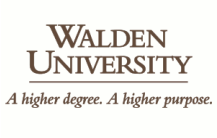

2018

Overcoming Data Breaches and Human Factors in Minimizing Threats to Cyber-Security Ecosystems

Manouan Pierre-Marius Ayereby
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Manouan Pierre-Marius Ayereby

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Anthony Lolas, Committee Chairperson,
Applied Management and Decision Sciences Faculty

Dr. Robert Levasseur, Committee Member,
Applied Management and Decision Sciences Faculty

Dr. Nikunja Swain, University Reviewer
Applied Management and Decision Sciences Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2018

Abstract

Overcoming Data Breaches and Human Factors in Minimizing Threats to Cyber-Security Ecosystems

by

Manouan Pierre-Marius Ayereby

MA, American Intercontinental University, 2003

BS, Georgia State University, 2000

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

November 2018

Abstract

This mixed-methods study focused on the internal human factors responsible for data breaches that could cause adverse impacts on organizations. Based on the Swiss cheese theory, the study was designed to examine preventative measures that managers could implement to minimize the potential data breaches resulting from internal employees' behaviors. The purpose of this study was to provide insight to managers about developing strategies that could prevent data breaches from cyber-threats by focusing on the specific internal human factors responsible for data breaches, the root causes, and the preventive measures that could minimize threats from internal employees. Data were collected from 10 managers and 12 employees from the business sector, and 5 government managers in Ivory Coast, Africa. The mixed methodology focused on the *why* and *who* using the phenomenological approach, consisting of a survey, face-to-face interviews using open-ended questions, and a questionnaire to extract the experiences and perceptions of the participants about preventing the adverse consequences from cyber-threats. The results indicated the importance of top managers to be committed to a coordinated, continuous effort throughout the organization to ensure cyber security awareness, training, and compliance of security policies and procedures, as well as implementing and upgrading software designed to detect and prevent data breaches both internally and externally. The findings of this study could contribute to social change by educating managers about preventing data breaches who in turn may implement information accessibility without retribution. Protecting confidential data is a major concern because one data breach could impact many people as well as jeopardize the viability of the entire organization.

Overcoming Data Breaches and Human Factors in Minimizing Threats to Cyber-Security Ecosystems

by

Manouan Pierre-Marius Ayereby

MA, American Intercontinental University, 2003

BS, Georgia State University, 2000

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

November 2018

Dedication

This doctoral endeavor is dedicated to my father, Mr. Manouan A., and mother, Mrs. Essomah A., for making me who I am today, and my son, Jean-Josue, and my daughters, Hannah-Marie and Essomah, for supporting me all the way. A special thanks to my adoptive mom, Pamela Patterson and my niece, Mariam Kahn, for their encouragements and special assistance throughout my academic career. My brother, Ngandu Leandre, who never gave up on me. Robin Smith, my best friend, who has been a constant source of knowledge and inspiration to me throughout this journey. No matter how difficult and distant the goal seemed to be, her confidence was my inspiration to press on. Thank you all for encouraging me at every opportunity to finish this major endeavor in my life.

Acknowledgments

I thank my LORD for sustaining me with His love, care, and strength to enable me to walk through this journey.

It is also with my deepest gratitude and warmest affection that I dedicate this dissertation to Dr. Anthony Lolas, for your never-ending enthusiastic encouragement and wisdom. I thank you for first being my chair and committee member during my proposal work, and later for encouraging me to the finish line while I worked on my last two chapters.

I am equally grateful to Dr. Nikunja Swain of the Walden Research Review Board for your expert guidance. Last, but not least, I extend my sincere gratitude to Dr. Robert Levasseur, my methods expert, for lending his time and subject matter expertise to my research.

I am forever grateful to all those at whatever organization and to everyone else I did not mention but contributed in some fashion to the successful completion of this dissertation.

Thank you,

Pierre-Marius

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Propagation of network communications has changed the nature of businesses, resulting in an unprecedented magnitude of threats and vulnerabilities to business information systems. Security risks from data breaches fall into the following four basic patterns, which were first identified by Auray and Kaminsky (2007): integration as an employee, opting to be independent, the path of fraud, and parallel remuneration under a masked identity. This categorization is still used today to understand then modes through which many internal data breaches occur. Many security hackers use these approaches to build progressively split identities as hackers and professionals.

Although there have been many theories about data breaches, many historical theories are still relevant in the context of increasing numbers of data breaches due to external and internal human factors. Pierce's test (1976) of Durkheim's (1951) social order theory is still relevant and a useful method to understand the role of human factors in systems attacks and data breaches. Durkheim theorized that social and economic changes contribute to the disturbance of existing goals and norms that push people into novel social settings. These individuals use essential means such as malicious malware to attain their intrinsic objectives, which could be economic, religious, political, retributive, or social. Similarly, the motivation for committing cyber-crimes has multiple facets such as external threats as well as internal threats from employees, both deliberate and accidental. These threats frequently become viable because of a lack of involvement by some top managers in the development of organizational plans and efforts designed to mitigate cyber-attacks. Thus, the results of this study could have positive social

implications by providing insights on how managers and organizational leaders can prevent data breaches and protect organizational as well as customer information.

Background of the Study

The proliferation of emerging information technology (IT) is a primary reason for economic and technological advancements across Africa. Advancement in IT has changed the nature of business activities and has permitted businesses, governments, and consumers to buy, sell, or request services via the Internet. Additionally, the financial industry, governments, customers, and many other organizations and individuals access their information or make transactions over the Internet. Businesses and governments are communicating more than ever with their customers virtually and globally through network communications. This global network of electronic communication systems has increased business transactions rapidly and has transformed the nature of data exchange worldwide.

This expansion of information processes also has increased risks significantly. Threats have expanded from mass malware and industrialized attacks that target individuals and their access privileges to long-term exploits of the more adept adversary, whose tactics are difficult to discern from a legitimate user's activity (Forrester, 2011). The potential for cyber-crimes has increased in sophistication by outpacing defenses.

With the Internet of things (IoT), a large number of people are using smart devices, which seem to be intelligent enough to be dangerous. As more mobile devices become IP-enabled, they are instrumental in BotNets because a cyber-hacker may infect the mobile devices with malicious software and control them without the owners'

knowledge through spam, inappropriate messages, or other platforms used for distributed attacks. Tracing the sources of the distributed attacks are difficult while overwhelming a target is easier. In past years, activists and blackmailers have used distributed denial of service attacks, while many cybercriminals have used distributed reflection denial of service attacks. The latter focuses on a handful of protocols, including the simple network management protocol (SNMP), which is an application layer (Layer 7) protocol commonly used to manage devices with IP addresses.

Unlike other distributed denial of service and distributed reflection denial of service attacks, the SNMP attacks permit malicious actors to hijack unsecured network devices such as routers, printers, cameras, and sensors and use them as bots, which are web robot scripts to attack third parties. The SNMP attacks are a major concern because a number of devices could be compromised easily, including remote devices such as printers and sensors which, generally, are not secured, leaving them open to exploitation. Devices such as sensors used in motion detectors, control valves at power plants, door locks for bank vaults, and traffic signals can be compromised easily as well. Search engines such as Shodan could reveal such connected devices, many of which are entirely without security.

The stateless protocol such as user datagram protocol used by SNMP is subject to IP spoofing, which is a forgery or fake IP address. A reflection denial of service (DoS) attack using SNMP is an amplification attack because an SNMP request generates a response that is typically at least three times larger, which could allow an attacker to port-scan a range of IP addresses to identify exploitable SNMP hosts. An attacker sends an

SNMP request to these hosts using the spoofed IP address of the target server, while replies of hosts saturate the bandwidth of the target, making it unavailable. The raw response size of the traffic is amplified significantly, enabling the SNMP reflection attack vector to become a dominant force.

The sources of data breaches continue to grow. McAfee (2014), which is a provider of endpoint security software, reported that there were nearly 8 million new pieces of malware just in the third quarter of 2014. Additionally, malicious and high-risk mobile apps are on the rise. Trend Micro (2014), for instance, identified 195,000 malicious Android apps in September 2014. Preventing malware attacks on systems is still a challenge with emerging mobile devices and concepts, such as bring your own device (BYOD), which is a growing threat with an increase in smartphones and tablets that are available in the market. Even though smartphone sales declined by 1.3% in 2014, mobile phone sales reached 2.5 billion units in the world. This proliferation creates significant challenges for cyber-security personnel, whereas rendered network communications are even more vulnerable to cyber-attacks.

Most IT managers and top organizational leaders continue to view cyber-terrorism and attacks by hackers as top security concerns together with malware infections and application vulnerabilities. Moreover, the list of significant security concerns is growing in length and diversity. As a result, the exposure footprint is expanding due to the BYOD movement in the work environment. From a security perspective, implications of BYOD involve more untrusted devices connecting into corporate networks and enterprise public-facing websites; consequently, as more mobile devices become accessible, employees

may participate in malware propagation and BotNet-based attacks, leading to significant data breaches.

Many organizations may not be able to change either the BYOD phenomena or how they conduct their operations. Networks, whether they are private or public, are circulatory systems of the business. Malicious and unwanted traffic clogs these electronic arteries and increases risks that may impact maintaining stable operations, reaching profitability objectives, managing brand reputation, complying with regulations, and safeguarding sensitive data.

Many organizations rely on an assortment of gateways and filters to purify their network traffic to diminish these risks. Although logical, this approach is dependent on the effective and timely identification of threatening traffic, prevention of intrusion, and updating security policies and malware and intrusion signatures with equal accuracy and speed. However, this critical task is difficult due to the involvement of many factors, such as steady escalation in traffic volume and origins, evolving network and computing infrastructures, traffic patterns, and hacker sophistication in evading detection and gaining access (Adebayo, 2012). In many organizations, employees may exploit the company's trust for personal gain or malicious intent by exposing the company's sensitive information and data to a third party. These resilient threats increase significantly when considering the unprecedented volume and magnitude of external threats to internal vulnerabilities that lead to data breaches causing major disaster recovery efforts in government and business information systems in the Ivory Coast.

Data breaches have their roots in politics as well as in the lure of easy money, notoriety, and personal or malicious motivations. Therefore, understanding the impacts of human behavior on the creation of dysfunctional information processing could help to secure information systems to prevent data breaches and compromised information. Increasing data breaches and human errors impede information availability, confidentiality, and integrity, which are significant concerns to many organizations and citizens because data breaches are getting worse and information is compromised more frequently. As a result, data breaches from human errors could weaken an organization's ability to exercise a greater level of dynamic control over its valuable information leading to a loss of public trust. Decision makers of most organizations should understand the impact of data breaches and their role as leaders in preventing cyber-threats that impact the organization.

Problem Statement

The general problem I investigated in this study was the internal human factors contributing to data breaches that adversely affect many organizations. The specific problem was how managers could protect the information system of an organization against internal human factors that contribute to data breaches, and could minimize threats to cyber-security ecosystems in Ivory Coast, Africa (see Dutta & McCrohan, 2011). Many researchers and security practitioners agreed that successful cyber-attacks are due to data breach triangulation hackers use to gain access to information systems. Many financial institutions and other organizations continue to suffer the consequences of data breaches through human factors, social environments, or system flaws. A report

by the Identity Theft Resource Center (ITRC, 2014) indicated that in January 2014, Target, which is a popular discount retailer, stated that hackers stole more than 70 million credit and debit card data between November 27 and December 15, 2013. In October 2013, hackers accessed 5.6 million social security numbers and other personal data since 1998 from servers at the South Carolina Department of Revenue (SCDOR, 2013). Symantec (2013) underlined that the majority (88%) of reported data breaches were due to attacks by outsiders. A report by the International Organization of Security Commissions (IOSCO, 2013) indicated that 53% of stock exchanges were under cyber-attacks during 2012. McAfee (2014), an endpoint security software provider, reported that there were nearly 8 million new malwares just in the third quarter of 2014. The National Institute of Standards and Technology (NIST, 2013) took a more holistic approach to information security and risk management due to emerging cyber-threats and emphasized that maintaining cyber-security hygiene is critical to the availability of information residing in systems.

Purpose of the Study

Cyber-threats come from both external and internal sources. However, the purpose of this study was to provide executive managers with a guideline to prevent data breaches from cyber-threats by focusing on internal sources because many organizations in Ivory Coast and other African countries have less effective information systems security controls, resulting in pervasive vulnerabilities, undetected breaches, and unknown amounts of damages and thefts. These deficiencies place Ivory Coast information systems assets at risk for inadvertent or deliberate misuse and financial

information at risk for unauthorized exposure. From my perspective, it seemed that the Ivory Coast government has delegated many central IT responsibilities to the French government and private IT contractors in France. In addition, IT contractors appeared to not understand Ivorian human behavioral aspects, while executive managers did not seem to know anything about overseas contractors. Furthermore, it appeared that the government did not establish any clear guidelines about which IT operations should be kept in-house. Similarly, many African governments appear to lack an overall plan to function effectively because of their deep divisions and changing focus due to political instability, causing dysfunctions in the decisions of managers. Consequently, data breaches are often unnoticed due to the unavailability of information and the lack of a framework to protect critical infrastructures from cyber-threats. Ivory Coast has seemed to face increasing cyber-security challenges with the proliferation of emerging technologies and network communication devices in the knowledge-based global economy. I examined the significant cyber-security challenges that Ivory Coast businesses face and what role top executives and managers could play in overcoming human factors that contribute to internal data breaches.

Research Questions

I developed the following three research questions for this study:

RQ1: What are the internal human factors that contribute to data breaches and compromised information in the Ivory Coast emerging business environments?

RQ2: What are the root causes of the internal human factors that contribute to data breaches and compromised information in the Ivory Coast businesses?

RQ3: What preventative measures could managers use to minimize the threat from human factors, which are related to an internal employee, that contribute to data breaches or compromised information?

These research questions were linked to a survey and open-ended interview questions that provided the basis for the collection of data discussed in Chapter 4. Participants were Ivorian government executives, financial executives, IT managers, and information systems technicians, who had at least 3 years of experience in their positions. I used the collected data to determine the significance of dysfunctional managerial processes and the impacts on managerial decisions.

Theoretical Foundation

The Swiss cheese model of human error was the primary theory used in this study. The theory holds that flaws exist in each layer and could lead to an accident if they are aligned despite many layers of defense between hazards and accidents. This has historically been a problem for managers. During the last 25 years, many researchers have proposed similar taxonomies. For example, Swain and Guttman (1983) argued that organizational conditions contribute to human errors. Miller and Swain (1987) found that inadequate workspace and work layout, poor environmental conditions, derisory human engineering design, insufficient training and job aids, and poor supervision were the causes of human errors. Other researchers such as Perrow (1984), Pauchant and Mitroff (1992), Roberts (1990), and Sagan (1994) studied the impacts of organizational culture on the incidence of human errors. However, the Swiss cheese model is useful because it forces investigators to address latent failures within a causal sequence of events.

Although this model is a simple theoretical framework, it is not a prescriptive investigation technique and only has a few details on how to apply it in a real-world setting. Executive-level and IT managers should find out what holes there are, how big they are, and how they correlate so that they can be detected and corrected before an accident occurs (Wiegmann & Shappell, 1997). Although these references are over 20 years old, there is an urgent need to mitigate human errors in the context of growing data breaches, which cause increasing economic and operational damages to organizations today.

Many data breaches happen due to human negligence within organizations. A Computer Security Institute (2013) report indicated that over 46% of 351 survey participants stated that human errors and factors resulted in the most cost and damage to the organization. Monitoring employees and security awareness training remain lesser concerns for many organizations despite increasing global cyber-attacks. A cost-benefit analysis is often used to justify resource allocations, though obtaining accurate estimates for costs versus benefits is difficult. Using inaccurate data could undermine the quality of resource allocation decisions in combating data breaches. In 2013, the Computer Security Institute (CSI), in conjunction with the Federal Bureau of Investigation (FBI), conducted an annual computer e-crime and security survey and found that the motivation for stealing intellectual property and proprietary information is for financial gain (CSI, 2013). Studies by the United States Computer Emergency Readiness Team (US-CERT), Australia, Canada, News Zealand, and the United Kingdom also showed that incidents

involving human errors and factors remained a big concern for many organizations (US-CERT, 2018).

The outcomes of these and other studies indicated that the problems due to human errors and factors are real and pervasive. Some key findings reported by the Secret Service and Carnegie Mellon (2014) on human errors and recurring factors in organizations indicated that data breaches primarily happened due to the errors of insiders. Current employees caused the majority (56%) of incidents, followed by customers (32%). Similarly, they found that executives neither documented and consistently enforced policies nor had periodic security awareness training for all employees (Cummings, Lewellen, McLntire, Moore, & Trzeciak, 2014). Unreported incidents are a key challenge in deriving these statistics. In 2013, the study by the CSI and FBI indicated that only 42%, which was up from 25% from previous year, reported incidents to law enforcement (CSI, 2013). Similarly, the 2013 e-crime survey results indicated that two-thirds of cyber-crimes committed due to human errors were dealt with internally and not reported to law enforcement (CSO,2013). Reasons for not reporting incidents included loss of reputation, negative publicity, increased liability, inability to identify the perpetrator, and the acceptance that damage was not sufficient enough to report due to lack of skilled professionals (CSO, 2013). Unfortunately, the full impact of human errors will remain unknown unless top managers document and report to information assurance researchers so that they can analyze available cases related to human errors for possible solutions. Preventing human errors threat is critical and complex because employees are the most common points of entry in security breaches.

Employees have authorized accesses to the systems and information of organizations, and they have the inside knowledge of intuitive information operation systems of organizations. Security breaches due to human errors and their impacts come in many forms; in most cases, those errors are related to individuals' roles and responsibilities. Although a threat mitigation effort to overcome human errors and factors is complex and challenging, a risk management approach can be useful to guide the process. The probability of intervention by managers to prevent attacks or limit the damage done by attacks is slim because many managers and supervisors have less time and are likely to overlook many warning signs.

Human errors have the potential to cause harm from accidents. A cyber-crime survey showed that cyber-crime threats are on the rise and current attempts to counter them frequently continue to be unsuccessful. Many organizations could not defend themselves effectively against human errors and factors, and end users have limited or no technical expertise (PWC & CSO, 2013). Propagation of network connections and mobile devices have enabled employees to conduct and easily conceal their activities. Additionally, many organizations could not rival the persistence, tactical skills, and technological prowess of their potential cyber-adversaries.

Generally, people do not have malicious intent when they commit an error. Most human errors happen accidentally because of a lack of due diligence practices, which are designed to prevent data breaches. However, there are malicious intents involving employees who use their trusted access privileges to intentionally impair the organization when there are no roles and responsibilities for checks and balance. This deliberate harm

might be sabotage, destruction, theft, embezzlement, espionage, and so forth (Adebayo, 2012). Consequently, it is necessary for an organization to determine the human factors that might expose it to risks before data breaches occur. Correlation is a mathematical tool used frequently for analyzing a series of values, such as a time series, and for measuring the degree to which two or more quantities are linearly associated (Weisstein, 2008).

Autocorrelation is the correlation of a data set with itself. Autocorrelation analyzes serial dependency of data, that is, knowing the total time to resolve events today and what could be inferred about the time to resolve events tomorrow. Correlation time is used for analyzing security infrastructure because understanding relationships between incidents help analysts uncover hidden patterns in human factors. Trends are often more valuable than individual snapshots because baselines could be established to determine if operations are improving or declining across a wide range of security infrastructures. Because human behavior is at the core of information asset risks and consequently plays an essential role in the protection of such assets, the theoretical framework for this study was the Emmanuel and Daniele's (2011) theory of culturally-aware IT. This theory addresses the theoretical and technological aspects of IT about humans and their culture.

This theoretical approach provided the details on cultural awareness and insider human behavior that affected information systems and technology in general. The approach offered guidance to understand the internal human factors that contributed to internal data breaches and to prevent these data breaches. Additionally, it provided insights into the social environmental challenges and methods to overcome the human

factors that contribute to data breaches in order to minimize the adverse consequences of cyber-attacks.

Conceptual Framework

Information and data of many organizations are vulnerable to cyber-attacks across the globe due to the proliferation of network communications. Cyber-criminals use several approaches to gain unauthorized accesses to data of the affected organizations. I explored two basic approaches to generating an attack graph, namely the state-based approach proposed by Ammann, Wijesekera, and Kaushik (2002) and the host-based approach proposed by Ammann, Pamula, Ritchey, and Street (2005). However, several previous approaches have utilized both forward and backward chaining algorithms to develop an attack graph and to understand the objective of an attacker. Thus, to attain reachability of an attack graph, it is critical to determine all ports and hosts in a network that are reachable via TCP or UDP connections from all interfaces on all hosts in a network. Therefore, the state-based approach gives information at a more granular level, whereas the representation quickly becomes large and complicated even for a modest size network (Sheyner, Haines, Jha, & Wing, 2002). In a host-based attack graph, each node could be identified as a network entity and the edges may be privileges obtained after applying exploits among them. The host-based approach gives compact representations, which are used in visual representation and handled scalability at the cost of abstracting several low-level details related to exploiting correlation, vulnerability, and attacker privileges. For example, obtaining user-level privilege on a host, say Host AB, and escalation of that privilege to the superuser level, could be treated as two distinct states in

the state-based approach. Additionally, the attack graph shows weaknesses in the system for administrators and assists them to decide appropriate security measures to deploy. This host-based approach enables the combination of all individual privileges and retains the highest-level privilege as a graph edge. Availability of low-level details in a state-based attack graph depends on the level of risks that executives are willing to accept or reject if there was a system threat.

In the approach proposed in this study, I used the state-based forward chaining algorithm to generate an attack graph with the necessary exploits. The necessary exploits were the set of exploits, a subset of which could be used by an attacker, to obtain the goal because the forward reachable attack graph might contain redundancies. The runtime complexity of such a forward chaining algorithm could be represented by the polynomial $O(|A|^2 . E)$, where A and E represent the number of network state of beings and exploits, respectively, and where each vertex in the generated attack graph edges is used to represent the causal relationship among network states and exploits (Ammann et al., 2002). Additionally, a system administrator could discover how an actual attack might occur within a system by using a backward search in the state-based forward chaining algorithm.

Identifying and predicting threats require an understanding of the behaviors of cyber-attackers. An attack graph could help to organizations identify the most likely network attacks. To achieve this objective, securing the network using generated attack paths and applying the Boolean minimization are the best logical options (Sheyner et al., 2002). The proposed in-depth risk management methodology could be classified as: (a)

detection and removal of cycles onward accessible attack graph, (b) identifying all attack paths frontward available directed acyclic attack graph, (c) identifying the minimum possible network securing options for risk mitigation, and (d) identifying the likelihood attack path based on attack surface measure.

An attacker might use the stack and queues concept to exploit a vulnerability in network nodes of an organization to access data. However, the system administrator could use the state-based forward reachable attack graph if an attacker used a stack and queues concept of business data. The state-based forward reachable attack graph represents each pre and post-clause of the highest point and their contributory relationship, allowing the system administrator to see the rims loop algorithm, where the attack took place (Ammann et al., 2002). Consequently, a system administrator could have better visibility of the cause of the attack. Having a better visibility of business network communications is essential for IT managers to prevent cyber-attacks. Since 2000, several practitioners recommended that testing network communication was and still is critical to secure the internal network connectivity from remote attack (Jajodia, Singhal, Islam, Long, & Atluri, 2008). This approach demonstrates the methods used by cyber-criminals to launch an attack on the network by exploiting data vulnerability of an organization through a remote buffer overflow.

A successful execution of this attack immediately permits the attacker to gain the control of a network to steal business information remotely. The interloper used a solitary computer to send known exploit to access information that resided in the network. Thus, it is essential to have a non-redundant authentication in attack replica

approach to minimize data breaches (Ammann et al., 2002). In conjunction to these approaches, the British Standard BS 7799, the International Standards Organization 17799 (ISO 17799), the Generally Accepted Information Security Principles, the System Security Engineering Capability Maturity Model, and the Standard of Good Practice for Information Security delineated the best security practices for stakeholders involved in protecting information assets. Moreover, the Federal Information Security Management Act of 2002 (FISMA) and the NIST recommended mandatory security controls to mitigate data breaches or systems attacks.

Nature of the Study

Threats to business network communications have increased as interdependency of computer systems continue to increase rapidly. As a result, it is a challenge for many banks and organizations to provide efficient, secure, and documented access to their information systems at all levels from internal employees and contractors to external partners and customers. Most organizations do not have the technology to allow their system administrators to act in real-time and enforce access to computer systems across highly complex and ever-expanding business network environments. Many organizations are unable to create, modify, and delete user accounts, user profiles, and corporate policies, and cannot correlate data from human resources, financial, travel, procurement, and email systems.

Therefore, I used a mixed-method approach in this study because it is suitable for understanding internal human behavioral aspects that play vital roles in data breaches, compromised information, and confidentiality in many organizations. My focus on how

the processing of information could positively improve decisions and minimize data breaches was consistent with Emmanuel and Daniele's (2011) theory of culturally-aware IT. This theory helped me explain how human factors contribute to both external and internal data breaches and compromise information systems of many organizations. Thus, the objective of this research study was to determine how IT managers and top managers could control internal and external human factors to prevent data breaches. This research should help to pinpoint how collaborative processes are crucial to minimize data breaches and compromised information, where dysfunctional managerial functions are a danger to cyber-security ecosystems.

Definitions

Below I have provided operational definitions of keywords I used throughout the study.

European Union Directive 95/46/EC on the Protection of Personal Data: This is a legislative act of the European Union (EU) that requires member countries to meet certain requirements for data privacy protection without specifying the process. The impact has spread to the U.S. due to strict requirements governing the transfer of data to non-EU nations (EU Directive, 1995).

Federal Information Security Management Act of 2002 (FISMA): As defined by NIST, it is a law governing information security practices within U.S. Federal government agencies that requires annual audits of information security within each agency (FISMA, 2002).

Human error: Human error is defined at least in three ways: phenomenological, scheme lumps, and human biases or tendencies (Reason, 1990).

Human factor: The human factor is the relationship between technology and humans. It marks information related to human behavior, abilities, and limitations, and is taken into consideration during the design of tools, machines, systems, tasks, jobs, and environments for effective, productive, safe, and reliable human use.

In addition, I have developed the following definitions based on personal IT experience.

Computer security threat: The probable danger resulting from the exploitation of a vulnerability.

Cyber-security ecosystem: The interaction of public-private organisms and law enforcement to protect the critical infrastructures, national security, and economic interests of a country.

Data breach: A security incident in which sensitive, protected, or confidential information is released intentionally or unintentionally to an untrusted environment.

Data mart: A data repository designed to serve a community of knowledge workers based on bona fide need.

Disclosure (Disc): When information is revealed to an unauthorized individual.

Fraud: The deliberate misuse or misapplication of organizational resources or assets for personal gain or any theft of information by an insider.

Insider: A current or former employee, or temporary employee or contractor including business partners or customer, authorized end-user of IT resources of the

organization. Three common insider threats are fraud, theft of intellectual property, and sabotage of IT infrastructure.

Intellectual property theft: The use of IT by an insider to steal or expose valuable information assets of an organization.

Loss: When an asset is found in an unintended location and not where it was supposed to be, or when an asset cannot be located.

Risk: The association of threat, vulnerability, and impact.

Sabotage of IT infrastructure: The use of IT by an insider to harm IT resources of an organization.

Security vulnerability: An unintended flaw in software code or a system that can lead to a potential exploitation in the form of unauthorized access or malicious behavior (i.e., viruses, worms, Trojan horses, and other forms of malware).

Theft: When an asset is thought or known to have been taken without the permission of the responsible person.

Assumptions

The primary assumption of this study was that employees have an impact on assets, policy, and process of an organization and how they may affect data and other assets technology. Because employees are the weakest link in an organization in terms of data breaches, managers should have a method to overcome internal human factors effectively to minimize cyber-threats. Another assumption of this study was that the intended purposely selected sample of participants from five different organizations, consisting of Ivorian government officials, financial executives, chief information

officers, IT managers, and information systems technicians, was sufficient in responding to the survey and the interview questions in contributing to answering the research questions.

Scope

In this study, I addressed how people were an essential part of overall security and how they affected an organization's information assets. I focused only on overcoming data breaches, resulting from internal employees in information systems of an organization. Furthermore, I did not address in this study the technical design of information systems. There were 27 participants in this study purposely selected from five different organizations, consisting of five Ivorian government officials, four financial executives, five chief information officers, six IT managers, and seven information systems technicians, who had at least three years of experience in their position.

The focus of this study was to address the significance of dysfunctional managerial processes and their impacts on decisions to overcome data breaches and human factors related to information systems. Each participant received the survey questionnaire, which had an average completion time of fewer than fifteen minutes each, and the interview took approximatively thirty minutes. Moreover, the participants received an opportunity to review a compilation of the questionnaire responses, survey, and interview notes to ensure that the transcription was accurate, and their anonymity is protected. The entire process took less than 60 minutes to complete.

Limitations

There were several limitations to this study. First, the continued involvement of all participants was critical to the success of this study. Though the participants were volunteers without any compensation, they participated until the completion of this study. Second, there was the possibility that some participants provided diverse answers to survey, questionnaire and interview questions because of their cultural and ethnic differences. To minimize such risk, the participants answered the same set of questions. Although the participants came from five different organizations, they had the opportunity to ask any questions about the study. Lastly, five organizations and their participants were not perfect representations of decision-makers and end users in their organizations.

Significance of the Study

This project is significant because a large number of people have had their information compromised almost daily across the globe, and it seems to be getting worse. Preventing data breaches in organizations could prevent sensitive information about citizens from being exposed. Data breaches have adverse consequences for both corporations and consumers. Organizations, in particular, could face severe repercussions to their businesses, resulting in financial loss and reputational damages. Major data breaches often attract extensive media coverages, and, in some cases, a class action lawsuit filed by the affected customers against the company. In 2018, Facebook reported that data from 50 million users have been compromised, and the lawyers are lining up to file class action cases against the company.

Attackers tend to form a wicked community of learners, taking notes and sharing tips via the Internet. For example, typical cyber-thieves target local credit unions or regional banks. Some scholars found that the use of attack trees has been successful generally in identifying threats and risks to systems (Edge, Raines, Grimaila, & Baldwin, 2007). Protection trees are used, in conjunction with attack trees, to evaluate trade-offs between risk mitigation processes and to calculate the probability of each attack scenario affecting victims, which allowed the defender to identify attacks that exceed their risk tolerance. These countermeasures could help to model and determine the behavior of the adversaries. Also, attack trees captured and documented factors of the risk analysis.

Attack trees analysis approaches are valuable tools to demonstrate due diligence in the event of data breaches (Ingoldsby, 2009). Other researchers suggested using the textual clustering and data mining theory, which used probabilistic latent semantic indexing to generate links among documents, topics of interest, and people. From these links, an interest profile for an individual could be generated (Trillo, Po, Ilarri, Bergamaschi, & Mena, 2011). Therefore, the core of this research was to contribute to information security literature, in which only limited information is available about data breaches and human factors in the Ivory Coast. Although the focus of attack and protection trees was generally on the determination of overall system risk, the methodology was applicable equally to human factors threat domain. Attack trees formally represented all attack vectors and helped to determine which events might occur for an attack to be successful. It was important to begin determining risk level at each node to calculate metrics, such as the impact to a system if an action is accomplished

(Edge et al., 2007). Determining risk level of each node within the network of an organization was one possibility to pinpoint the likelihood of risk in the event of an attack.

Security practitioners are worried primarily about a DoS attack as a distraction for cyber-theft to use in combination with malware like SpyEye, Zeus, and Citadel. Criminals were hitting businesses that used small to mid-sized banks by distracting their victims for hours in a DoS attack on a bank. When an organization or individual could not confirm wire transfers because the bank network is down, the chances of being defrauded increase significantly. The Verizon 2009 data breaches investigation report highlighted that 93% of over 285 million records compromised in 2008 were from financial services firms.

Attackers continue to pursue soft targets internationally and create increased concern in emerging economies, especially concerning consumer data. Data thieves showed no partiality between larger enterprises and smaller establishments because they base their attacks on the perceived value of data and convenience (Verizon, 2009). A report by the Center for Strategic and International Studies (CSIS) (2014) showed that the cost of cyber-crimes increased from $375 billion in 2011 to $575 billion in 2013. Therefore, preventing data breaches and human errors and factors is critical, especially in the Ivory Coast, which appears to have dysfunctional managerial processes of information. Because of the limited research on this topic specific to Ivory Coast, this research could fill this gap by analyzing the significance of the problem of apparent data breaches and human factors that affected decision-making process to safeguard the information of

citizens. The results of this research could enhance Ivory Coast cyber- ecosystems by preventing data breaches and overcoming internal human errors and factors to minimize cyber-threats.

Significance to Practice

A study by Ponemon Institute, LLC (2014) on data breaches confirmed that a strong security posture helped organizations to reduce the cost of a data breach by $14 per record and lead to significant reduction in losses. Lost or stolen devices, third-party involvement in incidents, and notification and engagement of consultants increased the per capita cost of data breaches. Additionally, data breaches involving the lost or stolen devices could also lead to losses, for instance, cost per record could surge by $161.10 if a data breach involving lost or stolen devices (Ponemon Institute LLC, 2014). Verizon (2014) security experts also recommended the following controls to mitigate data breaches:

- do not use single-factor password authentication for anything that faces the Internet;
- set up automatic patches for any content management system such as Drupal and WordPress;
- fix vulnerabilities right away before hackers find them;
- enforce lockout policies; and
- monitor outbound connections.

Therefore, these advance practices demonstrate the criticality of top management involvement when dealing with employees' human errors and factors related to the system of organizations, applications, and data.

Significance to Theory

Data breach mitigations could be expressed as mathematical objects to model, analyze, construct, and determine the likelihood of preventing a data breach. The time that a problem lingers within the system or organization is an indication of the effectiveness of data breach prevention. The correlation time provides information about the average amount of time needed to recover from an incident. This measure could be expressed as the relationship between amounts of overlap in security events after removing fluctuations for weekly and daily trends, as well as for any periodic trends that might become apparent over more extended periods. Correlation time is relative to the current baseline of organizations, or to last month performance versus this month, or as compared to the target correlation time an organization established to minimize threats.

The autocorrelation function provides information related to future performance of security infrastructure. A positive correlation together with above-mean resolve time for today could indicate a high-security capability and business operation for tomorrow. The number of security events could decline and allow security infrastructure aptitude to leverage additional events and to respond to the effects. The inability of security operation systems to react to human behaviors could cause an individual security workload. Autocorrelation helps security infrastructures to have a better oversight of data settings and enables an analysis of data dependency and the total time to resolve

incidents. Additionally, correlation helps to uncover hidden patterns in data breaches and provides valuable information on system security. Security trend baselines are designed to evaluate whether security operations are improving or declining within an organization.

An organization security infrastructure could be expressed as mathematical objects to analyze and construct a secure e-transaction environment. The strength of e-transaction security of organizations depends on the effectiveness of their security infrastructure and the length of time taken bring a system online after a security incident. Correlation time is relative to the current baseline, or to last month performance versus an actual month or compared to the target correlation time of an organization.

An organization with a security infrastructure built with appropriate functionality could continue to operate normally in the event of a data breach. However, a large correlation time during a severe event or many simultaneous minor events could indicate a severe impact on business operations and security functionality. The correlation time could be a security assurance measure and a business risk index for extreme or multiple events.

Assessing security assurance is a recent discipline that is rapidly gaining momentum because government agencies and organizations realized limitations in their ability to measure the effectiveness of their security infrastructure. A central tenet of business management is that it could not be managed effectively if it could not be measured. The field approaches the security similar to other well-established disciplines, as a process, whose efficiencies could and might be measured with essential indicators.

However, the methodologies are not based on scientific and mathematical rigor that sustained other disciplines (Jaquith, 2007). Measurement of security assurance requires the identification and quantification of metrics. Quantification is driven by the need for probable security and accountability.

Assessing security assurance is a rapidly developing field, although still lacking the standards and broad consensus (Applied Computer Security Associates, 2013). The security assurance field has a strong demand for skilled information security professionals since 2007 due to the Internet global capability and availability features (Theoharidou & Gritazalis, 2007). Such demand is relevant still in many organizations, especially in Africa. Considerable controversies still exist regarding terms such as metrics, measure, score, rating, rank, or assessment results (Applied Computer Security Associates, 2013). Utilization of a baseline by the metrics to compare security status to determine improvement is the critical distinction between metrics and measurement.

Significance to Social Change

As interdependency of computer systems continued to increase rapidly, threats to business network communications were widened. As a result, banks and other organizations experienced challenges to provide efficient, secure, and documented access to their information systems at all levels, for internal employees and contractors as well as external partners and customers. Many organizations did not provide or process technology to allow their system administrators to act in real-time and enforce access to computer systems across highly complex and ever-expanding business network environment. Many organizations were unable to perform the creation, modification, and

deletion of user accounts, user profiles, and corporate policies as well as the correlation of data from human resources, financial, travel, procurement, and among others, email systems.

Therefore, this study could have a social change impact because it underlined how to implement accessibility of information without retribution. Protecting confidential data is a concern for every level of society. Moreover, this study provided insight on how to prevent external intrusions and internal human factors, which facilitated decision-makers to make better decisions and improve cyber-security ecosystems in Ivory Coast.

Summary and Transition

The nature of businesses is changing with more global network interconnection capabilities and availabilities. Attackers are incessantly reviewing their processes and techniques to ensure that they gain access to systems, information, and data of organizations. Despite multiple challenges in cyber-landscape, top managers of many organizations generally do not take proper measures to prevent data breaches, especially due to internal human errors and factors.

However, some companies did not even realize they had been compromised. They were unable to estimate the cost of intellectual property that they had lost to a competitor, a thief, or another nation-state. The tasks to protect information systems and data are not getting any easier because information in the world grows recurrently, and some companies are collecting and selling consumers information and data to other organization. Cyber-criminals are adapting to current protection strategies of many organizations and inventing new ways to access valuable data. Lack of security

awareness in many organizations leads to failures to implement even fundamental security practices that have been recommended by the NIST of the U.S. Commerce Department. Lack of awareness about the significance and scale of threats is a serious and ongoing problem to manage the state of information security. Consequently, many information security scholars and IT practitioners proposed methods to protect information assets and data of an organization adequately, which is the emphasis of Chapter 2.

Chapter 2: Literature Review

Preventing data breaches and internal human factor errors is a primary concern of IT managers and requires responsibility from everyone with access to IT resources. The number of successful data breaches is on the rise because uniformity of security across the industries is impossible; therefore, breaches are more likely in organizations with limited IT investment (Scott, 2010). To help prevent data breaches, the researchers at the Information Technology Laboratory (ITL) at the NIST developed the test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of IT; however, it is not mandatory to implement these measures and they are at the discretion of companies to decide how they would apply them. In any organization, three group levels, management, information systems or IT practitioners, and end users play a role in protecting IT assets. Though collaboration and support between each group are essential to efficiently protect from data breaches, senior managers play a crucial role in creating the appropriate environment to secure the IT assets of a business. The security responsibilities of senior managers include establishing security policies, ensuring enforcement, and financing the security programs over time.

Literature Search Strategy

The objective for the literature review search strategy in this study was to identify published literature regarding data breaches and overcoming internal human errors and factors. I used standard search strategies involving keyword searches of two online databases such as MEDLINE and Cochrane followed by the evaluation of the bibliographies of relevant articles. I also used websites of relevant organizations

including IBM, Google Scholar, Yahoo Scholar, NIST, Penomon Institute, Verizon, and Symantec, especially their published information regarding data breaches and overcoming internal human factors in the surge of global cyber-threats. I used the inclusion and exclusion criteria to identify potentially relevant peer reviewed articles, and evaluated the relevance of each article to the following research questions:

RQ1: What are the internal human factors that contribute to data breaches and compromised information in the Ivory Coast emerging business environments?

RQ2: What are the root causes of the internal human factors that contribute to data breaches and compromised information in the Ivory Coast businesses?

RQ3: What preventative measures could managers use to minimize the threat from human factors, which are related to an internal employee, that contribute to data breaches or compromised information?

I did not test any hypotheses in this study because of the use of qualitative mixed methods to understand better the internal human behaviors responsible for data breaches and to propose measures that managers could use to prevent breaches.

It was also necessary for the selected articles to address one of the predictor variables and either quality (as measured by processes or outcomes) or cost. Furthermore, the selected articles must have focused on strategies that could mitigate data breaches, cost, and overcoming internal human factors in the growth of cyber-threats. For instance, the NIST Special Publication (NIST SP, 2012) provided guidelines for developing security assessment plans and associated security control assessment procedures. The NIST is a joint task force comprising members from the U.S.

Intelligence Community, Department of Defense, and Committee on National Security Systems with the mission to develop a unified information security framework for the federal government and its contractors. The SP 800-53A, Rev. 1 and 800-53, Rev. 4 were developed to instruct organizations on enterprise-wide, near real-time risk management.

Managing risks from systems in the dynamic operational environments could affect organizational operations and assets, individuals, other organizations, and the nations, adversely. The guideline proposed by the NIST for developing security assessment plans is intended to support a wide variety of assessment activities in all phases of the system development life cycle including development, implementation, and operation (NIST SP, 2013).

Theoretical Foundation Approach to Data Breach

The propagation of network communications has changed the nature of businesses, resulting in an unprecedented magnitude of threats and vulnerabilities to business information systems. According to information security theories, the behaviors of internal employees could have severe consequences to business information systems and data with the growth in network communications. In their user behavior model, Aytes and Connolly (2003) emphasized users' perceptions of risk and choice and indicated that information security behavior of internal employees is a result of their own choices. They also argued that the behavioral choice could have personal and organization-wide implications (Aytes & Connolly, 2003). The influence of individuals on information security has been recognized in past research studies. For example,

Banerjee, Cronan, and Jones (1998) underlined that individual characteristics, judgments, and beliefs, including organizational issues (e.g., organizational ethical climate) could have an impact on the ethical behavioral intentions of information security employees. Forcht, Pierson, and Bauman (1988) emphasized the role of employees, their attitudes, actions, and sense of right and wrong in addressing information system security issues. These end user-centric considerations indicated a social perspective on the role of information systems security while emphasizing the capability of people to develop attitudes and a sense of right and wrong independently.

Auray and Kaminsky (2007) indicated that the security risks from data breaches could be categorized into four basic patterns: integration as an employee, opting to be independent, the path of fraud, and parallel remuneration under a masked identity. Since 2007, many individuals have used these procedural patterns to transform themselves into security hackers by developing a split identity and fragmenting their professional identity. The demand characteristics theory proposed by Orne (1969) is still significant and could help to understand some cyber-crimes. This theory emphasizes that the influence of peers affects people significantly such that an individual could decide to participate in the ideological or physical attacks either against individuals, groups, nations, or financial institutions to advance their beliefs or goals.

As a consequence of being a part of such a group, the individual could feel justified in fearlessly carrying out the harmful, dangerous, or even deadly tasks, ranging from personal assaults to mass suicide bombings because the group justifies its demands to execute such tasks based on ideologies. For example, religious groups may justify

their actions as mandated by their god with the expectation for spiritual rewards. Consequently, these participants are vulnerable to adverse influences because they believe in the value of their religious causes with the hopes that their involvement could contribute to improving their stature within their religions either in this life or in the after-life.

With increasing cyber-threats, many organizations focus more on IT architecture and software to prevent intrusions, whereas they spent fewer resources on understanding human behaviors responsible for preventing data breaches. Increasingly sophisticated data breaches have been occurring in governments and businesses ranging from major newspapers, defense contractors, and cutting-edge technology companies across the globe (Forrester, 2011). Researchers at the Ponemon Institute LLC (2013) calculated that the average annual cost of data breaches for 234 organizations was $7.2 million, with a range between $375,387 and $58 million. The success of advanced persistent data breaches continues to affect a large number of citizens due to the exposure of their information. Many scholars have debated the surging problem with cyber-attacks from different controversial moral viewpoints. For example, as far back as 1781, Kant stressed that un-equal treatment could encourage people living in an imperiled status to choose their actions regardless of the impacts on the society or other individuals.

The question of universal moral standards is *what if everyone did that?* The moral could be worthless if everyone makes a moral justification for their actions because each one has different moral standards. Bentham's (1781) notion of pleasure is still relevant for understanding how cyber-criminals might justify their actions (Bentham,

1781). Bentham held that the justification for an action is determined by how long the pleasure would last, how intense it would be, and how likely it is to give further pleasure. People determine the degree of pleasures by subtracting any units of pain caused by their action. The remaining is the happiness value of their action, and Bentham called it a utility because the more pleasure that an action brings about, the more useful it is to society.

The principle of utility as a criterion of morals suggests that the right action produces a greater happiness than any alternative actions. The objective of Bentham's definition was to give words like right and wrong a descriptive connotation with an assumption that one should decide the right actions among various possible ways of acting in any given situation (Bentham, 1781). Therefore, the criterion of morals for each individual could influence their participation in data breaches.

Two basic paths to data breaches in many organizations are external and internal human factors. Similarly, cyber-crimes result from a combination of elements such as threats from employees and lack of involvement of top managers in mitigating cyber-attacks that damage the reputation and profit of many businesses. After data breaches, many of these businesses pay a third party to monitor the credit of customers and could face a class-action lawsuit.

Despite the growing number of data breaches and their negative consequences, the Ivory Coast government and most companies in the country appear to be inadequately protected from deliberate external and internal attacks, and the accidental loss of data by internal employees on their devices including desktops, laptops, and mobile devices.

Lack of appropriate managerial responses commonly results in less productivity, contributing to a loss in revenue generation. Further, the loss of sensitive company information or the inability to prevent unauthorized access could not only add costs to remediate any lost data, but also tarnish the corporate brand, shake shareholder confidence, and increase customer and employee concerns about data privacy, especially given the increase of BYOD practices.

Conceptual Framework

The architecture of a computer network has changed with advances in technology. The commercial and financial sectors, including all levels of government agencies, are pursuing a secure computer network architecture to safeguard the integrity of information exchange (Florence & Swamydoss, 2011). Nevertheless, hackers continue to steal personal data from computer systems on a daily basis. The cyber-attack on the South Carolina Department of Revenue (SCDOR) is the most significant breach against a state tax agency in the U.S. and affected nearly four million taxpayers, with estimates approaching six million in 2012 (SCDOR, 2012). This cyber-attack was successful because top managers did not ensure that SC DOR had the adequate security measures to protect personally identifiable information (PII) of taxpayers (SCDOR, 2012). Consequently, the state spent $20 million for added protection in the first year alone, and the state cabinet agencies and top managers were working on the security improvements. However, this data breach could have been prevented if top managers were willing to spend $25,000 on preventive measures to deter attackers to gain access to their information systems (Pardue, 2013).

This is one of the many challenges that top managers face to prevent the external human factors contributing to data breaches. Therefore, top managers should focus on internal human factors resulting from the dysfunctional managerial functions that impact the security of information systems. In the globally competitive market, the profit remains the most common motive for insider malicious activities and the profit motives are associated with money (Dutta & McCrohan, 2011). The competitive market economics is possible because of the use of electronic services in the financial institutions, which increased the need for security, principally due to the sensitive nature of information exchanged. For example, Internet banking systems require a successful security assessment or security evaluation process to mitigate Internet banking threats (Sujatha & Arumugam, 2011). The increasing success of data breaches is achieved because of the impossibility to achieve the uniformity of security across all industries; therefore, weaker links exist in organizations depending on their IT investment (Scott, 2010). Additionally, the success of data breaches is related to the complex behavioral motivational typology in the mounting risks of computer crime, especially in the Internet banking environment (Malathi & Baboo, 2011). Therefore, managers should provide security awareness to end users due to the complexity of security systems, and the nature of threats and attacks in the financial and other industries (Soerjadibrata, Jakarta, & Wagiyati, 2010). The threat of systems attacks is complicated, though understanding data breach process is helpful to prevent attacks.

Data breaches occur due to a series of intertwined and orchestrated events. Six top-level threat categories along with the prevalence are as follows:

- Hacking - 31% cause of data breaches;
- Malware - 25% cause of data breaches;
- Misuse - 22% cause of data breaches;
- Deceit - 12% cause of data breaches;
- Physical - 9% cause of data breaches; and
- Error - 1% cause of data breaches (Verizon, 2009).

Regarding malicious action against information systems, hacking is the leading cause of data breaches with the extensive library of hacking and intrusion techniques. The latest Verizon data breach investigations report (Verizon, 2015) provides the outcomes of data breach investigations within 70 organizations in 61 countries. Accordingly, the biggest incident threats are from four categories, namely miscellaneous errors (29.4%), crimeware (25.1%), insider misuse (20.6%), and theft/loss (15.3%), whereas the biggest data breaches are post intrusions (28.5%), crimeware (18.8%), cyber-espionage (18%), insider misuse (10.6%), and miscellaneous errors (8.1%).

Many intrusions exploited the fundamental mismanagement of identity. As a result, the intruder accessed via default and then shared the stolen credentials to a third party. Poor access control lists left a wide-open door for the assailant to walk through unchallenged and allowed cyber-criminals to:

- take the path of least resistance; or
- Use the SQL injection, which appears to be the common technique for hackers to gain access. This type of attack ranked second in prevalence (utilized in 16

breaches) and first in the number of records compromised (79% of the aggregate 387 million) (Verizon, 2015).

The bulk of attacks continued to target applications and services rather than the operating systems or platforms, on which they run.

Cyber-criminals used remote access services and web applications to gain access to corporate systems, whereas a smaller percentage of hackers targeted routers, switches, and other network devices. Malware is an essential component of nearly all large-scale data breaches. The most common malware delivery technique is the remote installation of malware after an attacker gains access to a compromised system.

New elaborate varieties of malware utilities could bypass existing data controls and encryption to create vulnerable data stores for future retrieval from the victim. Examples include:

- memory scrapers, which consist of sophisticated packet capture utilities and could identify and collect specific data sequences within unallocated disk space and from a page file;
- the percentage of customized malware is 69% of all samples encountered;
- most common in 2014 was the malware that had been created for attacks entirely from scratch, accounting for 87% of the 387 million records breached in the year;
- most malware used to compromise data may be detectable at the internetwork operating system (IOS) layer three level; and

- overall, 25% of breaches were caused by some form of misuse, including social engineering and phishing scams targeting attacks (Verizon, 2015).

Unfortunately, many organizations rely on the IOS layer three as the primary malware prevention and detection technique.

Organizations should self-assess to determine whether they are a target of choice or a target of opportunity. Random opportunistic attacks are when attacker(s) identified the victim when searching randomly or widely for weaknesses and then exploited the weakness, whereas the directed opportunistic attacks target the victim specially selected because they were known to have a particular weakness that attacker(s) could exploit. Similarly, fully targeted attacks occur when the victim is chosen first as the target and then the attacker(s) determine a way to exploit them. Targeted attacks accounted for 90% of the total records compromised. By a large margin and for the fifth year in a row, online data consisting of various types of servers and applications were the most frequently compromised assets, accounting for nearly all of the 285 million records breached across the 2008 caseload (Verizon, 2009). Thus, large and remotely accessible data stores remained the target of cyber-criminal activity. More records were breached in 2008 than any other single year and more than in the previous four years combined. The following top five breaches in 2008 accounted for 93% of total records compromised:

- Payment card breaches - near 80% mark and far outnumbered other data types by consuming 98% of all records compromised in the year.
- The clear majority of cyber-criminals were looking for a quick and easy payoff.

- Personal identification number (PIN) information associated with consumer payment card accounts were increasingly targeted in 2008.
- These attacks involved the identification and compromise of store magnetic strip data, together with a PIN, setting the stage for more damaging forms of identity fraud.
- PII was the second most compromised data type (Verizon, 2009).

Credentials give attackers the prospect of increased access for illicit activity and attackers appear to be exploiting that advantage. Additionally, organizations generally do not have a complete inventory of their IT assets, resulting in unknown opened ports or forgotten assets, such as:

- a system unknown to the affected organization or business group;
- an existing system storing data that is unknown to the organization;
- a system that had unknown network connections or accessibility; and
- a system that had unknown accounts or privileges.

Approximately half of the breaches investigated in 2008 consisted of at least one type of unknown (Verizon, 2009). The unknown impacts of a breached system remained unknowns; thus, increasing visibility and reducing variability in the IT operating environment should be a top priority for the risk management efforts.

Furthermore, there were various ATM attacks throughout the world even in the technologically advanced countries. Organized criminals installed cleverly disguised equipment on the front of an existing bankcard slot of the legitimate bank ATMs to steal the card number and the PIN. The equipment had a wireless PIN reading camera and was

housed in an innocent looking leaflet. Skimmers were mounted to the front of the standard ATM card slot that read the ATM magnetic strip and transmitted information wirelessly to the criminals. The criminals copied the cards and the PIN numbers to withdraw cash from many accounts in a brief time directly by hacking into the cash machine (Krebs, 2011). Therefore, recognizing the severity of cyber- threats helps organizations to shape the behavior of their customers.

Data Breach Review Analysis

During the last few years prior to this study, the number of data attacks has increased in business environments and in personal use environments. Protecting against any data breaches is the precondition for any e-transaction between users and organizations. To protect against data theoretically, an attacker might use a hypothetical network, which had five nodes A to E. The nodes represented only the system attackability measures, where attack surface measures were the node weights for the individual nodes. To replicate the trust between the hosts, the degrees of access should be set in the increasing order from the initial root to the authentication process to the full authorization of the user. In this situation, the practitioners suggest applying the algorithm, RelaxMatrix, to ensure access control on a bona fide need basis. Also, the fixed conversion may not exist for mapping the qualitative aspects of security to the quantitative values. Therefore, security system administrators could design a customized network to secure the specific needs of the business and to synchronize the network access levels. To achieve this, the algorithm backtracks could be applied sequentially, where node C could be introduced into the stack, which acted as the pivot node. The

backtracking could continue on the network because the neighboring node is reachable as per the adjacency of node C.

In the hypothetical network, the algorithm then searches for an alternative path to avoid the black nodes. The potential victim among the nodes is the node with the broadest measure of attack surface. The algorithm once again proceeds similarly and selects the second largest node until it reached the end of the node. The algorithm stops the search and returns the nodes falling and forming part of attack path to trace attack path that a potential intruder may use to commit a data breach (Manadhata, Flynn, & McQueen, 2006). Manadhata et al. (2006) underlined that the traceability of an attack path could be verified through an authenticated access from the file transport protocol daemon (FTPD) for Unix systems developed at Washington University (WU). WUFTPD is the most popular file transport protocol (FTP) daemon on the Internet, used on many anonymous ftp sites all around the world to mask a user's identity and the Pro FTP daemon (ProFTPD), which is a file transport protocol n FTP server and open-source software compatible with Unix-like systems and Microsoft Windows. In a hypothetical situation, this process reveals the vulnerability in the network at the WuFTPD and ProFTPD level. The hypothetical intruder first assaults the node with higher attack surfaces, and then attacker tracks back to the ProFTPD algorithm. This process could reveal the approach that the intruder uses to breach data if the access is not available (Manadhata et al., 2006). In this hypothetical situation, the intruders could also engage in criminal activities because data that they obtained could be used illegally.

The wider use of the Internet led to an increase in criminal activities such as identity theft, payment card fraud, and intellectual property theft. U.S. Department of Justice (2011) sentenced two Wellington men in a mail and aggravated identity theft ring. Wayne K. Roustan pleaded guilty to stealing credit and debit cards from a mailbox and using them to make purchases and cash withdrawals, costing victims $786,000 on February 12, 2011. Moreover, the human error and factor threat mitigations are appealing and urgent with the growing data breaches in financial network transactions. The reported losses due to human errors were 37%, resulting in the most cost and damage to any organization (CSO, 2013). Some organizations have filed civil complaints against some criminals.

In March 2012, Microsoft Corporation and co-plaintiffs filed a civil complaint against 39 persons caught in the illegal computer network activities using the Zeus and SpyEye BotNets, which were computers remotely controlled by hackers. Hackers used both Zeus and SpyEye to steal online banking information and then transferred funds to money mules or the U.S. residents with bank accounts, who could move the money out of the U.S. Microsoft was granted the court approval to seize 800 domains and several servers in Pennsylvania and Illinois that had been used to control the Zeus and SpyEye BotNets. Furthermore, the FBI arrested more than 100 Romanian-based criminal groups for a wire fraud scheme by selling items on Internet auction and online websites. The potential buyers were asked to wire money to bogus bank accounts. The suspected fraudsters received more than $10 million in reported profit, whereas the victims never received their purchased goods (Microsoft, 2012).

In another case, hackers from countries including Estonia, Russia, and Moldova reportedly hacked the Royal Bank of Scotland WorldPay computer network by defeating the encryption that was used to protect customer information associated with the payroll card processing system. Hackers used counterfeit payroll debit cards to withdraw $9.4 million of the salaries of employees from over 2,100 ATMs across at least 280 cities around the world, including in the U.S., Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, and Canada. In 2011, over $9 million was lost within 12 hours (Zetter, 2011)

Approximately 51% of the world population had an Internet connection in 2017 (world internet users statistics, WIS, 2017). The number of Internet users increased tenfold from 1999 to 2015 and reached 3.2 billion in 2015 (WIS, 2015). Similarly, growing digital technologies facilitate the frauds and schemes through Internet servers and digital communication devices located in physical locations. These locations might be different from the criminals or victims, posing the jurisdictional challenges in investigation and prosecution of cyber-criminals (WIS, 2014). However, financial institutions and other organizations could not stay indifferent due to the environmental changes of threats.

Clapper (2013) outlined that cyber-threats are the third most pressing threat to financial institutions and national security. Dutta and McCrohan (2011) indicated in their study that profit is the most common motive for malicious activities by an insider. The profit motive is associated often with power reassurance, that is, my beliefs are right, whereas yours are not. Another common manifestation of profit was the modus operandi of espionage. In espionage, individuals viewed selling secrets as a business rather than

an act of betrayal or treason. Undercover work might be a primary activity of insider threat. Two notable examples are Robert Hanssen and Aldrich Ames. Former FBI agent Hanssen provided classified manuscripts and precise information about the U.S. intelligence and capabilities to Russia extracted using his authorized access and credentials without hoisting any suspicion. He developed diverse methods to steal information and went home on many occasions quietly with confidential and classified documents and digital media. Hanssen committed espionage for more than 15 years before being caught and pleaded guilty to receive a life in prison in 2001, even though there were some indicators that something was amiss.

Between 1986 and 1994, a former Central Intelligence Agency officer, Aldrich Ames, provided classified human source information to the Soviet Union for over $2.5 million (Senate Select Committee on Intelligence, 1994). Despite an openly spendthrift lifestyle, his activities went unchallenged for eight years. This incidence highlights that mitigation of the human factors threat is a multidisciplinary problem requiring people, processes, and technology.

Scott (2010) stated that the advantages of cloud computing to mitigate this problem are well-documented. Although the system is stable in 2017, hackers might attack the system in the near future. Furthermore, the security of cloud computing delivery model appears to be unstable despite widespread acceptance in several emerging markets. These security concerns are legitimate among larger enterprises as well as small and medium businesses (SMBs). Unfortunately, various security and compliance point solutions could influence the view about data assets of an organization. Subsequently,

cloud security for one organization could be vulnerabilities for other companies, making the uniformity of security across all industries impossible.

However, there might be more natural ways to ensure sufficient levels of security and, therefore, compliance, depending on the business core needs. Due to a constrained budget or limited internal resources, information security compliance of SMBs differs from that of the larger enterprises because the former lacks the time and in-house skills to execute cost-effective controls. Consequently, the crown jewels of banks or other organizations are protected in the cloud. In the meantime, other practitioners such as Malathi and Baboo (2011) argued that it is critical to understanding the complex behavioral motivational typology in the context of increasing computer crimes, especially in the Internet banking environment. They also argued the necessity to authenticate the identity of customers accessing Internet-based financial services.

Many governments and business communities need new ways of conducting financial electronic transactions efficiently by developing a reliable and secure electronic transaction in the global market economy to ensure the protection of customer information and to reduce incidents of identity theft and fraud. Businesses run more electronic transactions in heterogeneous IT infrastructures; hence, monitoring of network interconnectivity is a challenge. Additionally, technology alone could not solve the insider threats due to human factors. Malathi and Baboo (2011) asserted that organizational policies and security processes are also insufficient and still relevant in 2018.

Power-reassurance included low-aggression behaviors that promoted or restored the self-confidence of the individual. The power-reassurance did not focus on human errors that cause mischief or test their skills in handling their daily tasks to minimize data breaches. Power-assertive refers to the use of moderate to high-aggression behaviors to promote or restore the self-worth of an individual, including a need for recognition and a desire to be seen as irreplaceable. For example, an employee used a contractor badge to gain access to the network operations center and offsite storage facility of a company, stole the backup tapes and caused system failures. The employee had hoped to be in a position to *save the day* because he had the backup tapes. However, he was captured in the hidden security cameras in the network operations center and offsite storage facility.

Anger-retaliation is another commonly associated behavioral motivation in human factors and includes revenge, retaliation, ideology, and sabotage. Timothy Lloyd is the first American sent to prison under new laws against deleting critical organizational files. Lloyd sought revenge against his company after being demoted and the prosecution established the guilt after the forensic analysis of a hard drive found in Lloyd's garage revealed a *time bomb* code used to delete the files. His malicious actions cost his organization, Omega Engineering, an estimated $10 million in damage. Opportunistic malicious human behavioral threats occur when a moral conundrum arises between pursuing selfish and selfless actions. Often, this behavior takes place when an opportunity for satisfaction coincides with the low probability of discovery.

There is only a limited understanding of the human behavioral aspect to holistically approach the network systems security. Malathi and Baboo (2011) also

supported research that could help to understand the human behavioral aspect holistically through deductive reasoning, leading to human error and factor threat mitigations. Understanding the human behavioral aspect, primarily related to electronic services in financial institutions, is critical because of the sensitive nature of information exchange (Sujatha & Arumugam, 2011). Internet banking systems require an effective security assessment or security evaluation process to mitigate Internet banking threats. In particular, information systems auditor should have the necessary knowledge, technical and operational skills to review the technology and the risks associated with Internet banking.

A new authentication approach presented by this security assessment or security evaluation process provides a threshold for the end users to reduce system security risks. Analysis of text-based authentication using images in the banking system is the basis of this security assessment and provides a great value in terms of convenience, customer intimacy, time-saving, inexpensiveness, and coherence in banking sectors. Nevertheless, security in the banking sectors remains volatile and complex. Soerjadibrata et al. (2010) underlined the complexity of security systems in the financial industry and suggested managers to provide security awareness to the end users. However, most end users lack the minimum skills and knowledge about the use of the system. They also found that role-based administrator rights to control information access is a prerequisite for optimal performance and systems protection.

The flow of data reporting systems and operating financial electronic transaction is of a security concern. Florence and Swamydoss (2011) explained that the change in

computer network architecture with advances in technology such that the commercial and financial sectors including the government agencies are pursuing the secure computer network architectures to safeguard the integrity of information exchange. Active networks represent a new approach to network architecture and provide a more resilient network infrastructure. The network security is mainly based on the network architecture, which gives the security spectrum in network system architecture and highlights security issues. Therefore, an inclusive design of network architecture, such as peer-to-peer network, client-server model, network security, authentication, national counter intelligent and security center, and the consideration of human factors, is suggested to assess security issues.

Human factors threats have increased with the proliferation of the passwords of the end users. Byungrae and Franz (2009) argued that Internet security is one of the latest concerns along with extensive use. One-time password (OTP) is the first security medium for strengthening the stability of electronic financial transactions. Byungrae and Franz (2009) proposed a method that generates the OTP key using location and fingerprints. The fingerprint is one of the key personal authentication factors and could create a variable password key for single information use. This approach helped reduce system security flaws as evident from a simulation conducted by Byungrae and Franz (2009).

The multi-agent system (MAS) is another approach when dealing with human factors threats. Talib, Rodziah, and Rusli (2010) suggested that the one-way secure financial system, which is based on the use of MAS problem-solving multi-agent

simulation construction of synthetic worlds collective robotics technique, could be beneficial to increase the security of cloud data storage. The system users could use the proactive and reactive features provided by the MAS techniques for cloud data storage security. A set of agent communities forms the architecture of the system.

Moreover, MAS could be used in a cloud platform for serving the security developed using a collaborative environment of Java agent development. To solve increasing system security concerns, MAS architecture offers several security attributes generated from four key security policies, namely correctness, integrity, confidentiality, and availability of user data in the cloud. Talib et al. (2010) also described an approach for businesses to build a secure cloud platform using the MAS architecture, which uses specialized autonomous agents for specific security services and allow agents to interact to facilitate security of cloud data storage.

Other practitioners such as Salve, Suraj, Rahul, and Harshad (2011) argued that technologies define the need in every sector, and it is vital that enterprises, including the financial sector, consider the changing needs of customers. To satisfy the financial needs of customers, executives at banks have been utilizing new technologies such as the Internet, which led to the development of e-banking despite the problems. However, using new technology such as the Internet and e-banking would not solve the security problems for banks without considering human factors. The potential use of mobile devices in financial applications such as banking and stock trading requires an increased security for e-banking. Salve et al. (2011) outlined that the objective of e-banking is to provide a secure environment for various types of transactions and focused on two-step

security for authentication, that is, the use of *mobile banking* and *steganography* to improve the communication channel. To enhance the security, they proposed data encryption to hide the patterns and provided a system based on the biometric information, that is, face recognition.

Selecting appropriate countermeasures have become a central concern for security practitioners due to human threats. Granadillo, Daniel, Mustapha, Nabil, and Herve (2012) highlighted the necessity to have traceability of security events from the analysis of attacks to selecting appropriate countermeasures for the risks. Furthermore, the design of network and system devices is heterogeneous with different characteristics and functionalities that increase the complexity of selecting appropriate countermeasures. Therefore, Granadillo et al. (2012) introduced an ontology-driven approach to address the complexity. The proposed model considers two main aspects of this field; they are information manipulated by the security information and event management environments and the operations applied to this information to achieve the desired goals. To reach the goal, they used BotNets to illustrate Internet vulnerabilities for a secure Internet transaction.

Network communication systems have flaws that lead to security breaches. Morais, Cavalli, and Martins (2011) asserted that network communication systems are intrinsically parameter random access memory (PRAM) and the flaws in the network communications could lead to security breaches in applications, which a malicious user could exploit to cause security failures in the system or could take total control of the vulnerable system. Therefore, they introduced a new attack injection approach based on

attack modeling to perform security testing and to detect any potential security vulnerabilities. Morais et al. (2011) used attack trees to describe the system flaws and derive similar attack scenarios. Attack scenarios are refined to executable scripts for testing tools that oversee attacks against the system. They used real attacks such as denial of service and cipher suite rollback attacks to the wireless application protocol, currently used in the low-tier mobile devices, to support their assertion. The experimental results suggested that the approach could achieve high efficiency in uncovering vulnerabilities to reduce security risks.

Human factor threats have increased mobile device accessibility. Pefuegnot, Laurent, Aurelien, Thibault, Julien, and Louis (2011) highlighted that the mobile transactions pose severe threats to e-banking because the end users ignore security precautions associated with mobile phones in e-banking, providing hackers a platform to launch malicious codes to intercept and hijack the system with even a smart card. An attacker might use a keylogger to capture the amount of the payment displayed in the terminal to fool the user or to steal the credential. Pefuegnot et al. (2011) proposed a security mechanism based on the graphical Turning test to prevent mobile transaction submissions by the malware. The graphical Turning test sustained the mobile transaction solution and strengthened the security mechanism of entrusted handheld devices. It also underlined a proof of concept to implement and test the feasibility of SIM card to determine the mobile phone performances and security level.

The mobile phone performance and security level are challenges for many organizations around the world since 2008. Wamyil and Mu'azu (2008) explained that

the global system for the mobile communication network, knowns as GSM, is a worldwide standard for mobile communication such as voice calls, short and multimedia messaging services, known as SMS and MMS, and global packet radio service, known as GPRS, used for Internet connectivity. Some of these services have possible security vulnerabilities. Wamyil and Mu'azu (2008) also investigated the security measures used in the GSM networks and found that they were inadequate to the current cyber-threats, including authentication, encryption, equipment identification and subscriber identity confidentiality, as well as the manifestation of network vulnerabilities including SIM, SMS, encryption and signaling attacks. These mobile devices are widely used in many developing countries for diverse purposes and could have a major role in information system security (ISS) breaches.

The outcome of ISS breaches differs from damaging database integrity to physical destruction of whole information system facilities. Geric and Hutinski (2011) indicated that information systems face different types of security risks, which could originate from inside or outside of the facility intentionally or unintentionally. The security risks could cause disruptions in negligible vital segments of information systems or with significant interruptions in information systems functionality. Accurate calculation of losses caused by such incidents is difficult due to some small-scale ISS incidents, which might not be detected or could be detected after a significant time delay.

A portion of these incidents results from an under evaluation of ISS risks. Geric and Hutinski (2011) also addressed the different types and criteria for ISS risks classification and outlined most common classifications used in literature and practice.

They delineated a standard set of criteria that could be used for the ISS threats classification, which could be useful to compare and evaluate different security threats and could help organizations to manage their ISS risks or threats better.

The computer security plan assistant (SPA) could manage ISS risks or threats. Hunteman, Evans, Brownstein, and Chapman (2009) argued that the industries should use the computer SPA, which is an expert system for reviewing Department of Energy (DOE) automated data processing (ADP) security plans. The computer security policies of the DOE stipulate to review and update the ADP security plan periodically for all DOE sites. The Center for Computer Security at Los Alamos National Laboratory sponsored BDM International Inc. to develop SPA using an expert system shell, called XI-Plus. Furthermore, the SPA runs on an IBM or compatible personal computer and consists of a series of questions about the ADP security plan. An SPA user answers the questions related to information systems based on the ADP security plan. The SPA end-user reviews each section of the security plan in any order until all sections have been reviewed. The SPA user might stop the assessment process after any section and resume later.

A security plan review report is available after the appraisal of each section of the security plan. The security plan review report provides a written assessment of the completeness of the ADP security plan to the end user. The security practitioners then test the SPA results at Los Alamos and provide a report on system security posture of organizations. This approach helped in mitigating security risks or threats within information systems of organizations.

Data Breach and Human Factor Security Framework

Most organizations lack a cyber-security strategic roadmap for securing their IT assets, resulting in constant attacks on information systems and data breaches. In general, these attacks and data breaches are undisclosed, especially in Ivory Coast and other West African countries. Most banks lack the following three overarching strategic goals to drive their cyber-security strategy and guide their future direction: (1) Manage and control access to applications, information, and data, (2) Protect the infrastructure that contains applications, information, and data, and (3) Protect information and data. The dynamics of the cyber-security threat landscape and implications for modern electronic transactions have moved away from nuisance and destructive attacks in favor of activities motivated by financial, political, and religious gains.

Moreover, a considerable number of network owners across the globe did not require a network license to receive an IP address. However, the network topography across the globe uses a nonunified standard and does not have to obey physical and logical network topologies, resulting in poorly designed network topologies and unprotected compromised servers. The expansion of network communications did not consider the network architecture layouts of LANs and WANs as well as the advantages and disadvantages of each layout and the optimal application. Nearly every hosting provider, who hosts millions of websites, email servers, DNS servers, database servers, VOIP gateways, resulted in compromised servers, websites, and applications because many of the providers offer little if any deep packet inspection to their customers.

A firewall and demilitarized zone do not ensure the full security of the network topology. Most often organizations do not know they have compromised customer data in their network. Firewalls stop screening data in the OSI model at the session, presentation, and application layers, where most exploits could occur. Therefore, cyber-criminals might use DMZ and firewall failures to stop exploits or other means to commit data breaches within an organization.

Data Breach Process

The cyber-threat landscape is more dynamic than ever because attackers are rapidly adapting to new security measures developed and implemented to protect computers systems. The current security threats identified in the Internet security trend reports are:

- increased professionalism and commercialization of malicious activities;
- threats that are increasingly tailored for specific regions;
- increasing numbers of multi-staged attacks;
- attackers targeting victims through banks exploiting trusted entities; and
- convergence of attack methods according to the North American Industry Classification System (NAICS), which is the standard used by the Federal statistical agencies to collect, analyze, and publish statistical data related to the U.S. business economy (NAICS, 2011).

The old mainframe platforms pose a challenge because the active security tools are not available for the old mainframe. Cyber-criminals continue to automate and modernize their techniques toward low-risk attacks against weaker targets. Hacking

incidents and malware attacks have increased together with an increase in the involvement of the activist groups in data breaches. Furthermore, information systems attacks happened at the general support system, where 94% of the compromised data involving servers were up from 18% (NAICS, 2011). These threats remain the preferred tools used by the external agents to commit most information systems attacks and data breaches.

Many attacks continue to manipulate the authentication process using the stolen or guessed credentials and access information systems. The globalization of network communications is a primary challenge to identify locations of cyber-threats agents because most breaches do not require the physical presence of attackers. The following three categories of cyber-threats exist:

- External threats: They originate external to the organization and the network of partners, for example, former employees, lone hackers, organized criminal groups, and government entities. They also include environmental events such as floods, earthquakes, and power disruptions. Typically, external entities are not trusted or privileged.
- Internal threats: They come from within the organization, for example, executives, employees, independent contractors, interns, as well as internal infrastructure. Insiders are trusted and privileged, and the level of trust and privilege vary among individuals.
- Partner threats: They include any third party sharing a business relationship with an organization, for instance, suppliers, vendors, hosting providers, and

outsourced IT support. Some level of trust and privilege are implied between business partners (NAICS, 2014).

The involvement of external agents is a major threat and occurs mainly with the assistance of the insider agents in many cases, for instance, the Equifax data breach in 2017. The motive of outsider threat agents is variant and outsider attacks remain at the peak within information systems attacks and data breaches, specifically in the financial industry.

A resurgence of hacktivism activities against the financial industry is increasing with the concept changing from the *cult of dead cow in the late 19th century* of website defacements to coordinated denial of service attacks and other jaunts to express disagreement or obtain bragging rights to review. The activist groups add data breaches to their repertoire with a heightened intensity and publicity. Similarly, data breaches with money-driven motive continue to focus on opportunistic attacks against weaker targets. Attackers steal smaller hauls of data from a large number of smaller organizations presenting a lower risk to attackers. In contrast, the activist groups could use some of the most dangerous attack vectors, such as drive-by attacks, targeted attacks, consumer attacks, metasploit attacks, internal attacks, Botnet attacks, and scripted attacks.

Objectives of Cyber-Attacks

There are many motivations for cyber-attacks. Internet security threat reports revealed that attackers use various techniques to avoid detection and prolong their presence in the system to steal information, hijack the computer for marketing purposes,

provide remote access, or otherwise compromise confidential information for profit (NAICS, 2014). Common cyber-crimes include:

- theft of credit card and other financial data
- theft of personal information, that is, identity theft
- extortion motivated by a threatened information disclosure
- extortion based on threatened denial of service
- alteration of data on web pages or other trusted sources
- economic gain, retribution, or political purposes
- exploitation of operating systems for a remote control for denial of service
- exploitation of operating systems for remote control of spyware installation
- commercially-motivated information theft
- theft of defense secrets for the national interest

Vectors of Cyber-Attacks

Majority of the vulnerabilities are related to the web applications and other avenues of attacks include:

- Software bugs and software with an inadequate patch or poor configuration such as passwords and unnecessary services could lead to the following attacks: simple remote exploit, worms, external remote-control software (bots), rootkits, spyware, keystroke loggers, and information disclosure such as network or configuration details;

- Flawed protocols and weak network architectures could allow the following attacks to succeed: man-in-the-middle attacks, snooping/sniffing, and session hijacking;
- Curiosity, carelessness, and even the desire to be helpful proliferates these attacks: social engineering, phishing or spear phishing, viruses, IM messages with attachments or hyperlinks to an infected site, email messages with attachments or hyperlinks to an infected site, and password disclosure;
- Improper physical security practices, lack of proper inventory controls, and lax data destruction practices lead to the theft of computer systems, drives, laptops, PDAs, cell phones and smartphones; the loss of tapes, disks, USB keys and devices with sensitive data; and the leak of confidential information on machines/drives that are donated or resold to dumpster divers; and
- Failure to address the backup and recovery issues as well as business continuity planning lead to loss of critical data, extended service interruptions, loss of revenue and reputation, and failure to meet service level agreements and financial penalties.

Sources of Cyber-Attacks

Attackers are increasingly sophisticated and organized, and they have begun to adopt practices that are like traditional software development and business practices. Alarmingly, the global decentralized networks of collaborative malicious activity (BotNets) have become so pervasive that they are *rented* or *sold* as commodities in the Internet underground economy. Another indication of the commercialization of

malicious activity is the emergence of phishing toolkits, which are a set of scripts that allow an attacker to set up phishing websites automatically to imitate the legitimate websites of various companies and to generate corresponding phishing email messages. One significant sign of a phishing toolkit is the hosting of numerous phishing websites on a single IP address (NAICS, 2014) and the use of phishing kits is increasing rapidly on a wide-spread level.

The phishing toolkits utilize the BotNets to target unsuspecting customers. The financial industry faces severe challenges combating these BotNets, which use numerous attempts to defraud the electronic payment system to steal several millions of dollars from victims (NAICS, 2014). Other prevalent cyber-attackers include amateur and professional computer hackers, organized crime gangs, professional and non-state sponsored actors such as terrorists and political activists), rival corporations, nation-states seeking competitive advantage, angry and unethical employees, contractors and consultants, outsourced or subcontracted employees and firms, and software and hardware vendors looking for financial benefits (NAICS, 2014). These cyber-attackers may use multiple techniques of sources attacks, which are diverse and focus primary on easy targets.

Targets of Cyber-Attacks

Internet security trends have identified increased attacks aimed at client-side applications and increased use of evasive tactics to avoid detection. Additionally, large widespread Internet worms have helped smaller more targeted attacks focusing on fraud, data theft, and other criminal activities. Although software vendors and enterprises try to adapt to the changing threat environment by implementing security best practices,

attackers have begun to adopt new techniques such as targeting malicious code in client-side applications. Commonly targeted applications include web browsers, email clients, and other desktop applications (NAICS, 2014). However, cyber-attacks targets vary and include Internet applications, Intranet applications, database servers, web servers, mail servers, DNS servers, wireless networks, desktops, laptops, PDAs, routers, switches, appliances (e.g., smart printers), PBXs and telephony infrastructure, network devices, VPNs, flash media, cell phones and smartphones, and IDS/IPS equipment.

Networks Threats

With well-equipped tools, a hacker could primarily do an investigative work to identify a target host within a network to discover any weaknesses it might have. The network scan could help to locate the hosts and ports together with the identification of possible victims. Internet registration bodies and DNS servers could provide information about the networks because domain names and IP address mapping are simple to access by hackers.

Hackers could find the network information from a router that uses SNMP for management purposes, especially, if the router has the default public community string enabled. Hackers could utilize *whois*, which a UNIX-based command from Internet registration sites and the lookup command from the Windows command line to display lists of registered IP addresses, domain names, and possible connections. Alternatively, they could use the traceroute command to identify the intermediate networks in a path to a host. Importantly, less sophisticated hackers could access information when a network

administrator leaves the DNS information in the public domain because the DNS has a distributed database that records types of equipment and operating system used.

After the identification of the network components, hackers could identify the individual machines connected to the network via *war-dialing*, which is a program that calls a given list or range of phone numbers and records. Those that answer with the handshake tones are possible entry points to computer or telecommunications systems.

Due to these activities, the financial institutions and other organizations should assure the confidentiality, integrity, and availability of their information and information systems. Perhaps, the most significant example of a nation-state sponsored BotNet attack is the cyber-attacks launched by the Russian hackers against Estonia. The Russian hackers launched the cyber-attack as a retaliation to the defacement of a statue of Lenin in Estonia, which knocked the entire country off the Internet.

Web-based Malicious Activity

The 2013 Data Breach Investigations Report indicated that malware was responsible for over one-third of data breach cases investigated. The malware was the cause of 40% of data breaches, resulting in 90% of total compromised records (Verizon, 2013). Malicious codes have evolved to reflect the recent emphasis on web-based attacks and led to the following issues:

- The emergence of malicious code altered web pages on compromised computers.

- The malicious modified code on the compromised computer redirected the browser to malicious websites that could further compromise the user's computer.
- PIN information associated with consumer payment card accounts was increasingly targeted in 2012. Personally identifiable information (PII) was the second most-compromised data type. 674 instances of massive data breaches were recorded by late 2012.
- Data of 45 million people were exposed.
- More than $56 billion worth of ID theft occurred since 2005.
- 94 million credit cards worth of $450M were lost as of mid-2012.
- In addition to theft-sensitive government information, personal privacy and business secrets are compromised as well (Verizon, 2013).

Today, criminals are frequently attacking business websites due to the availability of new technologies.

Criminal Website Attacks

Because data breaches occur through network communication, understanding the usefulness of attack path in the network and the vulnerability score are essential in securing the confidentiality, integrity, and authenticity of data or information. The vulnerability score is provided on a 10-point scale and is computed based on the technical report on the common vulnerability scoring system version 2.0. Mell, Scarfone, and Romanosky (2007) asserted that the probabilities of attacking the WU-FTPD and PoFTPD are 0.8 and 0.2, respectively. Mell, Scarfone, and Romanosky indicated that the

probability of attacking the WuFTPD is more than that of the ProFTPD because the WuFTPD access is that of an authenticated user. A vulnerability score of 7.0 or more is categorized as critical. Additionally, attacking the ProFTPD from WuFTPD has a higher probability compared to the direct attack.

The assigned probabilities are log-normalized followed by the multiplication by a factor of 10. This approach was verified using the Dijkstra single source shortest path algorithm, resulting in the same attack path as discovered by the proposed methodology. Ammann et al. (2005) proposed the following attack path: Attacker → WuFTPD → ProFTPD. Therefore, many security practitioners have assumed that a vulnerability score of 7.0 or more could provide a root level access to the attacker on both the WuFTPd and the ProFTPD. Similarly, the access level between the WuFTPD and the ProFTPD gets upgraded to the root from authenticated access, providing information on the paths that the hacker took to compromise the business information.

The following two attack paths are available for a hacker to choose: (1) Attacker → WuFTPD → ProFTPD and (2) Attacker → ProFTPD. In both processes, a hacker uses an algorithm to confirm the access type level. Thus, the security practitioners consider the path identification holistically as one method to stop a network cyber-attack (Ammann et al., 2005). The goal is to reduce the risk and secure the network after the path identification. Understanding this concept could assist to mitigate the risks and avoid the security vulnerabilities on a node on the attack path. Thus, the path identification is not an isolated process and has to work with the risk mitigation and

human errors and factors. The iterative result process could lead to overall improvement of security of the network.

Attack graph provides a holistic analysis of the system security against the objective of an attacker and is useful for proactive identification of possible risk management measures. Furthermore, the graph also addresses the issue of the cyclic dependencies and proposes the detection and removal of probable network flaws. The generated attack paths are used to represent the assault target network security conditions.

The Boolean logic minimizer helps to identify the minimum possible automated network security options and to find the possible attack niche in the polynomial time complexity, known as the host network of attack surface measures. The Boolean methodology can be adapted for active human factors risk mitigation in an organizational network based on the theoretical models and practical technologies. However, the increase in wireless technology has resulted in the multi-stage threats in such networks. The consideration of wireless threat analysis in networks is due to the growing research interest in wireless financial e-transaction and electronic authentication. Criminal attacks use different electronic agents to commit data breach. The findings from the 18 organizations showed that their data breach was caused by a malicious insider or an outside hacker (Ponemon Institute LLC, 2013).

Employee Negligence in Data Breaches

In many organizations, data breaches occur due to the negligence of employees or internal policies regarding malicious codes. Ponemon Institute LLC (2013) found that the main cause of a data breach for 51 organizations was the employee or contractor

negligence accounting for 49% of incidents followed by 37% for a malicious or criminal attack, and 23% for system glitches including a combination of IT and business process failures. Mitigation of such growing security concern depends on managers implementing measures to tackle internal human factors threats.

Access to Applications, Information, and Data

Cyber-security threats to network communications have increased because of the rapid increase in interdependency of computer systems. As a result, challenges to banks and other organizations are to provide an efficient, secure, and documented access to their information systems at all levels, from internal employees and contractors to external partners and customers. Most banks and other organizations do not provide the technology to allow their system administrators to act in real-time. Similarly, they do not enforce access to computer systems across highly complex and growing financial industry network environment.

Banks and other organizations cannot create, modify, and delete user accounts, user profiles, and corporate policies as well as the correlation of data from human resources, financial, travel, procurement, and email systems. Additionally, banks and other companies face web-based threats such as malware, which is analogs to cyber-vandalism and generally spreads through trojans, rootkits or backdoors keystroke loggers ransomware (KPMG, 2013). Growing and sophisticated malware increase the complexity of emerging security threats landscape.

New Threats to Security Landscape

Emerging Technologies

Cloud computing offers scalable and virtual resources as a service over the Internet. *Cloud* refers to the Internet infrastructure as a service. Because most cloud computing services are not regulatory compliant, business entities are responsible for preventing regulatory data from residing in the cloud. Furthermore, services are not customizable to organizational security standard because there is no one size fits all lines of attack and organizations must adhere to service provider technology standards. The pros and cons of cloud computer system are given in Table 1. Segregation of data is not segmented physically, and many customers data are segmented via the use of VLANs.

Table 1
Cloud Computer Strength and Weakness Analysis

Pros	Cons
Fast start-up	Bandwidth considerations
Scalability	Application performance
Business agility	Data security
Faster product development	Economies of scale
No capital expenditure	Adoption
	Interoperability

Mandatory Security Controls and e-Financial Transactions

The FISMA (2014) states that the agency program officials should conduct the annual enterprise continuous monitoring (eCM) security controls assessments to mitigate

system security breaches and should have mandatory security controls. Mandatory security controls are assessed in conjunction with one-third baseline for security controls based on the FISMA year of systems (e.g., year 1, 2, or 3). The NIST (2013) suggests that mandatory security controls are the most volatile, that is, most affected by ongoing changes to the information system or environment of operation. Additionally, they are most critical to protect organizational operations and assets, individuals, other organizations, and Nation, resulting in frequent testing using an approved organizational risk assessment method. This process could assist the agency to implement a more disciplined and structured approach to managing, controlling, and documenting changes to an information system or environment.

The annual testing of mandatory security controls could minimize or eliminate the potential threats or vulnerabilities associated with systems. Mandatory security controls are reviewed and adjusted to address current threats at the beginning of each FISMA year, July 1. These controls are tested at every eCM annual assessment unless the control could fit at least one of the following criteria:

- Control is a risk-based decision during a previous cyber-security assessment and is re-validated to ensure risk-based decision status.
- Control is a known open risk against a system, that is, an open plan of action and milestones (POA&M) weakness.
- Any control with a known vulnerability as long as the weakness is still open.

During the annual system security control assessment, a list of mandatory controls to be tested for each eCM annual assessment is provided to the owner of the system or

application. The following eleven mandatory controls in seven control groups exist, namely access, audit and accountability, configuration management, planning, identification and authentication, systems and communications protection, and system information integrity. These controls represent operational, technical, and management controls presented in NIST SP 800-53 r4.

Vulnerability Analysis and Assessment

The NIST (2013) recommendations stressed that industries could scan for vulnerabilities among tools and automated parts of the vulnerability management process to detect software flaws and improper system configurations. Vulnerability analysis measures the vulnerability impact of systems or hosted applications and is done at least monthly for all systems and upon the identification of new vulnerabilities by following the steps outlined below:

- Analyze vulnerability scan reports and results from security control assessments.
- Remediate legitimate vulnerabilities by risk assessment.
- Share information obtained from the vulnerability scanning process and security control assessments with designated persons within the organization to eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
- Allow for possible false positives in a scan report and vulnerabilities that have been determined to be an acceptable risk.

Vulnerability scanning tools should have the capability to readily update the list of information system vulnerabilities identified through the scan at least biannually or upon the identification of new vulnerabilities. Vulnerability scanning procedures should demonstrate the breadth and depth of coverage with information system components scanned and vulnerabilities checked. Some financial industries and other organizations should discern information that is discoverable by adversaries. Automated mechanisms should detect the presence of unauthorized software in information systems and notify designated officials to mitigate system vulnerabilities. Vulnerability analysis and assessment should address any system weaknesses through the POA&M process, which is a key document in security authorization package and is subject to federal reporting requirements established by the Office of Management and Budget. The POA&Ms updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. Therefore, the NIST recommends to maintain and document information systems by developing, implementing, and managing a process for ensuring the security of POA&M weaknesses.

The vulnerability analysis and assessment could remedy information security actions to mitigate risks to organizational operations and assets, individuals, other organizations, and the Nation. Furthermore, NIST (2013) outlined concepts related to minimum information security risk and helped companies to define, monitor, and report on information security performance, which is an outcome-based metrics to measure or evaluate the effectiveness or efficiency of information security program and the security controls employed to conduct the day-to-day operation. Some companies should

disseminate, and periodically review and update a business impact analysis to analyze the loss or degradation of each asset including customer information. The review could impact business functions of organizations and determine the time, at which the critical operations could be affected. For this reason, companies should know their recovery time objective (RTO).

To effectively apply RTO, companies may analyze the consequences of the loss or degradation of each asset and establish the necessary recovery time frames. The maximum RTO for a critical asset should be specified when full functions of the system could be back online before significant impacts are felt. The system RTO should be consistent across the time that it would take to impact national security, homeland security, economic stability, and health and welfare of the American people (NIST, 2013). The RTO approach helps managers to determine the period that a company could stay off the network without having business operations.

Cyber-Security Operations Roadmap Challenges

Many organization clientele services rely on the seamless interconnectivity of internal and external systems to deliver mission-critical applications via an electronic storefront of Internet-based services to customers and partners as well as Intranet-based services to employees. Meanwhile, the nature of cyber-threats to Internet-based business transactions has been changing rapidly. Some financial institutions and other industries have difficulties in protecting sensitive personally identifiable information regardless of whether it is created, distributed, or stored and whether it is typed, electronic, handwritten, printed, filmed, computer-generated, or spoken.

Threats to information and information systems have risen dramatically and many information and information systems in financial institutions and other industries do not have adequate protection from criminal, insider, or self-inflicted accidental (human factors) events that could weaken their security and degrade public trust and confidence. Intruders could disrupt the operation of information systems of banks. Most financial institutions and other organizations information systems do not take preventative, detective, and corrective measures to reduce vulnerabilities to cyber-threats before they could be exploited.

Despite the reality of such threats and potentially catastrophic results, many financial institutions face challenges to protect information and information systems from criminal, insider or self-inflicted accidental events weakening the security. Though many banks and other organizations have progressed to a certain extent in protecting customer accounts and information, they have not leveraged the technology to full capacity to modernize account activities due to the rapid growth of cyber-criminals and emerging transcontinental cyber-threats (Berghel, 2011). Many customers still have confidence in banks and maintaining this confidence is vital for the survival of the financial industry and other organizations.

Time Span of Breach

The timeline of events leading up to and following a data breach varies considerably. Pre-attack phase could provide some information about target acquisition, reconnaissance techniques used, and warning signs existed before the attack. In 2013, investigators found at least some indication of pre-attack phase or research involvement.

Intruders explored network and systems of victims until they found a desired point of attack. Criminals could access data in a matter of minutes or hours most of the time the compromise is undiscovered or uncontained for weeks or months in the majority of the cases. Overall, some organizations discovered breaches slightly quicker in 2013, though it was not quick enough to contain damages (Ponemon Institute LLC, 2013). Many organizations contain the damage by stopping the bleeding and do not refer to complete remediation of root problems.

Once a breach is contained, organizations remove unauthorized access and exposure of information; however, the majority of the breaches require weeks or more to control and only a few could be contained in less than a couple of days. Nevertheless, it could take a prolonged period if disaster recovery preparedness plan of organization is inadequate. Consequently, many organizations could not respond when a crisis occurs. Data breaches suggest that the utilization of detective controls among breach victims is relatively low:

- Some large organizations did not have intrusion detection systems.
- Others had deployed IDS; but, it has not activated them.
- Monitoring network activity with IDS, though not in locations or assets involved in the breach.
- Some organizations do not have prescriptive compliance requirements for event detection.

In addition to low detective capability, most organizations are not equipped to respond adequately to breaches when they are discovered, with only 38% of victims had

an incident response plan. Investigators found signs of anti-forensics in over one-third of cases in 2013 because companies did not want to tarnish their reputation and removed evidence of criminal actions to manipulate post-incident investigations (Ponemon Institute LLC, 2013). This attitude underlined the behavior of some organizations when dealing with human factors threats.

This approach also highlighted the attitudes of companies toward monitoring and testing networks:

- Tracked and monitored access to network resources and cardholder data (9% compliant).
- Recurrently tested security systems and processes (17% compliant).
- Kept a policy that tackled information security (17% compliant).

The situation is prominent in the financial industry and other organizations with an online card payment system due to the risk of non-compliance (Verizon, 2013). Hackers also use anti-forensics measures with data wiping, data hiding, and data corruption.

Secure Trusted Information and Information Systems

Secure and trusted information and information systems are vital to financial modernization in the global economic system. Many bank customers, trading partners, and other organizations rely on trusted information to achieve key personal and mission objectives. Each phase of financial industry business processes is dependent on the availability of reliable and uncompromised information, information systems, and business processes. Therefore, availability of a secure information environment is essential in the context of increasing attacks on information systems and must be a

critical component in the modernization of technology by organizations to reflect changing customer account activities in the global economy. A secure and trusted information path is important for clienteles to access information with confidence in integrity.

However, network communications have vulnerabilities with computer operating systems. In general, many companies do not update security patches that Microsoft or Apple releases on a daily or weekly basis. Consequently, cyber-criminals use flaws in the software and computer operating system vulnerabilities to attack the integrity, availability, and confidentiality of information systems.

Electronic Authentication of Financial Transactions

An electronic transaction policy should form the basis to determine the authenticity of the electronic transfer of financial information to mitigate frauds. However, the authentication should not be standardized across the financial industry because it could make it easier for hackers to exploit every system. The digital signature key is particularity to secure customer e-transaction authenticity and requires public key digital signatures of each bank for financial transactions. Therefore, financial institutions should implement a certificate public cryptographic key to provide proof that an authenticated person has made the transaction. Financial electronic transactions policy should address e-authentications of clientele with *bridge certification*.

However, financial e-authentication should be agile to adjust quickly to changing financial threats as mandated by the Federal information processing standards stipulated by the NIST. The banking industry is the pioneer to develop policies and best practices

for e-authentication, including the development of methods based on public certificates and other cryptographic credentials, to secure payment, collection, and collateral transactions. As a result, certification authority of banks could have to work under the authority of Treasury root certification authority, which could issue a single certificate validating authorized agent of the bank and the status of the bank as a designated agent of Treasury.

The individual bank should have the authority to issue certificates to end users. Moreover, the governments and financial industry could allow banks to have their cryptographic credentials, which could ensure financial e-transactions security and minimize e-transaction frauds. Therefore, governments and the financial industry should coordinate strategies to combat e-transaction frauds to achieve security equilibrium.

Compliance to Payment Card Industry Data Security Standard

The payment card industry data security underline the following threats related to the compliance deficiency in financial institutions and other organizations: guarded cardholder data, stored data (11% compliant), encrypted transmission of cardholder data and sensitive information across public networks (68% compliant), upheld a vulnerability management program, used and regularly updated security patched (62% compliant), developed and maintained secure systems and applications (5% compliant), implemented strong access control measures, confined access to data on bona fide need to know (24% compliant), assigned a unique ID to each person with computer access (19% compliant), limited physical access to cardholder data (43% compliant), frequently monitored and tested networks, tracked and monitored all access to network resources and cardholder

data (5% compliant), recurrently tested security systems and processes (14% compliant), preserved an information security policy, and kept a policy that tackled information security (14% compliant) (Ponemon Institute LLC, 2013). Among them, protecting stored data, developing and maintaining secure systems, and applications tracking and monitoring access to network resources and cardholder data are the most important because they are responsible for several major breaches over the past five years. Many researchers indicated that protecting against data breaches and controlling internal threat sources are major challenges in the context of ever-changing network communications in global political dominant leadership and competitive market economy. Because protecting against data breaches in Ivory Coast has not been investigated in detail, the purpose of this study was to contribute knowledge to this gap based on information collected from professionals on the protection of information and prevention of data breaches.

Summary and Conclusions

Many financial institutions and business environments continue to evolve with growing network communications across the globe. The clientele of the financial industry has switched predominantly to an online money transfer system to pay their bills or make international payments. Also, customers are using telex transfers (TT), through which they transfer money, make payments, or purchase merchandises to secure interbank transactions. However, financial e-transaction environment has created new types of financial frauds such as identity fraud and e-transaction flaws. To mitigate financial e-transactions irregularities, countries such as the U.S. have promoted generally

accepted accounting principles, which is the financial accounting standards for fraud prevention. Tracking of financial e-transaction is possible with the financial interbank communications through the bank identifier code, providing the financial e-transaction security system to reduce frauds. However, the effectiveness of tracking financial e-transactions is still a challenge in the global market economy because countries, organizations, and banking systems do not have the same information security capability. Consequently, the banking industry and many organizations, including governments, should build a uniform security information, security environment, policies, and laws across the globe to protect their systems and customers. Therefore, I will discuss in Chapter 3 about the research methods and challenges to data breach to understand how data breaches and internal human factor threats could be overcome so that top managers could control data breaches and internal human factors effectively.

Chapter 3: Research Method

Many organizations in Ivory Coast and other African countries have significant deficiencies in information systems security controls, resulting in pervasive vulnerabilities, undetected breaches, unknown amounts of damages, and numerous thefts. These deficiencies could increase the risks of deliberate misuse and unauthorized exposure of Ivory Coast information system assets. The focus of this study was to investigate significant data breach challenges faced by the Ivory Coast citizens and the role that executives or managers could play to minimize cyber-security threats.

Research Design and Rationale

I chose the research design for this study based on contextual features and research problems. The following three research questions investigated in this study were:

RQ1: What are the internal human factors that contribute to data breaches and compromised information in Ivory Coast emerging business environments?

RQ2: What are the root causes of the internal human factors that contribute to data breaches and compromised information in Ivory Coast businesses?

RQ3: What preventative measures could managers use to minimize the threat from human factors, which are related to an internal employee, that contribute to data breaches or compromised information?

Therefore, I used a qualitative research methodology involving a survey consisting of 20 questions. Furthermore, I used a design that involves intense examination of a small number of entities without varying independent variables or

controlling confounding variables. In addition to the surveys, I utilized open-ended questionnaires, coded interviews, and systematic observation for data collection (see Straub, Boudreau, & Gefen, 2004). Since this was a qualitative study, I used open-ended questions to obtain the feelings of the participants and probed their understanding through additional questions depending on their responses. The qualitative research paradigm focuses on the process rather than the product or outcomes (Merriam, 1988) and emphasizes individual experience and descriptions of life situations. Therefore, I sought to explore the life experiences of the individual participants, particularly what they understood about the impact of human factors on data breaches and the ways to mitigate them.

In most cases, the data breach events were accidental, while they were intentional in many other cases. However, data is valuable regardless of whether the breach is accidental or criminal and the media reported numerous high-profile examples of the data loss. A compilation of a few cases is shown in Table 2.

Table 2

Examples of Data Loss

Company name	Year	Compromised records
Sun Trust	2018	1.5 million
Equifax	2017	140 million
Home Depot	2015	94 million
Sony Corporation	2011	77 million

The results of data loss could lead to brand damage, damage to shareholder faith, legal fees, class action lawsuits, public relations costs, regulatory fines, victim notification for state disclosure laws, credit monitoring services, free goods and services to retain customers, service downtime, breach investigations, lost customers, and lost revenue. Furthermore, most data resided in data centers, where data loss occurs due to a lack of security controls on servers, storage, content, and networks. Further, data centers have been going through a generational change over the last few years with consolidation, virtualization, and the use of cloud services. Data loss could continue to increase if the security of data centers is not factored in, preferably at the design and architecture phase of construction, in the context of the increased complexity of the next-generation data centers coupled with the massive amount of data they store and process. Thus, I used seven steps in the research design process:

1. Acceptance: Do I have a goal that determines the design process?
2. Analysis: Do I have themes related to the design problem?
3. Definition: Do I define the problem and steps related to the planning of the work?
4. Ideation: Do the research questions inquire sensual experiences and feelings of the participants'?
5. Idea Selection: Are the themes specifically related to the research problem?
6. Implementation: Will I be able to recommend that will contribute to social changes?

7. Evaluation: Will I be able to objectively critique the proposed process and findings?

Role of the Researcher

The role of a researcher in this study was as a participant observer, interviewer, data collector, and analyzer. I purposely selected 27 participants for this study, consisting of five Ivorian government officials, four financial executives, five chief information officers, six IT managers, and seven information systems technicians who had at least 3 years of experience in their positions. This study addressed the significance of dysfunctional managerial processes and their impacts on leaders' decisions about overcoming data breaches and human factors related to information systems. The group did not receive any training in this study and completed the survey, questionnaire, and open-ended interview questions to provide robust data for analysis. I used the snowball sampling technique for selecting the participants by asking a participant to choose the next one from the list of pseudonyms. Ultimately, the role was to probe the participants and then listen to and process their responses before asking more probing questions to get a detailed understanding.

Methodology

Measurement is critical in cyber-security as well as quantitative research to ensure the trustworthiness of the system or the results of the study. Therefore, I used the validation decision tree proposed by Straub et al. (2004) to prioritize incident report assessment as opposed to other validation approaches such as internal validity and

statistical conclusion validity. After verifying the numbers, I conducted a trend analysis to correct and validate data.

When conducting the data analysis, I ensured that the date of the data breach incident was reported to CSIRC-CI aligned with the month and year associated with the incident. An incident could involve one asset or multiple assets. For the latter, I included all assets when determining the volume of assets for the compromised data risk assessment; however, I included incident only once when determining the volume of incidents based on incident type, location, and a related company. Thus, when deciding appropriate data analysis techniques, I also used the decision tree concept proposed by Hair (1995), leading to reduced bias and correct decision during data analysis.

Assumptions

Many security practitioners and scholars have made several assumptions related to the theories for protecting data and mitigating data breaches within information systems. The researchers at the ITL, NIST developed test methods, reference data, proof of concept implementations, and technical analyses to safeguard data and advance the productive use of IT (NIST, 2012). The NIST special publication series reports have highlighted the ITL research, guidelines, and outreach efforts in ISS as well as collaborative activities with industry, government, and academic organizations. Some scholars have argued that attack trees are used successfully to identify threats and risks to the system, while protection trees are used in conjunction with attack trees to evaluate trade-offs in the risk mitigation process (Edge et al., 2007). While the focus of attack and

protection trees is generally on the determination of the overall system risk, the methodology is applicable equally to the human factors threat domain.

Attack trees formally represented all attack vectors and helped to determine the events that might occur for attacks to be successful. Calculation of metrics, such as the impact to a system if an action is accomplished, requires the determination of risk level for each node (Edge et al., 2007). Others have used textual clustering and data mining theories, which used probabilistic latent semantic indexing to generate links among documents, topics of interest, and people. From these links, an interest profile for an individual could be generated (Okolica, Peterson, & Mills, 2008). Therefore, these assumptions emphasize that an organization needs to protect data because cyber-incidents could have a significant impact on data breaches.

Cyber-Incidents in Cyber-Attacks

Data analysis was based on the following coding of incidents reported in the electronic tracking (e-trak) database:

- Disclosure (Disc): Information is revealed to an unauthorized individual.
- Loss: An asset is found in the undesired location or cannot be located.
- Theft: An asset is thought or known to have been taken without permission from the responsible person.

I adopted the above codes to organize the reported incidents into three-dimensional data to ask a consistent and specific set of questions of all data.

Participant Selection

Twenty-seven participants in this study represented the sample population of government officials, financial executives, IT managers, and information systems technicians who had at least 3 years of experience in their position and actively used computer systems in their work environment. These requirements were necessary to ensure that the participants reflected the minimum skills necessary to secure computer systems. The requirements also ensured that the participants had a detailed understanding of information assets and their protection.

Additionally, the possibility of conducting appropriate statistical analyses was another factor considered during the participant selection. Consequently, I provided the participants with information to ensure that they understand social and ethical issues to enable them to form opinions and attitudes. I ensured that each member of the group understood the basic concepts involved in the study. In this process, I provided the groups with a series of questions written on cards to address and discuss, which allowed me to reduce any bias in data compilation. I then checked whether the groups were comfortable with audio recording and found that two-thirds of participants were not. Consequently, I took notes and shared them with respective participants for concurrence. Additionally, I developed a questionnaire to capture their incident reports in five West African countries.

Instrumentation

I used an e-trak database to control and track data breach incidents involving disclosures, losses, and thefts reported through CSIRC-CI. For each incident reported,

the database contained information on the type of incident, asset(s), types of PII/SBU, risk assessment code, the location of the incident, relevant dates, and the number of impacted individuals and businesses. I reviewed incidents for accuracy by checking the consistency between the key facts narrative and type of incident, type of asset, and location of the incident. I also reviewed incident notes and the origination for cases with conflicts and made the required corrections on the database. After validating the extract from the CIS report, I matched data against the dashboard reports from e-trak to verify the accuracy of the number of incidents. This process allowed me to check and include background information on reporting, risk assessment, and notification processes for incidents reported to CSIRC-CI. I did so to ascertain if there were no significant changes to the processes outlined in the previous trend analysis report.

ABC bank employees reported incidents involving disclosure of PII or loss or theft of IT assets. After I received the incident reports, I entered the information into incident management by utilizing e-trak database system to track and manage them throughout incident management process, including the risk assessment determination, reporting, and to allow potentially impacted individuals to be notified, if necessary. Thus, to validate the findings, I used the 2012 data loss barometer (KPMG, 2012) and the 2013 Internet security threat report (Symantec, 2013).

The KPMG report exposed some of the latest trends and statistics for lost and stolen information in 2012 across the world as well as the trends over the last five years. Over 82 countries are represented in 2012, whereas over 96 countries are represented over the last five years. The report revealed data loss incidents and respective locations.

Data loss incidents increased by 40% since 2011 with hacking being the primary cause accounting for 60%. Internal threats reduced significantly, whereas external threats doubled. The worst performing sectors in terms of the total number of incidents were technology, financial services, retail, and media over the last five years. Over the past five years, over one billion people have been affected by data loss incidents around the world with publicly disclosed incidents increased by 40% in the last two years.

Data loss incidents in financial services reduced by 80% in the last five years, although they were still the fifth worst performing sector in the first half of 2012. From 2008 through 2012, KPMG (2012) reported that hackers accessed 681 million records, which could increase with growing connectivity. The majority (88 %) of reported data breaches were due to attacks by outsiders. However, the insider threat still remains high in the form of lost laptops, misplaced memory sticks, deliberate or accidental data theft by employees. For example, the U.K. Information Commissioner fined and prosecuted more businesses because of insider mistakes than outsider attacks. Most SMBs should be vigilant about their internal employees and anonymous hackers alike.

The highest number of identities were stolen in January 2012 due to a single breach involving over 24 million identities, whereas the numbers mostly fluctuated between one and 12 million stolen identities per month for the rest of the year. The average number of monthly breaches for the first half of the year was 10.7 million, which increased to 15.4 million in the second half of the year, resulting in a 44% increase (Symantec, 2013). The level of data breach demonstrates the growth of human factor

threats and their consequences on organizations if managers did not take proper measures to mitigate threats.

Procedures for Recruitment, Participation, and Data Collection

The purposely selected samples included five Ivorian government officials, four financial executives, five chief information officers (CIO), six IT managers, and seven information systems technicians. I used three data collection approaches such as survey, questionnaires, and interviews, which were investigated and validated as mentioned in the methodology and instrumentation sections. I conducted data collection in two phases after the approval of the Institutional Review Board at Walden University. During the first phase between January 2011 and December 2012, I evaluated secondary data collected from five African countries including Ivory Coast, whereas the second phase of data collection focused on Ivory Coast from October 1 to November 3, 2017, depending on the availability of the participants. I personally contacted all the participants, who agreed to participate in this research, to reduce the number of non-respondents. I used a multi-tiered strategy of assertive tracking for all initial non-respondents by approaching them a second or even a third time via email or phone call. The key to having low turnout responses was to develop a personal relationship with the participants.

Table 3
Monthly Incident Reports

Month	FY11 Incidents				FY12 Incidents			
	Disc	Loss	Theft	Total	Disc	Loss	Theft	Total
Jan	85	35	10	**130**	201	47	11	**259**
Feb	100	36	9	**145**	222	47	14	**283**
March	219	32	5	**256**	187	59	10	**256**
April	207	30	9	**246**	169	40	11	**220**
May	231	34	9	**274**	141	51	5	**197**
Jun	194	60	9	**263**	198	69	13	**280**
Jul	243	52	10	**305**	253	47	7	**307**
Aug	221	54	14	**289**	269	45	22	**336**
Sept	203	47	11	**261**	324	65	7	**396**
Oct	194	58	21	**273**	307	55	9	**371**
Nov	188	50	10	**248**	271	61	12	**344**
Dec	158	58	6	**222**	175	46	8	**229**
Total	2,243	546	123	**2,912**	2,717	632	129	**3,478**
% FY Incidents	77.0%	18.8%	4.2%	100.0%	78.1%	18.2%	3.7%	100.0%

The peak volume of total incidents was the unimodal distributions for FY11 and occurred in July (Table 3). However, the volume remained consistent throughout the year with January and February reflecting the lowest volumes. In FY12, the distributions

were not skew with less consistent volumes and the peak volumes were bimodal distributions and occurred in September and October. The histograms for reported incidents in both years were nonsymmetric distributions, and the disclosure was the most recurring incident with 77.0% in FY11 and 78.1% of total incidents.

Recurring Incidents Breakdown Disclosures

Table 4 provides a breakdown of all disclosure incidents reported in 2011 and 2012. The number of disclosure incidents reported monthly for two years did not show any significant pattern. In FY11, disclosures appeared to follow a varying pattern based on the highest frequency in the months, whereas incidents did not reach their peak until September and October in FY12. The total number of disclosure incidents per month for the year 2012 was 2,717, which is 21% greater than the total of 2,243 for 2011. Similarly, the average number of disclosures per month increased from 187 to 226.

Table 4
Monthly Disclosure Reports

Month	FY11	FY12
Jan	85	201
Feb	100	222
March	219	187
April	207	169
May	231	141
Jun	194	198
Jul	243	253
Aug	221	269
Sept	203	324
Oct	194	307
Nov	188	271
Dec	158	175
Total	2,243	2,717
Average/Month	187	226

Losses of Wireless Aircards, Mobile Phone Devices, and USB Units

Table 5 provides a breakdown of all losses reported in 2011 and 2012. Incidents followed a similar, though not identical reporting pattern with the highest volume reported in June for both years. Accordingly, a total number of losses per month in 2012 was 632 with 16%, which is greater than the total of 546 for 2011. An average number of losses increased from 46 to 53 per month, which could be because of increased volume and types of assets, such as wireless air cards, BlackBerry devices, and USB units, assigned to employees.

Table 5

Monthly Losses

Month	FY11	FY12
Jan	35	47
Feb	36	47
March	32	59
April	30	40
May	34	51
Jun	60	69
Jul	52	47
Aug	54	45
Sept	47	65
Oct	58	55
Nov	50	61
Dec	58	46
Total	***546***	***632***
Average/Month	*46*	*53*

Thefts of Laptop, Mobile Phone, and Wireless Card

The number of stolen mobile devices reported in 2011 and 2012 are given in Table 6. The variation across the month did not show any clear pattern. For FY2011, the volume of incidents was consistent except for October with 21 thefts. In contrast, the

highest volume of 22 was recorded in August in 2012. The total number of thefts per month in 2012 was 129 accounting for a 5% greater than the total of 123 for 2011. The monthly average of thefts increased slightly from an average of 10.3 in 2011 to 10.8 in 2012.

Table 6

Monthly Theft Report

Reporting Month	FY11	FY12
Jan	10	11
Feb	9	14
March	5	10
April	9	11
May	9	5
Jun	9	13
Jul	10	7
Aug	14	22
Sept	11	7
Oct	21	9
Nov	10	12
Dec	6	8
Total	***123***	***129***
Average/Month	***10.3***	***10.8***

Background Data Analysis

Interpretation of the Monthly Incident Reports for FY11 and FY12

Table 7 reflects the number of incidents and assets used in this analysis. Because one incident could contain multiple assets, the number of assets was more significant than the number of incidents.

Table 7

Incident Types

Type of Incident	Incidents			Assets		
	FY11	FY12	% Change	FY11	FY12	% Change
Disclosure (Disc)	2,243	2,717	21.1%	2,347	2,802	19.4%
Loss	546	632	15.8%	592	668	12.8%
Theft	123	129	4.9%	165	186	12.7%
Grand Total	2,912	3,478	19.4%	3,104	3,656	17.8%

From FY11 to FY12, the ABC Bank experienced an increase of 21%, 16%, and 5% increase in disclosures, losses, and thefts, whereas the number of assets lost, stolen, or disclosed increased by 18%. Thefts were the only incident type, where the number of assets increased at a higher rate than the number of incidents, suggesting that the thefts were more likely to involve multiple assets. Thus, I investigated recurring monthly incidents for FY11 and FY12, and their impacts on data breaches.

Analysis of Incidents

This section included data on the overall number of incidents for disclosures, losses, and thefts. For each reporting month, disclosures generally represented the

highest number of incidents, followed by losses and thefts. For FY11, disclosures accounted for 77% of all incidents, followed by losses at 19% and thefts at 4%. The percentages for FY12 were almost identical, with disclosures at 78%, losses at 18%, and thefts at 4%. Populations for FY11 and FY12 incidents were 2,912 and 3,478, respectively, and determined based on reported incidents.

Examination of the Previous Incident Reports and Analysis

I hypothesized that the monthly incidents are statistically significant and have an impact on data. I tested the hypothesis using the analysis of variance (ANOVA) test, which is an inferential statistical test whether the means are different significantly from each other. It assumes that the dependent variable has an interval or ratio scale. In this example, I tested the response to the question to determine incidents impact on data. The null hypothesis, $H_{0,}$ was $\mu_{Disc} = \mu_{Loss} = \mu_{Theft}$, where μ represents the mean incident, whereas the alternative hypothesis, H_a, was $\mu_{Disc} \neq \mu_{Loss} \neq \mu_{Theft}$ at a significance level α of .05. Because the incident was ratio scaled approximately and had three groups, the between-subjects ANOVA was appropriate. I analyzed data using IBM SPSS software.

Descriptive Statistics

Output 1

For each dependent variable (e.g., IncidentNum), I obtained the descriptive output consisting of sample size, mean, standard deviation, minimum, maximum, standard error, and confidence interval for each level of the (quasi) independent variables and presented in Table 8.

Table 8

FY11 & FY12 Descriptive Incident Reports

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
FY11 Monthly_Disc	12	186.92	49.379	14.254	155.54	218.29	85	243
FY11 Monthly_Loss	12	45.50	11.342	3.274	38.29	52.71	30	60
FY11 Monthly_Theft	12	10.25	4.070	1.175	7.66	12.84	5	21
FY12 Monthly_Disc	12	226.42	57.830	16.694	189.67	263.16	141	324
FY12 Monthly_Loss	12	52.67	9.029	2.606	46.93	58.40	40	69
FY12 Monthly_Theft	12	10.75	4.434	1.280	7.93	13.57	5	22
Total	72	88.75	91.498	10.783	67.25	110.25	5	324

Output 2

The ANOVA results indicated that there was a statistically significant difference among incident types, $F(5, 71) = 105.11$, $p = .000$. I used the Tukey's Honest Significant Difference (HSD) test as the post hoc multiple comparisons test to identify specific conditions that were different from each other. As evident in Table 9, the majority of *p* values for mean difference are less than .05 suggesting the statistically significant difference between mean values. Among them, eight values are greater than .05 and correspond to a comparison between Loss and Theft conditions, indicating that both conditions are not significantly different in terms of incident outcomes. In contrast, Disclosure, Loss, and Theft conditions were significantly different.

Table 9

Tukey's HSD Results

Dependent Variable: FY2011-2012 Incident Reports

Tukey HSD

(I) FY2011-2012 Incident Types	(J) FY2011-2012 Incident Types	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
FY11 Monthly_Disc	FY11 Monthly_Loss	141.417*	12.941	.000	103.43	179.40
	FY11 Monthly_Theft	176.667*	12.941	.000	138.68	214.65
	FY12 Monthly_Disc	-39.500*	12.941	.037	-77.48	-1.52
	FY12 Monthly_Loss	134.250*	12.941	.000	96.27	172.23
	FY12 Monthly_Theft	176.167*	12.941	.000	138.18	214.15
FY11 Monthly_Loss	FY11 Monthly_Disc	-141.417*	12.941	.000	-179.40	-103.43
	FY11 Monthly_Theft	35.250	12.941	.084	-2.73	73.23
	FY12 Monthly_Disc	-180.917*	12.941	.000	-218.90	-142.93
	FY12 Monthly_Loss	-7.167	12.941	.994	-45.15	30.82
	FY12 Monthly_Theft	34.750	12.941	.092	-3.23	72.73
FY11 Monthly_Theft	FY11 Monthly_Disc	-176.667*	12.941	.000	-214.65	-138.68
	FY11 Monthly_Loss	-35.250	12.941	.084	-73.23	2.73
	FY12 Monthly_Disc	-216.167*	12.941	.000	-254.15	-178.18
	FY12 Monthly_Loss	-42.417*	12.941	.020	-80.40	-4.43
	FY12 Monthly_Theft	-.500	12.941	1.000	-38.48	37.48
FY12 Monthly_Disc	FY11 Monthly_Disc	39.500*	12.941	.037	1.52	77.48
	FY11 Monthly_Loss	180.917*	12.941	.000	142.93	218.90
	FY11 Monthly_Theft	216.167*	12.941	.000	178.18	254.15
	FY12 Monthly_Loss	173.750*	12.941	.000	135.77	211.73
	FY12 Monthly_Theft	215.667*	12.941	.000	177.68	253.65
FY12 Monthly_Loss	FY11 Monthly_Disc	-134.250*	12.941	.000	-172.23	-96.27
	FY11 Monthly_Loss	7.167	12.941	.994	-30.82	45.15
	FY11 Monthly_Theft	42.417*	12.941	.020	4.43	80.40
	FY12 Monthly_Disc	-173.750*	12.941	.000	-211.73	-135.77
	FY12 Monthly_Theft	41.917*	12.941	.022	3.93	79.90
FY12 Monthly_Theft	FY11 Monthly_Disc	-176.167*	12.941	.000	-214.15	-138.18
	FY11 Monthly_Loss	-34.750	12.941	.092	-72.73	3.23
	FY11 Monthly_Theft	.500	12.941	1.000	-37.48	38.48
	FY12 Monthly_Disc	-215.667*	12.941	.000	-253.65	-177.68
	FY12 Monthly_Loss	-41.917*	12.941	.022	-79.90	-3.93

*. The mean difference is significant at the 0.05 level.

Output 3

The homogenous subset results listed the groups in the order of ascending means. As evident in Table 10, Loss and Theft incidents might not have any impact if they were not discovered, whereas Disclosure incidents could have a high impact on confidentiality, integrity, and availability.

Table 10

Homogenous Subsets of Incidents

FY2011-2012 Incident Reports

Tukey HSD[a]

FY2011-2012 Incident Types	N	Subset for alpha = 0.05			
		1	2	3	4
FY11 Monthly_Theft	12	10.25			
FY12 Monthly_Theft	12	10.75			
FY11 Monthly_Loss	12	45.50	45.50		
FY12 Monthly_Loss	12		52.67		
FY11 Monthly_Disc	12			186.92	
FY12 Monthly_Disc	12				226.42
Sig.		.084	.994	1.000	1.000

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 12.000.

Output 4

The impacts of incidents could change over time. Therefore, independent variables, incidents, might have different impacts on their dependent variables according to the number of incidents. Thus, I conducted a bar graph analysis to understand the FY12 and FY11 incidents within groups.

Analysis of the Bar Graph

As evident in Figure 1, the number of incidents in FY12 had increased for Disclosure and Loss and remained the same for Theft. Therefore, Disclosure was the worst incidents accounting for 78% from FY11 to FY12.

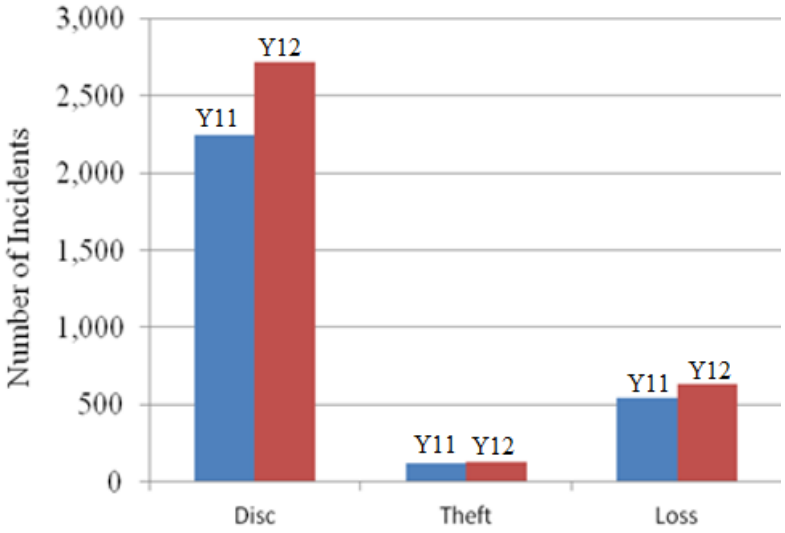

Figure 1. Three major incidents (Disclosure, Theft, and Loss) from annual reports.

Issues of Trustworthiness

Trustworthiness is a significant concept as it enables a researcher to explain virtues of qualitative terms outside of parameters, which are generally used in the quantitative study without the bias nature of data collection and analysis. Additionally, trustworthiness shows that the results are accurate and consistent, and the outcomes of data analysis are genuine. Therefore, it is important that each step during the analysis, such as data collection, data treatment, data organization, and the result reporting, is trustworthy (Elo et al., 2014). Credibility, transferability, dependability, and confirmability are the measures used to evaluate the trustworthiness of a qualitative study (Houghton, Casey, Shaw, & Murphy, 2013). The overall hypothesis of this case study underlined the following accepted conclusions:

- Average incident scores among disclosure, loss, and theft were different.

- Average disclosure scores were more significant than even the combined average of loss and theft.
- Statistic results showed that disclosure incidents were widespread.

Credibility

I used continual observation, utilization of existing concepts, and the agreement of participants with transcription of their interview, and triangulation to establish the credibility. Participants had the chance to review copies of transcriptions of the interview, survey and questionnaire, and to correct any mistakes or misinterpretations of their responses. The internal validation process of triangulation is an important method to improve the credibility and validity of study outcomes (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014). Selecting participants of different genders, with different levels of education, and with varying experience levels was useful for triangulation.

Data were sorted from the highest to lowest based on the total asset volume. A large number of different types of assets were consolidated into similar categories. For FY11 and FY12, the top five asset types by volume were hardcopy documents, sensitive data, wireless air cards, mobile phones, and laptops. Except for laptops, other categories experienced an increase from FY11 to FY12. The volume of incidents involving hardcopy and sensitive data was reflective of the use of a large volume of customer contact and correspondence the ABC Bank initiated through mail and fax. In addition, there was a significant increase in wireless air cards and USB units because these assets have been distributed widely to employees. In contrast, there was an overall decrease of

7% in the number of laptop losses and thefts. Because of the large volume of PII that these assets could contain, the decrease in these incidents is significant.

Transferability

Transferability is defined as the degree, to which study outcomes can be generalized to another population (Munhall, 2012). Sample size and the diversity of the participants are some of the factors that determine the transferability of study outcomes. The study participants consisted of male and female genders, who came from five organizations and fulfilled the selection criteria. Therefore, this study results may have some transferability since the participant responses related to data breach incidents were diverse (Table 11). Table 11 contains data on the volume for a different type of assets involved in each incident type and provides a breakdown of the percentage of disclosure, loss, and theft incidents for each type of asset. Additional details about the top six asset types by volume were provided in the following subsections. In addition, the RQ survey, questionnaire and interview questions were the same for each participant and I did not significantly interfere when they responded.

Table 11

Reported Asset Types

Asset Types by Volume	Disclosure		Loss		Theft		Total		Change
	FY11	FY12	FY11	FY12	FY11	FY12	FY11	FY12	
Hardcopy	1,702	2,150	229	236	26	20	1,957	2,406	23%
Sensitive data	642	652					642	652	2%

Asset Types by Volume	Disclosure		Loss		Theft		Total		Change
	FY11	FY12	FY11	FY12	FY11	FY12	FY11	FY12	
Wireless aircard			108	167	27	25	135	192	42%
Mobile phone			132	150	26	19	518	169	7%
Laptop			34	40	60	47	94	87	-7%
USB				12	4	39	4	51	1175%
Grand total	2,344	2,802	592	668	165	186	3,104	3,656	18%

Dependability

Dependability is the extent that the study could be repeated by other researchers to get consistent results. That is, the dissertation should provide adequate information for a person to replicate the study in Africa. Such information includes adopted methods, study context, population, samples, and sample selection criteria. Therefore, scrutinization of the study and the outcomes could be possible (Thomas & Magilvy, 2011). It even appeared that organizations in Africa countries have similar causes of data breach issues due to the outdated business environment, in which they continue to operate.

Hardcopy documents or sensitive data accounted for almost all of the disclosure incidents, whereas losses of hardcopy documents accounted for 39% of all losses in FY11 and 35% in FY12 (Table 12). Losses of wireless aircards increased from 18% of all losses in FY11 to 25% in FY12 and laptop losses remained constant at 6% of all losses for each year. Thefts of laptops showed a decrease from 36% to 25% of overall thefts. The USB units had the highest increase in thefts, rising from 2% of thefts in FY11 to 21% in FY12.

Table 12

Combined Asset Types

Consolidated Asset Type	Disclosure		Loss		Theft		Total	
	FY11	FY12	FY11	FY12	FY11	FY12	FY11	FY12
Hardcopy	773%	777%	339%	335%	116%	111%	663%	666%
Sensitive data	227%	223%					221%	118%
Wireless aircard			118%	252%	116%	113%	44%	55%
Mobile phone			222%	222%	116%	110%	55.1%	44.6%
Laptop			66%	66%	336%	225%	33%	22.4%
USB				22%	22%	221%	00.1%	11.4%
Grand Total	1100%	1100%	1100%	1100%	1100%	1100%	1100%	1100%

As evident in Table 13, hardcopy documents experienced the highest volume of incidents, increasing from 63% of all assets in FY11 to 66% on FY12. Table 13 provides a breakdown of incidents involving hard copy documents based on the location of the loss or theft or the method of disclosure. Key finding included:

- Incidents involving hardcopy documents sent through the mail had the highest volumes, followed by the fax and ABC Bank facility. Hardcopy incidents in the mail generally involved sending incorrect documents to the customer.

- The greatest percentage increase of 241% was related to incidents involving the transcript delivery system, where transcripts were sent to an incorrect third party.
- Hardcopy documents disclosed in-person increased by 65% and generally involved false documents handed to a clientele or third party.

Table 13

Hardcopy Incident Locations

Consolidated Location	Disclosure		Loss		Theft		FY Totals		Grand Total	% Change
	FY 11	FY 12	FY 11	FY 12	FY 11	FY 12	FY 11	FY 12		
ABC Bank	142	130	1122	1130	44	11	1168	1161	329	-4%
Transcript delivery system	441	3140					441	3140	181	241%
Shipment	111	116	771	773			882	889	171	9%
In person	440	666					440	666	106	65%
Vehicle	11	12	76	7	116		823	818	41	-22%
Public transport	11		88	44	11		110	44	14	-60%
Hotel	22	2	22		11	1	25	10	5	-100%
Grand Total	11683	22122	2221	2224	222	117	11926	22363	4289	22.0%

Conformability

The concept of confirmability is a comparable concern to objectivity and refers to the degree, to which data can be confirmed or corroborated (Cope, 2014). There are

various techniques for improving confirmability such as an audit strategy, where the researcher checks and rechecks the transcription to ensure their accuracy. I shared the transcription with participants so that they can review and clarify if there were any discrepancies.

The Veterans Affairs Office of Inspector General reported a laptop and external hard drive containing the names, birth dates and social security numbers of about 26.5 million active-duty troops and veterans were stolen on May 3, 2006, from a veteran affairs data analyst in Aspen Hill. The theft was the largest information security breach in the history of the government and raised fears of potential mass identity theft. As a result, the Department of Veterans Affairs agreed to pay $20 million to current and former military personnel to settle a class action lawsuit on behalf of men and women, whose personal data was on the stolen laptop. Subsequently, I could conclude that cyber-incidents have severe impacts on data breaches due to human factors. From this assertion, I developed the *data breach triangulation blueprint* as shown in Figure 2.

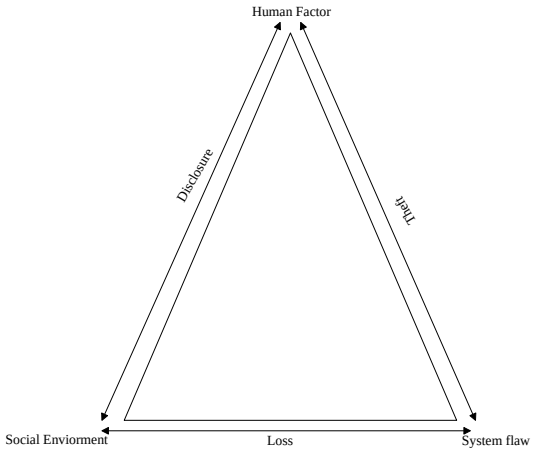

Figure 2. Data breach triangulation blueprint.

Ethical Procedures

The rules governing the access to information or data for researchers are not defined clearly on the international level. For example, mobile network providers are subject to different regulations on data retention depending on their location. Data retention laws are under debate because they conflict with the privacy requirements (Bloomberg, 2014). Meanwhile, privacy regulations are on a national level despite the international operations of mobile network providers. Data protection directive of the E.U. (95/46/EC), for example, only covered the E.U. citizens or within the E.U. territory (Gasson, Kosta, Royer, Meints, & Warwick, 2011).

Most African countries lack a locally binding legal framework to govern the release of data. Therefore, data release follows an ad hoc framework, in which the only binding commitment to privacy and data protection was made between researchers and the company through a non-disclosure oral agreement. The francophone, West Africa countries, use a version of strict data protection regulations from France established by the Commission Nationale Information et Liberte, although the implementation and enforcement are a problem due to social and cultural factors. In addition, Ivory Coast is not a signatory; hence, many companies operate with minimum or no data protection policy.

In most African countries, enforcement regarding the protection of data and citizen rights is weak, resulting in limited power for organizations to use and distribute data under their own patronages. In addition, data protection or retention is at the discretion of companies in Ivory Coast or other Africa countries. Thus, constraints from

the Ivory Coast regulator on privacy seemed to be minimal. Consequently, in most African countries, many people mentioned that signing a formal document outlining privacy and consent would not be necessary, and it would perhaps discourage potential participants in many African countries. The most recommended practice for a researcher was to build mutual trust with the participants by understanding and respecting their culture and social environment to conduct a successful research study because the participants preferred to remain anonymous and confidential. Ethical risks in international research are substantial, complex, and continue to grow, especially in developing countries like Ivory Coast and many West Africa countries. To ensure that the participants, populations, and communities were not harmed or exploited, I also followed the U.S. regulations, though it might increase risks, for example, around the informed consent, where the cultures were different from the U.S. The international research ethical risks are beyond the boundaries of the research oversight infrastructure of Walden University. Thus, risk mitigations must rely on thoughtful and informed judgments; otherwise, researchers may not pursue research in these areas or may not overcome ethical challenges in protecting human research participants in developing countries, especially in Africa, related to data breaches.

Summary

In summary, uniform solutions to prevent data breaches are difficult due to human-related factors. Despite the existence of the emerging technologies that could prevent data breaches, hackers still launch a significant number of attacks by exploiting the weaknesses in information systems of organizations or their employees. Therefore,

organizations require a strong leadership to upgrade technology frequently and to ensure that the internal human factors do not cause any data breaches. In this dissertation, I interviewed 27 participants, who had insights on how to develop solutions to prevent data breaches occurring due to internal employees in the Ivory Coast cyber-ecosystems. Hence, one-third of the interviews were focused on external data breaches, whereas two-thirds were on internal human factors data breaches. This chapter elaborated on the experimental design used in this study to collect data needed to address the research questions. The ANOVA test followed by the Tukey's post hoc test found that overcoming data breaches and internal human factors are essential to minimize the cyber-security threats. Chapter 4 provided an in-depth analysis of data collected in this study followed by Chapter 5.

Chapter 4: Results

Introduction

Several organizations and government entities continuously experience data breaches caused by external people or internal employees. Many organizations and government entities are aware of the risks that internal human factors might pose to the data security of a company. Historically, outsiders have carried out data breaches, costing hundreds of thousands of dollars (often millions more). However, traditional security measures could control outsider threats. In contrast, threats due to internal human factors, specifically accidental errors or deliberate acts, cause relatively more damages to an organization (PWC, 2015). Therefore, the purpose of this study was to provide executives with guidelines on the prevention of data breaches from cyber-threats by focusing on internal human behavior.

I used a qualitative mixed-methods approach to comprehensively capture user experience because it could be difficult to answer *why* and *how* with a quantitative study alone. I examined the assumed causal relationship between the internal human factors (i.e., employees behaviors), and the occurrence of data breaches or compromised information. Speicfically, I used this qualitative approach to identify the assumed root causes of threats from internal human factors. In addition, I used this approach to understand the perspectives of participants on how managers can minimize internal human factor threats that contribute to data breaches or compromised information.

The three research questions focused on *why*, *how many*, and *how widespread*. This chapter contains data analysis which I used to answer the following three research questions, where each RQ was categorized by subthemes:

RQ1: What are the internal human factors that contribute to data breaches and compromised information in the Ivory Coast emerging business environments?

RQ2: What are the root causes of the internal human factors that contribute to data breaches and compromised information in the Ivory Coast businesses?

RQ3: What preventative measures could managers use to minimize the threat from human factors, which are related to an internal employee, that contribute to data breaches or compromised information?

This chapter also contains evidence of trustworthiness, and descriptions of the setting, demographics, data collection timeline, and coding. The results section describes results based on the categorical findings and theoretical results. Finally, I revisit the conceptual framework for this study and discuss it alongside the phenomenal theory of internal human factors related to cyber-threats to organizations.

Study Setting

The study site was Abidjan, Ivory Coast, West Africa, between October 1 and November 3, 2017. I did not have any community partners; therefore, I liaised unofficially with some Ivorian community stakeholders, including the government officials and the heads of department in organizations in Abidjan, Ivory Coast to identify the prospective participants. I discussed the purpose of the research with these officials and emphasized the benefits of the outcomes of this research study to minimize the human factors of

employees that contribute to data breaches or compromised information. Then, I requested that officials distribute the research flyer to their employees to solicit their participation in the research study. Interested participants contacted me directly via phone to maintain their privacy and confidentiality.

Selection of Research Participants

The research participants consisted of government ministers, department heads, CFOs, branch managers, CIOs, IT division managers, and information systems technicians (see Table 14). I used the snowball sampling process for the target population to build purposely selected samples for this study. I started with unofficial visits to different organizations and requested that managers distribute the flyers to their employees as the population seed for the snowball sampling. With each visit, the size of the sample and snowball grew. I chose the next organization for the visit by logically assessing the potential for obtaining the perspectives that were beneficial to the study. Eventually, I sampled from five organizations and 50 employees. Although I received expressions of interest from 50 employees from five different public and private organizational structures within Abidjan, Ivory Coast, only 27 participants agreed to participate in the study. All participants read and signed the consent form in duplicates and retained a copy for personal record purposes before the research study began.

Table 14

Participant Description

Organization	Type	Number
Comp X&T	Government ministers	1
	CIOs	3
	IT division managers	2
Comp Z & C	Government ministers	2
	CFO	2
	Information systems technicians	3
Comp B & X	CIOs	2
	Government minister	1
Comp T & C	IT division managers	4
	Government ministers	1
Comp C & Z	Information systems technicians	4
	CFO	2

Demographic Data

I did not collect any specific demographic details such as age and race. The selected participants included both genders, including 20 men and 7 women. Most participants had the privilege to access accounts, whereas some participants had some level of elevated permissions in the computer system of organizations or supervised employees with such elevated permissions.

Survey, Questionnaire, and Interview Data Collection

The instrument used for this research consisted of surveys developed by Basu and Muylle (2011) and O'Keeffe, Buytaert, Brozovic, and Sinha (2016), a questionnaire, and interview scripts using semi-structured questions including open-ended questions and the Likert scale questions. These semi-structured questions were helpful for collecting descriptions of experiences related to creating IT business values, maximization and evaluation, and for understanding techniques to overcome data breaches due to human factors. Phenomenological studies include observation, note taking during the interviews, and field notes, which were essential to understanding the operative of internal human factor threats.

To ensure the privacy of the participants and their organizations, I assigned each participant a different alias such as Comp1 and Emp1 for five selected organizations. I conducted the survey for four days from October 3 to October 6, 2017. The participants completed 21 survey questions, including open-ended questions and questions with 1 to 4 scales ranging from *zero important* to *highly important*. On the fourth day, I collected the survey data by appointment only. Then, participants completed 21 questions from the

questionnaire from October 10 to October 13, 2017. Each participant had aliases, such as 4hjb5, k67rb, and w3ev1, to protect the identities. Data was collected by appointment only in a private hotel meeting room on the fourth days. Last, each participant answered 16 face-to-face interview questions. The interview comprised three parts with the first part focusing on the risks related to malicious insiders and unintentional insiders, while the second part focused on data access and responsibilities of employees using the 1 to 5 scales. The third part concentrated on the state of cyber-defense using the 1 to 5 scales. The interviews lasted between 15 minutes and 30 minutes, and took place in a private hotel meeting room between October 17 and October 19, 2017. Participant received aliases such as Ca45 to protect their identity.

I entered the collected data in a Microsoft Excel spreadsheet and reviewed their usability. The collected data were secured using logical (i.e., authorization, authentication, encryption, and password) and physical (i.e., restricted access and locked file cabinets) protections in Abidjan, Ivory Coast. I changed the key code and door-lock combinations regularly to prevent all physical access to data. I used data discovery tools to identify sensitive data that were inadequately protected. I used a safe and secure network IPSec protocol to protect research data while in transit over a public or private network. I also used different names from actual data while data was at rest. Lastly, I used SecureZip to protect all data on a laptop and encrypted USB. All research data will be kept for at least 5 years as required by Walden University before proper disposal.

Data Coding

The collected data were recorded in a Microsoft Excel spreadsheet according to their themes. Then, I used the statistical frequency and proportion to tabulate the categorical data and the corresponding codes are given in Appendix A. Discrepant cases did not emerge, possibly due to the nature of the study. The findings were factored into the analysis and data segments were inductively incorporated into a subcategory or category. Emergent themes expanded my understanding of the existing theoretical framework proposed by Loch et al. (1992). Furthermore, I shared the collected data, including the interview transcriptions, with the respective participants for validation and to protect their identity and privacy.

Evidence of Trustworthiness

The evidence of trustworthiness was evident from the research design, data collection, data analysis, and interpretation. Use of the grounded theory concept and a constant comparative method increased the validity of the study. The participants reviewed their responses to the survey, questionnaire and interview for clarity along with the subthemes, core categories, and theoretical findings after completion of the study, contributing to the trustworthiness of the study. Participants had multiple opportunities to review data and clarify or correct whenever required.

Further, the purpose of a qualitative research is not to generalize findings, rather, it is to understand a phenomenon (Corbin & Strauss, 2008, p. 319). Therefore, it is difficult to generalize the results of this study to other organizations. However, the concepts, including core categories and theoretical conceptualizations and models

emerged from this study, could be considered by other organizations. The knowledge gained could be applied to other organizations, at least after a critical review, despite the potential differences between workplace environments. Corbin and Strauss (2008) stated that "concepts should apply to many organizations, though specifics might differ" (p. 320).

Coding is primarily an analytical process and several past studies have provided guidelines for coding. For example, Miles and Huberman (1994) stated that emergent themes should be linked to a theoretical model (pp. 134-137). Models are the simplification of reality; hence, investigator and peers should determine the degree that a model describes the event and perform proper validation of the models (Denzin & Lincoln, 2003, p. 278). Denzin and Lincoln (2003, p. 278) discussed that the grounded theory models generally should be validated using the experts. In this study, there were no informants and the subject matter experts were the participants. Therefore, the theoretical models were developed and shared through the constant comparative process, as if they were mainly a quasi-peer review.

Results

The results of this study are divided into the following three subsections according to the themes:

- Internal human factors that contribute to data breaches.
- Root causes of internal human factors that contribute to data breaches.
- Preventive measures to minimize the internal human factors that contribute to data breaches.

Many researchers have adapted the human information processing models to illustrate the errors of individuals at different stages of a business. Conzola and Wogalter (2001) discussed the impacts of incentives from the environment on the human sensory system using the communication-human information processing model and the findings are still relevant. A subset of information is attended to, comprehended, and aligned (or misaligned) with attitudes, beliefs, and motivations of an individual, resulting in the behavioral responses. With the increase in new connected devices, many new and unknown security threats have emerged from megatrends and technologies such as BYOD, mobility, cloud computing and internet usage, as well as internal accidental and malicious actions, introducing organizations to a multitude of new risks contributing to data breaches.

Research Question 1

Many documented data breaches were accidental due to unintentional employee behaviors. Human errors often are patterns of recurrence when examined over time. Information breaches due to internal human factors are caused by individuals, who seek to damage organizations or undermine information security due to various causes. Instead, the human errors causing negative impacts are often the consequences of ineffective system conditions, process features, or individual employee characteristics, and are known as the system induced human errors (Norman, 2013). The insider threats continue to be mostly accidental and carelessness. A holistic approach to identifying the internal human factors responsible for data breaches and compromised information in Ivory Coast is essential to protect the landscape of Ivory Coast cyber-ecosystem.

Internal Security Challenges and Recommendations

Unintentional exposure of organizations to risks due to the actions of some employees could damage organizations. Eighteen participants commented that many employees in Ivory Coast engage in behaviors that could put the corporate and personal data at risk. Eleven participants mentioned that top managers generally do not allocate proper resources for IT-related projects, whereas five participants stated that IT professionals are often unaware of the behaviors of employees and that it is a business-wide challenge to prevent data leakage or breaches due to lack of funds. According to 15 participants (56%), the most prominent internal challenges for most security professionals are errors of employees, ineffective security deployment and managing hostile behaviors. Endsley (1995) called the above challenges as the situation awareness and defined as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (p.36). Furthermore, 14 participants (52%) agreed that implementing adequate security measures and controls are critical to overcoming the internal security challenges. Seventy percent of the participants indicated that executives could achieve the maximum returns in business if they have a good knowledge and understanding of emerging global business and technology requirements with the IoT. They also commented that providing continuous exposure and training to IT managers on the business and technical skills could maximize the return from the IT investment, which agrees with the view of Rodgers (2000) that the effective decision making to reduce error rates generally depends on having a good situation awareness. However, resolving

internal security challenges is inefficient if an organization does not address workplace violence with adequate mitigation plans.

Workplace Violence Impact on Data

The definition of workplace violence is the unsafe climate and job environment for employees and the survival of an organization. Twenty-six participants (96%) said avoiding the ethnic discrimination and detecting the unhappy employees could reduce workplace violence on data or information of an organization. Thus, 14 respondents (52%) indicated that an organization should have security guards to protect itself both inside and outside of its perimeters. In addition, 12 of them suggested that the workplace crisis team should assist or investigate any issues related to workplace violence with a zero-tolerance policy. Having workplace violence mitigation and dissuasion plans could allow organizations to operate in a safer environment and diminish some insider accidental threats.

Insider Accidental Threats: Causes and Mitigations

Although external actors are considered as the biggest threat to cyber-security of an organization, many documented data breaches are due to various unintentional behaviors of employees (Sarabi, Naghizadeh, Liu & Liu, 2016). Accidents due to human errors often form patterns of recurrence when examined over time (Pond, 2003). As Julius Caesar said to Brutus, *Et tu, Brute?*, which means *Even you, Brutus, my best friend,* when Caesar resigned himself to his fate. Therefore, it is critical to identify the root causes of insider accidental threats and their mitigation to avoid the Caesar fate within organizations. Additionally, human factors and performance indicators such as

high subjective mental workload, lack or loss of situation awareness, and mind wandering could increase the likelihood of human errors, resulting in incidents related to internal systems, data, or information (Martin & Jones, 1984). The results of this study indicated that 19 participants (71%) attributed the insider accidental threats to human failures trusted employees and lax cultural environments.

Human inadequacies resulted in costly accidents by insiders with access to the most sensitive information. To mitigate insider accidental threats, 14 respondents (52%) recommended developing a security culture from top to down and setting up automatic alerts for sensitive devices at risk. Furthermore, 18 respondents (67%) mentioned that malicious employees, unzipped sensitive data, and untrained employees are the leading causes of insider deliberate threats. Additionally, 13 participants (48%) suggested that implementing employee training to identify the risks accurately and improving overall security posture could reduce insider deliberate threats. Furthermore, 15 participants (55%) said that an organization should provide an effective phishing detection and information security training, whereas 14 participants accounting for 52% suggested security+ and network+ certifications as additional training.

Precautionary Measures to Minimize Insider Threats

The new components during expansion of IT infrastructure of an organization could introduce new vulnerabilities, whereas not all employees understand rapidly changing IT environment (Sarabi et al., 2016). Consequently, companies are exposed to internal threats from employees. According to 18 participants (67%), ineffective software patching, management, password sharing and recycling, and absence of

encryption are the security issues faced by many organizations. Furthermore, 21 participants (78%) stated that managers could develop a culture of security solution, security awareness, and computer login limitations to change employee attitudes to minimize insider threats. Attitudes do not have any significance unless people choose vector, namely positive, negative, or neutral, which define eventually the outcomes of the human existential environment at work or in society.

There are greater concerns when dealing with internal security threats. Twenty-two participants (82%) attributed internal security threats challenges to ethnic factors, organizational culture, and non-malicious insiders. The participants agreed that attitudes are learned behaviors, habits, perceptions, and judgments. Therefore, understanding insider threats is essential for managers to develop multiple approaches to reduce insider threats. Thereafter, managers determine to adopt or keep the mitigation methods within an organization to combat insider threats. Developing a positive business attitude helps employees to take initiative to improve their skills by voluntarily enrolling in more security courses to be more efficient in their security management responsibilities. Most participants tried to take more security courses to fill the knowledge gap and understand the business better to realize the maximum benefits from IT investments (Table 15).

Table 15

Security Management Responsibilities

Security element	Preferred selected topics	Results
Security management	Operations security/Cyber- security trends	89%
	Effective security awareness	85%
Personal security	Conducting effective security self-inspection	81%
	Employee internet access security	85%
Information systems security	Fundamentals of information security systems	85%
	Protecting business operations	85%
Global security issues	Critical infrastructure threats	78%
Information security	Mobile device security risks	93%
	Identity theft techniques	89%
Physical security	Disaster planning	81%
	Protecting information from physical threats	78%
Professional development	Communicating security risks to senior managers	78%
	Proving value as a security professional	70%

Training and awareness programs should focus on enhancing employee skills and behaviors, and help them to identify possible cognitive biases and limitations that could lead to a higher risk of committing such errors or judgment. Additionally, the participants mentioned that the positive attitude of an organization could help employees to fulfill their roles and responsibilities effectively and to have a comfortable work life. It is important for employees to combine positive thinking and attitude, which are the core of success and a brighter future in life and at work. Therefore, the benefits of having

adequate training and awareness programs are diverse and important for a better relationship between organizations and employees.

Security Awareness Training

Employees are the critical human component for information security of an organization and the awareness program provides employees with tools and information that they require to make the security as the second nature. Twenty participants (74%) were interested in participating in continuous security awareness training programs and preferred to extend security awareness training workshops to developing the effective security procedures, policies and a technology control plan. Moreover, 21 participants (78%) emphasized that organizations should include user behavioral analysis, data protection, and mobile device management to minimize data breaches by overcoming internal threats. Furthermore, 25 participants (93%) identified the location as the predominant factor that determines their participation in security awareness training, while the registration fee was a concern for 23 respondents (85%). According to them, examining and analyzing insider threats is a common practice in developing the characteristics of the most critical incidents in the form of a general set of models such as management and education of the risk of insider threat (MERIT) models. The models identify common patterns, contributing factors and observables, and mitigation measures targeting effective training topics due to the employee feedback. Improved understanding of employees about the impacts of computing behavior on the security of the company could lead to positive results for the company. However, the

overconfidence of companies and institutions in their labor force could make them vulnerable to malicious employees (Appendix A).

Research Question 2

Twenty-seven participants thought that internal human factor threats are difficult to prevent because generally, they are unintentional. Therefore, a holistic approach to security is vital in the modern threat landscape to combat the risks due to unintentional or malicious intents. The approach should address effectively insider and outsider threats together with successful management of both unintentional and intentional threats posed by internal human factor threats (employees).

Organizations Incident Types

Their betrayals of employees through corporate espionage, embezzlement, data theft, or double-crossing damage many organizations profoundly. Trusted insiders of organizations could have the power and the will to damage the organization. After the infamous National Security Agency data leaks and various well-publicized thefts of corporate resources, including the intellectual property, customer lists, or money, executives have focused on developing the best approach to protect their information assets from malicious insiders and to detect potentially problematic employees beforehand.

Employees often have access to the most sensitive information. Six participants (21%) mentioned that the most successful security attacks by employees are the exposure of sensitive data, theft of intellectual property and the introduction of malware. Additionally, 13 participants (48%) indicated that disclosure of sensitive data, loss or

theft of IT Assets and malicious codes are the leading incident types within their organizations. According to 17 participants (63%), most incidents happened after work hours with 37% of incidents occurred in cars when employees were in transit to home with IT assets, 30% were because employees left assets unattended on their desks or not secured in office, whereas 22% of them happened in a hotel when traveling.

Nineteen participants said that 63% of assets were lost, whereas 37% were stolen from the locked areas. Meanwhile, 56% were not in locked areas and 19% were unknown. Interestingly, 48% of the stolen assets did not show any signs of forced entry and 33% of them occurred by the forced entry. X, Z, B, T and C facilities, office desks, cabinets, and storage room share 85% of the lost or stolen assets. Further, 17 participants (62%) mentioned that the stolen assets were in the unsecure places, whereas 23% of these incidents were unknown and only 15% were locked in secure areas. Meanwhile, assets of organizations were lost or stolen from 78% of interiors and 22% of trunks of the vehicles. The participants indicated that 48% of the lost assets were laptops or phones and 18 participants (67%) confirmed that these laptops and mobile devices did not have any enterprise disk encryption, whereas 63% of them did not have any cable locks. Twenty-three research participants (87%) agreed that most IT security threats are due to the unintentional mistakes of the insiders than any malicious abuse of privileges.

Disclosure of Sensitive Data

Sending the sensitive documents to unintended recipients is a primary insider error. According to 14 participants (52%), the sensitive data were disclosed due to the errors in faxing, lost packages and the errors in emailing. Companies notified the local

mail coordinator in 48% of the disclosure cases, whereas 37% did not. Moreover, 22% of incidents were unable to trace. Furthermore, 63% of these incidents occurred with the local post office and 37% with the internal mail delivery. Access to data, even highly sensitive data, is difficult for many organizations to manage because of the changing business environments and the complexities of the modern workforce. Most companies in Ivory Coast did not appear to have any data protection or there was no enforcement if they did.

Data Protection

Most companies in Ivory Coast did not appear to have the SBU data protection. Twenty-one participants (78%) pointed out the non-existence of data protection laws or the laws did not consider the social cyber-threat. Furthermore, 74% of the companies did not have an internal review code to protect their data. Because the cyber-threat landscape is evolving continuously, the most sophisticated threats are constantly changing to adapt to the defenses against them, especially with the access to increased mobile devices and changing business environments.

Internal Risk Factors

The insider threats are intense because of increased mobile and hyper-connected world. Almost every employee has the multiple interconnected devices that could compromise information of a company. Similarly, the social norms are shifting, eroding loyalty between employers and employees (Coburn et al., 2018). According to the participants, the internal risk factors are due to 26% of careless or negligent, 22% of inadvertent exposure, 19% of email accidents, 11% of BYOD, and 7% of curiosity,

innocent actions, and malicious insiders. Furthermore, 27 respondents stated the following:

- security softie (weak) - 30%;
- Non-enforcement of the security policy – 26%;
- gadget geek (overly knowledgeable of business assets) - 19%;
- business work environments - 15%; and
- Saboteur (deliberate destruction of company data or assets) and squatter (intruder accessing organization data without right or title) – 10%.

Most participants said that increased data breaches could be primarily due to the internal threats. The risk factor threats of employees could be a major threat to businesses in Africa. Efforts to mitigate the internal threats, such as additional security controls and improved vetting of new employees, could remain at odds with the efficiency measures. More internal human factor threats with malicious intent could emerge as more employees in Ivory Coast place their ethics, ethnic groups and perceptions above those of their employers (Appendix A).

Research Question 3

Twenty-three participants identified several internal human factors threats related to data leakage, for example, fraudulent actions through an integrity breach, loss of availability, or business continuity because of the mistakes or deliberate actions. In general, internal threats could cause significant impacts on business because of the privileges that employees have over IT, being responsible for their actions, in contradiction to external threats.

Dealing with Insiders Risks

Twenty-seven participants said that management of insider risks should consider malicious, negligence and accidental risky behaviors. Once the risk is identified and assessed, executives should implement the technical and management controls and align the roles, responsibilities, and privileges throughout the employment life cycle. They also indicated that many executives in organizations in Abidjan, Ivory Coast are not aware of the complexity and unfamiliarity of the new cyber-security threats, and do not have the expertise to deal with the internal human errors.

Security Measures to Reduce Internal Human Errors

Seventeen participants mentioned that human error is not defined comprehensively in the academic literature because the errors could occur in cognition and behaviors. Features of the tools, tasks, and operating environment could have an influence on human errors (Dekker, 2002). In this study, I defined human error as a failure. Furthermore, the participants indicated that managers should consider the business environments to reduce the internal human errors, especially in Africa, where employees are more loyal to their ethnic groups than organizations. Therefore, they argued that managers should focus on implementing adequate security measures to mitigate internal human errors. Figure 3 shows the percentages of the security measures used to reduce the internal human errors. Appendix A Part I has additional information.

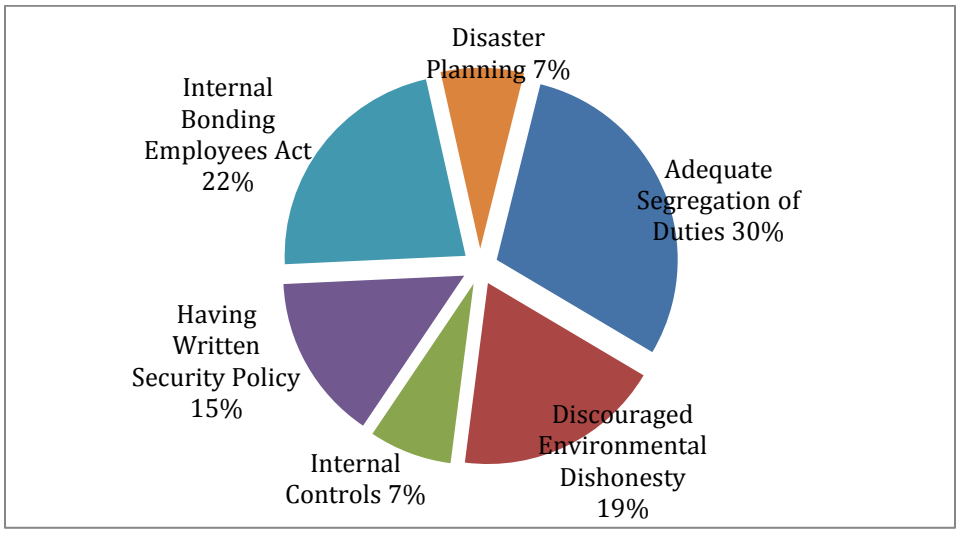

Figure 3. Reducing internal human errors.

The participants underscored that the above security measures could mitigate the internal human factor threats. Because employees have access to sensitive information on a regular basis and are aware of the protection, they could steal or leak information easier than outsiders. Employees could leak data accidentally by attaching the wrong file to an email, sharing on social media, losing a laptop or USB drive, or through some other mistake, which an outsider typically could not do. Furthermore, these security measures could help managers to overcome several essential malicious insider threats, including fraud, intellectual property theft, sabotage, and espionage. In this research, the participants identified the critical factors that characterized the different type of insider threats. Twenty participants (74%) thought that managers should implement the following efficient security solutions to reduce internal malicious risks:

- a process to identify assets and vulnerabilities;
- identify the likely attack methods;

- identify all privileged accounts and credentials;
- establish proactive and reactive strategies; and
- No Windows power user groups.

Similarly, 23 participants (85%) suggested that it is important for managers to implement the following security solutions to reduce unintentional employee risks:

- multifactor authentication;
- employees controls;
- risk assessment;
- password management system;
- BYOD policy;
- security controls; and
- security policies.

The participants also emphasized that managers should secure data in the following breakdown structures due to the internal data breaches:

- track sensitive data – 30%;
- qualitative risk analysis approach – 26%;
- information classification - 19%;
- computer ethics - 15%; and
- quantitative risk analysis approach - 10%.

Some sensitive information requires special care and handling because the inappropriate handling of data could result in data breaches.

Sensitive Data Dwelling

Data and applications reside on the network, endpoints, and in the continually evolving cloud ecosystem. Seven participants (25%) admitted that most sensitive data are not in a secure store in most organizations. However, the Ivory Coast businesses are entering into the global market with the IoT. As a result, it is important for these organizations to secure a multitude of applications, users, devices, and infrastructures. Twenty-seven participants said that the traditional methods are common in most organizations to store sensitive data in Ivory Coast and the use of encryption to secure data regardless of their storage formats according to the following breakdown:

- floppy disk - 26%;
- flash drive - 22%;
- CD - 19%;
- hardcopy - 15%;
- Windows 2003 server - 11%; and
- data discovery - 7%.

Having improper data storage and protection could lead to the breach of data privacy and the security of the confidential personal information. Additionally, improper data storage could create a significant data cost.

Reducing Big Data Cost

The Ivory Coast businesses had the need to reduce the cost of expensive data protections according to 27 participants. Eighteen participants (66%) expressed the need for reducing data protection cost in the following order:

- move complete or partial data to the cloud;
- implement data variable length deduplication, which is a technique to delete duplicate data; and
- archive data.

Moreover, 18 participants (66%) indicated that reducing data protection cost could help organizations to meet the audit compliance requirements, which can be achieved if managers is:

- being sensitive to changes in their industry;
- keeping compliance data and documentation secure;
- paying attention to legacy IT systems;
- having a disaster preparation readiness plan;
- bringing known flaws to the forefront; and
- knowing employees with access to data, applications, and systems, when, why and what.

Data Access and Responsibilities of Employees

Most participants expressed a significant concern about the access to data because data access tended to be unstructured in many organizations. They also stressed that managers should not focus solely on the perimeter security, leaving the enterprise data being vulnerable to insider threats. Organizations could rely on the static security perimeters to protect the onsite data centers; however, this is not a viable strategy due to the growing reliance on mobile and IoT devices as well as new threat types.

The employee threats could range from accessing data without proper authorization or downloading unauthorized software without understanding the potential risks. According to 13 participants (48%), they often had the access to data, whereas five (19%) had somewhat often and three (11%) had somewhat very often, regardless of their roles and responsibilities. Moreover, 14 participants (52%) mentioned that information security is only the responsibilities of IT. In contrast, only five participants (19%) said it is the responsibilities of all employees. It is worthy to note that most organizations in Ivory Coast did not have any internal data policies according to 15 participants (56%), whereas 14 participants (52%) mentioned that data protection enforcement significantly lacks within most organizations in Ivory Coast. Two-thirds of participants agreed that data security is not the responsibility of everyone in the organization, whereas the rest, mostly CIO, IT managers and technicians, thought that everyone should protect the sensitive information and data for the survival of organization (Appendix A Part II for more information). Unfortunately, many organizations do not identify new vulnerabilities quickly, especially in West Africa. This is compounded by the anytime, anyplace, anywhere nature of accessing business data, everywhere from inside the network to application layers and mobile devices.

Cyber-Defense

Twenty-seven participants mentioned that several organizations and government entities were in the news lately across the globe due to data breaches caused by external people or internal employees. They stated that many organizations need to implement security best practices and programs best suited to mitigate internal security threats. To

effectively mitigate security threats, managers should know the state of their cyber-defense before implementing any security measures.

Cyber-Defense State

Increased access to data of organizations on mobile devices and the use of cloud-based services create new vulnerabilities together with IoT. The participants from five different organizations had mixed perceptions of security threats and the measures used to counter them. Sixteen participants (59%) indicated that existing security systems in Ivory Coast could not capture cyber-security threats sometimes. Therefore, 24 participants (88%) were unsure whether organizations could prevail from advance cyber-attacks or stop insiders from stealing corporate information. However, 12 participants (44%) strongly agreed that many businesses in Ivory Coast would not survive.

However, 15 participants (56%) agreed that organizations could implement a strong security program to withstand the targeted insider attacks. However, 11 respondents (41%) were of the opinion that the monitoring sensitive data is a challenge in Africa, especially in the Ivory Coast (Figure 4). Employees of many organizations in Ivory Coast are affiliated and loyal to their ethnic groups, regardless of the policies or security measures of an organization. Therefore, it appeared that almost anyone could have the access to sensitive data of an organization without any bona fide need by being a member of an ethnic group (Appendix A Part III for more information).

Eight participants highlighted that executives should develop a holistic approach to cyber-defense and develop a culture of data security. Furthermore, they also stressed that effective data protection must encompass end-to-end encryption solutions for

endpoint devices, databases, networks, and applications (Refer to Appendix A for more information).

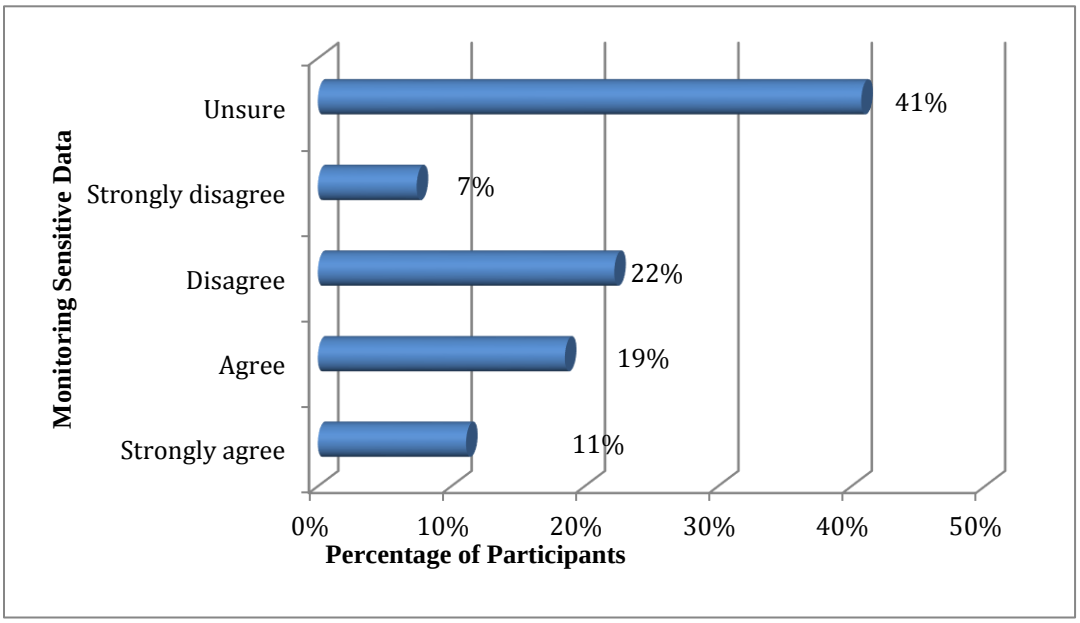

Figure 4. Monitoring sensitive data.

Summary

According to the results of this study, managers should consider information security in a broader organizational context of mission or business success. With the global market economy and interconnectivity, the support of the executive managers seemed to be lacking in addressing emerging threats with internal human factors. An organization could not achieve the missions and business success without addressing the internal human factor threats in the global market economy with the IoT. The human factor threats are likely to increase in the coming years and could be a significant threat to organizations. Efforts to reduce these threats, such as additional security controls and improved vetting of new employees, could remain at odds with the efficiency measures.

More insiders with malicious intent could emerge because the increased number of employees prioritize their own ethics and perceptions over those of the employers.

The dysfunction among the workforce is a challenge to mitigate the internal human factor threats. The commitment of managers to create cyber-security awareness and training programs could have a critical impact on the perception of the staff about responsibilities in relation to securing organization information systems and maintaining safe cyber-environments. Recognizing the importance of managing security risks and establishing appropriate governance structures for managing such risk are critical for organizations in Ivory Coast. Chapter 5 contains the interpretation of the findings, a discussion of research limitations, recommendations for further research, and the implications for social change.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

The purpose of this study was to provide executives with a framework to guide them in deciding how to prevent data breaches from cyber-threats by focusing on internal human behavior. The interconnected world with its network communications has changed the ways people do business with the IOT, leading to increased cyber-attacks on information and data of organizations. Security practitioners have proposed many conceptual frameworks, including the state-based approach (Ammann et al., 2002) and the host-based approach (Ammann et al., 2005), to reduce the unauthorized access to data and thereby to mitigate cyber-attacks. These conceptual frameworks are useful for understanding the behaviors of cyber-attackers and preventing any possible attacks. Specially, the host-based approach allows an organization to monitor its network and discover vulnerabilities in the broadband access network. Additionally, it enables an organization to have a clear view of its measurement performance metrics to establish the service level agreements for providing guaranteed and business class services.

Sheyner et al. (2002) recommended the Boolean minimization approach to permit managers to have an in-depth understanding of the risk management methodology to identify the likely attack path based on attack surface measures. Consequently, the British Standard BS 7799, the International Standards Organization 17799 (ISO 17799), generally accepted information security principles (GAISP), system security engineering capability maturity model (SSE-CMM), and the standard of good practice for information security have stipulated the best security practices for the stakeholders of all

organizations. The objective of these security best practices is to guide an organization to protect assets from internal human factor threats and outsider threats. Additionally, FISMA and NIST have recommended mandatory security controls to reduce epidemic data breaches or systems attacks.

Furthermore, other security practitioners such as Swain and Guttman (1983) have emphasized that human errors could be a result of organizational conditions, including work layout, poor environmental conditions, insufficient human engineering design, inadequate training and job aids, and inadequate supervision. Other researchers such as Perrow (1984), Roberts (1990), Sagan (1994), and Pauchant and Mitroff (1992) indicated that organizational culture has an impact on human errors. Although these authors called attention to these issues decades ago, it is interesting that their findings are still relevant today. In Chapter 4, the study results showed the impacts of internal human factor threats on data breaches, underscoring the theoretical foundation of the primary research theory. The Swiss cheese model focuses on hidden failures within the causal sequence of events. This model is a theoretical framework and is not a prescriptive investigation technique with some application to a real-world problem. The study results showed that top managers and IT managers should identify the problems, their magnitude, and their importance to detect and correct before an accident (Wiegmann & Shappell, 1997). These findings should help managers implement security measures to reduce internal human factor threats.

Interpretation of Findings

Managers should monitor their information systems and data vigilantly because of changing work ethics, the mobility of employees, interconnected devices of employees, and perspective about corporate data. The truism "amateurs hack systems, while professionals hack people" has relevance as security technologies designed to stop hackers, spies, phishers, and frauds are compromised by human weaknesses, namely inattention, incompetence, and complacency. The study results revealed that the behaviors of employees are a key risk factor to compromised information assets (see Aytes & Connolly, 2003). Internal human factor threats are common in most organizations and could continue to be the case. For instance, 73% and 18% were outsiders and insiders, respectively, among 600 breaches analyzed in Verizon's (2013) data breach investigation report.

The latest report (Verizon, 2014) also revealed similar results, with 72% of breaches involving outsiders, whereas 25% were related to insiders. The limited commitment from top executives to ensure the availability of sufficient resources for organization-wide risk management programs contributed to internal human errors and factor threats. The IBM Cyber-Security Intelligence Index Report (2015) indicated that 55% of attacks were carried out by either malicious insiders or inadvertent actors and could have potential impacts on successfully executing organizational missions and business functions if senior leaders or executives are not committed to making risk management a fundamental mission. Most organizations appeared to address risk as a strategic capability and an enabler of missions and business functions across

organizations. As a result, they did not manage information security risk organization-wide to address the following essential elements:

- assignment of risk management responsibilities to top managers;
- ongoing recognition and understanding by top managers about information security risks to organizational operations and assets, individuals, other organizations, and the Nation;
- establishing and communicating organizational risk tolerance throughout the organization including the guidance about the impacts of tolerance on ongoing decision-making activities; and
- accountability by top managers for their risk management decisions and the implementation of effective and organization-wide risk management programs.

Thus, most top managers in Ivory Coast did not appear to have established a joint task force with security institutions because the existence of an organization is part of the IoT. Despite employees of many Ivorian organizations carrying mobile devices to their workplace, many organizations did not have any security measures to regulate the growing number of BYODs or understand internal human factors risk and mitigation as a part of their critical responsibilities. The behaviors of employees and managers are the key contributors to ensure the security of data and information systems and to prevent damage from malicious or unintentional attacks or data breaches (Banerjee et al., 1998). The absence of an effective ethical security climate could impact the ethical behavioral intention of employees in protecting an organization's data and systems.

Security Awareness

Inadequate security awareness training could prevent employees from transitioning from the most significant security risk to the greatest security asset. Thus, information security is predominantly about educating employees. Top managers should recognize that explicit and well-informed decisions are essential to balance benefits gained from the use of information systems with associated risks such as purposeful attacks, environmental disruptions, or human errors causing mission or business failures. Information security risk requires the best collective judgments of individuals and groups who are responsible for strategic planning, oversight, management, and day-to-day operations.

Hence, protection of assets from internal human factor threats is crucial for managers because the business survival of the IoT is data and information. Top managers did not seem to take actions to:

- motivate employees to follow policies and procedures,
- stop employees from opening suspicious email attachments,
- greatly minimizing the damage done in the event of an attack,
- prevent the weak link targeting from internal and external threats,
- avert damage from revenge hacking by disgruntled employees,
- ensure employees take password protection seriously, and
- maintain zero workplace violence.

A successful organization should focus on people, processes, and technology in a similar order. Technology provides automatic safeguards and processes; however,

managers should provide security awareness to end users because even organizations with strong security practices are vulnerable to human error (Soerjadibrata et al., 2010). Often, focus on the people is insufficient, but it is critical to raising awareness about their carelessness. Thus, technology and processes must be combined with employee education so employees are aware of threats and can guard against them. The safety of an organization relies on continuous education of employees about identifying suspicious communications and new possible risks.

Detect, Deny, and Disrupt Internal Attacks

Twenty-one of the participants mentioned that they are unsure if their organizations could withstand cyber-attacks because most organizations' managers did not know their assets, what to look for, how to detect and disrupt internal human factor threats. Further, the participants pointed out that full features of existing security systems have not been activated in the organization, that is, managers use only default settings or do not implement threat intelligence services. Most organizations did not have relevant data inventory or data were captured, retained, or shared correctly. Companies with outdated SIEM, firewalls, and endpoint protection did not have real-time correlation and fine-grained rules, which prevented from elevating the criticality of primary indicators. A mature IT security or IT operation department should build their defenses to address the betrayal or mistake by an insider and remain alert against external threats. Architecture and toolsets should be flexible and capable of looking inside and outside the organization to detect and mitigate threats to data security. In August 2015, the FBI reported that the loss due to the scam phishing business email was over $1.2 billion (FBI,

2015). Many organizations in Ivory coast did not seem to have proper security measures to combat in real time internal human factor threats or cyber-attacks.

Data Collection and Aggregation

Some practitioners such as Malathi and Baboo (2011) argued that it is critical for an organization to understand complex typology of data collection, retention, and aggregation across functional boundaries, product silos and organizational groups. The key consideration is the identification of the most valuable for an organization. However, twenty participants in this study mentioned that security and IT teams do not work in collaboration as business partners, leading to difficulty in identifying critical assets, developing baseline for appropriate assets use (i.e., applications, users, time of the day, and typical workloads), relevant indicators of an attack, and security. For example, an accounting database server could have sensitive data, communicate using specific ports and protocols, have a finite set of approved applications and users working within typical workdays, and occasional peaks such as end-of-month reporting. An attacker could attempt to exploit the SQL vulnerabilities in a database or operating system, which can be mitigated through countermeasures, such as application whitelisting, database activity monitoring, and network intrusion-based prevention. According to the results of this study, many companies do not document and baseline their assets for IT team to set alerts for and act on any unusual behavior. Despite growing threats with mobile devices in workplace, most IT teams do not have adequate number of skillful workers to identify the internal hosts attacks and have the visibility into the internal hosts as well as the correlation with unusual port or protocol combinations, for example, initiation of a

sudden communication by a database server over port 80 via FTP (IoA 2), which could be identified by a baseline profile. Similarly, the database server could communicate to a system in the DMZ (IoA 3), which could be the path for data theft; however, most organizations do not have the visibility for data breaches because they still use traditional unencrypted data storage methods.

Internal Human Factor Threats and Responsibility for Preventing Data Breaches

Internal human factor threats are considered generally as an organizational failure, that is, human resources, managers, executive officers, and IT departments are responsible in some way for actions of an insider. In some cases, IT department could be responsible for not detecting malicious activity due to incorrect implementation of technical tools, though the department is not empowered in some cases to detect and mitigate the activity due to maintaining confidentiality, integrity, and availability of IT systems. Malicious insider activities are typically driven by some ideological or psychological disagreements with the mission or values of the organization. However, detection of such situation is the responsibility of managers, not the IT department. Although outsiders are more likely to act maliciously with data of an organization, the source of the highest risk is generally employees.

External hackers are looking continuously for the weaknesses to exploit and the most significant vulnerability is the carelessness, ineffective security deployments or misguided actions by insiders. Employees could fall victims to phishing schemes or social engineering attacks, or they open unrecognized emails, or they access corporate systems while sitting in an internet café. The participants of this study revealed that data

protection applications are not up-to-date and the business continuity plans almost do not exist or at the highest risk of not working. Furthermore, the participants outlined that the following employee behaviors unknowingly created security risks in several ways and provided access to external sources to cause damage to the organization:

- carelessness with emails;
- negligence with mailings;
- password sharing and recycling;
- loss or theft of IT assets; and
- not using encryption.

Limitation of the Study

In this study, I did not investigate all organizations in Abidjan or any other organizations outside Abidjan, Ivory Coast. There were no community partners from Abidjan involved in this study. Additionally, there was the possibility that some participants provided diverse answers to survey, questionnaire and interview questions because of their cultural and ethnic differences. To minimize such risk, I provided the same set of questions to the experimental and control groups used in this study. Kahneman, Slovic and Tversky (2013) found that human tendencies and cognitive biases influence human behaviors.

Schneier (2008) discussed extensively various risks and the inability of humans to assess the magnitude of risks within an organization correctly. Furthermore, he studied human limitation in accessing risks and underlined the following five critical methods, through which people incorrectly assess the magnitude of risks:

- exaggerating spectacular and rare risks, whereas downplaying more common risks;
- experiencing difficulties in determining risks outside of their normal situation;
- underestimating risks under control and overestimating risks out of control;
- perceiving personal risks to be higher than anonymous risks; and
- overestimating risks that are the object of public discussion (CMU/SEI-2013-TN-022 | 13 2008).

Many of the factors associated with malicious insider crimes, particularly those relating to motivational factors, did not seem to play a role in unintentional insider threats (UIT) cases. Reactions to failure tend to focus on individual employee, who committed the error, instead of developing strategies to avoid it by examining work environment and systems (Dekker, 2002). Dekker (2002) divided a system into a proximal sharp end (including people, who are in direct contact with critical processes) and a distal blunt end (an organization that shapes, drives, and supports activities at sharp end). In addition to providing resources, blunt end creates constraints and pressures that can lead to errors at the sharp end.

Recommendations

Building a Culture of Trust

Executive managers in an organization must nurture a culture of trust between organization and insiders. Organizations with a high level of insider risks should expand their insider threat and security awareness programs. Additionally, technical and management controls should be placed in locations, where managers trust their insiders,

to assist them to perform trusted responsibilities without a problem. Furthermore, managers should foster a culture that makes an organization worthy of trust in return. Therefore, cultivating a culture of trust could help to mitigate cyber-threats because insider attacks or insider mistakes are not expected and often not detected. The former president of U.S., Ronald Reagan, said that "trust but verify" backgrounds and actions of your insiders before handing over digital keys to your systems. Thus, security measures are necessary to curtail data breaches and insider errors.

Minimizing Data Breaches and Human Factor Threats

The best approach is to implement different layers of security by conducting background checks, implementing a policy of least privilege, and regularly reviewing and revoking data access privilege. Furthermore, implementing role-based control for access to any critical data, ensuring the logging, and capturing successes and failures could be useful. Data loss prevention software could help businesses to filter the internet traffic, prevent critical data from being mailed offsite, and protect end-points from being used maliciously.

In contrast, a robust patch management strategy and a periodic vulnerability assessment could help to prevent the outside attackers in addition to different layers of security using anti-virus solutions, network behavior analysis, and log monitoring. Furthermore, it is important for an organization to avoid ad-hoc handling of sensitive information. Although top managers strives to secure their corporate applications and infrastructure, the porting of information from these protected environments in a distributed manner, using many other computing devices including laptops, phones,

cloud, and to devices outside of company's domain, could create the most significant threat to data security.

Top managers of organizations should establish and continuously improve their information security policies to address access, handling, communication, and storage of corporate information. Otherwise, productivity and morale of employees reduce. Despite credible risks posed by inside and outside threats to enterprises and organizations, human costs of insider threats are significant for managers to identify the potential source of threats and monitor their activities. Similarly, business costs of outside threats could result in closing down of a company.

Preventive Measures to Minimize Internal Employee Human Factor Threats

Management of an organization should be prepared to tackle emerging cyber-threats. Minimizing threats requires an understanding of the threat characteristics by the insiders such as employees or trusted third parties, resulting from the pressure after reorganizations or transfers and grievances. Additionally, external factors such as the status of a relationship, unexpected expenses or health-related issues could lead to the careless attitude among employees. The non-technical staff and contractors, such as lawyers, with some level of access to data, could be another source of unintentional insider threats for both business-to-business and business-to-customer companies. Thus, it is important to provide a proper training for staff on security practices, although it is difficult to train and control external contractors with the access to data or systems. Consequently, control of their access to data should be through software measures and contractual agreements. Monitoring insider threats are generally the primary

responsibility of the human resources department during the hiring process through various internal employee background checks, security, and IT teams. Security teams should use external cyber-activity monitoring tools to extract online activities such as posts, rants, and tweets that could indicate whether a threat is imminent. In general, cyber-criminals exploit credit cards or bank account of an organization, though they could extract information and use them in social engineering or other schemes.

The overall market costs due to compromised accounts or personal records are in the order of million dollars across the world with the significant reputational costs to the trusted organization, the identity of which has been used to trick employees because it is difficult to regain the trust of customers. Implementing proper security measures to prevent insider and outsider threats depend on the business model along with data collection and utilization to achieve the mission. In the case of insider threats, managing risks should extend across the malicious, negligence and accidental risky behaviors. Additionally, managers should:

- have a zero tolerance for workplace policy breach based on the Denise Brown McZinc group behaviors approach, that is, forming-storming-norming-performing. Four phases are necessary for the team to grow, face up to the challenges, tackle problems, find solutions, plan work and deliver results. Additionally, strong communication skills of the leaders could help to build trust and establish group collaboration among employees;
- be sensitive to changes in their industry;
- secure compliance data or documentation;

- pay attention to the legacy of IT systems;
- having a disaster preparation readiness plan;
- bring known flaws to forefront;
- Develop a proper identity and access management plan for data, applications, and systems;
- move data or partial data to the cloud;
- monitor sensitive data; and
- build cyber-defense.

Furthermore, managers should implement at least the following security measures to curtail growing cyber-attacks and prevent internal human factor threats:

- have a process to identify assets and vulnerabilities;
- identify likely attack methods;
- identify privileged accounts and credentials;
- established proactive and reactive strategies;
- have no Windows power user groups;
- multifactor authentication;
- employees controls;
- risk assessment;
- password management system;
- BYOD policy;
- security controls;
- security policies;

- have data variable length deduplication;
- deploy encryption in motion across all platforms; and
- use agile methodologies of development and operations, which is a collaboration between lines of business, development and IT operations.

The crucial next approach is to establish the tolerance for risk in the organization by identifying factors to measure such as life, health and safety, environmental protection, and intellectual property, and the degree of severity of an impact, that is, production loss or financial impact. Managers could articulate the impacts of a compromised device or component, information or systems environment by setting the tolerance levels. Consequently, managers could change the attitude of employees to the consequence-based approach from *What could happen?* and *What if something happens?* to *When something happens, how bad will it be?* The focus could move to mitigation controls to minimize the impacts. With continuous improvement to both network and endpoint security, these hybrid techniques are likely to increase. It is critical for organizations to ensure they have proper controls, audit, and protection to detect and trace insider threats.

Recommendations for Further Research

The following recommendations for further research could expand the understanding about cyber-threats to organizations:

- investigating factors contributing to careless acts and technical problems that lead to insider human errors together with the development of effective mitigation strategies;

- investigating ineffectiveness of leaders to build a culture of shared ownership for cyber-risks;
- investigating about setting up partnerships between public and private sectors and ensuring that the leadership engages and supports cyber-security programs;
- examining the role of managers in avoiding issues between the Ivory Coast ethnic groups and political groups that could lead to malicious attacks; and
- examining the data protection process used by organizations in Abidjan to minimize internal human errors.

Cyber-security continues to lag in Africa, resulting in delays in implementing a resilient cyber-security. Training and awareness programs have their limits and organizations could not eliminate human errors associated with risk perceptions and other cognitive or decision-making processes. A comprehensive mitigation strategy should include novel and effective automatic safeguards against human factor threats. Malicious insider threat and UIT have many common contributing factors in areas such as security practice, organizational processes, management practices, and security culture. However, they also have significant differences, for example, human errors play a significant role in UIT. Therefore, UIT mitigations should focus on strategies for improving productive work environments, healthy security cultures, and human factors that increase the usability and security of the system and decrease the likelihood of human errors.

Observable Reflection by the Researcher

Due to the interdependence in growing global digital economy, failure of one organization could affect many other organizations, especially with businesses becoming a part of the IoT. Because governments, enterprises, and other organizations are not restricted within a controlled perimeter in the current environment, they require a novel security strategy for integrated ecosystems. Many organizations in Ivory Coast do not protect themselves against growing threat of cyber-criminals. The methods used for daily business transactions have not evolved and still rely on outdated technology without any significant cyber-security protection. Consequently, many government and private industries are vulnerable to cyber-attack. Some Africans have little trust in governments, particularly on repressive or autocratic leadership, and said that officials spy on the citizens. Additionally, lack of information sharing due to ethnic and political divisions within private and public sectors significantly affects the fight against cyber-crimes.

The IoT could provide an increased accessibility to criminals to exploit naive users with limited experience with technology to introduce viruses and malware in government and business information systems. In Ivory Coast like other African countries, skills shortages and lack of education about potential cyber-threats are the primary reasons for the lack of protection against cyber-attacks. Ivory Coast government expects other donors to build their cyber-ecosystems instead of allocating funds for cyber-security defense. This passive attitude could be detrimental in the context of increasing cyber-attacks because internal homegrown solutions are effective in protecting

data and information systems. Therefore, the African governments initiate programs to develop their cyber-security defense reflecting their unique social environment.

Therefore, African countries should develop their protection solutions against cyber-threats internally rather than solely relying on outsiders. Additionally, the Ivory Coast government and private sectors must not launch their e-systems without guaranteeing security. Otherwise, e-systems for crucial national systems and infrastructure should be on a separate network through a secure network. In general, emails of many organizations are insecure, and criminal organization could exploit email to breach security quickly and easily. Therefore, it is critical to implement the use of secure sockets layer (SSL) certificates for the communications between simple mail transfer protocol (SMTP) servers and the public essential infrastructure (PKI) SSL/PKI certificates for SMTP server to client communications.

Implications

The primary implication of this study is that the identification of internal risk factors is the primary step to overcome internal human factors threats and data breaches in organizations. With the increasing use of mobile devices and laptops, management should have a clear visibility about internal network access (i.e., Internet and intranet) and IT assets. Employees, executives, suppliers, or partners of an organization are the common sources of data risks and problems due to the following reasons:

- Organizations allocate security and training budgets based on an inadequate understanding of business risks and compliance requirements of privacy laws,

trends and technologies, and therefore are poorly prepared to adequately safeguard data within their environment.

- Due to the lack of continuity between the roles and departments, data can pass through several people and it is difficult to track the activities of each individual, increasing the risk of data mishandling.
- Because most insider attacks are not reported, it is difficult to assess the effectiveness of certain third-party security measures. Additionally, it is unrealistic to expect anyone to make correct procurement or hiring decisions if he or she does not understand problem, risk, law, or technology.
- Training and awareness programs about privacy and digital diligence for every employee are critical to understanding the impacts of their role and actions on data and security. However, most training programs are inadequate across government and private organizations.

Potential Implications for Social Change

The results of this study could help top management to understand internal human factor threats and potential mitigation strategies to avoid data breaches. Additionally, knowledge generated in this study has extended cyber-security literature, especially in the Ivory Coast, where there was little information about the state of cyber-security. This study results also provide both categorical and theoretical knowledge that may be considered by academia, industry, government, and public at large. In the context of increasing data breaches and social scrutiny over data breaches, it is critical for

organizations to prevent every data breach because one data breach could impact millions of people.

Information security is a part of the strategic business security strategy of an organization. An attack on unprotected or poorly protected information systems could cause the loss of confidence in the institution and lower the stock price (Telang & Wattal, 2007). Overcoming internal human factor threats should focus on maintaining a productive data flow, work setting, work planning and control, and employee readiness. For example, implementing widely tested and implemented security best practices throughout the organization as stipulated by practitioners and government agencies such as NIST in the industry should impact internal human factor threats mitigation goals positively. Furthermore, educating managers and employees should mitigate data breaches and overcome internal human threats. The compilation of the results of this study could help to improve awareness of the leaders and employees of cyber-security threats (Table 16). Combining the vigilance of humans with advancements in technology could enable an organization to build many layers of protection to improve cyber-security risk management to achieve business objectives.

Table 16

Tactics to Educate Leaders of Organizations

Goal	Best Practice	Tactics
Explain the importance of the information security	Use stories/news headlines before metrics	Describe real-life and hypothetical security scenarios, show the business objectives related to information technology/system, and describe the positive and negative scenarios
	Draw every effort to business objectives	Show the corporate objectives, underline the support of IT for business projects and initiatives, and report security metrics
	Communicate with the board	Build a profile of each board member, consider their backgrounds when developing a presentation, and ask them questions about priorities, risk tolerance, and reputation
Know the technology touchpoints of the organization	Get involved in product development	Collaborate with marketing team to understand customer security expectations, with legal and compliance team to meet privacy requirements, and use DevOps development to streamline security reviews
	Map your digital ecosystem	Create blueprints of data flow, payments, and other customer engagement and integrate inventory with IoT, smart agents, mobile apps and other emerging technology.
	Anticipate the technical roadmap	Generate formal planning sessions with CTO, CDO, or other roles to develop the new systems, ask about the long-term

Goal	Best Practice	Tactics
Build the followers	Foster security champions	Implant security experts in lines of business (LOB)/identify LOB partners, use contacts to gather business intelligence and communicate priorities and maintain a security log connection with ongoing training and communication
	Prioritize culture over the process	Establish a sense of joint responsibility rather than the sets of rules, utilize existing culture and communication channels if possible, and highlight success stories more than losses and violations to boost the morale of the employees.
	Empower employees	Give employees opportunity in front of critical meetings and audiences and empower the employees to enforce rules comfortably without retribution

Conclusions

Increased use of computer and mobile devices together with the digitalization of businesses operations requires an informed and knowledgeable manager, who understands vulnerabilities and threats to data and information assets of the organization and develops strategies to overcome internal human factor threats to protect data and assets. Without strong security measures, a disgruntled employee could share data and information with a competitor because employees know the type and storage locations of sensitive data.

Because of the lack of understanding and training, some employees could provide access to digital intruders unintentionally. Additionally, the source of most data breaches is the insider of a company accidentally or intentionally. Breaches through a contractor or other service providers, for example, in the case of the Wyndham hotels, Target, and

the Home Depot breaches, are another common type of breaches. Therefore, it is essential to develop and continuously update a robust internal security policy to educate employees and mitigate risk. Although it is impossible to eliminate every threat, organizations could have protocols that could minimize the damage due to an internal data breach. Top managers should consider the resource tradeoffs that the time is taken to ensure a safe culture versus maximizing the output, creativity, speed, and worker satisfaction. Individuals do not consider risk consciously when facing high workloads and tight deadlines. Managers should focus on risk avoidance strategies, for example, proactive system designs versus reactive ones and negligence versus normal security and usability. In summary, the occurrence of an internal data breach threat factor without at least a negligent action by an insider is relatively rare.

The policies and controls dealing with a data breach, for example, the employee security training and organizational information security policy, fine-grained access controls, and comprehensive network monitoring could improve breach vulnerability. Top managers should be responsible for improving cyber-security because the global payment systems, private customer data, critical control systems, and core intellectual property are at risk. Managers have the responsibility to understand the security intelligence maturity level of their organizations based on their IT security and business risk posture. Additionally, managers should evaluate the appetite of organizations for risks based on their capabilities to mitigate and plan to close any potential security gaps. With proper application of new security technology and strong public-private partnerships, organizations could protect their information systems assets and could

become robust and resilient. However, poorly implemented IT security rules and procedures could hinder organizations from achieving the mission and could impact customer privacy adversely.

References

Adebayo, A. O. (2012). A foundation for breach data analysis. *Journal of Information Engineering and Applications*, *2*, 17-21. Retrieved from http://www.iiste.org/Journals/index.php/JIEA/article/view/1721

Ammann, P., Pamula, J., Ritchey, R., & Street, J. (2005). A host-based approach to network attack chaining analysis. *Proceedings of the 21st Annual Computer Security Applications Conference*. IEEE, Tucson, AZ. doi:10.1109/CSAC.2005.6

Ammann, P., Wijesekera, D., & Kaushik, S. (2002). Scalable graph-based network vulnerability analysis, *Proceedings of the 9th Conference on Computer and Communications Security*. ACM, Washington, DC. doi:10.1145/586110.586140

Applied Computer Security Associates (2013). Layered assurance workshop, *Proceedings of the Annual Computer Security Applications Conference*. Retrieved from https://www.acsac.org/2013/workshops/law/

Auray, N., & Kaminsky, D. (2007). The professionalization paths of hackers in IT security: The sociology of a divided identity. *Annales Des Télécommunications, 62*(11-12), 1312-1326. doi:10.1007/BF03253320

Aytes, K., & Connolly, T. (2003). A research model for investigating human behavior related to computer security. *Proceedings of the Americas Conference on Information Systems 2003*, 2028-2029. Retrieved from https://aisel.aisnet.org/cgi/viewcontent.cgi?referer=https://www.google.com.au/&httpsredir=1&article=1726&context=amcis2003

Banerjee, D., Cronan, T. P., & Jones, T.W. (1998). Modeling IT ethics: A study in situational ethics. *MIS Quarterly 22*(1), 31-60. doi:10.2307/249677

Basu, A., & Muylle, S. (2011). Assessing and enhancing e-business processes. *Electronic Commerce Research and Applications, 10*, 437-499. doi:10.1016/j.elerap.2010.12.001

Bentham, J. (1781). *An introduction to the principles of morals and legislation*. Kitchener, Ontario: Batoche Books.

Berghel, H. (2011). The state of the art in identity theft. *Advances in Computers, 83*, 1-50. doi:10.1016/B978-0-12-385510-7.00001-1

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum, 41*(5), 545-547. doi:10.1188/14.ONF.545-547

Center for Strategic and International Studies (2014). *Net losses: Estimating the global cost of cyber-crime economic impact*. Retrieved from http://csis.org/files/attachments/140609_rp_economic_impact_cyber-crime_report.pdf

Clapper, J. R. (2013). *Worldwide threat assessment of the US intelligence community*. Retrieved from http://www.intelligence.senate.gov/130312/clapper

Coburn, A.W., Daffron, J., Smith, A., Bordeau, J., Leverett, É., Sweeney, S., & Harvey, T. (2018). *Cyber-risk outlook*. Cambridge, England: Centre for Risk Studies, University of Cambridge.

Computer Security Institute (2013). *17TH Annual 20120/2013 computer crime and*

security survey. Retrieved from gatton.uky.edu/FACULTY/PAYNE/ACC324/CSISurvey2013.pdf

Conzola, V.C., & Wogalter, M.S. (2001). A communication–human information processing (C–HIP) approach to warning effectiveness in the workplace. *Journal of Risk Research*, *4*(4), 309-322. doi:10.1080/13669870110062712

Cope, D. G. (2014). *Methods and meanings: Credibility and trustworthiness of qualitative research*. Paper presented at the Oncology Nursing Forum. doi:10.1188/14.ONF.89-91

Corbin, J., & Strauss, A. (1990). *Basics of qualitative research*. Thousand Oaks, CA: Sage.

Corbin, J., & Strauss, A. (2008). *Basics of qualitative research*. Thousand Oaks, CA: Sage.

Cummings, A., Lewellen, T., McLntire, D., Moore, A. P., & Trzeciak, R. (2014). *Insider threat study: Illicit cyber-activity involving fraud in the U.S. financial services sector* (Report No. CMU/SEI-2014-SR-007). Retrieved from https://resources.sei.cmu.edu/asset_files/SpecialReport/2014_005_001_28137.pdf

Cyber-Security Organization (2013). 2013 Cyber-security watch: Organizations need more skilled cyber-professionals to stay secure. *CSO Magazine*. Retrieved from http://www.cert.org/archive/pdf/Cyber-SecuritySurvey2013.

Dekker, S. (2017). *The field guide to human error investigations*. Burlington, VT: Ashgate Publishing Company.

Durkheim, É. (1951). *Suicide, a study in sociology*. Glencoe, IL: The Free Press.

Dutta, A., & McCrohan, K. (2011). Management role in information security in cyber-economy. *California Management Review*, *45*(1), 67-87. doi:10.2307/41166154

Edge, K., Raines, R., Grimaila, M., & Baldwin, R. (2007). The use of attack and protection trees to analyze security for an online banking system. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*. doi:10.1109/HICSS.2007.558

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis. *Sage Open*, *4*(1), 107-115. doi:10.1177/2158244014522633

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, *37*(1), 32-64. doi:10.1518/001872095779049543

FBI (Federal Bureau of Investigation) (2015). *Business email compromise.* Retrieved from https://www.ic3.gov/media/2015/150827-1.aspx

Federal Information Security Management Act of 2002, 3, Pub.L.No.107-347 U.S. Cong. § 35-44 *et seq.* (2002).

Florence, M. L., & Swamydoss, D. (2011). Security issues in computer network architecture. *Journal of Global Research in Computer Science*, *2*(7), 153-156. Retrieved from http://www.jgrcs.info/index.php/jgrcs/article/view/42

Forcht, KA., Pierson, JK. & Bauman, BM. (1988). Developing awareness of computer ethics. *Proceedings of the ACM SIGCPR Conference on Management of Information Systems Personnel*, ACM: Maryland, USA.

Forrester (2011). *As enterprises look beyond auditing and monitoring: Look Beyond*

Native Database Auditing To Improve Security, Audit Visibility, And Real-Time Protection. Retrieved from http://public.dhe.ibm.com/common/ssi/ecm/en/niw03042usen/NIW03042USEN.PDF

Gasson, M. N., Kosta, E., Royer, D., Meints, M., & Warwick, K. (2011). Normality mining: Privacy implications of behavioral profiles drawn from GPS enabled mobile phones. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 41(2),* 251-261. doi:10.1109/TSMCC.2010.2071381

Geric, S., & Hutinski, Z. (2011). Information system security threats classifications. *Journal of Information and Organizational Sciences*, *31*(1), 51-61. Retrieved from https://hrcak.srce.hr/21445

Granadillo, G., Daniel, G., Mustapha, Y. B., Nabil, H., & Herve, D. (2012). An ontology-based model for SIEM environments, *Proceedings of the 7th International Conference in Global Security, Safety and Sustainability*, Springer, Greece.

Hair, J. H. (1995). *Multivariate data analysis*. New York, NY: Prentice Hall.

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher, 20*(4), 12-17. doi:10.7748/nr2013.03.20.4.12.e326

Hunteman, W. J., Evans, R., Brownstein, M., & Chapman, L. (2009). *Computer security plan development using an expert system* [Issue Brief LA UR 90 2260]. Retrieved from http://www.osti.gov/servlets/purl/7052277-ChbG3e/

IBM cyber-security intelligence index report. (2015). *Analysis of cyber-attack and*

incident data from IBM's worldwide security services operations. Retrieved from https://essextec.com/wp-content/uploads/2015/09/IBM-2015-CyberSecurity-Intelligence-Index_FULL-REPORT.pdf

Ingoldsby, T. (2009). Attack tree analysis. *Red Team Journal*. Retrieved from http://redteamjournal.com/2009/01/attack-tree-analysis

IOSCO (2013, July 16). *Cybercrime, Systemic Risk and Global Securities Markets*. Retrieved from http://www.world-exchanges.org/insight/reports/iosco-publishes-paper-cyber-crime-systemic-risk-and-global-securities-markets

ITRC (2014). *Data breach report*. Retrieved from https://www.idtheftcenter.org/images/breach/ITRC_Breach_Report_2014.pdf

Jajodia, S., Singhal, A., Islam, T., Long, T., & Atluri, L. V. (2008). An attack graph-based probabilistic security metric. *Proceedings of the 22nd Annual IDIP WG 11.3 Working Conference on Data and Application Security*, IFIP, London.

Jaquith, A. (2007). *Security metrics: Replacing fear, uncertainty, and doubt paperback*. New York, NY: Addison-Wesley.

Kahneman, D., Slovic, P., & Tversky, A. (2013). *Judgment under uncertainty: Heuristics and biases*. Cambridge, England: Cambridge University Press.

Kant, I. (1781). *The critique of pure reason*. Retrieved from http://www.gutenberg.org

KPMG (2013). *Cyber-crime: A growing challenge for governments* [Cyber- Vandalism]. Retrieved from https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cybercrime.pdf

KPMG (2012). *Data Loss Barometer-A global insight into loss and stolen information*. Retrieved from http://www.kpmg.com/uk/en/services/advisory/risk-consulting/pages/data-loss-barometer-2012.aspx

Krebs, B. (2011). *ATM skimmers: hacking the cash machine*. Retrieved from http://krebsonsecurity.com/tag/atm-skimmer

Loch, K. D., Carr, H. H., & Warkentin, M. E (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 15*(2), 173-186. doi:10.237/249574

Malathi, A., & Baboo, S. (2011). An enhanced algorithms to predict a future crime using data mining. *International Journal of Computer Applications*, *21*(1), 1-6. Retrieved from https://pdfs.semanticscholar.org/195a/247055cd1be24a4f27c607fc8c6a75a64f2f.pdf

Manadhata, J. W., Flynn, M., & McQueen, M. (2006). Measuring attack surfaces of two FTP daemons. *Proceedings of the 2nd ACM Workshop on Quality of Protection,* ACM, Virginia, USA. doi:10.1145/1179494.1179497

Martin, M., & Jones, G. V. (1984). Cognitive failures in everyday life. In J.E. Harris & P.E. Morris (Eds), *Everyday memory, actions and absent-mindedness* (pp.173-190). London: Academic Press.

McAfee (2014). *Data loss by the numbers*. Retrieved from http://www.mcafee.com/us/resources/white-papers/wp-data-loss-by-the-numbers.pdf

Mell, P., Scarfone, K., & Romanosky, S. (2007). *A complete guide to the common vulnerability scoring system version 2.0*. Retrieved from http://www.first.org/cvss/cvss-guide.pdf

Merriam, S.B. (1988). *Case study research in education: A qualitative approach*. San Francisco,CA: Jossey-Bass.

Microsoft Corporation (2012). *Microsoft complaint against Zeus botnet operators*. Retrieved from http://blogs.microsoft.com/blog/2012/07/02/microsoft-names-defendants-in-zeus-botnets-case-provides-new-evidence-to-fbi/

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook.* Thousand Oaks, CA: Sage.

Miller, D. P. & Swain, A. D. (1987). *Human error and human reliability.* New York, NY: John Wiley & Sons, Inc.

Morais, A., Cavalli, A., & Martins, E. (2011). A model-based attack injection approach for security validation. *Proceedings of the 4th International Conference on Security of Information and Networks,* ACM, Sydney, Australia. doi:10.1145/2070425.2070443

Munhall, P. L. (2013). *Nursing research*. Sudbury, MA: Jones & Bartlett Learning.

NAICS (North American Industry Classification System) (2012). *Industry groups by percent of breaches larger organizations*. Retrieved from http://www.naic.org/annual_report/index.htm

NIST SP (National Institute of Standards and Technology Special Publication) (2012). *Risk assessment code* (800-53 rev3). Retrieved from

http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

NIST SP (2013). *Guide for assessing the security controls in federal information system and organizations* (SP 800-53A Rev1). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

NIST SP (2013). *Security and privacy controls for federal information systems and organizations* (SP 800-53 rev4). Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-53r4

Norman, D. (2013). *The design of everyday things*. New York: MIT Press.

O'Keeffe, J., Buytaert, W., Mijic, A., Brozović, N., & Sinha, R. (2016). The use of semi-structured interviews for the characterization of farmer irrigation practices. *Hydrology and Earth System Sciences, 20*(5), 1911-1924. doi:10.5194/hess-20-1911-2016

Okolica, J. S., Peterson, G. L., & Mills, R. F. (2008). Using PLSI-U to detect insider threats by data mining e-mail. *International Journal of Security and Networks, 3*(2), 114-121. doi:10.1504/IJSN.2008.017224

Pardue, D. (2013). *Hacked: One year later millions of residents at risk for life after data stolen from Revenue Department,* Retrieved from http://www.postandcourier.com/article/20130831/PC16/130839853

Pauchant, T.C. & Mitroff, I.I. (1992). *Transforming the crisis-prone organization*. San Francisco, CA: Jossey & Bass.

Pefuegnot, D., Laurent, C. L., Aurelien, T., Thibault, T., Julien, I. C., & Louis, L. J.

(2011). A security mechanism to increase confidence in m-transactions. *Proceedings of the 6th International Conference on Risk and Security of Internet and Security Systems*, Timisoara, Romania. doi:10.1109/CRiSIS.2011.6061836

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. New York, NY: Wiley & Sons.

Pierce, A. (1967). The economic cycle and the social suicide rate. *American Sociological Review*, *32*(3), 457-462. doi:10.2307/2091092

Ponemon Institute LLC (2013). *The risk of insider fraud U.S. study of IT and business practitioners*. Retrieved from http://resources.idgenterprise.com/original/AST-0060004_Ponemon_2013_Insider_Fraud_Survey_Results.pdf

Ponemon Institute LLC (2013). *2013 Data breach attacks*. Retrieved from http://www.ponemon.org/data-security

Ponemon Institute LLC (2013). *2013 State of the endpoint*. Retrieved from http://www.ponemon.org/local/upload/file/2013%20State%20of%20Endpoint%20Security%20WP_FINAL4.pdf

PWC (PricewaterhouseCoopers) (2015). *Information security breaches survey 2015.* Retrieved from https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

PWC & CSO (2013). *2013 State of the cyber-crime survey*. Retrieved from http://www.pwc.com/us/en/press-releases/2013/cyber-crime-threats-continue.jhtml

Reason, J. (1990). *Human error*. Cambridge, England: Cambridge University Press.

Roberts, K.H. (1990). Some characteristics of one type of high-reliability organization. *Organization Science, 1(2),* 160-176. doi:10.1287/orsc.1.2.160

Sagan, S.D. (1994). Toward a political theory of organizational reliability. *Journal of Contingencies and Crisis Management, 2(4),* 228-240. doi:10.1111/j.1468-5973.1994.tb00048.x

Salve, A., Suraj, K., Rahul, P., & Harshad, D. (2011). Survey on 2 steps security for authentication in M-banking. *Control Theory and Informatics, 1*(1), 25-33. Retrieved from http://www.iiste.org/Journals/index.php/CTI/article/view/695/588

Sarabi, A., Naghizadeh, P., Liu, Y., & Liu, M. (2016). Risky business: Fine-grained data breach prediction using business profiles. *Journal of Cyber-security, 1*(1), 15-28. doi:10.1093/cybsec/tyw004

SC DOR (2013). South Carolina department of revenue data breach. Retrieved from http://www.sctax.org/security.htm

Schneier, B. (2008). *Schneier on security*. Indianapolis, IN: Wiley Publishing.

Scott, W. (2010). Cloud Security: Is it really an Issue for SMB's. *Computer Fraud & Security*, *2010*(10), 14-15. doi:10.1016/S13613723(10)70133-0

Senate Select Committee on Intelligence (1994). *An assessment of the Aldrich H. Ames espionage case and its implications for U.S. intelligence.* Retrieved from http://fas.org/irp/congress/1994_rpt/ssci_ames.htm

Sheyner, O., Haines, J. S., Jha, L. R., & Wing, J. M. (2002). Automated generation and analysis of attack graphs. *Proceedings of the IEEE Symposium on Security and Privacy,* IEEE, Berkeley, USA.

Soerjadibrata, I., Jakarta, S., & Wagiyati, S. (2010). Financial reporting system analysis on security Cinere Estate. *Computer Engineering and Intelligent Systems*, *2*(4), 136-148. Retrieved from https://media.neliti.com/media/publications/211952-none.pdf

Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information systems*, *13*(1), 380-427. Retrieved from http://aisel.aisnet.org/cais/vol13/iss1/24

Sujatha, R., & Arumugam, S. R. (2011). An analysis of text-based authentication using images in the banking system, *Computer Engineering and Intelligent Systems*, *2*, 136-148. Retrieved from http://www.iiste.org/Journals/index.php/CEIS/article/view/376/264

Swain, A., & Guttman, H. (1983). *Handbook of human reliability analysis with emphasis on nuclear power plant applications, US Nuclear Regulatory Commission Technical Report (NUREG/CR- 1278*). Washington, DC: Government Printing Office.

Symantec (2013). *Internet security threat report* (18). Retrieved from https://scm.symantec.com/resources/istr18_en.pdf

Talib, A. M., Rodziah, A., & Rusli, A. (2010). Security framework of cloud data storage based on multi agent system architecture: Semantic literature review. *Computer and Information Science*, *3*(4), 175-186. doi:10.5539/cis.v3n4p175

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software*

Engineering, 33, 544-557. doi:10.1109/TSE.2007.70712

Theoharidou, M., & Gritzalis, D. (2007). Common body of knowledge for information security. *IEEE Security & Privacy*, *5*(2), 64-67. doi:10.1109/MSP.2007.32

Thomas, E., & Magilvy, J. K. (2011). Qualitative rigor or research validity in qualitative research. *Journal for Specialists in Pediatric Nursing, 16*(2), 151-155. doi:10.1111/j.1744-6155.2011.00283.x

Trillo, R., Po, L., Ilarri, S., Bergamaschi, S., & Mena, E. (2011). Using semantic technique to access web data. *Information Systems*, *36*(2), 117-133. doi:10.1016/j.is.2010.06.008

U.S. Department of Justice (2011). *Two Wellington men in mail and aggravated identity theft ring*. Retrieved from http://www.justice.gov/usao/fls/PressReleases/110426-03.html

U.S. (Computer Emergency Readiness Team) (2018). *Cyber incidents worldwide*. Retrieved from https://www.us-cert.gov/ncas/alerts/AA18-284A

VA Office of Inspector General (2006). *Review of issues related to the loss of VA information involving the identity of millions of veterans* (06-02238-163). Washington, DC: Government Printing Office.

Verizon (2009). *2009 data breach investigations report*. Retrieved from http://www.verizonenterprise.com/resources/security/reports/2009_databreach_rp.pdf

Verizon (2013). *2013 data breach investigations report*. Retrieved from https://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-

2013_en_xg.pdf

Verizon (2014). *2014 data breach investigations report*. Retrieved from https://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf

Verizon (2015). *2015 data breach investigations report*. Retrieved from https://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf

Wamyil, M., & Mu'azu, M. (2008). Information Manager. *Information System, 6*(1), 16-24. Retrieved from http://ajol.info/index.php/tim/article/view/27226

Weisstein, E. W. (2008). *Time Series analysis*. Retrieved from http://mathworld.wolfram.com/TimeSeriesAnalysis.html

Wiegmann, D. A. & Shappell, S. A. (1997). Human factors analysis of post-accident data: applying theoretical taxonomies of human error. *International Journal of Aviation Psychology, 7(1),* 67-81. doi:10.1207/s15327108ijap0701_4

WIS (2017). *Internet world stats*. Retrieved from http://www.internetworldstats.com/stats.htm

WIS (2015). *Internet world stats*. Retrieved from http://www.internetworldstats.com/stats.htm

WIS (2014). *Internet world stats*. Retrieved from http://www.internetworldstats.com/stats.htm

Zetter, K. (2011). *Russian convicted of $9 million RBS worldpay hack avoids jail.* Retrieved from http://www.wired.com/2011/02/rbs-hacker-avoids-jail/

Appendix A: Survey

1. What are the biggest internal challenges facing you today as a security professional?

2. As an information system (IS) person what do you recommend overcoming these challenges?

3. How do you deal with workplace violence that may jeopardize organizations data or information?

4. What recommendations can you suggest to reduce workplace violence?

5. What are the root causes of insider accidental threats?

6. What recommendations would you like to suggest mitigating insider accidental threats that may compromise an organization's data?

7. What are the root causes of insider deliberate threat?

8. What recommendations would you like to suggest reducing insider deliberate threats that may compromise an organization's data?

9. What trainings do you think are more effective?

10. In what areas would you like further training to do your job more effectively?

11. In your opinion, what precautionary measures do you think management can use to minimize insider threats?

(12) Please indicate the degree of importance below (Highly important = 4, very important = 3, important = 2, and little important = 1) associated with the following topics in carrying out your security management responsibilities.

Security Management

National Industrial Security Program (NISP) Operating Manual (OM) implementation [ ]

National Industrial Security Program (NISP) Operating Manual (OM) Changes [ ]

Risk management strategies [ ]

Risk management best practices [ ]

Cyber-security threats [ ]

Cyber-security trends [ ]

Security Contingency Plan (SCP) vulnerability rating matrix [ ]

Need to know based access [ ]

Systems and Applications documentation [ ]

Operations security (OPSEC) [ ]

Cyber espionage [ ]

Security Contingency Plan (SCP) [ ]
Internal Security Contingency Plan (SCP) security policy [ ]

Insider threat program [ ]

Social engineering exploit techniques [ ]

Personnel Security

Effective security awareness [ ]

Effective Security training techniques [ ]

How to improve your briefing skills [ ]

Security clearance processing [ ]

Adjudication (Man making decision) [ ]

legal issues (regarding protecting personal information) [ ]

Conducting effective security self-inspections [ ]

Security violation prevention [ ]

Information Systems Security

Employee Internet Access (EIAS) security requirements [ ]

How to manage a contamination incident [ ]

Computer security fundamentals [ ]

Network security fundamentals [ ]

Reporting requirements for cyber intrusions [ ]

Fundamentals of information security systems [ ]

Information Security

Phishing [ ]

Hacking [ ]

Social networking risks [ ]

Identity theft techniques [ ]

Data breach countermeasures [ ]

Mobile device security risks [ ]

Critical infrastructure threats [ ]

How to conduct vulnerability assessments [ ]

Proprietary information protection strategies [ ]

Physical Security

Disaster planning [ ]

Disaster recovery [ ]

Workplace crime [ ]

Workplace loss prevention [ ]

Access control technologies [ ]

Sensitive Compartmented Information Facility (SCIF) construction standards [ ]

Classified storage program [ ]

How to protect your information from physical threats [ ]

Global Security Issues

Protecting business operations [ ]

Zero tolerance of violence at workplace [ ]

Understanding Export Controls [ ]

Understanding business economic espionage threats [ ]

Global terrorism [ ]

Domestic terrorism [ ]

Cyber warfare techniques [ ]

Cyber warfare tactics [ ]

Critical infrastructure threats [ ]

Professional Development

How to have a sustainable security budget [ ]

How to excel at managing people [ ]

Effective Communication Skills [ ]

How to communicate security risks to senior management [ ]

Proving your value as a security professional [ ]

(13)Please, briefly describe any security issues.

(14) Please, list three most challenge internal security threats.

Security Awareness training

(15) Please indicate your level of interest in participating in continued security awareness training by clicking on the box below to select your choice (Very interested = 3, Moderate interest = 2, No interest = 1)

(16) What if any, of the following topics would you be interested in learning more about in an extended security awareness training workshop. (check all that apply)

How to Develop A Technology Control Plan
Understanding Export Control Requirements
OPSEC Planning and Requirements
Creating Effective Security Policies
Creating Effective Security Procedures
Special Access Program Orientation
Train the Trainer Workshop
Information System Security Basics

(17) Do you have an interest in a security awareness training session that is not listed above? If so, please describe it.

(18) Please indicate the degree of importance (Extremely important=4, Moderately important=3, and Not important=1) the following factors have on your decision to implement a security awareness training event.

Location

Speakers/Instructors

Amount of time away

Conference content

Peer interaction, networking

Registration fee

Time of year

(19) Your Comments: Please use this space below to offer any additional suggestions or comments that you believe would enhance the security awareness training to alleviate data breaches and overcome internal threats.

(20) Will you be interested in having continuous security awareness training (Yes = 4, Very likely = 3, Not likely = 2, and no = 1)?

(21) If not, please tell me why:

Appendix B: Questionnaire

1) Please indicate below the incident types that occur in your organization

Incident Type (Check only one and where a selected box=1)

Root Compromise
User Compromise
Loss or Theft of IT Asset (e.g., Computers, Laptops, Routers, Printers; Removable Media; CD/DVD, flash drive, floppy)
Disclosure of Sensitive Data
Sensitive data includes infrastructure/configuration data, packages lost during shipment, hardcopy records, personally identifiable information (PII) of individuals, including personnel and job applicant information, tax information (including tax information of corporations).
Denial of Service
Malicious Code
Policy Non-Compliance
Unauthorized Access and/or Penetration Attempt
Probe/Scan
Phishing/Social Engineering
Misuse of Resources/Policy Violation
Exercise/Response Testing

2) When did the incident occur, Day/Night?
3) Where did the incident happen?

4) Describe the circumstances of the "Disclosure of Sensitive Data" incident: (Check onl one)

Package lost during shipment
Error in Faxing
Error in E-mailing
Machine/manual stuffing, processing or computer programming error
Invalid/Incomplete written/Oral authorization
Misrepresentation of identity or authority
Established procedures inadequate to establish customer's or representative's identity
Established procedures to confirm customer's identity not followed
Please, describe other (s)

5) Type of Location where the incident occurred (Check only one)

Electronic Transmission or Processing Error
Hotel
Company Facility
Public
Residence
Vehicle

Client Site Transportation
During Shipment Other

If the incident occurred during shipment (Yes=2, No=1, and unknown=0):

6) Was the local Mail Coordinator notified? Yes No

7) Shipping Company: *(e.g., Post Office/internal mailing)*

8) Was the Asset Lost or Stolen?

Lost
Stolen

9) If the Asset was Stolen, was it stolen from a locked area?

Yes
No
Unknown

10) If the Asset was Stolen, were there signs of forced entry?

Yes
No
Unknown

11) If Lost or Stolen at an XZB Facility, what was the specific storage location of the Asset?

Desk Cabinet Storage Room Other

12) If Lost or Stolen at an XZB Facility, was the specific storage location of the Asset locked?

Yes No
Unknown

13) If Lost or Stolen from a Vehicle, where was the Asset located in the Vehicle?

Trunk
Interior
Exterior

14) Type of Asset Lost or Stolen (Check all that apply)

Laptop	Thumb	Phone
Desktop	Drive	Backup tape or other media
	CD Rom	Other
BlackBerry	Floppy	

15) Was Enterprise Disk Encryption (EDE) installed on the laptop?

Yes
No
Unknown

16) Was the device powered off?

Yes
No
Unknown
Not Applicable

17) Was the cable lock engaged?

Yes
No
Unknown Not Applicable

18) Does XZB have Internal Review Code (IRC)?

Yes
No
Not Applicable

19) Is SBU data protected by law (e.g., confidential data or data that can be used to impair business processes, system configurations, and/or identify weaknesses)?

Yes

No

20) What type of risks do you think that employees pose?

21) Lastly, please provide below any additional roots causes of internal human factors that contribute to data breaches and compromised information.

Appendix C: Interview Questions

Part I- Dealing with malicious insiders and unintentional insiders risks

1. What type of security measures do you think adequate to reduce internal human errors?
2. What type of security solutions do you think management should implement to reduce risks posed by malicious employees?
3. What type of security solutions do you think management should put in place to reduce risks posed by unintentional employees?
4. How do you secure data to address the insider human element of an organization?
5. Where does sensitive data reside across your enterprise?
6. How can your organization reduce the cost of expanding data protection needs?
7. How can your company meet audit compliance requirements?

Part II- Employees data access and responsibilities

Using a 1 to 5 scale where (not often, 1= somewhat often, 2= often, 3= somewhat very often, & 5= very often). Please place a check mark in front of your answer.

8. Please rate your overall experience with data access and protection.

Not often
Somewhat often
Often
Somewhat very often
Very Often

9. Is information security only IT responsibility?

Not often
Somewhat often
Often

Somewhat very often
Very Often

10. Do you have internal data protection policies? If so,
    Not often
    Somewhat often
    Often
    Somewhat very often
    Very Often

11. How data protection is enforced?

    Not often
    Somewhat often
    Often
    Somewhat very often
    Very Often

Part III- Please indicate the degree of agreement below (Strongly agree =5, agree =4, disagree =3, strongly disagree =2, and unsure =1) associate with the following topics regarding the state of Cyber-defense within your organization. Please place a check mark in front of your answer.

12. Do you agree that cybersecurity threats sometimes fall through the crack of existing security systems?
    Strongly agree
    Agree
    Disagree
    Strongly disagree
    Unsure

13. Do you agree that your company is protected from advanced cyber-attacks?
    Strongly agree
    Agree
    Disagree
    Strongly disagree
    Unsure

14. Do you agree that your company' security can stop insider cybercriminals from stealing corporate information?

Strongly agree
Agree
Disagree
Strongly disagree
Unsure

15. Do you concur that it is possible to implement a security program that can withstand all targeted insider attacks?

Strongly agree
Agree
Disagree
Strongly disagree
Unsure

16. Can your organization monitor sensitive data?

Strongly agree
Agree
Disagree
Strongly disagree
Unsure

Appedix D: Results - Survey, Questionnaire, and Interview Questions

RQ1-What are the internal human factors that contribute to data breaches and compromised information in Ivory Coast emerging business environments?

Res_Savy1_v1.xlsx

RQ2– What are the root causes of internal human factors that contribute to data breaches and compromised information in Ivory Coast businesses?

Res_Ques2_v1.xlsx

RQ3- What preventative measures can management use to minimize the threat from internal employee human factors that contribute to data breaches or compromised information?

Res_Inter3-v1.xlsx

Appendix E: Emergent Themes

RQ1– What are the internal human factors that contribute to data breaches and compromised information in Ivory Coast emerging business environments?

Internal Security Challenges and Recommendations

Workplace Violence Impact on Organizations Data or Information

Insider Accidental Threats Causes and Mitigations

Precautionary Measures to Minimize Insider Threats

Security Awareness Training

RQ2– What are the root causes of internal human factors that contribute to data breaches and compromised information in Ivory Coast businesses?

Organizations Incident Types

Disclosure of Sensitive Data

Data Protection

Employees internal risk factors

RQ3- What preventative measures can management use to minimize the threat from internal employee human factors that contribute to data breaches or compromised information?

Dealing with malicious insiders and unintentional insiders risks

Security Measures to Reduce Internal Human Errors

Sensitive Data Dwelling

Reducing Big Data Cost

Employees data access and responsibilities

Data Access and Responsibilities

Cyber-defense

Cyber-defense State

Appendix F: Research Flyer for Participants

Overcoming Data Breaches and Human Factors in Minimizing Threats to Cyber-security Ecosystems in Ivory Coast

I am conducting this Study for my Walden Dissertation.

CONTACT INFORMATION

To find out more about this study, please contact:

- Pierre M. Ayereby
- 43-45-06-78
- Manouan.ayereby@waldenu.edu

Principal Researcher: **Pierre M. Ayereby**

The purpose of this research is to provide executives with a framework to guide them in deciding how to prevent data breaches from cyber-threats by focusing on internal human behavior.

To participate in this research, you must:

- Be Government Ministers
- Be Department Heads
- Be CFOs
- Be Branch Managers
- Be Chief Information Officers (CIO)
- Be IT Division Managers
- Be Information Systems Technicians
- Have at least three years of experience in your roles
- Complete the research questions, not on your organization' s Times

Participation in this study involves:

- Complete a survey within two to three days
- Complete a questionnaire within two to three days
- Complete a 30-minute one-on- one face-to-face interview
- Make a time commitment of 1 hour in the second week from the research starting date,
- In a designated hotel meeting room, in Rivera, Abidjan
- You will receive no compensation-Your participation is voluntary