Assessment of Security Issues in Banking Sector of Libya

Salima Benqdara
University of Benghazi
Benghazi, Libya

Almabruk Sultan
University of Benghazi
Benghazi, Libya

Awad Elfergani
University of Benghazi
Benghazi, Libya

ABSTRACT
Information security in the banking sector is heavily controlled as banks store and manage their clients' private information. Information security has always been the responsibility of the information technology (IT) department in organizations. Banks have become a component of the internet and daily lives. Libyan banks facade limited cash due to the part up political circumstance since 2014, as a result of limited cash individuals incapable to get their salaries. To solve this problem, most of Libyan banks are set up online electronic installment arrangements to assist individuals in buying their day by day needs. However, Cyber-attacks increasing day by day, and this is the challenge facing by banking where data is critical. These incidents could be prevented by implementing adaptable countermeasures promptly and minimizing risk. In this paper, a framework is proposed to assess the information security issue in Libyan banks. The study aimed at the assessment of security strategy in Libyan banks to identify security gaps. To achieve the aim of this study data collected by interview information security staff to evaluate the current security strategy in Libyan banks.

General Terms
Security, Risk Assessment.

Keywords
Keywords: Information Security, CIA, Risk Assessment, Security Assessment.

1. INTRODUCTION
Nowadays, technology has become a part of almost every field particularly the business sector and the banking division. The reliance on technology is so much that managing an account segment cannot be thought of without the use of innovation. But innovation has too brought an entire set of challenges to be managed with which incorporate outside dangers driving to cyber fakes, the higher effect due to purposefulness or inadvertent acts of inner representatives, unused social building procedures utilized to pick up secret accreditations [1]. The competitive nature of managing the banking, at the side the critical esteem of the assets they oversee, commerce and innovation organizations must take all steps essential to secure their resources. A compromise of these data resources seems to have a serious effect on the bank, bank clients, shape an infringement of laws and directions and adversely influence the notoriety and money related soundness of the bank [2].

Information security alludes to the security of the confidentiality, integrity, and availability of computerized data and of the systems that process, maintain and report this information; amid processing, storage and dispersal of yield. As with other business assets, the information requires security to guarantee that it is available and confidential which its integrity is protected where necessary [3]. information security gives the administration processes, technology, and assurance to permit business administration to guarantee business transactions can be trusted; guarantee IT administrations are usable and can fittingly stand up to and recover from disappointments due to error, deliberate attacks or catastrophe; and guarantee critical confidential information is withheld from those who ought to not have access it [4].Studies have to show that non-technical issues are as important as technical issues in defending an organization's sensitive data. Technical security controls are fundamental but they ought to be correctly indicated, designed, created, implemented, arranged, used and maintained steps that all include human beings. An exclusive focus on the technical aspects of security, without due thought of how the human interatomic with the system, is lacking. Success in information security can be accomplished when organizations contribute in both technical and socio-organizational assets [5].

The banking sector in Libya, like other countries in the region, is the foundation financial services provider for the economy. As Libya is from developing countries face several challenges in the development of technology compared to most developed countries [6]. Most banks in Libya are suffering a huge lack of liquidity, which affected the daily lives of every citizen across the country. As a result, Libyan banks deployed online electronic banking payments through mobile phones [7]. Due to reports, researches, and results of the interview, e-banking services require information security controls related to internet-based services that are not adopted in public Libyan banking [8] [9]. Besides, a recent report from Microsoft announced that the computer system in Libya has faced the highest infection of malicious and unwanted software compared to worldwide [10].

This paper has proposed a framework to assess the information security issue in Libyan banks. The study aimed at the assessment of information security identify the security gaps and selecting appropriate controls for these gaps. The rest of the paper is organized as follows: Section 2 discusses the related works. In section 3 present the proposed approach. Section 4 describes the flow of the experiment. The results and discussion of findings are presented in Section 5. Finally, Section 6 concludes the paper.

2. RELATED WORK
In an effort to address the security gaps, in this section discuss the published papers have provided solutions in an organizational or technical approach.

Shuaieb (2013) suggested an analysis of the factors affecting Internet banking adoption in Libya. The author highlighted the challenges facing the spread of electronic banking in Libya, such as, the weakness of security systems achieved in

the field of electronic commerce and the lack of an appropriate environment for electronic commerce.

Alemu and Omer (2014) proposed a cloud computing conceptual security framework for Banking Industry to addresses security, privacy, legal and compliance, and regulatory issues through conducting a systematic literature review on cloud computing and banking industry security standards, policy and best practices coupled with the interview as methods of data collection. The Authors are followed by ISO-27001 risk assessment and treatment to identify what bank's assets need protection and how to implement security control. They suggested either to accept, avoid or transfer risks. The point of disagreement in this paper is that the risks to the bank's customers' data cannot be accepted or transferred because once they are accepted they have accepted a weakness that could be breached later, so it should be put at a lower risk level with observation. .

Folorunso et al. (2016) introduced an online questionnaire to assess the computer and network security strategies for Nigerian Banks as a case study, the samples are limited to computer security experts and information technology department staff in banks. The security strategy that they are asking is regarding passwords, antivirus, firewalls, encryption, IDS, and IPS. Also, the study investigates if the Nigerian banks have experienced any form of attacks on their systems. The security strategy of the Internet-based services, which require more security strategy such as DMZ, is not mentioned in the study. The study findings that Nigerian banks are using effective computer and network strategies after, implementing almost all security strategies and they rarely experience malicious attacks of any form.

3. PROPOSED APPROACH

The population of the study is limited to computer security experts and information technology department staff in some of the Libyan banks. This paper proposes a framework to assess the information security issue in Libyan banks. The study aimed at the assessment of the security strategy to identify security gaps in Libyan banks. To achieve this goal, the data collected by interview information security staff to assess the current situation of the security in Libyan banks. Then suitable methodology for addressing the gaps will be based on selecting a reliable reference from international standards, assessing the current status of the network by interviewing the banks' information security officers and analyzing the current situation by identify the security gaps and selecting appropriate controls for these gaps. The primary reference of information security controls is NIST 800-53 revision 5. One of the targeted Libyan banks is selected to know its feedback about the outcomes of the security controls document. The overall methodology of this study is based on two phases as follows:

• Data Collected: A qualitative research method was followed by conducting an interview with information security staff in bank A, B, C and D to collect data on the current security situation and appliances that protect the security situation performance in Libyan banks. The Sample size for this research was comprise of the entire person belonging to or associated with banking professionals and IT Sector of banks A, B, C and D. They were IT professionals, Network and system administrators and Security Officers. The Data collected was from employees through a structured interview questionnaire. The Data was collected from employees through a structured interview questionnaire. The questions are followed down-up approaches (i.e low-level technical controls questions related security devices). The questions of the interview are prepared in advance, they are mapped to seven categories of data as shown in Table 1and 2.

Table 1: Mapping interview questions to interview aspects

Question(s)	Interview aspects
Q1	Sample position.
Q2	Any compliance with information security standards .
Q3	Any kind of attack that bank has been experienced.
Q4	Symptoms of (distributed) denial of service attack.
Q4,Q5, Q7 and Q8	Security strategy requirements.(Table 3.2 in details)
Q6	Current e-banking services.
Q9	Customer request path.

Table 2: Interview questions mapped to security strategies requirement

Question(s)	Security strategies requirement
Q5-3, Q8-4,5	Prevention.
Q5-3, Q8-4,5	Detection.
Q5-1,2	Perimeter defense.
Q5-4	Application layer
Q7	Compartmentalization (DMZ), including web server
Q8-1,2,3 Q7-4,Q3	Layering.

The process of the propose approach as follows:

• Data Analysis: After data and information are collected risk assessment analysis and statistical tools are used to analyze those collected data. Evaluating the current status of the security strategy by interviewing the banks' information security officers and analyzing the current situation by identify the security gaps and selecting suitable controls for these gaps. In this study, the risk matrix is used to define the level of risk by considering the category of probability or likelihood against the category of consequence severity. This is a simple mechanism to increase the visibility of risks and assist management decision making [15].

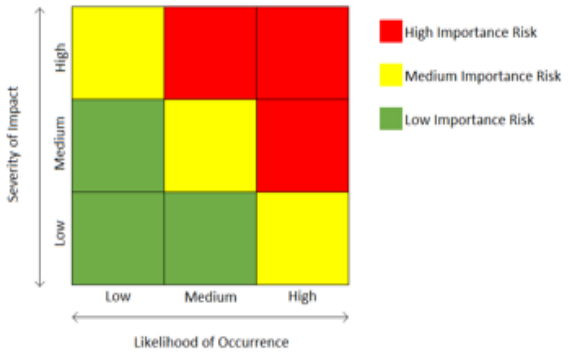

Fig 1: Risk Matrix

• Defining the corresponding controls that mitigate the potential threats and fix the vulnerabilities, these controls are selected from NIST. Priority was determined for the controls needed by the bank based on the CIA security level of each strategy by comparing them with the CIA that supposed to make critical assets safe. These controls will be used to improve security situation performance in Libyan banks.

4. EXPERMENTAL SETUP

This section describes the experimental setup which containing two parts

•Analyzing the current situation by identifying the security gaps based on data analyzed.

•In this study, a risk matrix is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity.

•Defining the corresponding controls that mitigate the potential threats and fix the vulnerabilities, these controls are selected from NIST..

5. RESLUTS AND DISCUSSION

5.1 Collected Data Result

Table 3 presents a summary of the implementation of the Information security standard used by Banks. The results in Table 3 showed that Bank A is not followed any type of information security standard. Whereas, banks B and D are selected ISO/IEC 27000 series, however they have not applied it. This can be attributed to the availability of corporate security policy in banks B and D. However, they have not applied it which resulting in effects on information security characteristics of (CIA) Confidential, Availability, and Integrity. The results find that the bank database and core banking will affect the integrity of it. Also causes in forcing the bank to disconnect it is the most valuable asset that will decrease the bank's reputation and it is monthly income. It can be concluded that the absence of awareness program and lack of Information security management has contributed to the shortage of identifying information security risks and selection of acceptable standards for the bank

Table 3: Information security standard used by Banks

Bank name	Answer	Standard name
Bank A	No	No thing
Bank B	Not activated	ISO 27001
Bank C	No answer	No answer
Bank D	Not activated.	ISO 27000

Table 4: Attack that bank has been experienced

Bank name	Answer	Attack type	Impact
Bank A	Yes	Remote Access Trojan (RAT)	Email website by replace the control page with attacker's page
		Web spoofing	Making money transfer
Bank B	No	No	No
Bank C	No answer	No answer	No answer
Bank D	No	No	No

In table 4 above the overall result in the kind of attack, that bank has been experienced. The table shows that Bank A is attacked by RAT and MiTM or web spoofing. The results indicated that attacks allow an intruder to have access inside the internal network and allow them to deep scan the network to identify the IDP, DMZ, and the firewall. Moreover attackers able to modify the log and database which results in the ability to delete the transaction from the log which causes critical risk for the bank. It is important to protect the bank system and detect the intrusions as soon as possible.

Table 5 explains the attack symptoms that can be observed during work, such as a slow network or could not get the service. Table 5 shows that there is a potential of DDOS attack which meaning effects on banking services and profits. The results find that the client cannot able to access his account when there is a DOS attack which affects the availability of the bank services. Also, the DDOS attack will cripple the network that causes disconnected to the internet and the banking services to be unavailable without IDP and a firewall to block the attack. The results concluded that this vulnerability will affect bank services stability daily. This risk is considered high for the bank.

Table 5: Symptoms of denial of service attack

Bank name	DDoS symptoms	Answer
Bank A	Need to restart equipment or device	Yes
	Slow network	Sometimes
Bank B	Need to restart equipment or device	No
	Slow network	Yes
Bank C	No answer	
Bank D	Slow network	Sometimes

Table 6 illustrates the availability of network components that achieve security strategies such as WAF, IPS, IDS, external firewall, internal firewall, DDoS protection device. The results show that DMZ, application layer and security layers and perimeter defense are partially implemented. However, prevention and detection not implemented. Whereas the boundary protections are required to prevent and detect malicious and other unauthorized communication. The results indicated that the security strategy implementation in the bank is very weak, which will become a target for attackers. Although the bank cannot able to identify the attack nor pervert it, which leads to vulnerable to any type of attack that causes the critical risk to the bank.

Table 6: Security strategy implemented

Bank name	Security strategy	Answer
Bank A Bank B Bank D	Prevention	Not implemented
	Detection	Not implemented
	Perimeter defense	partial implemented
	Compartmentalization	Not implemented
	Application layer	Not implemented
	Layering	Not implemented.

Table 7 below illustrates the current e-banking services provided by the banks and the type of services that are informational, communicative and transactional. This type of information is considered a critical asset to bank A. The most critical assets are services that shared on the internet for banks' customers. As presented in table 7 in terms of current e-banking services and the customer's request questions. The answers show that the customer's request does not go directly to the banks, but is transferred to a local company as a third party and

then sent to the bank. The interview expressed, orally, concern about inadequate third-party security capabilities and it does not fully comply with the security policies of some standards and this poses a major risk to the bank. This study focuses on hosting internet banking system by Libyan banks without any relation to the third party

Table 7: Security strategy implemented

Bank name	e-banking service online
Bank A	-Web site for Informational services. -Mobile application for communicative services via internet and telecommunication. -Mobile application and payment card for transactional services via internet.
Bank B	-Web site for Informational services. -Payment card for communicative services via telecommunication.
Bank D	-Informational services -payment card for transactional services via telecommunication. -There are no online banking services.
Bank C	No answer

5.2 Security Requirement Analysis

As presented in table 7, in terms of current e-banking services showed that the most critical assets are services shared on the internet for banks' customers. Figure 2 demonstrates the types of current e-banking services. The Figure shows that Transactional services are considered as the highest risk type since they allow the customer to change the bank's financial data such as transferring funds. This type of service greatly affects information security characteristics of (CIA) which result in a direct financial loss to the bank. Therefore this type of service requires a more secure network.

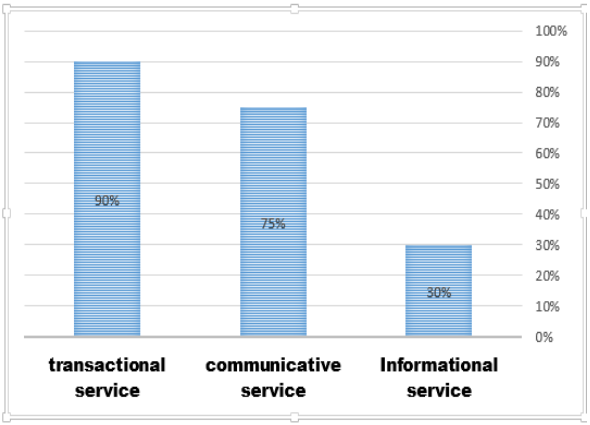

Fig. 2. Level of risk for types of financial services

Table 8 illustrates the security level of Confidential, Availability and Integrity CIA for transactional services that should be achieved in banks. The results indicated that the probability of denial services is high which means the lack of banking services and profits Availability. Besides, the current data which reaches the customers not integrating, therefore the current probability is consider low. However the data which are not integrity have significantly impact on the bank's reputation and may cause financial loss. Moreover, the activation of encryption protocols is lacks hence the

transmission of data in bank is not Confidential. Thus the possibility of this risk is high and its impact causes financial problems for the bank and customers

Table 8 CIA security level of critical asset

CIA	**Probability** of compromised information or losing access to information	**Impact** on pubic customers and banks	**Security level** (Probability + Impact = Security Level)
Availability	High	High	High
Integrity	Low	High	Medium
Confidentiality	High	High	High

Figure.3 illustrates the security strategies of the perimeter network in the bank. The result shows that the security strategies implemented by 28 % and 25 % for DMZ and Layering, respectively. The Application layer and Perimeter defense implemented by 33 % and 50 %, correspondingly.in terms of Detection and Prevention, and the results showed that prevention and detection not implemented. The results showed that there are weaknesses in the security strategies in the absence of perimeter network security components. The results concluded that the Absence of DMZ implementation allows the attacker to scan and access the entire network. Moreover, without the device to detect it nor prevent it, the hacker will be able to modify the transactions log and the database which leads to effect the bank integrity and confidentiality.

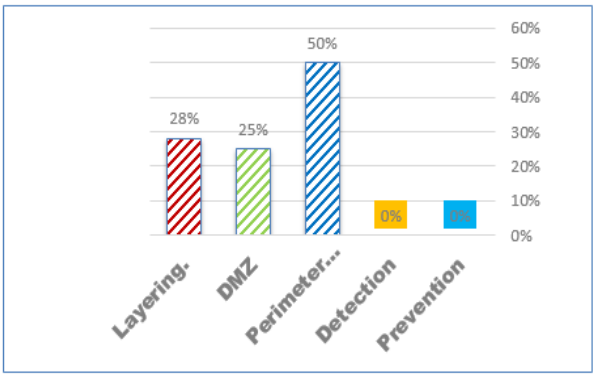

Fig. 3. A security strategy implemented in the bank

Figure 4 illustrates the percentage of each security strategy is needed to secure a perimeter network. The security strategies for the perimeter network are required to prevent and detect malicious and other unauthorized communication and the secure perimeter network. The results indicated that to achieve CIA, the DMZ implementation is a vital component which will help the network to be separated with a zone that would make harder for the attacker .moreover, Detection and prevention are one of the keys to maintaining the security level in the institute without them the bank would be an open gate to the public. Therefore, the security strategies for the perimeter network are required to prevent and detect malicious and other unauthorized communication.

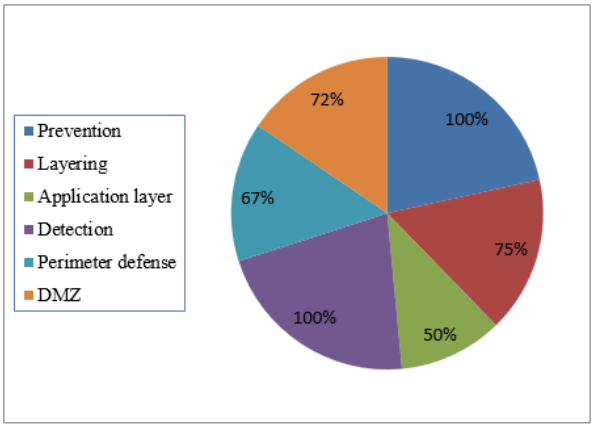

Fig. 4. A security strategy that required by the bank

Figure .5 illustrates the security strategy elements and the CIA of critical assets that should be protected. The results showed that the CIA security level is high since the absence of network security components that needed to achieve layers strategy. To improve this strategy controls such as Defense-in-depth, Attack surface reduction, and Layered structures required to achieve by compliance with NIST security. Application layer strategy had a similar result the CIA security level is high Because of the deficiency of network security components that needed to achieve application layer protection strategy such as WAF appliance. This strategy is achieved by controls, for example, boundary protection, prevent exfiltration, least functionality, information output filtering, and transmission confidentiality and integrity. The results of the Prevention and detection strategy are high for CIA security Because of the absence of the IPS and IDS which needed to achieve prevention and detection strategies. DMZ, Detection strategy and Perimeter defense had a similar result that the CIA security level is high since the absence of network security components such as DDoS protection, router, web server, and firewall for DMZ, IPS, IDS, and WAF. These strategies are achieved by controls, for example, denial of service protection, least functionality, System interconnections, boundary protection, least functionality, system monitoring, and system-generated alerts.

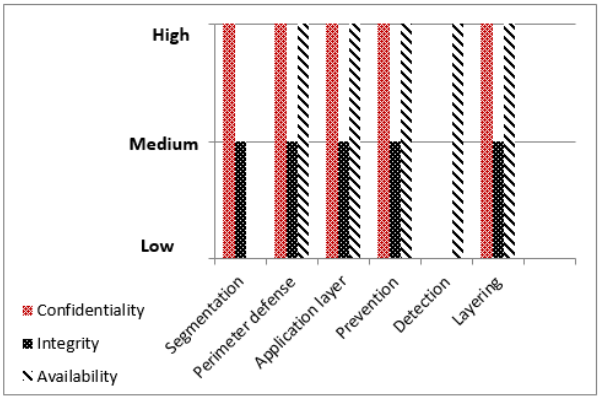

Fig. 5. CIA that required to be protected by every security strategy

6. CONCLUSION AND RECOMMENDATION

In this study data collected on the current security situation for some of the banks in Libya then analyzed using the risk assessment matrix and static tool to identifying the critical assets that need to be protected. The results showed that there are security gaps in the current security system which is responsible for share customer's information as to their request. During data analysis, vulnerabilities were mapped to known potential threats and the impact of these threats on security characteristics. CIA was determined. Based on the probability and impact of the bank's information, availability and confidentiality were the most affected by the current security flaw. The management of information security in Libyan banks should improve its processes and be aware of the benefits and advantages arising from information security standards. The results showed that there is no deployed to the standard on reality. Information security management is free to choose the appropriate standards for the bank. The Libyan banks should implement a comprehensive and adequate set of information security components that aid in addressing threats on the technical, process and people levels based on identified information security risks and the appropriate controls that are necessary to mitigate the identified risks. Also, The Libyan banks should compile and implement a formal well defined information security policy and its derivatives (guideline, Procedure, and Standard) that give guidance and direction to all members and stakeholders on the Bank regarding the management and protection of information assets. Further, The Libyan banks should also work on assurance and recovery controls. Avoidance control is proactive guarantees that trying to minimize or mitigate the risk of intentional intrusion.

7. REFERENCES

[1] G.Gopalakrishna "Report of the Working Group on information security, electronic banking, technology risk management, and tackling cyber frauds", RBI, Mumbai, Maharashtra, January 2011 Available: https://rbi.org.in/ scripts/ NotificationUser.aspx?Mode=0&Id=6366.

[2] Zahoor, Z., Ud-din, M., & Sunami, K. (2016). Challenges in privacy and security in banking sector and related countermeasures. International Journal of Computer Applications, 144(3), 24-35.

[3] Whitman, M. E., & Mattord, H. J. (2011).Principles of information security. Cengage Learning.

[4] Alabed, S. H., & Hanandeh, R. (2013). The Impact of Implementing Information Security Management Systems on E-Business Firms: Case Study in Jordanian Banking Sector. Middle East University.

[5] Ayalew, G. (2016). Assessment of information Security Culture in the Banking Industry: the Case Study of Development Bank of Ethiopia (Doctoral dissertation, St. Mary's University).

[6] Elmadani, M. (2015). The Study of Service Quality in Libyan Commercial Banks (Doctoral dissertation, University of Huddersfield).

[7] Ibrahim ,A. (2017). Cash crisis pushes Libyans to virtual payments. Accessed Nov, 2018. https://phys.org/news/2017-08-cash-crisis-libyans-virtual-payments.html Conference, Edith Cowan University, 75-82. Perth, Australia.

[8] Pack, J. (2017). Libya's Liquidity Crunch and the Dinar's Demise: Psychological and Macroeconomic Dimensions of the Current Crisis." US-LIBYA Business association Washington. Accessed Sep, 2018. http://www.us-lba.org.

[9] Elgahwash, F., Freeman, M., and Freeman, A. E. (2014). Improving online banking quality in developing nations: A Libyan case.

[10] Microsoft, "Security Threats", Microsoft Corporation, 2018. Accessed Feb, 2018 https://msdn.microsoft.com/en-us/library/cc723507.aspx

[11] Shuaieb, E. (2013). Factors affecting the adoption of Internet banking in Libya.

[12] Alemu, M., and Omer, A. (2014). Cloud Computing Conceptual Security Framework for Banking Industry. Journal of Emerging Trends in Computing and Information Sciences, 5(12), 921-930.

[13] Ogunwobi, Z. O., Folorunso, S. O., & Alebiosu, O. (2016). Evaluation of Computer and Network Security Strategies: A Case Study of Nigerian Banks. In OcRI (pp. 85-90).

[14] Tytarenko, O. (2017). Selection of the best security controls for rapid development of enterprise-level cyber security. Naval Postgraduate School Monterey United States.

[15] Anthony (Tony) Cox Jr, L. (2008). What's wrong with risk matrices? Risk Analysis: An International Journal, 28(2), 497-512.