Information Security Incident Response Management in an Ethiopian Bank: A Gap Analysis

Completed Research Paper

Tsedale Yohannes
Addis Ababa university, Ethiopia
ytsedaley@gmail.com

Lemma Lessa
Addis Ababa university, Ethiopia
lemma.lessa@gmail.com

Solomon Negash
Kennesaw State University, USA
snegash@kennesaw.edu

Abstract

Banks facilitate spending and investment, which fuel growth in the economy, however, despite their important role in economy, banks are nevertheless susceptible to failure. Banks, like any other business, can go bankrupt. But unlike most other businesses, the failure of banks, especially very large ones, can have far-reaching implications. Ethiopian Banks continually increase their dependence on IT systems. The advancement of technology and an increasing use of IT solutions exposed banks for attacks more than ever. Even though, banks are deploying prevention mechanisms to keep out hackers and attempts of cyber-attacks, incidents occur occasionally. This tells there is a need for an effective and efficient management of information security incidents. International standards and guidelines for incident management exist but, researches that assess current practices are few in literature. This research conducted as a qualitative case study in which current practice of a bank's information security incident response management assessed with the aim to identify gaps from the best practice. The data was collected through interview. The finding revealed that bank x don't have a predefined and separate information security incident management plan. But, to some extent it was compliant with international standards and guidelines in some of incident handling procedures. An alarming finding that indicated bank x never performed rehearsal was highlighted in this study. Lack of employees' awareness, information gap among departments, lack of experienced and skilled incident handlers and enhancement of new threats were among prominent challenges identified. Finally, recommendation for successful information security incident management was proposed.

Keywords

Information security incident, information security incident management, incident response team

Introduction

Worldwide, businesses continually increase their dependence on IT systems, even for routine business processes. The business processes which directly rely on information systems and the supporting IT infrastructure often require high levels of availability and recovery in the case of an unplanned outage. Industries and governments are becoming increasingly accountable for how data is managed, protected, and secured. Policies and regulations vary from industry to industry, and the overall landscape of technical requirements continues to grow in complexity.

The financial industry traditionally leads in terms of stringent regulations for data protection, security, and contingency copies of financial data; others are quickly migrating towards a completely electronic format for data. Banks facilitate spending and investment, which fuel growth in the economy, however, despite their important role in economy, banks are nevertheless susceptible to failure. Banks, like any other business, can go bankrupt. But unlike most other businesses, the failure of banks, especially very large ones, can have far-reaching implications. As we saw during the great depression and most recently during the global financial crises and the ensuing recession, the health of the bank system can trigger economic calamities affecting millions of people. (Temsgen, 2016)

Organizations can't afford to be nonoperational due to regional power outages, cyber-attacks or hardware failures. Every minutes applications and systems are down translates into lost revenue. Like any other organizations, banks are exposed to some kind of risks that can damage their business in different ways and threaten their survival. Therefore, it is vital to develop and implement contingency plans to prevent the risk, to be to recover from disaster and to minimize the damage when the risk occurs as well. Incident response, disaster recovery, and business continuity planning are components of contingency planning (Michael.E.&Herbert.J.,2011).

The discussion of contingency planning begins with an explanation of the differences among its various elements, and an examination of the points at which each element is brought into play. An incident is any clearly identified attack on the organization's information assets that would threaten the assets' confidentiality, integrity, or availability. An incident response (IR) plan addresses the identification, classification, response, and recovery from an incident. A disaster recovery (DR) plan addresses the preparation for and recovery from a disaster, whether natural or man-made. A business continuity (BC) plan ensures that critical business functions continue (Michael.E.&Herbert.J.,2011)

If a catastrophic incident or disaster occurs, the primary functions of these three types of planning are as follows: The IR plan focuses on immediate response, but if the attack escalates or is disastrous (e.g., fire, flood, earthquake, or total blackout) the process moves on to disaster recovery and the BC plan. The DR plan typically focuses on restoring systems at the original site after disasters occur, and as such is closely associated with the BC plan. The BC plan occurs concurrently with the DR plan when the damage is major or ongoing, requiring more than simple restoration of information and information resources. The BC plan establishes critical business functions at an alternate site (Michael & Herbert, 2011).

In recent years, an increasing number of information security incidents have been reported. Typical incidents include both general and single purpose attacks caused by malware, in addition to minor errors with severe consequences. Hence, organizations need to be prepared to handle incidents caused by both known and unknown vulnerabilities. Several well established standards and guidelines addressing incident management exist and a number of factors are also involved in determining how successfully organizations respond to information security incidents (Hove & Tarnes, 2013).

Problem Statement

The 2014 pricewaterhousecoopers Global state of Information Security Survey (2014) claims that the rate of security incidents detected in the past twelve months increased by more than 25% and more than double since 2011. The Kaspersky 2013 Global Corporate IT Security Risks Survey (Kaspersky 2013), estimate that the financial losses from security incidents and data breaches are in the millions of dollars within the past years.

Responding to security incidents is becoming increasingly imperative in business environments. A poneman (2016) study on data breaches reports that 48% of attacks involved malicious activity, 25% were due to negligent human factors, and 27% involved business and information technology process failures. The report goes on to indicate that the mean time to identify an incident is, approximately, 201 days and the mean time to contain an incident once discovered is 70 days. The reality is that the effects of a breach can be very destructive to an organization. This destruction can be experienced in the form or ransom ware, system downtime, and intellectual property theft, reducing customer confidence, and facilitating attacks on other organizations (Grispos et al, 2017).

Banks are one of the huge elements that constitute the financial system across the globe. They dominate the Ethiopian financial system with nearly 95% share of assets,97% share of deposits, 94% share of loans

and advance, and 77% equity share of the financial sector on average(Nigussie, 2017,p.9) , such a huge financial sector need to have a structured way to continue business and restore operations in the event of a sudden outage. Like any other organizations, interruptions to information technology system services can have a severe impact on banks and its ability to carry out its basic functions. IT resources are essential to most business processes and organizations depend up on information systems that operate effectively without serious interruptions (Susan Snedaker, 2007). An increasing use of digital solutions suggests that organizations today are more exposed to attacks than before. Recent reports show that attacks get more advanced and that attackers choose their targets more wisely. Despite preventive measures being implemented, incidents occur occasionally .This calls for effective and efficient information security incident management (Hove.G. &Tarnes.M.2013).

According to Grispos et al(2014), security incident increasingly impact organizations, it is imperative that organizations have the ability to investigate, report and, ultimately, improve overall security efforts based on previous security incidents. Several standards and guidelines addressing incident management exist. Using those standards, Hove.G.&Tarnes.M(2013), has studied information security incident management current practice in three Norwegian organizations, the researchers described that: As we have only studied a limited number of organizations, our result is not generalizable and thus it would be interesting to conduct the same study with a larger number of organizations. This can verify whether our findings apply to organizations in general (p.112).

Few student researchers in Ethiopia have tried to study information security in financial industries from different perspectives. Kelime(2013), he proposed information security management framework for banking industries in Ethiopia. Another student, Abeselom(2015), he assessed that practice, challenges and prospects of information security policy in Ethiopian banking industries. Recently, Daniel (2017) has tried to study the effectiveness of information security management in Ethiopian financial sectors. His focus was card banking. On the other hand, among the elements of contingency plan, BC and DR has got some coverage by local student researchers. Asheber (2017), has tried to identify potential challenges in relation to business continuity management. Negussie (2017), has studied about information technology disaster recovery practices of Ethiopian commercial banks. While the student researchers studied information security, they haven't discussed information security incident management practice in their research. DR and BC have studied by the student researchers specifically. but the third element of contingency, incident response didn't get enough attention by the researchers., literature shows that there is lack of local research that address information security incident management practice. Hove.G&Tarnes.M (2013), also mentioned that few studies of current practices in information security incident management have been conducted. As per the knowledge of the researchers, there is no study which is conducted on information security incident management current practice of Ethiopian Banking Industries. Therefore, this research is intended to study the current information security incident management practice at a bank in Ethiopia.

Related Works

Hove and Tarnes (2013)has studied the three Norwegian companies and they identified that all had incident management plans in some form. This included plans and guidelines for handling specific types of security incidents, established routines, incident management handbooks for the incident response team, and plans for communication during incidents. They also emphasized that, for organizations with distributed organizational structures there are many sources of information hence knowing how much information to share can be difficult more over they have identified that in cases where IT operations are outsourced, collaboration during incident management is even more challenging. Even minor incidents can be problematic if all assume the incident to be someone else's responsibility. Although the researchers focused in all five phases of information security management guidelines which is provided by ISO, they did not make in depth study for each of the phases equally on top of that their study bases the organizational culture of those three Norwegian companies under their study. These calls for further study in the area, hence generalization is impossible. MariaB.Lineand EirikAlbrechtsen have tried to examining the suitability of industrial safety management approaches for information security incident management, but they only focused on plans, compliance, and situational adaptation; training; and learning from incidents.

Line and Nils (2015) has also researched challenges met during preparedness exercises for information security incidents in six power industries. They have used observation as a data collection instrument and they have identified that outsourcing reduces preparatory activities and post incident evaluations are not performed. These researchers also didn't focus in all five phases of ISO guideline. Security incident response criteria were researched by Grispos et.al. They have used an empirical research with a data collection method interview. Their focus was only in preparing security incident response criteria. These researchers pointed that there are fundamental problems with existing security incident response process solutions.

Other researchers, Shedden, et al.(2011), conducted a research to explore organizational learning concepts. They have used a focus group method to find out that response to incident is largely informal. they have highlighted that the need of a new incident model that incorporates informal learning practice. The focus of these researchers were also only on the single phase of incident management. An exploratory study that investigated the security incident activities of practitioners was conducted by Welinger, et al.(2007). They have used interview as a method of data collection. The objective of their study was to determine what skills, tools and strategies were required to manage and handle security incidents. The result showed that practitioners often used pattern recognition and hypothesis generation during the analysis of security incidents. This research also didn't cover all phase of incident management practice.

Research Design and Methods

The main objective of this research was to assess the current practice of information security incident management at bank x of Ethiopia, using international standard in identifying the gaps and proposing possible solution.

Research Approach

In order to satisfy the objective of this research, a qualitative research was held. The main characteristic of qualitative research is that it is mostly appropriate for small samples, while its outcome is not measurable and quantifiable. Its basic advantage, which also constitutes its basic difference with quantitative research, is that it offers a complete description and analysis of a research subject, without limiting the scope of the research and the nature of participant's responses. A qualitative approach also focuses on process and understanding based on rich description of body of knowledge(Bell, 2005).

Data Collection Methods

Among the qualitative data collection methods face to face semi-structured interview E-mail interview were used., in order that the information is richer and has a deeper insight about the subject of this research more over interview is seen as being one of the most important sources of information in a case study (Robert.K.Yin, 2009). A reasonable number of interview questions were open-ended so that respondents can have a chance to provide additional and detail information. Interview questions were adapted from an international information security incident management standard and guideline, ISO/IEC 27035.After conducting interviews internal documentation requested from participant that would assist the researchers in collecting synthesizing and cross- referencing responses (Shwaz&Hirschhein, 2003).Because of bank x's security policy and confidentiality reason the researcher couldn't access those documents.

Data Source

The method of purposive sampling was used to identify the data source of this research. Purposive sampling belongs to the category of non-probability sampling techniques, sample members were selected on the basis of their knowledge, relationships and expertise regarding a research subject (Freedman et al, 2007).The target population of this research was IT staffs who were working at bank x's head office. But for this specific research, the researcher identified the participants based on their current role, which was related to the issue of this research. Hence, the participants of this research for in person interview were 4 managers from different IT departments: information system security manager, infrastructure and application manager, ATM and e-payment manager and the security operation center team leader.

Participants for e-mail interview were those in which it was not possible to access them for face to face interview due to the sensitivity of their work.these participants are 9 cyber-attack analysts,who work at security operation center of bank x..

Validity and Reliability

Validity issues need to be considered when designing a research project and evaluated when analyzing the credibility of research results. Construct validity concerns whether a study measures what it sets out to measure (Robson.C, 2011). Both interviewees and the researcher may be biased, either consciously or unconsciously (Diefenbach.T,2009). Bias may be overcome by a number of strategies, such as triangulation and member checking. Data triangulation means using several methods for collecting evidence, such as interviews, document analysis, and observations. This allows for studying a phenomenon from different perspectives and increases data quality (R.K.Yin,2009).Member checking involves returning data material to the respondents for review and shows that their contributions are valued. Reliability is concerned with the consistency, stability and repeatability of the informant's accounts as well as the investigators' ability to collect and record information accurately (Selltiz et al 1976:182). It refers to the ability of a research method to yield consistently the same results over repeated testing periods.

In order to reduce risks to validity and reliability of this research, the researchers performed the following tasks:

- So as to eliminate the researcher effects, Field and Morse recommended that researchers undergo extensive and rigorous training as interviewers and observers before undertaking qualitative study. The researcher of this study was exposed herself for several online and face to face trainings about the subject of this research. The researcher's practical experience about the subject of this research was very helpful to move from un-trusted stranger to a trusted and friendly person during the research process.
- To reduce sample bias, sample selection was based on the ability of the respondents to provide data relevant to the research questions. The researcher's judgment based upon the best available evidence to choose interview participants who know enough was applied.
- The researcher clarified the nature of the research for the participant of the interview. There was a discussion between the researcher and each of the interviewee 2 days before the interview conducted. During the discussion participant were able to understand why the research conducted in their bank, how the data collected, and for what purpose it used. Hence, it was possible to build a trust-relationship among the interviewees and the researcher.
- Due to sensitive nature of our research topic, the research participants were assured that their organization's name would remain Anonymous. Accordingly, for the purpose of this study the name of the bank is considered as "Bank X"). This encouraged the informants to speak openly and honestly about different issues. The results of the research were offered to the participants. They were also notified of the ability to withdraw at any time from the research. This provided an incentive to participate and reduced the fears to be identified by others in disclosing information.
- Similarly, because the subject of this research is sensitive, the interpersonal context under which the data gathered was taken in to consideration by the researchers. Particular attention to confidentiality had paid. Interview conducted at bank x office's after making sure that both the researchers and the interviewees were not exposed to be overheard by others in the environment.
- Analysis and findings of this research was sent via email for the face to face interview participant of this research. Three of them reviewed and returned it in time. The researchers took their review into consideration to validate the findings.
- Face to face interview and survey as e-mail interview was data collection tools and used as a means of triangulation.

Key Findings

This research was aimed to assess information security incident management practice at bank x of Ethiopia. In order to meet the objective of this research and to answer for the research questions, a thorough investigation was done using ISO/IEC 27035 guidelines in performing qualitative in-depth face-to-face and e-mail interview. Accordingly the summery of key findings are presented as follows:

Systematic approaches to incident management activities contribute to respond successfully for an incident. As it is described in many of international standard and good practices, information security incident management policy, plan and procedures are part of an organization incident management capability. Bank x don't have a separate information security incident management policy and plan that could help them to respond for incidents in an organized and better way from what it is practical currently. It is not deniable that, not having such important plan and procedures can pause question if an organization really have effective and efficient way of incident response.

The majority of this research participant revealed that the security operation center cyber-attack analysts are playing the role of an incident response team together with few focal persons in other IT departments. But cyber-attack analysts who participated in the survey pointed out that information gap among departments and response delay are notable challenges that affect incident management practice at bank x. this may indicate that the collaborative effort to respond for an incident is not satisfactory at bank x. it seems this finding call for establishment of well-organized and comprehensive incident response team.

Besides, an incident response is a highly collaborative activity, the skill and experience of incident responder and usability of security tools are an issue for the diagnosis work. Experience of incident handler can be achieved in two ways, through rehearsal and post incident learning activities. It is not a good practice to wait for an incident occurrence to learn from it, rather it is recommended to conduct scenario based rehearsal to enhance incident responder experience and to identify gaps to be managed beforehand. The finding of this research is indicating that bank x didn't perform rehearsal. This might have certain connection with the fact that bank x is suffering from lack of highly skilled and experienced incident responders.

In order to create security positive environment, it is believed that training and awareness creation program plays a vital role. Training is a common key factor for an organization to strengthen their response capabilities. The participant of this research indicated that bank x provide information security incident handling training for IT and security operation center workers. They also mentioned that their bank conduct information security awareness creation program for business staffs. On the other hand, most of the interviewee and the survey participant highlighted that lack of information security awareness among employees is a challenge for information security incident management practice at bank x. this may lead us to the conclusion bank x is not performing training and awareness program in an effective and efficient way to create security positive environment.

Apart from the limitation regarding usability and accuracy problem they have, automatic monitoring and detection systems are best suited for detecting known attacks. Manual detection mechanisms such as users, technical staffs and external notification supplement the limitation of automatic detection mechanisms such as, a problem of detecting new attacks which are specifically tailored and targeted. According to the participant of this research, Bank X widely implemented globally well-known and internationally recommended automatic incident detection mechanisms. We believe that, that deployment of a separate security operation center at bank x, which is first of its kind in the country indicates that, the undeniable commitment of top level management to secure their IT infrastructure. This is supported by from the statement of almost all participants in the interviewee. Bank x also uses manual detection mechanisms to detect incidents but there is a grey area which indicates utilization of users as a network sensor for the bank is not sufficient. This is supported by the description of interviewees that pointed out, the absence of security incident registration form for users to use it, uncertainty about logging security incidents in the incident tracking system and lack of awareness.

Challenges of information security incident management at bank x identified in this research are:

- Accuracy of monitoring tools. Inaccurate monitoring tools affect prevention and detection of incidents negatively. It also leads to wrong decision of the response process.

- Lack of skilled and experienced incident handlers. Not having skilled and experienced incident handlers influence the capabilities of an organization in recognizing and responding to incidents.
- Lack of security awareness among employees. An environment which is not security positive increase the frequency if incidents and the negative impact caused by them.
- Information gap among departments .effective incident response requires collaboration and coordination throughout the organization, information gap can be a barrier for such collaborative work.
- Response delay. It can result in a catastrophic consequence that might incur major cost to the organization.
- Enhancement of new threats. Emerging threats creates the need for a well established capacity for responding to unwanted incidents. such a capacity is influenced by organizational human and technological factors. still it might be impossible and economically infeasible to prevent all incidents.

Discussion

How Does Bank X of Ethiopia Perform Information Security Incident Management?

Several international standards pointed out that the importance of having an information security policy for an organization .ITIL, ISO and SANS stated that information security policy should be communicated throughout the organization and employees have to familiar with the policy. Bank x has developed an information security policy though it seems it is not well established across the entire branches of the bank. This is supported by the interviewees where the infrastructure and application manager stated that, it is very difficult to deal with those employees who are not information security sensitive.ATM and E-payment manager also agreed with that, some employees lacks knowledge about what they are allowed to do and not to do. Bank x is not compliant with ISO/IEC 27035 standard recommendation of having a specific policy for handling information security incident .All the interviewees agreed on that there is no separate policy and plan that only address information security incident management at Bank x.

Bank x classify information assets depending up on their sensitivity and value, this is supported by all interviewees. It is compliant with recommendation from ISO/IEC 27002 standard that additionally emphasizes the relevance of information classification to ensure proper protection of information. The three companies studied by Hove and Tarnes (2013) all classified information including classification of incidents based on the severity and damage they cause. Bank x also classify incidents for proper management depending up on their risk. Participant of the interview stressed on that classification of incidents is vital for proper incident handling process.

A finding from the study of Joatun et al (2009), Identified the need for a short and common plan for incident response. In the study of Hove and Tarnes(2013), all the three Norwegian companies had incident management plan in some form, This included plans and guidelines for handling specific types of security incidents, established routines, and plans for communication during incidents. This supports that the finding bank x has incident handling procedure though it is not approved by top level management. The security manager and security operation center team leader mentioned that, they have incident handing procedure in which they use it without gaining approval from management. This might indicate, there is lack of common understanding among technical IT staffs and management staffs towards incident handling, we believe that it is an alarming finding as it tells bank x have no formal and clearly defined document that will guide incident handling process during incident occurrence.

The establishment of IRT is highlighted in standards and guidelines. NIST recommend that team members have to have diverse back grounds so that they can handle different incidents that occur. According to NIST, usually teams consist of highly technically skilled persons and teams should have at least one member with expertise in each major technological category. Participant of the interview at bank x assured that security operation center workers acts as an incident response team and they work in collaboration with other IT staffs when it is needed, But ISO/IEC 27035 standard recommends having a permanent response team. Bank x don't comply with this recommendation as they don't have their own IRT but dedicated IT staffs and security operation center cyber-attack analysts for incident handling. This finding is similar with the finding of Ahmad et al (2012) at financial organization; the response to high

impact incidents is coordinated by a high impact incident response coordination team, while other incidents are handled by a network incident response team more independently. Companies construct teams based on the incident and one of them has a specific team that is involved for major incidents.

Bank X conducted training and awareness creation program that addresses various security issues. According to ISO/IEC 27035 standard, employees' awareness and participation in incident management procedures are important. Even though employees at bank x had attended courses or other awareness raising activities, there is still a room for improving security knowledge and awareness in order to create security positive environment. This observation is further supported by statement from infrastructure and application manager. He mentioned that it is very important to address the need of IT staffs and other employees to take part in security related training as information security incident handling process can't be only the responsibility of security operation center workers. This is similar with the finding from the study of the petroleum industry by Joatun et al (2009) that identified individual awareness related to information security should be improved. Bank X never used rehearsals to identify areas of improvement yet. Conducting emergency preparedness exercise is however considered challenging; it ensures that participant train on the right things, that the scenario is realistic and useful for real situations. The security manager stated that it is difficult to conduct rehearsal and they never considered its importance. He stressed that it is not a good practice to keep incident handling procedure without checking its functionality. Bank x is not compliant with the recommendation of ISO/IEC 27035 standard to conduct rehearsal.

As it is recommended by most relevant standards and guidelines, bank x has implemented monitoring systems such as IDS/IPS, SIEM system, antivirus solutions, firewalls in which they have configured monitoring functionalities, DMZ, network flow analysis, mail monitoring tools and other security monitoring tools are in place and use, the tools currently in use however have their limitations. The security manager described the fact that high rate of false positive alerts from security information event management system is one of the challenges in using automated monitoring systems. Study by Werlinger et al (2010) also revealed that a lack of accuracy in tools, resulting in high false positive rates. Furthermore interviewees mentioned that the challenge to hire senior cyber-attack analysts who can investigate and analyze sophisticated correlations makes a concern usability of tools. It is notable that efficient detection often requires intimate knowledge about the organization systems and services. Complexity and lack of properly trained security specialists may lead to rely on notifications to detect incidents. The finding from the study by Koivunen(2010) also showed that, of the incidents studied, none of the victims of the security breaches seemed to have discovered the incident on their own.

Notification of incident might be from users, IT employees or external third parties. Bank X uses email and phone to notify and report incidents which are detected manually. Even though bank x have ticketing or incident tracking system where incidents to be registered, the security operation center team leader stated that they were not exhaustively logging information security incidents which are reported manually. Commonly reporting channels mentioned at bank x were security manager, security operation center workers and immediate IT support staffs. Cyber-attack analysts who participated on the survey revealed that, there is no dedicated form for reporting information security incidents identified by users manually, so that the user can register what they have observed. Out of 7, 5 of the survey participant said this.ISO/IEC 27035 standard recommends report that comes from any sources should be filled in a separate format and has to be approved by point of contact. Bank x doesn't comply this. Some studies report on challenges with having all incidents registered in the system.Cusick and Ma(2010), report that some issues are observed but not logged, typically when the case is considered to be non-critical. We believe that lack of proper communication might be the root cause of challenges with having all incidents registered. The case study by Hove and Tarnes(2013) included a survey of regular employees, it was found that few of the employees knew to whom security incidents should be reported and that they were not sure which incidents to report.

According to ISO/IEC 27035 standard recommendation, the point of contact should conduct an assessment to determine whether the information security event should be classified as information security incident or is in fact a false alarm. Assessment may be also conducted by the person who identified the security incident, if he/she has the appropriate level of competence to determine whether the security event is an incident or false alarm. This is supported by from the statement of security manager and security operation center team leader.

Though it is time taking for them to determine whether an alert is false positive or not, bank x'scyber-attack analysts perform assessment of security events using monitoring tools. This complies with ISO/IEC 27035 standard recommendation.

Bank x works in collaboration with third parties like INSA and national CERT in order to tackle some advanced attacks. It is in compliance with ISO/IEC 27035 recommendation. Another issue highlighted in the standard is forensic investigation; they work together with police if further forensic investigation is needed. This is supported by the study Hove and Tarens (2013), companies in some cases rely on third parties or the police for forensic investigation.

Post incident activities of bank x includes, conducting weekly, monthly and other additional meetings to review the cause of major incidents, The challenges they face and how it dealt with to respond for it. The security operation center technical staff team leader and security manager together with risk and program assessment staffs take part in the discussion. This is supported by participant of the survey and security manager. He stated that they have regular meeting to discuss on security incidents so as to incorporate the output from the discussion for further risk assessment tasks. It is similar finding as Werlinger et al(2010) reported the motivation for performing learning activities include keeping security practitioners updated on current threats, getting new ideas on how to resolve challenging incidents, discussing possible improvements of the incident management process. It complies ISO/IEC 27035 recommendation.

Experience sharing with trusted communities is a recommendation in most standards as post incident activity. It seems lesson learnt and other incident information is often available only to some selected few in Bank x. this is supported by survey conducted at bank x. among the 7 participant 4 of the cyber-attack analysts stated that, information gap among departments is one of the challenge for incident handling in their bank. We believe that sharing experience can make banks better prepared for incident handling. The ATM and E-payment manager noted that: it has to be clearly defined to which group they can share experience. He said that, I don't think that, it is necessary to make unavailable those important experiences, we identified in handling security incidents for trusted communities. This may imply that bank x is not benefiting from mutual sharing of experiences with other banking industries. So it is only partially compliant with ISO/ IEC 27035.

What Challenges Exist in Information Security Incident Management at Bank X of Ethiopia?

Challenges for security incident management were mentioned by interviewees and the survey participant. Among these, limitation of having experienced incident handlers, lack of employees awareness, and too much false positive alerts are highlighted by all of them. cyber-attack analysts pointed out that, information gap among departments, response delay which also supported by statement from security manager, enhancement of new threats and network connection problem especially from internet service provider are challenges for incident management practice at bank x. a study by Kurowski and Fring (2011) reported that the professional experience of employees is most relevant for performing analysis of incident followed by documentation of past incidents.

Conclusion

The main objective of this research was to assess the current practice of information security incident management at bank x of Ethiopia, using international standard in identifying the gaps and proposing possible solution. In this study, attempts were done to examine and compare the available international standards and guidelines to use it in comparing with the current practice. Qualitative in-depth study was used to assess practice of information security incident management at bank x.

The research pointed out that to what extent existing standards and guidelines are adopted in bankx's information security incident management process. We found that bank x has not a predefined and separate information security incident management plan in which they follow it strictly. But, to some extent they are compliant with an international standards and guidelines recommendation like ITIL and ISO. Some procedures such as incident classifications and escalation of incidents seem to be well performed. Automatic means of detecting information security incidents is widely implemented. There are also procedures and activities don't seem sufficiently established. Such as, collaborative work, incident

reporting process, training and awareness program, manual incident detection mechanisms, and post-incident activities like sharing of experience. Moreover we highlighted that, an alarming finding that rehearsal never been practical and not gained anyone's attention at bank x.

Challenges in handling incidents at bank x were also reveled in this study .these challenges were related to employees awareness, lack of skilled incident handlers, communication and enhancement of new threats.

Recommendations

We believe that, having systems in place to prevent and detect as many breaches as possible may be a good starting point of incident response. Today's threat landscape also requires a detailed incident response strategy to detect and respond to a breach, along with the expertise to execute it. Based on the identified current practice and challenges of information security incident management at bank x, we recommend the followings so as bank x and other organization may use it for a better way of managing information security incidents The management of bank x have to work together with IT department, so as sound and comprehensive standards or guidelines for information security incident management will be used recently.

- As soon as possible, IT department together with the management, they have to produce information security incident management policy and plan in order to ensure that information security incidents are reported, assessed and their harmful effects are mitigated.
- The management together with IT department have to establish an incident response team that consists of representative from technical security specialists' information technology specialists from each category; and relevant business staffs.
- Produce operating and formal procedures for the information security incident response team.
- Design and develop awareness and training programs: The management has to provide role-based educational and training opportunities for Incident response team members and for IT staffs; IT department together with incident response team have to expose all employees regularly to information security incident management awareness. The awareness techniques may include periodic emails, posters; and the management and IT department have to preserve communication with the academic institutions to address training gap.
- The Established incident response team has to conduct regular rehearsal to gain experience. Focus on challenging areas such as response delay, user report procedure, information gap.
- Encourage an environment to share information about incidents that could involve colleagues.
- Make sure employees are fully utilized as means of detecting incidents.
- The management and IT department have to produce formal policies on which means of information communication should be used and what should be disseminate and who should access it.
- Incident response team has to enhance post incident activities: Focus on the effectiveness of procedures, controls, training and awareness. And also share notable experiences with similar trusted financial industries and communities.

Challenges and Limitations

The topic of the interviews was information security, which tends to business confidential information, some interviewee Participants might refuse to speak against their bank. Their conscious or unconscious desire to make their bank and themselves look good from the outside could cause a certain bias. One of the basic steps in case study research is to be able to access the candidate sites and informants in order to ensure the best possible data quality. Despite the fact that "good" candidate bank has been chosen, accessing the key informants and the actual incident management practices on the ground was not as easy as we expected. Even though the researcher's impression was to interview more business staff personnel and IT technical staffs from each categories, the sensitivity of the research topic, time and resource constraints put a limitation on the number and selection of interviewees. A bigger sample would probably enhance the reliability of the research.

Future Works

In order to cope with the enhancement of new threats, we believe that, conducting more detail researches benefits banks and other organizations. We recommend future studies in the following area:

- Conduct the same detailed study on a large scale with in financial industries and other organizations.
- Research how the identified challenges can be resolved.
- The need for tailored information security incident management frame work for different organizations.
- Prospects and challenges of academic institutions in minimizing the scarcity of highly qualified information security personnel.

References

Abeselom .N(2015).Practices, challenges and prospects of information security policy in Ethiopian banking industry. (Unpublished master's thesis).Addis Ababa University, AddisAbaba, Ethiopia.

Ahmad,A.,Hadgkiss,J., and Ruighaver,AB.(2012).Incident response teams: challenges in supporting the organizational security function. Computer & security

Asheber.E(2017) Challenges In Relation to Business Continuity Management in Commercial Bank of Ethiopia: Information System Security in Focus.(unpublished master's thesis).Addis Ababa University, Addis Ababa, Ethiopia.

Beck,C.T.(2003).Initiation in to qualitative data analysis. Journal of Nursing

Campbell,D,T&Stanley,J.C(1963).Experimental and quasi-experimental designs for research. Chicago Rand McNally.

Cassell,C. and Symon,G.(2004).Essential guide to qualitative methods in organizational research. Sage publication Ltd.

Cusick,S.,MaG(2010)."Creating an ITIL inspired incident management approach: roots, response, and results." In :Network Operations and Management Symposium Workshop(NOMS Wksps), EEE/IFIP;2010.pp142-8.

Daniel.G(2017).Assessment of the effectiveness of information security management in the Ethiopian financial sector: card banking in focus.(Unpublished master's thesis).Addis Ababa University, AddisAbaba,Ethiopia.

Denzin,N.K.(1970).The research act: A theoretical introduction to sociological methods. Chicago: Aldine publishing co.

Diefenbach,T.(2009)" Are case study more than sophisticated story telling?: methodological problems of qualitative empirical research mainly based on semi-structured interview. vol.43,no.6,pp.875.

ENISA.(2011).Good practice Guide for Incident Management.

ENISA .(2008).A basic collection of good practices for running a CSIRT.

Ernest,B.,Richard,G.,Aidan,L.,andJohn,.S(2012). IT Service Management: A Guide for ITIL Foundation Exam Candidates. BCS, The Chartered Institute for IT, 2nd ed

George.G.,Willian.B.,Tim.S,(2014)"Rethinking Security Incident Response:The Integration of Agile principles," in twentieth Americas Conference on Information systems.Savammah.

George.G.,William.B.,David.B.,Tim.S.,Stacy.M,(2017). "Security Incident Recognition And Reporting: An Industrial perspective, "in: twenty-third American Conferences on Information Systems. Boston

Grispos,G., Bradley,G.W,Storer,T.,"Security Incident Response Criteria: A practitioner's perspective."

Hove.C.&Tarens.M(2013).Information Security Incident Management: An Empirical Study of Current Practice.

ISO/IEC 27000: 2012(E).Information technology-security techniques-information security management systems-overview and vocabulary. Second edition, International Organization for Standardization.

ISO/IEC 27035:2011(E). Information technology - Security techniques - Information security incident management - First edition. International Organization for Standardization.

ISO/IEC, \ISO/IEC 27000:2009 Information security management systems – Overview and vocabulary,".

Jaatun,MG.,Albrechtsen,E.,Line,MB.,Tondel,IA.,Longua,OH.(20 09). A framework for incident response management in the petroleum industry. Itjcritinfrastruch; 2:26-37.
Kaspersky.(2013).” Global Corporation It Security Risks:2013.”
Kelver,J.(2002).Incident Response in a Global Environment. GSEC version 1.2b, SANS.
Kelemie.T(2013). Information Security Management frame work for Banking Industry in Ethiopia.(unpublished master’s thesis).Addis Ababa University, Addis Ababa, Ethiopia.
Koivunen ,E.(2010).” Why wasn’t I notified: Information Security Incident reporting demystified.” in 15th Nordic conference in secure IT systems(Nordsec 2010).
Kothari (2004). Research methodology methods and techniques (2nded.). New Delhi:new age international.
Kurowski,S.&Frings,S.computational documentation of IT incidents as support for forensic operations.
Le compte,M.D., and Schensul,J.J.(1999). Analyzing and interpreting ethnographic data. Walnut Creek,CA ;Altamira press.
Le Comple, M.D &Goetz,J.p.(1982).problems of reliability and validity in ethnographic research. Review of educational Research 52(no1) 31-60
March,Sand.G.Smith(1995). Design and natural science research on information technology, Decision support systems 15,pp. 251-266.
Maria B, L.(2013). A Study of Resilience within Information Security in the Power Industry, IEEE Africon, Mauritius.
Maria,B,L.,Inger,.A,Tndel,andMartin,.G,Jaatun(2014).” Information security incident management: Planning for failure,” in: 8th International Conference on IT Security Incident Management and IT Forensics (IMF) ,Munster, Germany.
Maria B,L., and Nils,B(2015). “Understanding Collaborative Challenges in IT Security Preparedness Exercises,” International Conference on ICT Systems Security and Privacy Protection, IFIP SEC, Hamburg, Germany.
Maria B,L. and Eirik,A. Examining the suitability of industrial safety management approaches for information security incident management, forthcoming in international Journal of Information and Computer Security, ISSN 2056-4961
Maria B.L., Inger,A.,Tndel, and Martin G,J(2014).”Information security incident management: Planning for failure,” 8th International Conference on IT Security Incident Management and IT Forensics IMF, Munster, Germany, ISBN 978-1-4799-4330-2.
Michael E.&Herbert J.(2011),Principles of Information Security.
Myers,M.D.andNewman,M.(2007).”The qualitative interview in IS research: Examining the craft,” Information and organization, vol.17,no.1, pp2(26).
Negussie.B (2017).Assessment of IT Disaster Recovery Practice in EthiopianCommercial Banks.(unpublished master’s thesis).Addis Ababa University, AddisAbaba,Ethiopia.
Northcutt,S.(1997). Computer Security Incident Handling, step-by-step. The SANS Institute.
Parileh, M.(2002). acquisition through case study development: a student researcher perspective. Communications the AIS 8(8): 360-379
Patrick,K.(2011).Incident Handler’s Handbook. SANS Institute of Information Security.
Paul,C.,Tom,M.,Tim,G.,and Karen,S.(2011). Computer security incident handling guide, NIST special publication 800-61,Revision 2.
Ponemon Institute.(2013a).”2013Global Cost of Data Breach.”
Ponemon(2016).”2016 Cost of Data Breach Study: Global Analysis”, ponemon Institute,p.32.
Pricewaterhousecooper(2014).”The Global State of Information Security Survey 2014.”
Robert K.Yin(2009),Cast Study Research Design and Methods, applied social research method series,5(4) Norwegian University of Science and Technology.
Robson,C.(2011).Real world research,3rded,John Wily & sons Ltd.
Schwarz.A&R.Hirschheim (2003).An extended plat form logic perspective of IT governance: Managing perceptions and activities of IT. Journal of strategic Information systems (12): 129-166.
Seltiz,C.&Wrightsman,L.C&Cook,W.S.(1976).Research methods in social relations. 3rd Ed. New york: Holt Rinehart & Winston.
Shedden,P.,Ahmad,A.,andRuighaver,A.(2011).”Informal Learning in Security Incident Response Teams.”ACIS 2011 proceedings.37.
Temsgen.A(2016).Tailoring IT governance framework for national bank of Ethiopia.
(Unpublished master’s thesis). Addis Ababa University, AddisAbaba, Ethiopia.

Welinger,R.,Botta,D.andBeznosou,K.(2007).”Detecting, Analyzing and Responding to Security Incidents: A qualitative analysis,” in :3rd symposium of usable privacy and security, ACM, pp.149-150.

Welinger,R.,Muldner,K.,Hawkey,K.,Beznosov,K.(2010).” preparation, detection and analysis: the diagnostic work of IT security incident response.” Information management & computer security (18), pp.26-42.