Abstract:

Complexity of information security has become a major issue for organizations due to incessant threats to information assets. Healthcare organizations are particularly concerned with security owing to the inherent vulnerability of sensitive information assets in health informatics. While the non-technical security management elements have been at the center of information security activities for many years, often only the technical management components (i.e., firewall, anti-virus) have been the main area of interest for many practitioners. The problem addressed in this quantitative study was the dearth of non-technical security management perspectives in the management of information security in health informatics. This quantitative, non-experimental study examined the impact of non-technical security management factors including organizational culture, security policy, and human actions on information security management. The survey instrument was hand delivered to healthcare practitioners at Korle-Bu Teaching Hospital, as well as to technocrats at the Ministry of Health in Ghana. Respondents returned one hundred seventy-seven usable surveys out of two hundred surveys. Survey data were analyzed using correlation and regression analyses. The results indicated a significant positive relationship between information security management and security policy ($r=.612$, $p<.001$), organizational culture ($r=.751$, $p<.001$), and human behavior actions ($r=.646$, $p<.001$). Findings from this study confirmed that organizations who better appreciate, and thus incorporate non-technical factors into the organizations’ overall security strategy at the onset, ensure effective management of information security. Given the seriousness of the threats to the security environment today and the lack of effective control mechanisms in place, findings from this study could offer important and potentially new perspective on information security management issues; the growing recognition of the influences of non-technical factors for developing comprehensive information security management.

Keywords security, security management, non-technical security, organizational culture, security policy, human behavior, security strategy

INTRODUCTION

For decades, information security professionals have recognized that solving security problems requires the use of technology, processes, and people [11]. However, many information security practitioners employ only the technical measure and process measure to protect information assets from being abused [30]. Yet these measures have not been as effective as expected because all identifiable security actions and procedures involve human element and therefore technology process alone cannot protect information assets [18]; [38]. Indeed, an organization with a comprehensive information security management in place could better be able to avert data mishandling than an organization with no security management policy [13]; [18]; [26].

Incessant security threats to information assets caused by non-technical elements, such as user’s inapt actions, continue to be problematic.
partially in health informatics [3; 7]. Security breaches caused by employee sloppiness in healthcare organizations showed over 32% increase in 2010; costing the United States’ healthcare industry between $4.2 billion – $8.1 billion annually [39]. This issue is also problematic in developing countries, which often lack efficient judiciary system to support the functioning of information security laws, if at all they exist [45]. The problem addressed in this quantitative study was the dearth of non-technical security management measures in the formulation of information security management by stakeholders in health informatics in Ghana.

Technological factors are not the only key to effective management of information assets from attacks [8]. The role of non-technical factors including organizational culture, security policy, and human behavior actions has seen little or no attention. Failure to include non-technical factors in security management could render the entire security measure inadequate and could expose organizations to enormous security risks [32]. This study attempts to fill the gap in academia, as research in organizations adopting a comprehensive information security management is practically a novel paradigm [12].

The purpose of this non-experimental quantitative study was to examine the impact of the non-technical security management factors including organizational culture, security policy, and human behavior actions on information security management in health informatics. The instrument for this study was a combination from three previously used valid, reliable, and tested instruments developed from the ISO/IEC 27002 Standard.

RESEARCH QUESTIONS AND HYPOTHESES

The general question this research study addresses is to what extent do non-technical security management factors influence the management of information security in the healthcare industry.

The following questions expand the above general question and serve as guide to the study:

RQ1: To what extent, if any, is there a relationship between organizational culture, as measured by leadership support and normative beliefs, and Information security management, as measured by confidentiality, integrity, and availability?

RQ2: To what extent, if any, is there a relationship between security policy, as measured by user awareness and behavior intention, and Information security management, as measured by confidentiality, integrity, and availability?

RQ3: To what extent, if any, is there a relationship between human behavior actions, as measured by compliance behavior and deterrent countermeasures, and Information security management, as measured by confidentiality, integrity, and availability?

RQ4: To what extent, if any, do non-technical security management factors of security policy (measured by user awareness and behavior intention), organizational culture (measured by leadership support and normative beliefs), and human behavior actions (measured by compliance behavior and deterrent countermeasures) predict Information security management (measured by confidentiality, integrity, and availability)?

The following hypotheses were generated in order to answer and analyze the research questions of the study:

H10: There is no statistically significant relationship between organizational culture as measured by leadership support and normative beliefs, and Information Security Management, as measured by confidentiality, integrity, and availability.

H1a: There is a statistically significant relationship between organizational culture as measured by leadership support and normative beliefs, and Information Security Management, as measured by confidentiality, integrity, and availability.

H20: There is no statistically significant relationship between security policy as measured
by user awareness and behavior intention, and Information Security Management, as measured by confidentiality, integrity, and availability.

H2a: There is a statistically significant relationship between security policy as measured by user awareness and behavior intention, and Information Security Management, as measured by confidentiality, integrity, and availability.

H30: There is no statistically significant relationship between human behavior actions as measured by compliance behavior and deterrent countermeasures, and Information Security Management, as measured by confidentiality, integrity, and availability.

H3a: There is a statistically significant relationship between human behavior actions as measured by compliance behavior and deterrent countermeasures, and Information Security Management, as measured by confidentiality, integrity, and availability.

H40: The non-technical security management factors of security policy, organizational culture, and human behavior actions, do not significantly predict Information Security Management, as measured by confidentiality, integrity, and availability.

H4a: The non-technical security management factors of security policy, organizational culture, and human behavior actions, are significantly predictive of Information Security Management, as measured by confidentiality, integrity, and availability.

LITERATURE REVIEW

Information security is a broad and multi-dimensional topic described across a wide spectrum of literature. Literature reviews on the topic are vast because information security has many pretexts and no common idiolect exists inside the information security community. Some of the known expressions used interchangeably are computer security, network security, information technology security, information systems security, and information assurance. We used the term “information security” in the present study to describe the protection of confidentiality, integrity, and availability (CIA) of information [29]. Originally, the domain of information security focused mainly on technology; the scope of information security broadened to encompass aspects such as information technology, management information systems, cryptography, policy, law, finance, and economics [20].

The objective of information security is to safeguard information assets from unapproved admittance or destruction. The fundamental principles to achieve that objective are the security triad of CIA. The CIA triad forms the basic building blocks of any good security initiative [46]. The disclosure, alteration, and denial (DAD) are three primary mechanisms of information security management, malicious individual use to overcome the three information security properties [46].

Disclosure happens when malicious individuals breach the confidentiality property of information security. Confidentiality, being part of the broader privacy concept, refers to the unauthorized access, disclosure, and use of information [20]. Confidentiality of information assets is guaranteeing that no one should have access to organization’s proprietary information except authorized personnel or entities only. Integrity refers to the reliability and trustworthiness of the information. It is when improper modification or destruction of information takes place in transit, which would lead to different result [11]. Availability defines the timely access to data in terms of functional significance. Integrity and availability prevent any accidental or malicious alteration as well as ensures that authorized parties have access to information when needed [20].

Because many organizations rely heavily on Information and Communication Technology (ICT) and the data and information involved, system availability at all times becomes very important [11]. The closer one moves toward one apex, the further one is removed from the other two. For a security breach to occur, at least one of the CIA Triad components must be compromised [11]; [20]. There is an incessant discussion about extending the classic triad of confidentiality, integrity, and availability despite
the fact that for many years, information security professionals have held the triad to be the central principles of information security [23].

Organizations face threats to their information assets from either external or from internal regardless of their type or size [12]. Internal threats include the intentional and the unintentional threats, and can go unnoticed and are riskier than the external attack [9]. Intentional threat ensues when an employee or a partner in an organization shrewdly sets out to cause damage or loss of data [34]. Unintentional threat arises when an individual inside an organization inadvertently caused damage to information assets or service [12]. Many researchers have concluded that intentional threat is more serious to information security [9]; [12]; [7].

A 2009 study by the Economist Intelligence Unit (EIU) found an increase in the number of organizations damaged by sensitive information appearing on blogs and other social media networks [12]. A security breach such as Denial-of-service (DoS), which occurs when cyber criminals hijack websites and in return deny everyone access, could cause an internet-dependent organization millions of dollars [31]. Several studies on the financial impact of security breaches on statistical reports on software vulnerabilities [10]; [34], and on computer crimes [14] have been published.

Information system practitioners suggest organizations must cultivate a comprehensive approach, which comprises both the human and technical dimensions when managing information security in their organizations [6]. Facets such as organizational culture, security policies, and human behavior actions could be perceived as the non-technical aspects, while the specific technologies (firewalls, encryption, and access control lists, to name some) could be described as the technical traits. Information and Communication Technology is pervasive in present-day society and pervades almost all forms of anthropological interaction. Today’s ICT provides unprecedented amounts of information to organizations and their employees. As more organizations conduct their business and exchange voluminous and sensitive materials over the Internet, exposure to information security attacks is also increasing.

The International Standards Organization /International Electro-technical Commission (ISO/IEC) 17799:2005 Code of Practice, document number 27002 is the most extensively recognized worldwide standard for information security management across industries and geography [40]. It is also the most suitable framework for addressing information security issues in organizations and in e-Government transactions [35]. The objectives and controls in ISO/IEC 17799:2005 are to meet the necessities recognized in risk assessment management [30]; [35]. The document is a common foundation and real useful guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities [29].

In spite of the importance of non-technical factors in safeguarding organizations’ information assets [20], only few publications in the information security literature address the some level of importance of the non-technical components [16]; [41]; [43]. Recently researchers in the field of management of information security recognized the imperious of including people and processes to ensure the quality of information in contemporary organizations. Non-technical factors (organizational culture, security policy, and human behavior actions) represent key components that stakeholders must address for an effective information security management [12].

The role of human and organizational factors has been examined from a range of disciplinary perspective [32]. Organizations often rely on security policies in situations when security technologies could not addressed human behaviors issues such as proper use of computer and network resources, appropriate password habits [26]. Many recent information security studies are on not only areas such as awareness, insider computer crime, governance, and policy compliance [53], but are on the human component aimed at the threat that human behavior might pose to the protection of information assets.
End users come across information security tasks when they utilize any ICT applications during the execution of their everyday activities in the organization [53]. While in the process of performing these information security tasks, end users exhibit a range of information security behaviors such as successful completion of tasks, failure to finish tasks, or even failure to initiate tasks [20]. This end user behavior, which is a complex human action that could influence the CIA of information security, is precarious to the realization of information security management efforts in the organization [17]; [20]; [26]; [43]; [52].

Behavior monitoring and compliance are key issues in information security deployment; because to write a policy is one thing, but to be able to enforce it is a very different thing. Information security researchers have called for close monitoring of insider behavior to ensure compliance with security requirements because most of the crimes committed by insiders are essentially a rational act [2]; [20]; [44]. It is only when activities are properly monitored that enforcement could be properly enacted [52]. Non-compliance behavior has an influence on end user’s security behavior [50]. Deterrence is the process of using fear of punishment, within the parameters of the law, to deter potential wrongdoers from acting. Deterrent techniques such as sanctions and policies are used as reminders to users to allay potential system abuse. The fear of a sanction for policy non-compliance of information security, positively shapes the security behavior of users of information technology [48].

In order for information security management policies to be effective, prospective wrongdoers must be made aware of the consequences for not following the policies and this fact must be documented as part of the published policy [50]. Failure to prevent or minimize security breaches due to end-user non-compliance is indicators of failed security management [52]. Information security policy simply is a document for the direction of information security inside an organization [28]. It deals with the integrity, availability, and confidentiality of electronic data transmission in the information systems [30]. Information security policy could be presented in many forms but the most important process of providing an effective security policy is for it to be in written form [29]. The ISO/IEC 17799:2005 institutes rules and common principles for initiating, implementing, maintaining, and improving information security management in an organization.

Information security policies are not designed to only delineate responsibilities and acceptable conduct in an organization [5]; [22], but also to serve as effective deterrents [48]. Proper implementation of information security policy as a deterrent could significantly influence the conduct of human behavior in the daily handling of patient data [52].

To counter the risks posed by inappropriate user action (intentional or unintentional), information security decision makers propose security awareness and education programs for users [4]; [15]; [19]; [30]; [44]. Lack of awareness by users indicating the existence of information policies and procedures could hamper overall information security objectives [30].

The Theory of Reasoned Action (TRA), a widely applied framework in information systems research [25], posits that behavior is determined by beliefs about that target behavior via the behavior determinant construct behavioral intentions. The direction of influence is from beliefs, to behavioral intentions and ultimately behavior. Human factors focusing particularly on end user perceptions, intentions, and behavior are critical elements for understanding how to move forward with information systems security [12].

Information security culture is defined as acceptable and often encouraged perceptions, attitudes, and assumptions that help protect information assets in an organization [17]. Security culture includes both security related beliefs and security related behaviors [42]. Information security researchers have long argued that organizations need an organizational security culture to ensure the security of their information assets [20]; [47]. The reason behind the surge in interest in information security culture is attributed to the realization by information systems researchers that the issue of
The most common national cultural model is Hofstede’s [27] framework, which classified national culture into five scopes. These scopes are: (a) power distance (a measure of equal distribution of power), (b) avoidance of uncertainty (how uncertain risk threatens cultural members), (c) individual information security management (the balance between duties and responsibilities), (d) masculinity (how gender is used to separate social roles), and (e) long term orientation (how specific culture influences human and organizational behavior and practices). Accordingly, to implement an effective informational security policy, the culture of the people must be examined and understood because the goal of a security culture policy is to effect behaviors and actions of the employees or the citizens (in the case of a nation). As employees may have legitimate access to information for their routine activities, their behavior should conform to ways that would not give rise to a culture where negligence is viewed as an acceptable norm [17]. It is important for information systems practitioners to remember that the most effective countermeasure is not always the technical measure, but a combination of both technical and non-technical elements.

The idea of leadership support being a necessary condition for successful implementation of information security management is well known [33]. Involvement is the prominence placed on risk management program by top management as the organization leadership shows noticeably support through its own behavior [17]; [30]; [33]. Attaining an ample top leadership pledge for cultural change process is the first constituent to information security management. Once management has committed to the new culture, the vision for organization’s information security culture should then be incorporated in to the corporate information security policy [30].

Many information systems researchers considered the role of social influence in terms of normative beliefs, subjective, peer, and descriptive norms [26]. While the information systems literature included variety of tags for subjective norm concepts, each of these concepts contain the notion that the individual's behavior is influenced by what the relevant others expect them to do [17]. The understanding that persons are more likely to conform with significant others’ prospects when those others have the ability to reward the desired behavior [33]. Social impact in information technology acceptance is intricate and could be contingent on variety of conditional effects as well [51]. Intention greatly influences an individual’s behavior, and behavioral change is ultimately the result of changes in normative beliefs [1]; which is based on whether or not an important individual requests the person to perform the behavior in question [25].

**RESEARCH METHOD**

This study employed a quantitative design and descriptive correlational methods to test the hypotheses and answer the research questions.

The sampling frame of this study was healthcare professionals from the Korle-Bu Teaching Hospital (which include physician consultants, surgeons, anesthetists, pharmacists, nurses/midwives, pathologists, radiologists, and laboratory technologists), and technocrats from the Ministry of Health. While the health professionals were selected because they would be the principle users of e-Health/Health Informatics, the technocrats were included because in addition to being the policy makers, these officials are more knowledgeable in the development of and implementation of Health Informatics/e-Health in Ghana.

In this study, 200 healthcare professionals and stakeholders were purposely selected to partake in the survey. A minimum sample size of 56 participants was needed to examine the impact of non-technical components of security measures on comprehensive management of information security.

Purposive samples are selected based on a prearranged benchmarks associated with the research [37]. It is incumbent upon researchers to conduct a thorough literature review to understand the “edge of the field” and whether the study population or question is a new or is
significant contribution. In this study therefore, purposeful sampling was considered because of lack of a reliable data as a result of the absence of a comprehensive information security management in the country’s overall ICT strategy.

We designed the survey instrument for this study to test the correlational relationships between the dependent variable (information security management) and the independent variables (organizational culture, security policies, and human behavior actions). The instrument is a combination from three previously used valid and tested instruments developed from the ISO/IEC 27002 Standard. The ISMC [11], the ISGF [17], and the ISCF [44] were used to measure information security management, security policy, organizational culture, human behavior actions, and their sub-dimensions.

In terms of the sample description, we used descriptive statistics to describe the sample in terms of gender, age, profession, education, and experience. Similarly, we used descriptive statistics to analyze survey items. The demographic characteristics showed that the sample was composed of males (63%) and females (37%). In terms of the age, the range of 30 to 50 years (62%) dominated. The professions of respondents were 20% physicians, 22% pharmacists, 18% nurses, and 20% public servants/government officials. A further 20% of the sample was “other” professions. Regarding level of education, 13% had Higher National Diploma education, 33% had bachelor’s degrees, 24% had master’s degrees, and 24% had doctoral degrees. Ten respondents (6%) did not provide a valid response to this question. Table 1 shows the sampled description of the variables, and resultant survey items.

In order to determine the internal consistency of the items, we calculated reliability statistics for each section of the survey. Likewise, we calculated the item-total scale reliability statistics to evaluate the contribution of each of the items to the scale, including corrected item-total correlations. We used Bivariate regression for each research question, to determine to what extent there was a relationship between the predictor (DV) and each of the criterion variables (IVs). An alpha level of .05 was used as a decision point for statistical significance.
Table 1

Description of Variables in This Study

<table>
<thead>
<tr>
<th>Type</th>
<th>Variable</th>
<th>Dimensions</th>
<th>Survey Items (No.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DV</td>
<td>Information Security Management</td>
<td>Confidentiality</td>
<td>6-7 (2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integrity</td>
<td>8-9 (2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Availability</td>
<td>10-11 (2)</td>
</tr>
<tr>
<td>IV</td>
<td>Security Policy</td>
<td>User Awareness</td>
<td>12-15 (4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Behavior Intention</td>
<td>16-19 (4)</td>
</tr>
<tr>
<td>IV</td>
<td>Organizational Culture</td>
<td>Leadership Support</td>
<td>20-23 (4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Normative Beliefs</td>
<td>24-27 (4)</td>
</tr>
<tr>
<td>IV</td>
<td>Human Behavior Actions</td>
<td>Compliance Behavior</td>
<td>28-31 (4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deterrent Countermeasure</td>
<td>32-35 (4)</td>
</tr>
</tbody>
</table>

Note. DV = dependent variable, IV = independent variable.

**Information security management** (ISM) – dependent variable. The ISM was measured by three dimensions: Confidentiality, integrity, and availability. The measure was anchored on a 5-point Likert-type scale ranging from 1 (strongly disagree) to 5 (strongly agree) such that higher scores indicated greater agreement with the items. The inter-item correlation matrix statistics for ISM items are shown in Table 2 below. The Cronbach’s alpha of .781 for the item-total reliability statistics scale indicates acceptable internal consistency reliability for the ISM section score.

Table 2

Inter-Item Correlation Matrix for Information Security Management

<table>
<thead>
<tr>
<th></th>
<th>(CONFID1)</th>
<th>(CONFID2)</th>
<th>(INTEG1)</th>
<th>(INTEG2)</th>
<th>(AVAIL1)</th>
<th>(AVAIL2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFID1</td>
<td>1.000</td>
<td>.100</td>
<td>.442</td>
<td>.415</td>
<td>.323</td>
<td>.395</td>
</tr>
<tr>
<td>CONFID2</td>
<td>.100</td>
<td>1.000</td>
<td>.442</td>
<td>.418</td>
<td>.339</td>
<td>.326</td>
</tr>
<tr>
<td>INTEG1</td>
<td>.442</td>
<td>.442</td>
<td>1.000</td>
<td>.450</td>
<td>.276</td>
<td>.486</td>
</tr>
<tr>
<td>INTEG2</td>
<td>.415</td>
<td>.418</td>
<td>.450</td>
<td>1.000</td>
<td>.313</td>
<td>.374</td>
</tr>
<tr>
<td>AVAIL1</td>
<td>.323</td>
<td>.339</td>
<td>.276</td>
<td>.313</td>
<td>1.000</td>
<td>.457</td>
</tr>
<tr>
<td>AVAIL2</td>
<td>.395</td>
<td>.326</td>
<td>.486</td>
<td>.374</td>
<td>.457</td>
<td>1.000</td>
</tr>
</tbody>
</table>

Note. CONF=Confidentiality, Integ=Integrity, Avail=Availability, Org=Organization, CONFID1= My org. has technical control to protect information security, CONFID2= My org. has information security practices to protect data, INTEG1= My org updates information resources, INTEG2= My organization has change management control, AVAIL1= Only authorized users have access to information, AVAIL2= There is an established access control in my organization.

**Information security policy** – independent variable. The independent variable information security policy was also measured by “user awareness and training”, and “behavior intention”. The item-total statistics for the eight Security policy items and descriptive statistics for security policy sub-dimensions are shown in Tables 3. Each of the items shared adequate variance with the rest of the scale. The lowest correct item-total correlation was for item INTENT1 (r = .318). The Cronbach’s alpha value for the total section was .745; for user awareness, the alpha was .665, and the behavior intention alpha was .608. This indicates adequate internal consistency for the section total, and questionable internal consistency for the two sub-domain scores.

Table 3
Item Total Statistics for Security Policy

<table>
<thead>
<tr>
<th>Item</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Squared Multiple Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWARE1</td>
<td>26.75</td>
<td>23.120</td>
<td>.523</td>
<td>.315</td>
<td>.701</td>
</tr>
<tr>
<td>AWARE2</td>
<td>26.12</td>
<td>25.253</td>
<td>.437</td>
<td>.344</td>
<td>.719</td>
</tr>
<tr>
<td>AWARE3</td>
<td>26.36</td>
<td>24.459</td>
<td>.438</td>
<td>.296</td>
<td>.719</td>
</tr>
<tr>
<td>AWARE4</td>
<td>26.73</td>
<td>23.969</td>
<td>.456</td>
<td>.271</td>
<td>.716</td>
</tr>
<tr>
<td>INTENT1</td>
<td>26.16</td>
<td>26.554</td>
<td>.318</td>
<td>.237</td>
<td>.740</td>
</tr>
<tr>
<td>INTENT2</td>
<td>26.07</td>
<td>25.330</td>
<td>.434</td>
<td>.320</td>
<td>.720</td>
</tr>
<tr>
<td>INTENT3</td>
<td>26.16</td>
<td>25.433</td>
<td>.427</td>
<td>.211</td>
<td>.721</td>
</tr>
<tr>
<td>INTENT4</td>
<td>26.03</td>
<td>25.317</td>
<td>.488</td>
<td>.300</td>
<td>.712</td>
</tr>
</tbody>
</table>

Note. Cronbach’s alphas: Security Policy (8 items) = .745, User awareness (4 items) = .665, Behavior intention (4 items) = .608.

Organizational culture – independent variable. The organizational culture variable was comprised of the sub-dimensions of leadership support and normative beliefs. Tables 4 includes the reliability statistics, the means, and the distributions for the organizational culture section and sub-dimensions. The Cronbach’s alpha for the organizational culture section was .791 indicating acceptable to good internal consistency. The internal consistency of the leadership support sub-dimension was poor/questionable (alpha = .585), and the internal consistency of normative beliefs was slightly higher, and in the acceptable range (alpha = .679).

Table 4.

Item Total Statistics for Organizational Culture Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Squared Multiple Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEAD1</td>
<td>25.62</td>
<td>28.771</td>
<td>.551</td>
<td>.400</td>
<td>.760</td>
</tr>
<tr>
<td>LEAD2</td>
<td>25.82</td>
<td>29.524</td>
<td>.444</td>
<td>.272</td>
<td>.776</td>
</tr>
<tr>
<td>LEAD3</td>
<td>25.88</td>
<td>28.666</td>
<td>.484</td>
<td>.316</td>
<td>.770</td>
</tr>
<tr>
<td>LEAD4</td>
<td>25.64</td>
<td>30.903</td>
<td>.388</td>
<td>.190</td>
<td>.784</td>
</tr>
<tr>
<td>NORM1</td>
<td>25.72</td>
<td>28.942</td>
<td>.532</td>
<td>.317</td>
<td>.763</td>
</tr>
<tr>
<td>NORM2</td>
<td>25.86</td>
<td>27.452</td>
<td>.560</td>
<td>.360</td>
<td>.757</td>
</tr>
<tr>
<td>NORM3</td>
<td>25.80</td>
<td>29.489</td>
<td>.437</td>
<td>.219</td>
<td>.777</td>
</tr>
<tr>
<td>NORM4</td>
<td>25.87</td>
<td>27.352</td>
<td>.582</td>
<td>.365</td>
<td>.753</td>
</tr>
</tbody>
</table>

Note. Cronbach’s alphas: Organizational culture (8 items) = .791, Leadership support (4 items) = .585, Normative beliefs (4 items) = .679.

Human behavior actions – independent variable. Two sub-dimensions: Compliance behavior and deterrent countermeasures were used to measure the human behavior actions variable. As shown in Table 5, the Cronbach’s alpha for the section was .648, indicating fair internal consistency for the section, and this level of internal consistency is deemed acceptable for research purposes.

Table 5

Item Total Reliability Statistics for Human Behavior Actions
RESULTS AND EVALUATION OF FINDINGS

The purpose of this research was to examine the impact of non-technical components and management of information security in health informatics. When dealing of assets control in the past years, Information Security practitioners have shifted their focus on people in the management and protection of information assets. This transference of strategy was because many practitioners in the information systems environment recognized that they cannot attain comprehensive information security by just installing technical solutions like IDS, firewalls, and implementing processes [43]. People/user issues must exert lots of influence when creating an organizations’ security strategy because people in these organizations maintain the technology and thus the day-to-day security processes [8].

Results of every research study, innately encountered some limitations due to many factors [36]. Thus, the results from the present study need to be interpreted in the context of some limitations. The first limitation of the study was that the outcome of the study might not be a true representative of the impact of non-technical factors on the management of information security in informatics in Ghana because the sample was from only two entities; the Korle-Bu Teaching Hospital (KBTH) and the Ministry of Health. Many institutions and organizations may be directly or indirectly involved with ICT in Ghana but were not included in the study due to the difficulty of getting permissions, and also due to cost. The use of purposive (non-probability) sampling is the study is another limitation. While the non-probability sample is not necessarily unrepresentative of the study population, it does not imply this study will not espouse the extent and the complexity of non-technical security management components in the management of information security in health informatics, as would have been a random sampling [54].

We took a number of measures in order to address the limitations and the concerns identified. First, we assured the study participants of the confidentiality of their information and they were fully aware that they could walk away from the survey whenever they felt uneasiness. The research data was safely stored under lock and key as a way of properly protecting the participants' confidentiality in the study because of privacy rights of the participants [54].

Information Security Management and Security Policy. The first question of the study was aimed at examining the relationship ISM, as measured by confidentiality, integrity, and availability and information security policy, as measured by user awareness and behavior intention. The null hypothesis was rejected in favor of the alternative hypothesis. Thus, the findings suggested that there is a relationship between security policy and the management of information security indicating that security policy predicts the management of information security in organizations. Literature research found that when employees have increased awareness and adequate training, the more likely
employees are to shape their behavior intention towards information security policy [30]; [44]. Organizations attain greater levels of security success when information security policy is the preliminary measure put in place in order to minimize the threat of objectionable use of any of the organizations’ information resources [44]. Security policy’s impact on the ISM was confirmed in the study as there was a positive correlation- r=.612(p<.001) between the two variables. The mean for security policy was 3.76 (SD = .70) with a range of scores from 1.50 to 5.00 out of a possible five. The mean for user awareness and training was 3.57 (SD = .78) and the mean for behavior intention was slightly higher at 3.95 (SD = .74).

The results also showed that there was a significant zero-order correlation between the user awareness and behavior intention sub-domains of security policy, and the ISM sub-domains of confidentiality, integrity, and availability. The finding is consistent with prior research [26]; [30]; [44] that in an existing information security management paradigm, the role of security policy is crucial. Similarly, the results confirmed the assertions by some of the researchers. In this study for example, while the highest mean in the user awareness and training domain was “My organization has specific guidelines that govern what employees are allowed to do with their computers” (M = 3.94), the highest mean in the behavior intention domain was “I intend to assist others in complying with information security policies” (M = 4.02). Multivariate analysis also revealed the both user awareness and behavior intention were significant predictors of the ISM sub-domains. When employees are made aware of the specificities within the security policy, they not only follow the policy but do intend helping others to respect the security policy as well.

There is a direct and indirect influence of security policies on users’ intentions with regard to information systems usage/abuse [15]. They contended that, users are less likely to engage in information assets misuse when users are aware that security policies exist. Furthermore, as Knapp et al. [30] explained, not only does awareness prepare users to receive the rudimentary ideas of security through a proper training program, but it alerts people in organizations to the subjects of information security [49]. In addition, inherent incentives of employees’ apparent effectiveness of their actions play a vital part in security policy compliance intentions of users [26].

Undeniably, the first step towards achieving comprehensive ISM is through security policies. Security policies and practices in organization, based on the ISO/IEC 17799:2005 framework, provide opportunities for organizations and governments to attain compliance and reduce the level of security breaches. Stakeholders must make certain that people/end users and IT administrators alike know what is expected of them in terms of data protection [24], else they may be tempted to act in a way they feel is appropriate. Information security awareness is the central construct in the formation of user behavioral intentions with regard to technologies [21]. Without proper awareness and training of written security policy, individuals might inadvertently damage or lose data because they may not know how they should appropriately handle such sensitive data [52]. Because control of data begins and ends with people [4], it is critical for policy makers and security professionals to recognize that peoples’ perceptions, intentions, and behaviors are dire elements in information security management.

Information Security Management and Organizational Culture. The next focus of the study was to examine the correlation between organizational culture, as measured by leadership support and normative beliefs, and ISM, as measured by confidentiality, integrity, and availability. The alternative hypothesis was supported and thus the null hypothesis was rejected. The organizational culture scores accounted for 56.2% of the adjusted variance in ISM scores. Study findings suggested that, consistency scores were statistically significant, β = .76, p < .001, and it was concluded that there was a positive relationship between the organizational and ISM. Based on the statistical tests, r = .751 (p < .001), there was a very considerable, statistically significant, positive correlation between ISM and organizational culture. In addition, there was a significant multivariate effect of leadership support (p <
Leadership support accounted for 39.6% of the variance in the sub-domains of ISM, whereas normative beliefs accounted for only 2.4% in the ISM sub-domain scores. The findings from research question 2 revealed that a very considerable positive relationship exists between ISM and organizational culture.

This study backs past researches in showing that leadership support and normative beliefs help in developing mindset and creating organizational culture that builds effective ISM strategy [11]; [20]; [30]. These non-technical factors (subjective norms, leadership, belief, and human behavior of ISM activities) could be more effective in achieving real ISM than just technical mechanisms such as firewall or anti-virus. Top management support is critical for executing security controls within organizations [30]. Organizations that experience support from the top management often get the flexibility of huge allocation of resources to deploy advanced security software. In fact, senior management support, which is the degree to which top executives support security priorities, can affect the scope of policies as well as the amount of managerial support and resources available to develop and implement information security policies in an organization.

The findings of this study further support the notion that both inherent and extrinsic instigators influence security behaviors. Apparent behavior of individuals, norms, attitudes, and perceptions can be inferred from what the individuals say and do, and core values [26]. The findings also supports past research [17] in showing that information security employees’ behaviors could be unfair by subjective norms and peer behaviors. In this study for example, the highest mean of 3.84 under the organizational culture variable was for “Top management style in my organization is characterized by conformity to good security practices” that encompasses the internal belief systems of each individual in the organization. Normative beliefs may arise due to an organizational culture security. Both inherent and extrinsic instigators, such as apparent behavior of management, influence behaviors [26]. A security culture mechanism should exist to direct employees’ conduct in organizations. Without such mechanism, employees could well relate with information assets in manners that may lead to risky behavior [33]; a situation that could cause damage to organizations’ information assets.

**Information Security Management and Human Behavior Actions.** The third research question focused on examining the relationship between human behavior actions, and ISM. The null hypothesis associated was rejected. The overall relationship ISM and human behavior actions was a positive one, r=.664 (p<.001). This means that in terms of human behavior actions, stakeholders are aware of the importance of compliance behavior and deterrence concerning achieving effective ISM. The adjusted variance in ISM scores, human behavior action score amounted for 41.4%. Of the relationships between the sub-domain scores, there were significant multivariate effects of p=.001 for compliance behavior and p<.001 for deterrent countermeasures. The mean for compliance behavior was 3.51.

Current research has shown that having adaptable human behavior actions not only increases the chances of successful ISM but also supports comprehensive information security strategy across the organization. As stated in some past studies [17]; [44], human elements actions explain how different issues could lead to causes of security breaches and vulnerabilities in organizations. Core incentives of users’ apparent effectiveness of their actions play an essential role in security policy compliance intentions [26]. Human behavior action has an influence on organizations’ information security management [32]. Organizations face more complex security threats now than was acknowledged. The challenge, is how to manage human behavior while trying to achieve optimal resources structure. Thus in order for organizations to formulate strategies in tackling security issues, researchers must study human behavior actions within the context of security management.

**Relationships between ISM and Security Policy, Organizational Culture, and Human Behavior Actions.** The focus of this final research question was to examine the contribution of all three IVs of security policy, organizational culture, and human behavior
actions to the prediction of ISM using multiple regressions. As indicated earlier, much of the prior research in IS was based on single or individual factors such as organization culture [17]; [44], top leadership support [20], and security policy [30]. We therefore combined at least three factors and pinched them against ISM. The results indicated that the null hypothesis was rejected and the alternative hypothesis was supported. In addition, we found that the three independent variables (IVs) (i.e., security policy, organizational culture, and human behavior action) significantly correlated to one another. The regression equation was less significant, \( F(3,170) = 83.524, p<.001 \), and the three IVs together predicted 58.9% of the adjusted variance in ISM scores. That is, non-technical factors were predictive of information security management.

The finding is an affirmation of the foundation of this study; that while individual characteristics may have impact on ISM, the combined factors do have much significant impact on organizations’ overall of information security management strategies. Additionally, the results from the study fully support the integrated framework of the study in that when of non-technical factors are better appreciated and incorporated into organizations’ security strategy at the onset; they positively affect the management of information security in organizations. Failure by information security practitioners and policy makers to incorporate the non-technical factors in to organizations’ security formulation strategy could lead to undesirable security management outcome for the organizations.

**RECOMMENDATIONS AND CONCLUSION**

This study examined the impact of non-technical security management factors on information security management in health informatics. The findings indicated the existence of a positive relationship between ISM and non-technical factors. Thus, we found that non-technical factors of security policy, organizational culture, and human behavior actions, are significantly predictive of information security management.

Past researches on information security management, in most cases, have only been on specific issues such as culture, policy, management support, and organizational size. Such studies are methodologically weak as they dwell on just one item for study. Based on the findings and the review of literature, it has become clear that using just a single item alone cannot be reflective measure of an effective information security management security threats. There is the need for information security practitioners and other stakeholders to integrate all of the security components in their attempt to achieve effective security control.

The results of this study make it clear that future prospects for further research are justified. Given that the results of this study were based on a relatively small sample of health organizations, attempts to generalize these results must be done with caution. Future studies can validate these results by replicating this study in other business sectors and or with bigger samples. Furthermore, we applied a quantitative method that relied on non-experimental design in this study. More in-depth mixed-mode methods that use a broader random sampling of participants in the healthcare industry would provide a more representative of the entire healthcare stakeholders. Finally, while this study was conducted in just one country, the findings are not limited to the country of the sub-region. Further research can also extend these results by incorporating this study in different populations with varying needs of information security management beyond the boundaries used in this study. While much work lies ahead, it is expected that this paper would generate further interest among researchers and organizations who are interested in identify the other antecedent factors not captured in our study that impact the adoption of a more pragmatic approach to information security management.

As security is a collective apprehension among stakeholders, combating information threats necessitates a comprehensive approach to guarantee that organizations’ information assets remain confidential, with impeccable integrity, and would always be available for authorized users.
REFERENCES


