Furnell, S., & Clarke, N. (2005). Organisational security culture: Embedding security awareness, education and training. *Proceedings of the 4th World Conference on Information Security Education*, 67-74.

Glasser, J., & Lindauer, B. (2013). Bridging the gap: A pragmatic approach to generating insider threat data. In IEEE Security and Privacy Workshops (SPW), 2013 (pp. 98-104). IEEE. doi:10.1109/SPW.2013.37

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In *Insider threats in cyber security* (pp. 85–113). Boston, MA: Springer. doi:10.1007/978-1-4419-7133-3_5

Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the insider cyber threat. *IEEE Security and Privacy*, *6*(1), 61–64. doi:10.1109/MSP.2008.8

Hayden, M. (1999). *The Insider Threat to U.S. Government Information Systems* (NSTISSAM-INFOSEC/1-99). National Security Agency.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4), 247–255. doi:10.1016/j.istr.2008.10.010

Hunker, J., & Probst, C. W. (2011). Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, *2*(1), 4–27.

Jones, A., & Colwill, C. (2008). Dealing with the malicious insider. *Australian Information Security Management Conference*, 52.

Kyobe, M. (2005). Addressing e-crime and computer security issues in homes and small organizations in South Africa. *European management and technology conference on the integration of management and technology*, 1-13.

Liu, D., Wang, X., & Camp, J. (2008). Game-theoretic modeling and analysis of insider threats. *International Journal of Critical Infrastructure Protection*, *1*, 75–80. doi:10.1016/j.ijcip.2008.08.001

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security*, *24*(5), 371–380. doi:10.1016/j.cose.2004.10.003

Martinez-Moyano, I. J., Rich, E., Conrad, S., Andersen, D. F., & Stewart, T. R. (2008). A behavioral theory of insider-threat risks: A system dynamics approach. *ACM Transactions on Modeling and Computer Simulation*, *18*(2), 7. doi:10.1145/1346325.1346328

McBride, M., Carter, L., & Warkentin, M. (2012). *Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies*. RTI International-Institute for Homeland Security Solutions.

McConnell, M. (2002). Information assurance in the twenty-first century. *Computer*, *35*(4), supl16-supl19.

McCormac, A., Parsons, K., & Butavicius, M. (2012). *Preventing and profiling malicious insider attacks (No. DSTO-TR-2697). Defence Science and Technology Organisation Edinburgh*. Command Control Communications And Intelligence Div.

Miller, R., & Maxim, M. (2015). *I Have to Trust Someone.... Don't I?* CA Technologies.

Molok, N. N. A., Ahmad, A., & Chang, S. (2011). Information leakage through online social networking: Opening the doorway for advanced persistence threats. *Journal of the Australian Institute of Professional Intelligence Officers*, *19*(2), 38.

Neumann, P. G. (2010). Combatting insider threats. In *Insider Threats in Cyber Security* (pp. 17–44). Boston, MA: Springer. doi:10.1007/978-1-4419-7133-3_2

Nguyen, N., Reiher, P., & Kuenning, G. H. (2003). Detecting insider threats by monitoring system call activity. In *Information Assurance Workshop*, 2003. *IEEE Systems, Man and Cybernetics Society* (pp. 45-52). IEEE. 10.1109/SMCSIA.2003.1232400

Nurse, J. R., Legg, P. A., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., ... Creese, S. (2014). A critical reflection on the threat from human insiders–its nature, industry perceptions, and detection approaches. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 270-281). Springer. 10.1007/978-3-319-07620-1_24

Park, J. S., & Ho, S. M. (2004). Composite role-based monitoring (CRBM) for countering insider threats. In *International Conference on Intelligence and Security Informatics* (pp. 201-213). Springer. 10.1007/978-3-540-25952-7_15

Probst, C. W., Hunker, J., Gollmann, D., & Bishop, M. (2010). Aspects of insider threats. In *Insider Threats in Cyber Security* (pp. 1–15). Boston, MA: Springer. doi:10.1007/978-1-4419-7133-3_1

Puleo, A. J. (2006). *Mitigating insider threat using human behavior influence models (No. AFIT/GCE/ENG/06-04)*. Air Force Inst Of Tech Wright-Patterson Afb Oh School of Engineering And Management.

Randazzo, M.R., Keeney, M., Kowalski, E., Cappelli, D.M., & Moore, A.P. (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector*. Academic Press.

Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report*, *15*(3), 112–133. doi:10.1016/j.istr.2010.11.002

Siponen, M., Pahnila, S., & Mahmood, A. M. (2006). A new model for understanding users' is security compliance. PACIS 2006 Proceedings, 48.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. doi:10.1108/09685220010371394

Stavrou, V., Kandias, M., Karoulas, G., & Gritzalis, D. (2014). Business Process Modeling for Insider threat monitoring and handling. In *International Conference on Trust, Privacy and Security in Digital Business* (pp. 119-131). Springer. 10.1007/978-3-319-09770-1_11

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, *24*(6), 472–484. doi:10.1016/j.cose.2005.05.002

Ula, M., & Fuadi, W. (2017). A Method for Evaluating Information Security Governance (ISG) Components in Banking Environment. *Journal of Physics: Conference Series*, *812*(1), 012031. doi:10.1088/1742-6596/812/1/012031

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*(2), 101–105. doi:10.1057/ejis.2009.12

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM*, *46*(8), 91–95. doi:10.1145/859670.859675

Yayla, A. A. (2011). Controlling insider threats with information security policies. *European Conference on Information Systems*, 242.

KEY TERMS AND DEFINITIONS

Compliance: The certification or confirmation that the person performing an action such as an employee does so in a manner which meets company rules and policies and the activity is carried out meeting standards and guidelines as per the conditions of a contract.

Cyber-Attacks: A cyber-attack refers to an assault against a computer system, network, or internet-enabled application or device. Hackers employ a wide range of devices to carry out such attacks. They include malware, ransomware and many other approaches.

Cybercrime: This refers to any illegal activity involving a computer, networked device or a network. Many cybercrimes take place purely for financial gain although some take place against computers or devices to impair them or disable them and others use computers to spread malware, illegal information, images, or other types of data.

Espionage: This is the act of acquiring private information without the authorization from the owner of the confidential information and it is often referred to as spying or obtaining secret information which can be political, military, or industrial in format.

Fraud: This refers to deception, wrongful or criminal misdoings which are solely intended to result in either financial or personal gain.

Malware: This is short for malicious software which is designed purposely with the focus of initiating damage on a computer, server, or computer network. Malware causes damage once it is implanted or introduced in some manner to the target computer in the form of executable code, active content or other software while the user is still unaware that their system has been compromised.

Mitigation: This is the action involved in reducing the force, severity, intensity or painfulness of something and as a result the seriousness or grief experienced from something unpleasant is therefore decreased.

Organizations: This refers to a group of people such as that found in an institution or association who collectively work together in an organized way to achieve a shared purpose or to successfully undertake and achieve collective goals.

Outsider: This is a person or individual who does belong to or who is not involved or included within a specific group of people or organization.

Sabotage: This is a deliberate action whose goal is to weaken an organization by causing disruption, obstruction or destruction. Those that engage in this process are referred to as saboteurs and they usually hide their identities due to the result of the penalties inflicted because of their actions.

Spam: Unwanted or inappropriate messages sent via the Internet normally to a large volume of Internet users usually for advertising purpose or to entice individuals to reveal personal information or spreading malware.