THE IMPACT OF INFORMATION SECURITY BREACHES ON BANKING INFORMATION SYSTEMS FROM THE YEAR 2000 TO 2009

Peter Tobbin & Paul Danquah

Abstract

This research seeks to analyze the impact of Information Security breaches prone to selected Ghanaian banking institutions from the year 2000 to 2009. The results of this work were obtained through the review of related literature, questionnaires and observation. The results obtained are analyzed using the evaluative reporting of the data, supported by tables and charts where applicable. Recommendations are subsequently made to address the security breaches identified. The outcome of the research tends to place the findings in context by elaborating on how the research findings and results contribute to the field of Information Security in general and what sort of broader implications these may have. This will allow for greater understanding of Information Security issues within the banking sector and hopefully prompt for further in-depth research into its impact on the institutions and customers as a whole. A recommendation is made to banks to define the Information Security policy and effectively implement the policies by educating all staff on acceptable and best practices.

Introduction

An information system is interrelated components working together to collect, process, store and distribute information to support decision making, coordination, control, analysis and visualization in an organization (Laudon and Laudon 2006). The last five years have seen a significant rise in the number of banks and other financial institutions (notably, savings and loan companies, insurance) in Ghana. This has led to an increase in the number of personal account holders in the country.

Parallel to this growth is the use of electronic payment systems and debit and credit cards for transactions. Also, the traditional banks in

Ghana have mostly migrated from the use of manual systems to electronic business transactions. At the heart of all these is the collection, storage and transmission of sensitive data by the banks. This research therefore seeks to assess the level of protection and preparedness that the banks have implemented to avert any possible information security breaches.

Information security is the confidentiality, integrity and availability of information assets (NIST handbook 1995). Confidentiality is the preservation of authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The assigned level of confidentiality is used in determining the types of security measures required for its protection from unauthorized access or disclosure. Integrity is guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. The level of impact of unauthorized modification or destruction of information resources determines the importance of maintaining the integrity of a resource. Availability is ensuring information is always accessible by authorized users with no or very limited outages.

Security breach is when confidential and restricted information of an individual is reasonably believed to have been acquired by an unauthorized person.

(Chapel and Stewart,2004). For example, acquisition of personal information by a staff/employee of an organization or agent for bona fide business purposes does not constitute a security breach, provided that the personal information is not used or subject to further unauthorized disclosure. Also, it can be described as any steps taken by an individual or group of persons to circumvent existing controls established to provide confidentiality, integrity and availability of an information system. This should include physical controls.

Over the last two decades companies have experienced a number of security breaches of significant impact. The 2002 Computer Crime and Security Survey, conducted by the Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) of the United States of America, reports that 90% of respondents detected computer security breaches within the past year (R. Power, 2002). A survey by Forrester indicated that, out of 410 Information Technology (IT) decision makers, about 75 percent reported that Information Technology (IT) security has become critical to their business planning and over 80 percent reported that they are concerned about financial losses from it (Muncaster 2006).

In another survey taken from risk managers of the U.S and European companies, computer risk was ranked as the top concern among European companies and the number two concern among U.S. companies (Hovav, A. and D'Arcy, J 2006).

All the banking institutions have information assets essential to their survival. Arguably, information in its various forms is one of the most important assets to most banks, be it printed, stored electronically, posted or e-mailed, shown on film or spoken. For most of these organizations, information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance and commercial image. An absence of information security in banking and financial organizations may threaten their integrity and, therefore, very existence. The economic implications of

corporate information security breaches remain an empirical issue.

This research seeks to analyze the impact of information security breaches on the Ghanaian banking organizations.

The research approach involves the review of related literature, censoring for related information via questionnaires and observation. The results obtained were analyzed using the evaluative reporting of the data, supported by tables, figures, and charts where applicable. The research is then summarized with recommendations.

Caveat on Results and Analysis

1. Most banks were quite reluctant to provide information regarding their experienced security breaches.
2. Banks were also unwilling to reveal security information regarding vulnerabilities on their networks and systems.
3. Some respondents within the same bank provided varying and contradictory information in their response to questions asked.
4. Most of the respondents indicated they were uncomfortable bringing their security issues to public knowledge especially information related to financial implications.
5. Some banks specifically indicated they considered the information required as confidential hence their inability to disclose.

OBJECTIVES OF STUDY

The specific objectives for carrying out this research are :

1. To identify the types of information security breaches experienced by the banking sector.
2. To assess the financial implications of the information security breaches on the banking sector
3. To determine the impact of information security breaches on the service level of banks

LITERATURE REVIEW

Evolution of Information Security Breaches

Even though it is possible to date the evolution of Information Security Breaches to the history of man, it is fair to limit it to the revolution of Information Technology and the Internet. In the past, information security breaches were mainly in the form of physical break-ins, unauthorized entries into critical infrastructure locations such as vaults in banks and disgruntled employees stealing information for competitors. These have historically been viewed as traditional property crimes where trespass, theft, and vandalism were the motives. The modern trend of using computer networks to remotely monitor and control unmanned facilities has also increased the possibility that these crimes could be used to conceal less discernible crimes. For example, the physical breach of a vault in a bank to steal money could be viewed as a simple case of burglary. In modern days however, such an event could just as easily be a distraction to draw the bank's attention and investigation away from the real motive.

The real motive in this context could be to gain access to the systems and devices within the facility (bank) in order to either launch an immediate electronic or cyber attack. It is also possible to introduce hardware or malicious software into the bank's network, thereby establishing an electronic or cyber foothold for future attacks or stealing sensitive information (Chapel, Stewart et al. 2004).

Forms of Information Security Breaches

Information security breaches can be categorized into several groupings: internal and external; structured and unstructured; technical and non-technical. Activities by employees of an organization, either intentional or unintentional can lead to an information security breach. For example, employees of a bank may steal the credit card information of customers and sell to cyber criminals. On the other hand, certain lack of appropriate employee training on the use of a system may cause an unintentional security breach.

Structured security breach is where organized steps of attack are applied in causing the security breach. An example of a structured security breach is applied in hacking, phishing or identity theft. Unstructured security breach is where certain activities especially on the Internet lead to a security breach in an organization's infrastructure.

Usually the perpetrators are s not even aware of the full (financial, legal, social, economic etc) impact of their actions.

Objectives of Information Security Breaches

According to Mohay (2003), there are as many reasons for performing information security breaches as there are network security attacks, but, there are a number of common themes, in no particular order.

1. **Industrial Espionage** – Companies may hire a cracker or hacker to try discovering competitors' secrets. This is usually the case when a company has fallen behind in the research and development sector.

2. **Vandalism** – This is typically a case of intent to destroy or sabotage where perpetrators do not reap any commercial benefits. There may be consequences for the perpetrator yet they seem to derive fulfillment from inconveniencing a lot of people.

3. **Accidents or Curiosity** – It is quite common to perform a network security attack completely by accident. It usually occurs when perpetrators are unaware of the Trojan on their system or they activate a malicious attachment received via email.

4. **Peer Recognition** – This scenario is most prominent in environments where hackers belong to a recognized community. Hackers operate with the mentality that the more difficult a system is to crack the better and the more systems successfully hacked the more popular one becomes within the community.

5. **Money** - Financial institutions make considerable efforts to reduce their risk from network security attacks, and with good reason. If a perpetrator can crack a bank they stand to make a ton of money. Hackers who are therefore selective about what they crack stand a good chance to reap financial benefits.

6. **Imperva (2004)** explains that other notable objectives are terrorism, political and religiously motivated hacking. Studies provide insights into the economics of information security, but do not investigate the actual magnitude of losses associated with information security breaches. Empirical research that examines the economic aspect of corporate information security breaches is largely descriptive in nature, and has focused on the direct financial cost of information security breaches. This descriptive research is comprised largely of survey results com-

piled and analyzed by professional organizations.

However, Gordon and Loeb (2002) indicated that the quantity and quality of survey data on the impact of information security breaches is limited, since many banking and financial institutions are unwilling or unable to quantify their losses. According to Patterson and Smith (2005), the combination of survey results and popular press reports leaves little doubt that information security breaches are commonplace among banks. What is unclear, however, is the economic impact of these breaches on financial institutions.

Arguments regarding economic impact of security breaches on banks

Kedrosky's argument from the article "Hackers prey on our insecurities" advanced that the economic consequences of these breaches on banking and financial institutions are highly consequential. This argument is intuitively appealing, as there are a variety of potential costs associated with information security breaches. These potential costs include a dent in reputation and credibility to public, loss of revenue, potential legal liability and activities associated with detecting and correcting the breaches which invariably becomes expensive.

The February 10, 2000 issue of The Wall Street Journal reported that a denial of service attack against Yahoo!, "brought Yahoo!'s website to its knees, costing it an estimated $500,000 in a scant three hours"; this suggests evidence that substantial economic costs are associated with information security breaches. As reported in CIO, The Yankee Group estimated the total losses related to the February 2000 denial of service attacks were $ 1.2 billion.

An alternative argument according to Gordon and Loeb (2002), however, suggests that the economic consequences of information security breaches are trivial over the long run. The intuition underlying this argument is that firms protect their most valuable information assets (e.g., secret formulas for key products, valuable customer data) at a higher level than their less valuable information. That is, since all information cannot be protected to the point where there is zero probability of a security breach, firms may allocate their security expenditures in a manner that minimizes the economic impact of security breaches. Accordingly, there is reason to believe that most information security breaches that actually occur may have a small (or insignificant) economic impact on the value of a firm.

Additional anecdotal evidence consistent with the insignificant economic impact argument includes consequences of a series of hacker attacks resulting in shutdowns at companies such as Yahoo! and Amazon.com in February 2000. On the day of the attack Yahoo! was shut down for almost 3 hours, and its Web traffic dropped 11% relative to the same day the week before the breach. However, by the next day, the number of unique visitors to the site returned back to normal, and up 9% from the same day of the prior week. The trends were similar for other companies hit by this denial of service attack.

The above statements are consistent with the argument that at least some varieties of information security breaches are viewed as a normal cost of business. For firms that are heavy users of information technologies, costs associated with the security breaches that occur may be similar to inventory shrinkage costs for a retailer.

Certainly, some efforts are taken to contain these types of costs, but by and large they are

viewed as a cost of doing business. The cost of eliminating these events/losses altogether may exceed the benefits. Data reported in the CSI/FBI 2002 "Computer Crime and Security Survey, Computer Security Issues and Trends" survey are consistent with this view. Thus, there is subjective and self-reported survey evidence consistent with each of two competing arguments regarding the economic impact of information security breaches.

A third argument made by T. Bridis in the article "E-Business: Microsoft takes steps to thwart hacker attacks". (The Wall Street Journal, January 29), says that information security breaches may have a net positive long-term economic impact on firms. This third argument is based on the premise that firms respond to breaches by making new investments in information security. Thus, an information security breach may signal imminent, and previously unanticipated, investments in information security. These investments might have long-term economic benefits that exceed the cost of the breach that spurred the investment. If this were true, the expected net economic consequences of both the breach itself and the anticipated future benefits of information security investments signaled by the breach would have to be considered.

The three main theories advanced in the above review points to the following:

1. Information security breaches have a highly significant negative economic impact on firms.

2. Most of these events have minimal economic consequences for firms.
3. Information security breaches may have a net positive long-term economic impact on firms.

A critical review and analyses of the three arguments stated above by Kedrosky, Gordon and Loeb, and Bridis reveals that in order to investigate these competing arguments concerning the economic impact of information security breaches using a rigorous empirical analysis, one needs to identify both the premises and substance of the arguments.

Indeed, while all information security breaches are potentially costly, those that involve access to confidential firm and/or customer data may be the most costly. That is, customers, stockholders, and other stakeholders would likely be willing to accept some types of information security breaches (e.g., denial of service) as a routine risk and a normal cost of doing business.

METHODOLOGY

The approach to this research involves gathering information from completed questionnaires and interviews. This study is a cross-sectional study hence various segments of the banking sector are sampled and relationships among variables investigated by cross tabulation. Data is gathered from both primary and secondary sources.

Primary data consist of gathering information from respondents of some banks and companies via the use of questionnaires and interviews whereas the secondary source included books, articles, journals, publications, bulletins, the Internet and other related literature for the purpose of the study.

Fifty (50) questionnaires were served to ten (10) banking institutions in Ghana whereas five individuals were interviewed. This comprises an average of five (5) respondents each

from the Information Technology departments of each of the ten (10) banks.

Random Sampling was used in selecting banking institutions for the research work. Specifically, the banks selected were Agricultural Development Bank (ADB) GH, Standard Chartered Bank (SCB) Ghana, Zenith Bank Ghana Ltd, Sahel Sahara Bank (BSIC) Ghana Ltd, Barclays Bank, Union Rural Bank and Awutu Emasa Rural Bank Agencies consisting of Winneba, Kasoa, Gicel and Bereku.

The reason for using questionnaires was to assess how they perceive the impact or effects of information security breaches on their daily operations and what appropriate measures they have put in place to mitigate these security breaches as well as the risk assessment aspect of the security breaches. This method was validated via peer review with other research faculty. The design of the questionnaire was reviewed by two peers and was revised in the light of their feedback. A sample of the questionnaire is provided in the appendix section of this paper.

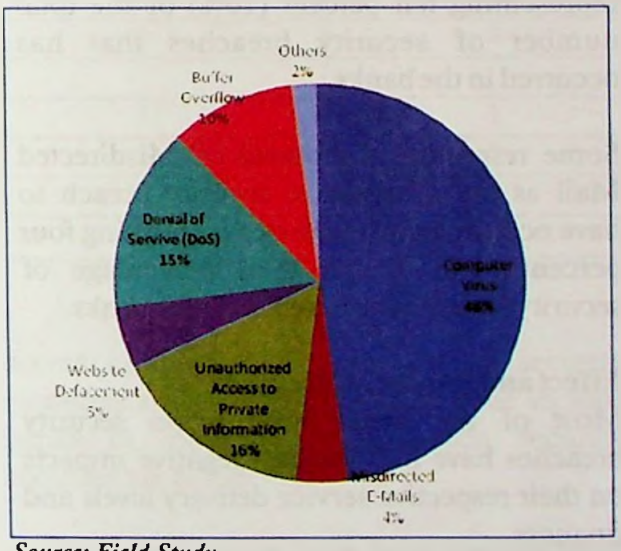
Analysis of data collected was done with Microsoft Excel 2007. The following techniques are used in the analysis; Quantitative data collected is analyzed using statistical tables and pie charts. All qualitative data is analyzed descriptively. Descriptive statistics are numbers that are used to summarize and describe data, descriptive statistics are just descriptive. They do not involve generalizing beyond the data at hand.

Caveat: Given a situation where respondents to the questionnaires provide varying or contradictory information from different sources within the same bank, an observational investigative approach is used to solicit accurate information. If a further probe proves futile then an average where possible was struck to resolve the contradiction.

Assumptions: The respondents predominantly from the Information Technology (IT) department of the banking institutions are the most appropriate source of information for this research. This assumption was made because the IT departments tend to be directly involved in resolving the security breaches as compared to most other departments.

RESULTS AND DATA ANALYSIS

Security Breaches Experienced by Banks in Ghana from 2000 to 2009



Source: Field Study

Six main different kinds of information security breaches had occurred in their various banks before. These are computer virus, misdirected mails, unauthorized access to private information, website defacement and denial of service, buffer overflow. The seventh type which is depicted by others encompasses any other type not listed.

Out of these six main security breaches popular among them was computer virus, denial of service attacks and unauthorized access to private information. Computer virus attack represents forty eight percent (48%) of the total number of information security breaches which has occurred in these banks.

Denial of Service (DoS) attack accounts for fifteen percent (15%) of the total number of the information security breaches that have occurred in the banks while Unauthorized Access to Private Information is sixteen percent (16%).

Buffer Overflow indicated as an Information Security Breach occurred in some banks representing ten percent (10%) of the total number of security breaches that has occurred in the banks.

Some respondents reported of Misdirected Mail as an information security breach to have occurred in their bank representing four percent (4%) of the total percentage of security breaches reported in all the banks.

Effect and Impact of Breaches

Most of the banks information security breaches have had various negative impacts on their respective service delivery levels and finances.

Impact on Finances: Below are tables showing the financial impact of Information Security breaches on the surveyed financial institutions.

Table 1. Average Cost of Repairing Information Security Breaches Annually from 2000 to 2009

Range of Expense (GHc)	Percentage (%)
0 - 1 000	70
1,001 - 5,000	13
10,001 – 20,000	0
20,001 - 50,000	17
Above 50,000	0
Total	100

Source: Field Work

Table 2. Financial Loss Via Information Security Breach from 2000 to 2009

Range of Loss GHc	Percentage (%)
0 – 1,000	70
1,001 – 5,000	0
5,001 – 10,000	0
10,001 – 20,000	13
20001 – 50,000	0
Above 50, 000	17
Total	100

Source: Field Study

Table 1 depicts the fact that 70% of banks spend less than GHc1000 to repair security breaches that occur on an average of annual basis whereas 13% of banks spend between GHc1001 and GHc5000 to repair. 17% of banks spend between GHc10,001 and GHc20,000.

Table 2 on the other hand depicts the fact that 70% of banks have lost less than GHc1000 via the experience of a security breach over the last decade whereas 13% of banks have lost between GHc10,001 and GHc20,000. 17% of banks have lost over GHc50,000.

Impact on Service Levels: Due to the varying technological setup of the banks and their respective methods of providing support, very different levels of service delivery seem to be experienced during security breaches.

Some of the banks have their IT service and support centralized whereas others have theirs decentralized. Typically banks with centralized IT service tend to have a different approach to resolving security breaches as compared to those with decentralized service and support.

All ten banks provided different average downtime duration experienced due to security breaches. The duration used to recover from a downtime from a security breach also varies for the banks respectively. The chart below attempts to average the man hours lost due to a compromise in security with respect to the various security breaches experienced in Ghana.

Table 3. Average Downtime caused by Various Information Security Breaches

Types of Breach	Average Monthly Rate of Occurrence (Hours)	Average Monthly Downtime (Hours)	Average Monthly Man Hours Lost
Virus Attack	3	3	3
Compromised	24	0	0
Password			
Denial of Service	1	1	1
Buffer Overflow	1	1	1
Misdirected Mail	0.5	0	0
Website Defacement	0.0075	0.7	0.7

Source: Field Study

Lurking Threats

The banks tend to be subject to various threats of the security breaches;

- Threat of intruders into the Banks Database
- Threat of Internet user accessing customer information on their web-related transaction systems
- Competitors accessing sensitive information on their systems

Mitigation Measures in Place

The response indicates that eighty seven and half (87.5%) of the total bank percentage have mitigation measures in place to check any form of information security breach that occurs in the banks. Some of the security measures and tools put in place by the various banks in mitigating information security breaches are as follows:

- Security policies have been implemented with all staff made aware of the content.
- Installation of enterprise antivirus software to protect the systems on the banks network from virus infection as well as regularly applying updates to the antivirus software
- Regular application of patches and hotfixies to Operating Systems and bank-

ing application software to correct errors, bugs and vulnerabilities identified in the software as and when they are released.

- Installation of efficient and reliable Intrusion Detection Systems (IDS) and firewalls (both software & hardware) from accredited and certified manufactures to prevent hacking activities on the banks network.
- Sniffers are available for monitoring breaches
- The use of Virtual Private Network Security (IPSec) and strong encryption methods to protect the access of sensitive assets (data) such as customer information and details from security breach.
- Remote monitoring and control of activities and tasks performed by staff or users on desktops of the various workstations in the banks.
- Encourage the use of long and stronger passphrase to secure customer data instead of passwords which could easily be cracked.

Summary of Analysis

Given the banks which were researched, the analysis above reveals the following;

1. Information security breaches have a relatively minimal negative economic impact on firms given the relatively low range of losses incurred in Ghana as a result of security breaches.
2. Information security breaches may have a net positive long-term economic impact on firms given the fact that it prompts firms to be more pro-active with prevention methods.

CONCLUSION

The research conducted on the banks concerning information security breaches within the banking and financial institutions has shown that majority of the banks were very much concerned with both internal and external security breaches and also all the banks have in one way or the other experienced information security breaches before.

Common among these security breaches were computer virus, denial of service attack, buffer overflow and unauthorized access to private information. The effects of these security breaches are Network and Service downtime and the repercussions involved including cost in fixing or restoring the systems and loss of revenue due to downtime.

Various causes of security breaches were identified during this research, among others were the lack of adherence to user-defined rules and regulations that govern the use of ICT facilities, poor security awareness on consequence of information security breaches, and unrestricted and uncontrolled access of ICT infrastructure or facilities.

Notable amongst these causes are the frequent usage of flash drives (pen drives) by staff and the abusive nature in which Internet facilities in the financial institutions are accessed.

A predominant challenge facing most banks, predominantly Rural Banks is the inability to effectively disable USB ports on computer systems that need not have them and how to deny internet connectivity and access to staff whose abusive usage of the internet facility and computer systems for unofficial duties compromises the security and eventually can lead to competitors assessing sensitive information of customers personal details.

The research also shows that most of the banks have no security risk assessment modules and are not adequately equipped in accessing or

calculating the impact of security breaches but have mitigation measures in place to check information security breaches.

Most of the institutions tend to have information security policies. However, it is not implemented hence no user-defined rules, regulations and standards are available to govern computer system usage.

The analysis of information gathered from the Banks indicates that Information Security breaches have a relatively minimal negative economic impact on firms given the low range of losses incurred in Ghana as a result of security breaches. These breaches may also have a net positive long-term economic impact on firms given the fact that it prompts firms to be more pro-active with prevention methods for the security breaches.

Recommendation

The most invaluable assets within the banking and financial sectors in modern day are information assets, and this information is predominantly on networks. The challenge with managing this form of business risk (security) is that there are no clearly defined metrics and standards to measure the level of information security risk in Ghana.

To accurately quantify risk caused by information security breaches calls for statistics, data and benchmarks to determine chance and frequency. Information risk assessment modules have by far been qualitative: typically it is done by classifying data sensitivity, defining risks for theft, disaster, hacking then evaluating the site against these risks.

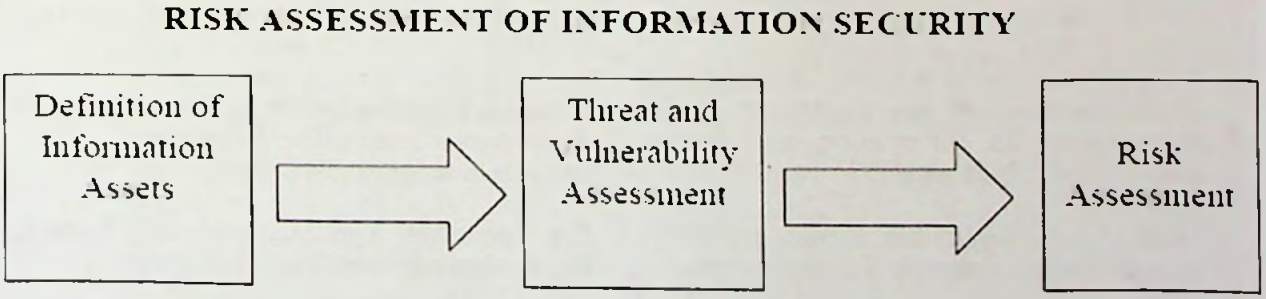
This tends to be more qualitative than quantitative. A proposal to quantify the risk assessment of Information Security breach includes the following;

1. Definition of information assets such as databases, files, customers records, software and hardware.

2. Threat and vulnerability assessment: determining the threat agent such as fire, flood, theft and its likelihood of occurrence. The class of threat such as disclosure, modification, destruction or removal and its impact upon occurrence and consequence on business.

3. Risk Assessment: This involves assessing the adequacy of existing safeguards to protect against potential threats and vulnerabilities that are likely to occur in the banks.

Figure2



Subsequently, financial institutions must define the Information Security policy and effectively implement the policies by educating all staff on acceptable and best practices. Security awareness must be an ongoing and evolving process; the management of financial institutions must ensure that regular security awareness programs are conducted for all staff.

Management and Boards should deal with information security issues proactively, rather than reactively as investment in information security is far more cost effective in a preventative rather than a remedial context.

REFERENCES

Dhillon, G., Principles of Information Systems Security: text and cases, John Wiley & Sons, 2007, ISBN 978-0-471-45056-6

G. Smith, Love Bug victims don't want a cure, The Wall Street Journal (May 8), A42 (2000).

George Mohay, Computer and Intrusion Forensics, Artech House Computer Security Series, 2003, ISBN 1580533698

Jason P. Patterson and Matthew N. Smith: Developing a Reliable Methodology for Assessing the Computer Network Operations Threat of Iran. (September 2005)

K.C Laudon and J.P Laudon, Management Information Systems, 2008, ISBN: 9780132415798

L.A. Gordon and M.P Loeb, The economics of information security investment, ACM Transactions on Information and System Security 5(4) (2002), 438–457.

Michael A. Caloyannides, Privacy protection and computer forensics, Limited preview - 2004

P. Kedrosky, Hackers prey on our insecurities, The Wall Street Journal (February 10), A18 (2000).

R. Anderson, Why information security is hard – an economic perspective, in: Proceeding of 17th Annual Computer Security Applications Conference (ACSAC), New Orleans, Louisiana, 2001.

R. Power, CSI/FBI 2002 Computer Crime and Security Survey, Computer Security Issues and Trends 18(2) (2002), 7–30.

Saadat Malik, Network Security Principles and Practices, (2003)

Spett, K.: Cross-Site Scripting, SPI Dynamics (2002). [Online]. Available:http://www.spidynamics.com/whitepapers/SPIcross-sitescripting.pdf (current 2002)

T. Bridis, E-Business: Microsoft takes steps to thwart hacker attacks, The Wall Street Journal (January 29), B4 (2001).

The Open Web Application Security Project: The Ten Most Critical Web Application

Security Vulnerabilities. The Open Web

Application Security Project (2004). [Online]. Available: http://www.owasp.org/documentation/topten.html (current 2004) The Wall Street Journal, Data show Web sites swiftly bounced back from hacker attacks (February 17), B8 (2000).

APPENDIX: QUESTIONAIRE FOR ASSESSING IMPACT OF INFORMATION SECURITY BREACHES ON BANKING INFORMATION SYSTEMS IN GHANA

(Please provide accurate information below and tick or select where appropriate.)

1. Name of Bank: ..... Department:.....
2. Position or Rank: ..... Gender (Sex): Male[ ] Female[ ]
3. What's the size of the bank's network in terms of computers (i.e. Servers, workstations/Clients/Nodes)?
   1 – 250[ ] 251 – 500 [ ] 501 – 1000[ ] Above 1000 [ ]
4. Has the bank experienced any form of Information Security Breach from 2000 - 2009?
   YES [ ] NO [ ]
   If YES, which of these information security breaches has ever occurred in your bank?
   Password Cracking [ ] Password Compromising [ ]
   Buffer Overflow [ ] Denial of Service (DOS) [ ]
   Web site defacement [ ] Hacked data [ ]
   Computer viruses [ ] Data lost or stolen in transit [ ]
   Misdirected mail[ ] Stolen Laptop or computer [ ]
   Vandalism [ ] Terrorism [ ]
   Information taken by rogue employees [ ]
   Unauthorized access to private information [ ]

Briefly describe how the bank was able to control this form of Information Security Breach:.....
.....

5. I s your bank adequately equipped in assessing or calculating the impact of Information Security breaches? YES [ ] NO [ ]
   If yes, do you think the risk assessment module(s) used by your bank is the best module for risk assessment? YES [ ] NO [ ]. Please explain:.....
6. Does the bank have an Information Security policy? YES [ ] NO [ ]
7. Has the bank implemented the details of its Information Security policy? YES[ ] NO[ ]
   If you answered NO to the above question please give reason(s) or explain why:.....
8. Has the bank provided measures to check or investigate whether staff or workers are adhering to the details of the Information Security policy implemented? YES[ ] NO[ ]
   If you answered YES to the above question please explain how:.....
9. Does the bank have any mitigation measures in place to check any form of Information Security Breaches? YES[ ] NO [ ]
   Please briefly explain (the mitigation measures) if you answered YES to the above question......
10. Does the bank grant equal internet connectivity access to all workstation users in the bank? YES[ ] NO[ ]

11. Does the bank grant access to other users apart from its legitimate staff/workers?
YES[ ] NO[ ]
12. Approximately how much has the bank spent to repair effects of Information Security breaches from 2000 - 2009?

GHC0 – 1,000	[ ]	GHC1, 001 – 5,000	[ ]
GHC5, 001 – 10,000	[ ]	GHC10, 001 – 20,000	[ ]
GHC20, 001 – 50,000	[ ]	Above GHC 50, 000	[ ]

13. Approximately how much has the bank lost to Information Security breaches from 2000 - 2009?

GHC0 – 1,000	[ ]	GHC1, 001 – 5,000	[ ]
GHC5, 001 – 10,000	[ ]	GHC10, 001 – 20,000	[ ]
GHC20, 001 – 50,000	[ ]	Above GHC 50, 000	[ ]

14. What is the average downtime (no service) experienced due to a specific security breach?

Types of Breach	Average Monthly Rate of Occurrence (Hours)	Average Monthly Downtime (Hours)	Average Monthly Man Hours Lost
Password Compromising			
Virus Attack			
Unauthorized Access to private information			
Compromised Password			
Denial of Service			
Buffer Overflow			
Misdirected Mail			
Website Defacement			
Hacked Data			
Vandalism/Terrorism			
Data lost or stolen in Transit			
Vandalism/Terrorism			

ABOUT THE AUTHOR

1. Peter Tobbin is a Lecturer with the Faculty of IT, Pentecost University College. He holds an MSc in Information Security, BSc HONs in Accounting, CISSP, CISM, CISA, CCIE, MCSE, CEH and ACCA certifications with over 12 years industry experience.

2. Paul Danquah is a Lecturer with the Faculty of IT, Pentecost University College. He holds an MSc in Information Security from Anglia Ruskin University (UK), BSc HONs in Computing from the University of Greenwich (UK), Graduate Diploma in MIS and the professional certifications MCSE and CCNP with over 8 years industry experience.