Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 5, May 2017, pg.267 – 284

Impact of Social Media Usage by Employees on Banking Information Security in Developing Economies

Abel Yeboah-ofori[1], Marian Owusua Aduamoah[2]

[1]Faculty of Informatics, Ghana Technology University College (GTUC) Ghana
[2]Post Graduate, Ghana Technology University College (GTUC), Ghana
[1] Ayeboah-Ofori@gtuc.edu.gh; [2] sparkledeeva@gmail.com

***Abstract:** The use of social media at the workplaces are posing serious threats and have already caused harm to the information security systems of some organizations and not excluding the banking industry. Social media is seen in almost every aspect of human life and businesses have used Social Media platforms to facilitate their business processes and maximize efficiency. Information Security is concerned with ensuring confidentiality, integrity and availability of data regardless of the form the data may take that is either electronic or print. Nevertheless, Social media is gradually making an impact on an organisation's information security without much effort because their carriers are employees. Some of the risk and vulnerabilities associated with social media on an organisation's information security are loss of productivity, cyber security threats, network vulnerabilities, loss of company reputation, litigation issues. However it is essential that management begin to address their security-related concerns with the use of social media. This study looks at the impact of social media usage by bank employees on the organisational information security specifically the banking industry. The case study research and findings were related to Banks as the sample population for banks in developing economies with employee's population of 200 and sample size of 60. The study result show that employees had positive attitudes towards personal use of social media, negative attitudes towards use of social media at the work place, and mixed attitudes on information security policies which include the awareness of security vulnerabilities and how strong the bank's information security policies were. The study also suggests countermeasures needed by banks to put in place to mitigate negative effects of social media use by employees on their information security.*

***Keywords:** Social Media, Information Security, Perceived Risks, Threats & Vulnerabilities, Developing Economies*

I. INTRODUCTION

Social media has emerged as an important strategic tool for organizations to facilitate communications with their employees, customers, and other external partners. Social media can be defined as a collection of online communication networks dedicated to internet community based user input data, content sharing and interaction. This includes web and mobile-based technology that allows users to collaborate with each other. In many businesses, social media helps to advertise products/services, promote brands and also connect to existing customers and build new relationships with potential customers. From the customers' perspective, a simpler and easier way of communicating about their good or bad experiences with a company is through social media. Businesses can then respond quickly to either feedback from customers, attend to customer problems and rebuild customer confidence through the same social media. Internally, employees use social tools to access information and resources needed for their work to be efficient.

Externally, social media grants businesses access to information about their customers and conduct research on the best way to enhance their operations to meet customer expectations and satisfaction.

On the other hand, it is essential for an organization to balance its need to operate business effectively as well as its need for protection. Information security is put in place to protect and secure an organization's systems, media and facilities that process and maintain information key to its operations. According to [18] "information security is the protection of information and minimizes the risk of exposing information to unauthorized parties". However, the bank's earnings and capital can be adversely affected when unauthorized persons get hold of their information and alters the data.

a. Effects of Social Media on Banks

The integration of social media tools in the workplace has posed vulnerability challenges to a bank's information security. [2], [22] although social media has been widely adopted by society, organisations have only recently realized their value.

In a Blue Paper Report by [19] presented to GFT, some credible banks in the international banking sector were mentioned as adopting social media in their operations. For instance Barclays Bank launched the Barclaycard community ring, which was to cater for users of credit card, giving a rich profile of each community member, rewards schemes for highly used credit cards and also getting feedback for service improvement. Barclays has also released their own phone apps that allow their customers to do mobile payments.

CitiBank US in an effort to have a great brand presence as a strategy of social marketing also adopted a portal on Facebook. With more than half a million likes, the bank maintains a positive agenda on their social media relations with customer. All operations at Fidor Bank are online and the bank describes itself as "banking with friends" [19]. The sign-on to Fidor Bank is through Facebook Connect and is one of the few banks that allow that. Their aim as a customer centric bank with technology and social media as a strategy has worked well and user/customer interaction on bank services and suggestions and expectations has helped the bank survive till date. Community banking and voice of customer in social media has helped in their strategy.

b. Business Benefits of Social Media for Banking

Social media provides faster, cheaper and interactive platform to disseminate information. Most banks have benefited from social media in their interaction with customers by:

- Bringing awareness to customers on basics of banking and finance
- Providing information on Government regulations that impact customers in banking industry, such as Know Your Customer (KYC), Anti-Money Laundering (AML), Customer Due Diligence (CDD).
- Creating brand presence through brand building in the form of pictures, videos, text or games.
- Education of customers on the do's and don'ts of Credit or Debit card usage

- Education of customers on identifying fake notes to avoid fraudulent monetary deals
- Projection of importance of data confidentiality and privacy of customer data.

c. Problem Definition

The impact and the intense effect of social media cannot be ignored and the early steps are taken can lead to the avoidance of risk inherently caused by employees and users of the institutions, the better. The main concern here is risk i.e. the risk that when the organization becomes vulnerable possess and therefore, the need to critically examine every processes to ensure information assurance, business continuity, efficient and effective business objectives to regularly checking, updating and instituting measures to curb usage.

The integration of social media tools in the workplace can also pose challenges to a bank's information security. Banks have become vulnerable because of the security risks attached to the wide use of social media in the workplace. The information security of an organization is instituted to protect their image and assets. Hence once an organization's information security is broken into, the risk of losing the business and trade secrets in the competitive market becomes high.

The use of social media by employees has been singled out among other factors as playing a vital role in this phenomenon [8]. It can be asked, what extent can be harmful? And how knowledgeable are employees on organization privacy? And do they know when to draw the line per the organization's security policies?

d. Aim

The study aims at researching into the impact of social media usage on the culture and information security policies in the bank. The risk that banks are exposed to by employees' usage of social media at work place, employee endangerment of company security and the risk factors associated with social media and information security.

e. Five Principal Challenges

The study will address the following question at the end of the study as posed by [20]. Wilson identifies the five principal worries that management faces with regards to social networking and information security. These are:

These five principle worries were identified as:

A. **Perceived Loss in Staff Productivity** – This is as a result of staff gossiping freely in an open environment and causing data leakage. Social media gives room for such free conversations on social network which may cause insecurities in the policies of the organization. An analysis of this principle will explain the effect of social media use at the workplace.

B. **Lack of Security Awareness** – It is the belief that the use of social networking websites is detrimental to company's information security. This is a result of most employees lacking training in information security issues and lack of awareness creation by management to ensure their workers or employees are cautioned on the endangerment of social media at the workplace.

C. **Reputational Damage** - Social media can be used as platform for damaging the reputation of a company and sometime this becomes easier when employees are mostly using social media. Hence leakage of information and other internal issues can easily be shared. The increased risk of liability may cost the company a large amount of money in clearing their name.

D. **Litigation Factors and Employee Morale** - A company can face lawsuits and bad publicity as a result of employee use of social networks. This cause threat to their information security and eventually makes them vulnerable to public scrutiny. This litigation factors eventually comes back to affect the employees and affects their morale negatively.

E. **Network Access** – Technically computer servers can only process so much information one at a time. The use of social networking website by employees at the workplace, alongside company emails, company computer programs, applications and software can slow down the servers. This is a result of the concurrent interplay of two or more websites. This affects the information systems network, exposing the company to risk. Such risks can be associated with data loss and network breaks, threats such as spam and malware.

II. Reviews of Related Studies

A. Definitions of Social Media

Reference [3] defined social media as web-based services that allow individuals to construct a public or semi-public profile within a bounded system. It allows list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. However the various social media platforms differ greatly in functionality and size.

B. Categories of Social Media

The main categories of social media are social networks, blogs, microblogs, online rating sites, social bookmarking, podcasts, forums/message boards, social knowledge/wikis, Geo-location and Multimedia.

C. Social Media Use by Employees

Although most organizations are intrigued by the business benefits of social media, other organizations however are still wary about social media usage. This is as a result of less productivity caused by employees viewing YouTube or Facebook at the expense of their work. Statistics show that most organisations including banks, put up with 45% of their workers' productive time being wasted on these aforementioned social networks and similar social media sites [14].

Reference [13] conducted a research on the Effect of Social Media Participation in the Workplace on Employee Productivity. Their findings indicated that there is extensive use of social media by most employees transferred from their personal life to the workplace. Also it was deduced that there is a link between social media use and job performance. The greater the personal use of social media the higher its negative effect on employee productivity.

Reference [4] in their journal research "Web 2.0: Conceptual Foundations and Marketing Issues," points out that organizations have begun to accept that social media applications can be used for more than just connecting individuals but also for communicating their branch and message to customers. However Strategic value is created for many organizations that create a strong flow of knowledge between the consumers and organizations through social media connection.

D. Information Security in Organizations

Every organization presumes to places value on its security and privacy. But not so much is invested in improving and maintaining it information security from unqualified persons. Unauthorized information which leaks out of the company can have very disruptive outcomes. Some of the factors reviews includes:

Lack of Awareness: The lack of awareness creation for employees on security and privacy responsibilities can cause a threat to the organization. [12] classified information systems security into five categories namely: Internal Control Assessment, Proactive Security Culture, Security Training, Security Policy Implementation, Individual Values and Beliefs in their research on "Developing Theoretical Base for Studying Governance: The Case of Information Security." Here they argued that an organization's information security does not depend solely on its technical features but also on employees' approach to security matters.

Reputational Damage

One of the major security issues that impacts on a bank is reputational damage. Here [17] in its submission in the Global Information Security Survey, argued that insider attacks are more successful than outsider attacks, and such weaknesses in an organisation produce high cost not only in monetary terms but their the image of the organization.

Lack Of Training And Security

Another challenge is the lack of training and security awareness that must be part of strategic imperative for the employees but has not been prioritized. [14] did a study on the topic "The Madness of Crowds: Employee Beliefs about Information Security in Relation to Security Outcomes" and they claimed that training and security awareness are essential components to improve organizational security.

To further establish the need for security implication of the use of social media, [6] also argued that "effective security organization, positive security leadership, monitoring of employees' behaviours and a clear designation of user roles and behaviours become beneficial countermeasures to improve security status". This will improve information security strategy through proper operational and technical procedures and ensure countermeasures in an environment where social media is prevalent as well as enhance an Organizational Security Measures.

Information Security Vulnerabilities

The increasing use of social media in the workplace and the lack of awareness of employees of their security and privacy responsibilities can be detrimental to the organisation. [8]. Posits that some identifiable threats of social media such as malware and illegal activities can cause damage to a banks reputation. Such threats leaves the information of a bank vulnerable to risks such as hacking, Denial of Service and fraud can lead to damaging effects to the banks financial standing and profit margins.

According to [5] "these concerns of vulnerabilities, has led many banking institutions to ban social media sites outright. For instance Credit Suisse and Lloyds TSB use security systems to block access to social media sites. However there is restricted access to Facebook in Citigroup and Goldman Sachs companies as advised by their management."

III.METHODOLOGY

A. Research Design

A cross sectional survey was adopted to identify the impact of social media usage in the banking industry in Ghana and the population comprises of of Eighteen (18) Bank branches located in Ghana, West Africa with survey population made up of two hundred staff. A non-probabilistic sampling technique was used to select of Sixty (60). However, not all targeted sample size responded to the questionnaires. A total Forty (40) questionnaires were completed and twenty (20) questionnaires were returned unanswered and only. Hence, the response rate of 67% was therefore used for the analysis.

B. Research Approach

The instrument used for this research was the structured questionnaires to collect the required data from staff of which all the questions were closed – ended. The questionnaire consisted of two sections. Section A: The socio-demographic information of respondents section in the questionnaire aimed at collecting information on the general background of the respondents as sex, work experience and educational background. Section B: focused on examining the Personal use of Social Media, use of Social Media at the Work place by Employees and its Impact on Organizational Information Security as well as Employee attitude. The section was measured on a Five Point Likert Scale for respondents to choose.

C. Data Collection & Analysis

Both primary and secondary sources of data were adopted for this study. The primary data was conducted by face to face means with respondents of the bank and helped in achieving the objectives of the study through questionnaires administered.

Data generated and obtained are those from first-hand information (primary data) by the researcher mainly by questionnaire. Secondary data was also gathered from sources like journals, books, business reports, magazine and articles of related information. Qualitative analysis was employed, data collected was sorted, edited, coded and entered in the software. Questions with Strongly Disagree, Disagree, Neither Agree or Disagree, Agree and Strongly Agree) option answers were coded as 1,2,3,4 and 5 ranks.

The analytical instrument for this study used was the Statistical Package for Social Science (SPSS) data analytic tool. Microsoft Excel was also used in calculating frequencies and drawing of graphs and charts to describe various sets of data and pictorial illustration of some results.

IV. RESULTS AND ANALYSIS

This section deals with the analytical presentation of results of the data collected from respondents in line with the key objectives. The research questions raised were:

1. What is the extent of the culture of social media usage by employees in their personal lives and at the workplace?
2. What is the level of awareness of organizational information security by employees?
3. How exposed is the bank to the risk of using social media during working hours?
4. What ways can information security be protected from being penetrated by employees' use of social media?

Keys for Analysing Table Results

KEYS	DESCRIPTION
n	Number of Respondents
N	Sample Size
Mean	Number of Respondents divided by Sample Size (n/N)

Std Dev.	Standard Deviation – Measures the deviation from the Mean. The deviation range is 0.0000 – 1.0000 for precision.
Std Error	Standard Error – Measures the error margin within the deviation range.

Table 1 - Keys for Analysis

Choice of Social Media by Employees

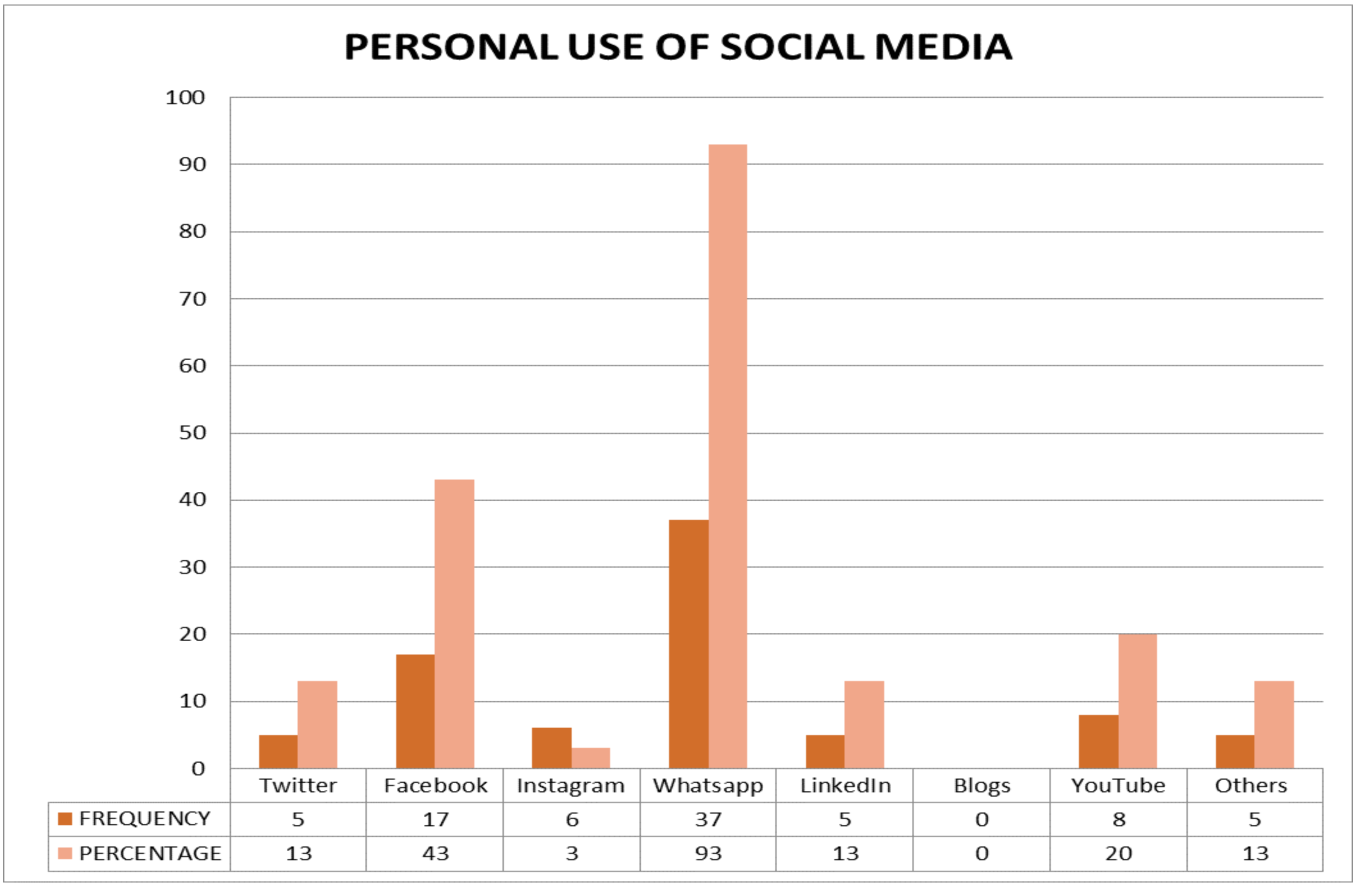

Figure 1–Bar chart for Social Media Choice by Employees   Source: Primary Data 2017

Frequency of Social Media Use Daily

Respondents were asked if they *spend about 10 minutes on social media daily* and the responses for either YES or No are tabulated below and further demonstrated on a pie chart.

RESPONSE	**FREQUENCY**	**PERCENTAGE**
YES	33	85%
NO	6	15%

Table 2 - Frequency of Social Media Use by Employees

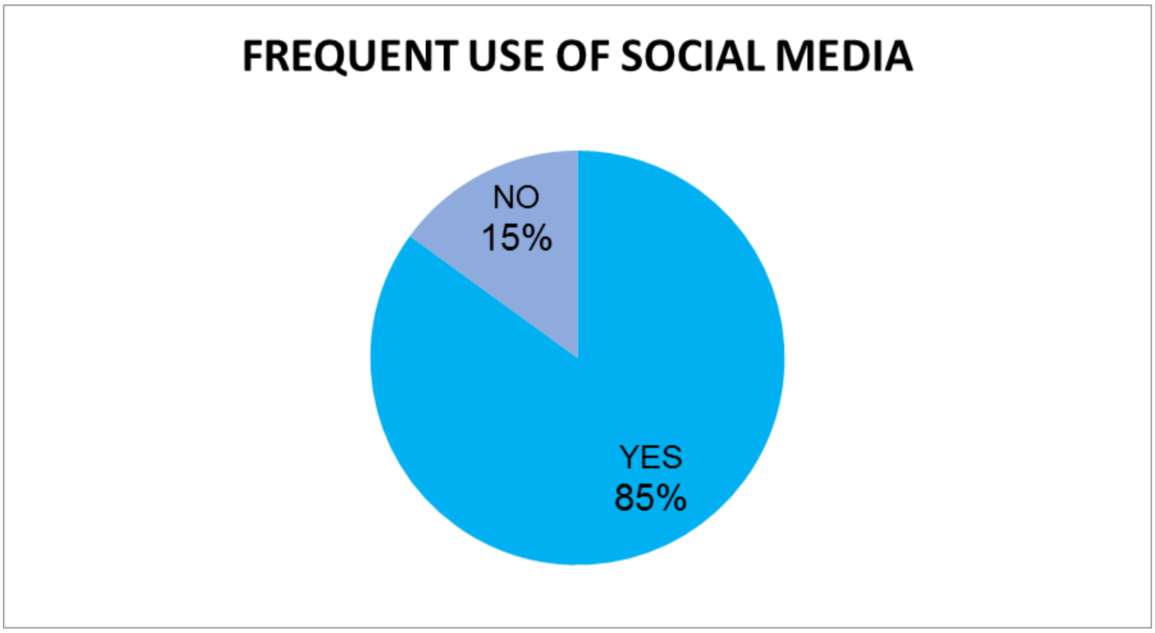

Figure 2 - Pie Chart Illustration of Frequent Use of Social Media by Employees

In the data gathering and analysis of the research questions above, this research was geared towards answering the following issues as raised by [20] in his quest to identify the principle worries that management faces with regards to social networking.

A. **Perceived Loss in Staff Productivity**
B. **Lack of Security Awareness**
C. **Reputational Damage**
D. **Litigation Factors and Employee Morale Network Access Vulnerabilities**

A. Perceived Loss of Productivity

It is a worry for most organisations that there is reduction or loss in productivity when staff use working hours for other things not included in job schedule. Such practices in the long run affect the company's profitability status. Involvement of social media extensively at the workplace for personal use can be detrimental to the organisation.

The researcher in this case study of Bank, the extent of social media use in personal lives of employees and to the workplace. Below is a table representation of the variables measured and the level on which respondents' indicated is shown in table 4.5 below.

Table 4A: Employee Personal Use of Social Media

Item No.	Item Statement	N	Mean	Std Dev.	Std Error
5	Would you say you spend about ten (10) minutes on social media daily	38	1.1538	0.36552	0.05853
6	Social media is important for keeping in touch with my family and friends	40	1.6000	0.9281	0.1467
7	Social media is an important tool for sharing information with my family and friends	40	1.7000	0.8533	0.1349
11	Social media makes my life better	40	2.7250	1.1319	0.1789
12	Social media services are the primary tool I use for communicating with my friends	40	2.0000	0.9607	0.1519

Source: Primary Data 2017

Scale: 1 = Strongly Agree, 2 = Agree, 3 = neither Agree nor Disagree, 4 = Disagree, 5 = Strongly disagree

From Table 4A, total mean of all responses for personal use of social media is 1.8. this was realised after finding the average of all the mean responses of the five item statements. Below are the workings:

$$\text{Total mean} = \frac{1.1538 + 1.6000 + 1.7000 + 2.7250 + 2.0000}{5}$$

$$= \frac{9.1788}{5}$$

$$= 1.8357$$

$$\approx \mathbf{2.0000}$$

From the approximate mean 2.0000 it can be concluded that employees of bank agreed that they use social media for personal use. Such as keeping in touch, communicating and sharing of information with family and friends. To them social media makes life better.

Table 4B: Use of Social Media at workplace

Item No.	Item Statement	N	Mean	Std Dev.	Std .Error
12 **YES** **NO**	Do you frequently respond on your social media during working hours?	38 6 32	1.842	0.3694	0.5995
13 **YES** **NO**	Do you use social media as part of your job schedule?	38 6 32	1.842	0.3694	0.5995

Scale: 1=Yes 2= No ***Source: Primary Data 2017***

From Table 4B, total mean of all responses for use of social media at workplace is 1.8. This was realised after finding the average of all the mean responses of the two item statements. Below are the workings:

Total mean = $\frac{1.8421 + 1.8421}{2}$

$= \frac{3.6842}{2}$

$= 1.8421$

$\approx \mathbf{2.0000}$

Similarly, from the approximate mean 2.0000 it can be concluded that employees of Bank do not use social media during working hours. It was also realised that use of social media was not part of their job schedule. This shows that management does not accept the use of social media during working hours and hence employees are not allowed to use it because it is not part of their culture.

Social Media Use: Personal and Work Place

ITEM	**MEAN**	**RESPONSES**
Personal Use of Social Media	2.0000	Agree
Use of Social Media at Workplace	2.0000	No

Table 5: Summary Table Social Media: Personal and Workplace

From the summary table 5 above, Personal Use of Social Media by employees was pegged at an approximated mean of 2. This proves that per the 5 – Likert Scale that was adopted for item statements, employees "Agree" to the use of social media constantly for personal use. Use of Social Media at Workplace was also approximated to a mean of 2 but on a different Likert Scale, Yes/No.

The mean of 2 signifies "No" and this means that employees do not use Social Media at the Workplace.

These results are further displayed on the bar chart below:

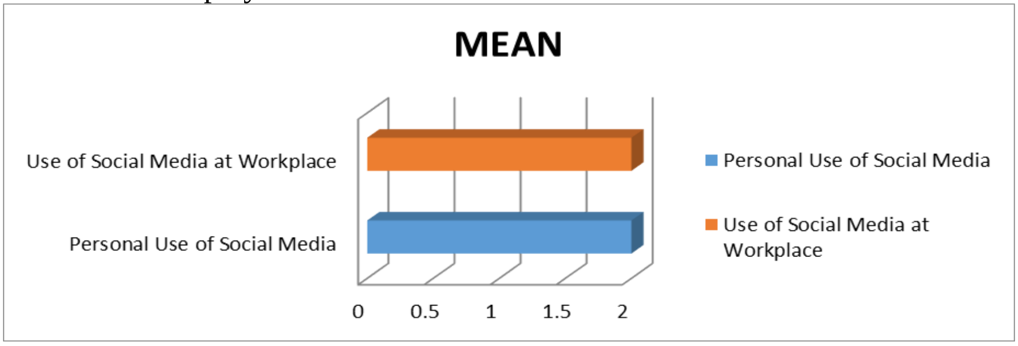

Figure 4.6 - Use of Social Media Personal and at Workplace

This figure 5.6 illustrates the mean of general view of employees on Social Media at the Workplace and Personal Use of Social Media. In both instances the results are favourable.

From table 4.5A, the analysis indicates that, the item/stem on the questionnaire: Social media is important for keeping in touch with my family and friends asked, had a mean score of 1.62 approximately 2.0 representing Agree on the likert scale with a deviation score of 0.928 within the error margin of less than one (0.14).

From the table above, it could be asserted that, majority of the staff of the Bank uses social media to keep in touch with family and friends during working hours. The next item statement (Social media is an important tool for sharing information with my family and friends) which was also measured in terms of strongly disagree as the least on the likert scale (coded 5) all through to the highest order of code 1 representing strongly agree had scores 1.7, 0.8533 and 0.1349 representing mean, standard deviation and standard errors respectively.

Similarly, the items; Social media makes my life better, Social media services are the primary tool I use for communicating with my friends scored a mean of 2.7250, 2.0, 2.0789 of approximately 3.0 and 2.0 each on the likert scale.

Thus, all items represented Agree on the likert scale except for the item ‘social media makes my life better which represented 3 meaning neither agree nor disagree. However, since, majority agreed on the scale we can opt for agree. This result is buttressed by the item in table 4.5B when the item ‘Do you use social media as part of your job schedule’ was scored on an approximate mean scale of 2.0 representing NO on the likert scale.

This further establish that, because management and board are aware of the impact of social media use on information security, this was excluded and ensured that staffs job schedules are not centred around social media.

B. Lack of Security Awareness

The level of security awareness with regards to organisation information security was tested. This is based on the literature that most employees are not security conscious and as a result of ignorance. Employees of the Bank were asked the following to ascertain if they lack security awareness:

Table 6- Security Awareness

ItemNo.	Item Statement	N	Mean	Std Dev.	Std Error
18	Does your bank's security policy inhibit your ability to share information with others social media platforms.	37	1.2703	.45023	.07402
21	My company trains employees to view information security as their responsibility	38	2.0789	1.0999	0.17843
22	The information systems of my company are monitored and thus, prevent security breaches	38	1.6842	0.6197	0.1005
23	There is an overall information security strategy in place at my organisation	38	1.7632	0.6752	0.1095
25	The employees are confident of their ability to demonstrate compliance	38	2.1842	0.8654	0.1403

Source: Primary Data 2017

Scale: 1 = Strongly Agree, 2 = Agree, 3 = neither Agree nor Disagree, 4 = Disagree, 5 = Strongly

From Table 4.6, total mean of all responses for level of security awareness or security attitudes is 1.80. This was realised after finding the average of all the mean responses of the two item statements. Below are the workings:

$$\text{Total mean} = \frac{1.2703+2.0789+1.6842+1.7632+2.1842}{5}$$

$$= \frac{8.98}{5}$$

$$= 1.80$$

$$\approx \mathbf{2.0000}$$

Similarly, from the approximate mean 2.0000 it can be concluded that employees of Bank have good attitude towards information security. Not only are they aware of information security policies but also adhere to it. Below is a chart to illustrate the findings:

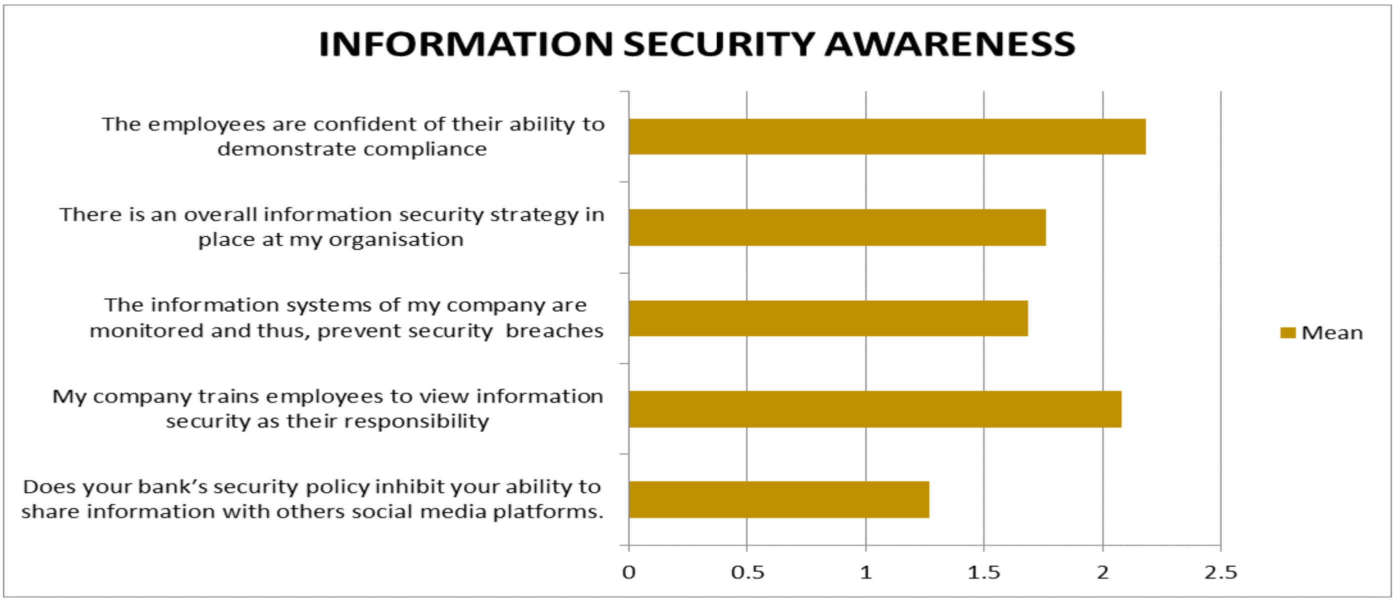

Figure 4.7 Information Security Awareness

The bar chart above (fig. 4.7) demonstrates the mean distribution of all the item statements on information security awareness. The mean range for all items is from 1 – 2 in approximation. This scale signifies "Agree"/ "Yes" as appropriate for the item statement. This confirms a positive a feedback on employees' awareness of organisational information security

C. Reputational Damage

The problem of risk associated with social media at the workplace was also tested. Such risks according to Literature, includes Reputational Damage. Such risks initiate vulnerability and put the bank in danger. It was necessary to test employees take on sharing personal information on social media, their concerns on privacy matters on social media, harassment on social media at workplace, etc. employees were asked the following to ascertain how exposed the bank to risk by the use of social media at the workplace by employees.

Personal Attitudes towards Sharing of Personal/Private Information on Social Media

ItemNo.	Item Statement	N	Mean	Std Dev.	Std Error
8	I do not share personal information on social media	40	2.4500	1.1756	0.1858
9	I am not concerned with the privacy of the information I share on social media sites	40	4.3500	0.8638	0.1365
10	It is important for me to fully understand the privacy options of social media technologies	39	1.6923	0.9501	0.1521
13	I share personal information with others via social media	40	3.1500	1.2100	0.1913
14	I trust social media sites with my private information	40	4.2750	0.9333	0.1475
15	I do not mind sharing private information on social media as long as it makes my life better	40	4.3750	0.8969	0.1418

Source: Primary Data 2017

Scale: 1 = Strongly Agree, 2 = Agree, 3 = neither Agree nor Disagree, 4 = Disagree, 5 = Strongly Disagree

Table 6 – Employees Attitudes towards Sharing of Personal/Private Information on Social Media

From the Table 6 above, the total mean of responses of the six questionnaires reviewed is 3.39. This indicates that employees neither Agree nor Disagree with sharing of personal or private information via social media. When employees Agree to *sharing of personal or private information on social media* it indicates that employees are not concerned about sharing everything about their life on an open social network. Hence they trust these networks with such information. Such attitudes give room for loose talk and leaking of information both personal and private which is not meant for public consumption.

When employees Disagree to sharing personal private information, they demonstrate concern of the kind of information that goes to the public about them. This makes them more cautious to avoid the harm of reputation.

The results of employees neither Agree or Disagree means that there is some uncertainty in sharing private information on social media. This means there could be some instances such information can be shared and other instances where such information are withheld. So there is some degree of risk for reputational damage due to leaking of information by employees. However it cannot be measured whether high or low.

Work Policy on Sharing Bank Information on Social Media

Item No.	Item Statement	N	Mean	Std Dev.	Std .Er ror
18	Does your company's security policy inhibit your ability to share bank's information with others on social media platform?	37	1.2703	0.4502	0.0740

Scale: 1=Yes 2= No **Source: Primary Data 2017**

Table 7 – Work Policy on Sharing Information on Social Media

From the Table 7 above, the mean of 1.2 indicates that employees agree that the Bank has security policies that inhibit the ability to share bank′s information with others on social media platform. This once again affirms the positive security attitudes of staff on organisational security.

However in merging their stand on sharing private information via social media and the company policies on sharing confidential information to other parties via social media means that there is a need to improve policies and also monitor staff. Their indecisiveness on sharing private information may end up causing more harm than good and can make the bank liable to risk.

Below is a diagrammatic illustration (Fig. 5.7) of the two tables on liability of risk and its effect on bank′s reputation.

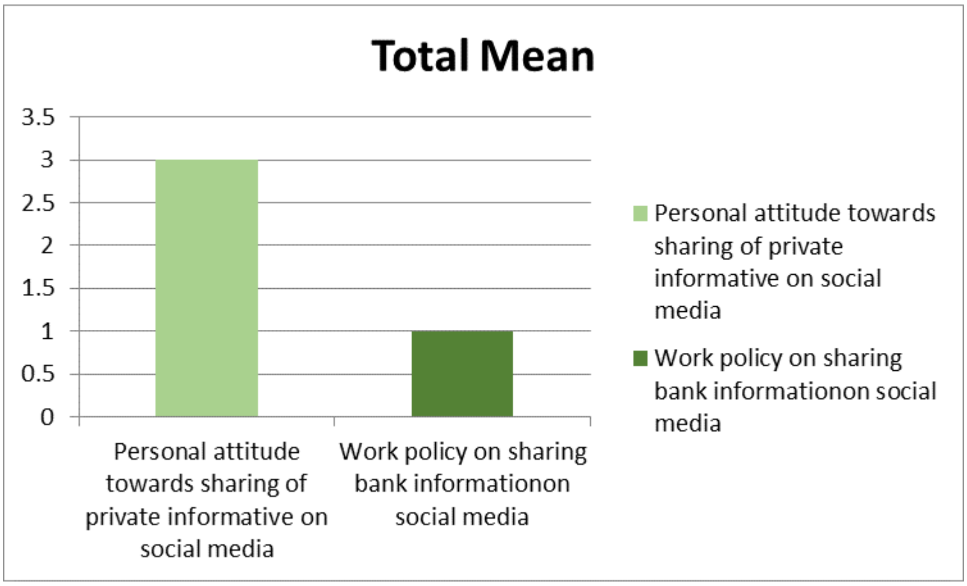

Figure 4.8 - Sharing of information : Personal attitude and Work Policy

D. Litigation Factors

Litigation issues arising from law suits such as harassment include; sexual harassment, cyber bullying and threats may cause financial Loses incurring due to compensations paid to clients in the event of data breaches, penalties rising from the breach of agreements and loss of productivity. Organizations fail to carryout cost benefit analysis and those loses required for counter measures and insurances.

This risk factor was examined with two questionnaires numbered 20 and 25 on a YES or NO likert scale followed by analytical computations of mean, standard deviation and error using the SPSS. The respondents were asked on the following to determine the degree of risk in the area of litigation, cost, bad publicity and demoralisation of staff. The analysis of Mean, Standard Deviation and Margin of Errors are shown in Table 8 below:

Table 8 – Litigation Factors

Item No.		**N**	**Mean**	**Std Dev.**	**Std Error**
20	Have you or any of your colleagues experienced any (Sexual) harassment on social media platform?	39	1.9231	0.2699	0.0432
25	Have you experienced or witnessed a situation in which social media caused harm to you or a colleague?	36	1.6389	0.4871	0.0811

Scale: 1=Yes 2= No **Source: Primary Data 2017**

The analysis of Litigation Factors had a weighted average mean score of 1.79 approximate 2 representing NO on the likert-scale for the items: The item *Have you or any of your colleagues experienced any (sexual) harassment on social media platform?* Had a mean score of 1.92 representing “NO” on the likert scale. This means sexual harassment may not be a risk factor in terms of social media. Similarly the item *Have you experience or witnessed a situation in which social media caused harm to you or a colleague* had a mean score of 1.63 which represent approximately NO on the likert scale.

The line graph below further visualises the results on litigation:

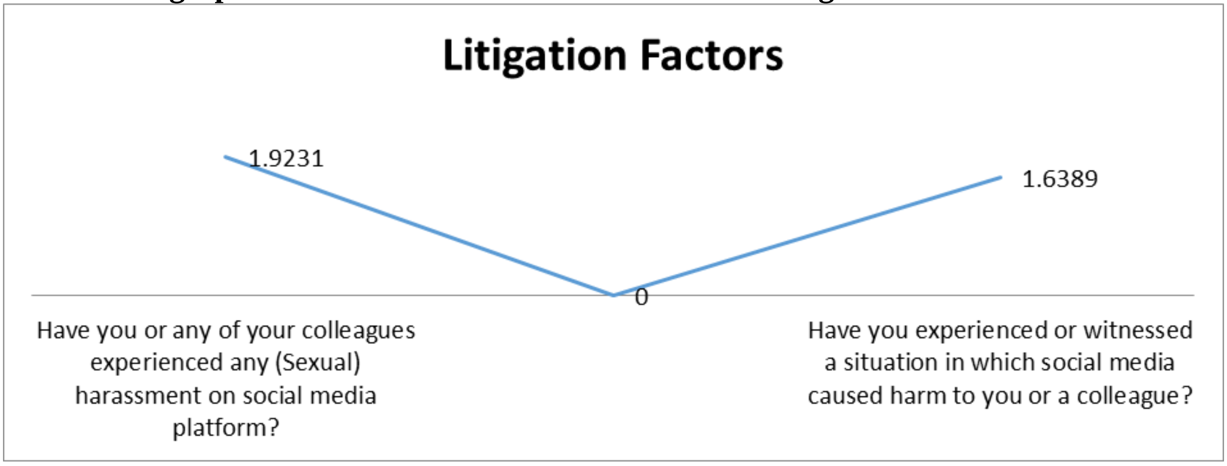

Figure 4.9 Litigation Factors

From the analysis above (Table 8 and Figure 4.8), it can be concluded that Bank as one of Ghana’s strong resilient banks has mechanisms in place that controls risk factors which are associated with use of social media and their information security. Thus risk factors such as sexual, workplace violence and bullying degrees of harassments which can lead to law suits, bad publicity, public ridicule and other litigation issues are absent in the bank.

E. Network Vulnerabilities

The access to corporate emails are available to staff during working hours as they can login to the network system from their mobile devices. This may slows down the server when social media sites run concurrently with corporate mails as well vulnerabilities such as data loss, network breaks and threats like spam and malware.

Employees of were asked *if network systems are monitored and thus, prevent security breaches* and the mean was 1.6842 which can be approximated as 2.00.
This is YES on the Likert scale. This means there are existing monitoring procedures to ensure employees do not involve any security breach.

They were also asked *if they often do not receive spam (unwanted) mails in their corporate mail* and the mean response was 2.9737 approximately 3.00. And this figure stands for neither Agree nor Disagree. Employees were not confident to answer it straight as a result of the sensitivity of the question.

Table 8 – Network Vulnerabilites

Item No.	**Item Statement**	**N**	**Mean**	**Std Dev.**	Std .Error
18	The information systems are monitored and thus, prevent security breaches	38	1.6842	0.6197	0.1005
22	Employees often do not receive spam (unwanted) mails in their corporate mail	38	2.9737	1.2837	0.2082

Source: Primary Data 2017

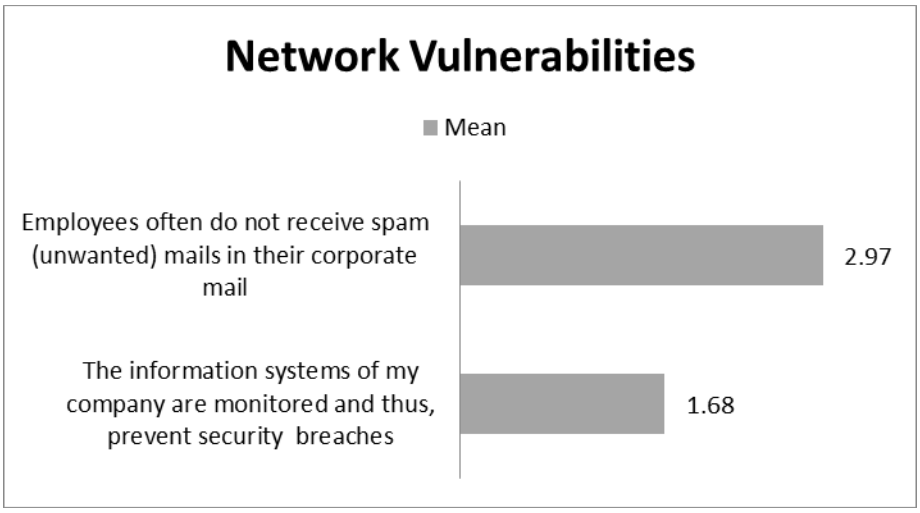

Figure 9 – Bar Chart on Network Vulnerabilities

Per the table and the figure illustrated above, it can be deduced that although bank has monitoring procedures, it should be tightened to avoid spam mails getting through corporate mails. Care must be taken to ascertain that although employees were uncertain on answering this question, it is a matter of great concern and management must pay great attention to it.

V. Conclusion

The research findings establish the negative impact of social media use by employees on Banks information security systems in Ghana. The effects can be explain first by the fact that, they use social media for their personal use at the workplace which impacts on productivity. Secondly, attitude of staff towards information security also revealed that employees are not aware of the dangers and implications of the level of information security vulnerability. Thirdly, the bank's exposed level of risk as a result of the use of social media usage was high due to lack of proper security system strategy in place to prevent and control unwanted spam and malware mails. Factors such as ligation issues and cost arising from cybercrime, cyber bullying, sexual harassment and threats may cause financial lose are some of the negative impacts. Studies shows therefore that, it is important to ensure there are control measure through constant training and awareness. Put in place preventive methods such as proper policy formulation, generating reports of staff abuse and warning them. Research findings further showed that there were significant positive perceptions of respondents in regards risk exposure, attitude and protection of information security. The results indicates that social media usage if not well managed may lead to a loss of productivity or reduced employee.

Further research work will be focused on the impact of threats and vulnerabilities of social media threats on banking industries electronic products and services on mobile devices in Ghana

References

[1] Ajzen, I. (1991). “The theory of planned behavior,” Organizational Behavior and Human Decision Processes (50), pp. 179-211.

[2] Awazu, Y., and Desouza, K. (2004). "*Open Knowledge Management: Lessons from the Open Source Revolution,"* Journal of the American Society for Information Science and Technology, (55:11), pp. 1016-1019.

[3] Boyd, D., and Ellison, N. B. (2007). *"Social Network Sites: Definition, History, and Scholarship*," Journal of Computer-Mediated Communication, (13:1).

[4] Constantinides, E., and Fountain, S. (2008). *"Web 2.0: Conceptual Foundations and Marketing Issues,"* Journal of Direct, Data, and Digital Marketing Practice, (9), pp. 231-244.

[5] Chi, M. Security Policy and Social Media Use: Use offenses to Inform Defense. Find Flaws Before The bad Guys Do. SANS Institute

[6] D'Arcy, J. (2005). Improving IS Strategy Through Procedural and Technical Countermeasures: An Analysis of Organizational Security Measures. Philidelphia, PA: Temple University Irwin L. Gross e-Business Reserch Report.

[7] Dillman, D. A. (2000). *Mail and Internet Surveys: The Tailored Design Method*. John Wiley & Sons, Inc, New Yor, NY.

[8] Dutta, S. & Fraser, M. (2009) When Job Seekers Invade Facebook. The McKinsey Quarterly.

[9] Fagnot, I. (2007). *"Behavioral Information Security," in Encyclopedia of Cyber Warfare and Cyber Terrorism*: Berkshire Publishing Group LLC, (1), pp. 199-205. Global Information Security Survey. 2002. Ernst & Young LLP.

[10] Goh, D. H.-L., Ang, R., Chua, A. Y. K., and Lee, C. S. (2009). *"Why We Share: A Study of Motivations for Mobile Media Sharing,"* Lecture Notes in Computer Science, (5820/2009), pp. 195-206.

[11] Kidwell R.E. (2010). Loafing in the 21st century: Enhanced opportunities and remedies for withholding job effort in the new workplace. Business Horizons, 1-10.

[12] Mishra, S., and Dhillon, G. (2006). *Developing Theoretical Base for Studying Governance: The Case of Information Security.* Paper presented at the Web 2006 - International Conference on Information System.

[13] Munene, A. G. & Nyaribo, Y. M. (2013). *Effect of Social Media Pertication in the Workplace on Employee Productivity*. International Journal of Advances in Management and Economics.

[14] Satyanarayana, A. (2009). Five Security Risks of Social Networking Websites.

[15] Schultz, E. E. (2002). "A Framework for Understanding and Predicting Insider Attacks," Computers & Security,(21:6), pp. 526-531.

[16] Stanton, J. and Stam, K. (2006). The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets- Without Compromising Employee Privacy or Trust, Information Today, New Bedford, NJ.

[17] Stanton, J. M., Yamodo-Fagnot, I., and Stam, K. R. 2005. *The Madness of Crowds: Employee Beliefs about Information Security in Relation to Security Outcomes.* Paper presented at the The Security Conference, Las Vegas, NV.

[18] Venter, H.S. & Eloff, J.H.P. (2013). A Taxonomy of Information Technology. Computers & Security. University of Pretoria. Article.

[19] Virgili, J.A. & Kaganer, E. 2012. Impact of Social Media on Financial Service Sector. Report Produced for GFT by IESE Business School.

[20] Wilson, J. (2009). Social Networking: The Business Case. Enginnering & Technology (4)10 54-56. IET Digital Library.

[21] Yates, D., and Paquette, S. 2010. *Emergency Knowledge Management and Social Media Technologies: A Case Study of the 2010 Haitian Earthquake*. Paper presented at the The American Society for Information Science and Technology Annual Meeting (ASIS&T).

[22] Yates, D., Wagner, C., and Majchrzak, A. 2010. *"Factors Affecting Shapers of Organizational Wikis,"* Journal of the American Society for Information Science and Technology, (61:3), pp. 543-554.