Effectiveness of Card Banking Security in the Ethiopian Financial Sector: a Gap Analysis

Daniel Gebrehawariat
IT Infrastructure and Security Department
Bunna International Bank
Addis Ababa, Ethiopia
danihawari@gmail.com

Lemma Lessa
School of Information Science
Addis Ababa University
Addis Ababa, Ethiopia
lemma.lessa@aau.edu.et

Abstract

These days, financial institutions such as banks are highly exposed to different cyberattacks and their electronic payment system is among the targets of the attack. This study is aimed at assessing the information security management practice with focus on electronic banking system in selected financial institutions in Ethiopia using international information security standard as a benchmark in order to identify the gaps and recommend the best security practices to help the financial institutions meet the required security compliance. Two financial sectors were purposively selected. All the IT staff in the IT departments of the two institutions were included in this study. Quantitative data was collected using PCI-DSS security standard questionnaire. In addition to the questionnaire, observation and document analysis was made. The result shows that most of the essential security management activities in the financial sectors do not comply to meet the international security standard. Similarly, the level of most of the indispensable security requirement that should be in place is found below the acceptable level. The study also revealed the major security factors that prohibit the financial sectors from the PCI-DSS security standard compliance. Thus, recommendations for practice are forwarded to support the financial sectors' effort to withstand and mitigate cyberattacks.

Keywords
Payment Card Industry, Data Security Standard, Card Data Environment, Automatic Teller Machine

1. Introduction

In the current competitive business environment, Information is the most valuable and fundamental asset in any organization. Therefore, protecting the security of information is very important and becoming a top priority for many organizations (Heru et al 2011). To protect this valuable asset, information, there should be a proper information security practice and management that keep information from a wide range of internal and external threats and preserve its value to the organizations. As Shi-Ming et al (2006) noted, if organizations follow the guidelines and standards to set up their security policy, they could own a tighter and more complete IT environment. Organization could also safeguard their business value and benefit from IT if there is a well-developed information security management. In addition to this, businesses also need to implement rules and controls around the protection of the valuable information and systems that store and process of information, and this protection is attained through the proper implementation of information security policies, standards, guidelines and procedures.

Security compliance is one of the major issues in information security management (Munirul et al., 2011). Different frameworks, guidelines, and standards were proposed by researchers, practitioners, consultants, and professional to protect organization information assets (Choobineh et al., 2007). The most widely used international standards are: COBIT, ISO 27001&2 and PCI-DSS (Payment Card Data Security Standard) Among these widely used standards, PCI-DSS is a very first industry-wide standard which focuses on the credit card industry that aims at achieving a strong protection of sensitive consumer and card data, and preventing major security issues. The standard sets mandatory requirements in many aspects, including secure networks, card data protection, access control, vulnerability management, security assessments and reporting (PCI Council 2010). To that end, any bank that runs ATM, POS (Point of sale) machine, issues debit cards, credit card and electronic payment sector that do business with the merchants need to be complaint to PCI-DSS security standard security compliance.

These days, data breaches occur regularly and as financial sector, banks and electronic payment sectors are very frequent target from hackers who often successfully compromise sensitive information. In this regard, being PCI-DSS security standard compliance is indisputable. The financial sectors are expected to be compliant to the security standard such as PCIDSS in order to be connected to the international payment brands. In addition to that, being security standard complaint will enable the financial sectors to protect their valuable asset from the current internal and external attacks. On the contrary, most banks and electronic payment processors in Ethiopia often fail complying PCI-DSS in time due to improper security settings, incorrect configurations, low levels of encryption and poor policies and procedures. Assessing those controls using PCI-DSS standard checklist could have prevented costs in business disruption as well as monetary fines and makes the financial sectors competitor in the international market by enabling them to provide international card services such as VISA International, MasterCard, Union Pay and the like.

As PCI- DSS standard is used to improve the security of electronic and online banking data and to facilitate consistent security measures to mitigate data breaches and fraud, the researcher will use PCI-DSS security standard checklist to assess the current information security management in the Ethiopian financial sector focusing on the card banking security on top of using ISO security standard checklist to assess the general aspect of information security management in the financial sector. The organizations selected for this study are financial sectors in which one is from the banking industry and the other is from the electronic payment processing. As a banking sector, bank ABC provides all the major banking services that a commercial bank is expected to provide with the vision to be the bank of choice for customers, employee and shareholders and the mission to be customer focused financial services through competent, motivated employees and modern technology to maximize the value of its stakeholders. The Bank is among the four banks that issues electronic payment card and PIN security numbers at its premises to provide card banking service to its customers. The second financial sector where this research is conducted is XYZ S.C. It a consortium owned by six Ethiopian private banks established in 2009 by the visionary banks to save the high investment cost of the modern payment platform and deliver electronic payment services to financial institutions with a shared system. It commenced operation officially on July 5, 2012. Thus, this research focuses on the information security management in the financial sectors focusing on the card banking services.

1.1 Research Problem

Protecting individuals' financial information is one of the fundamental activities to be undertaken by all financial organizations to enhance the business. Business partners, suppliers, and vendors are seeing security as the top requirement, particularly when providing mutual network and information access. To provide fast and appropriate response to security incidents and to ensure interoperability between the financial sectors, there is a need for a systematic and predefined information security management. And to that end, it is crucial to assess the current security management of the financial sectors.

Here in Ethiopia, most of the banks have implemented a core banking system that interconnect all branches with the head quarter, and few banks and electronic payment system processors are connected to the international payment system on top connecting to a national switch to transact electronic payment services using ATM and POS (Point of Sale) machine. For all these, technology plays a vital role for carrying out the delivery of financial services whereas the risk followed the implementation of these technologies and the problem associated with it are not well considered. According to Spremic (2011), adopting industry best practices (e.g. CobiT, ISO 27000, PCI-DSS) and adjusting IT infrastructure with high-level executive objectives makes companies to lower IT risks, which is related to infrastructure and operational risks. And the security standard, PCI-DSS, is used to assess the information security status of organizations and provide a mitigation and road map to make the organization secured and complaint.

The financial sectors are expected to be compliant to the security standard such as PCIDSS in order to be connected to the international payment brands. In addition to that, being security standard complaint will enable the financial sectors to protect their valuable asset from the current internal and external attacks. On the contrary, most banks and electronic payment processors in Ethiopia often fail complying PCI-DSS in time due to improper security settings, incorrect configurations, low levels of encryption and poor policies and procedures. Assessing those controls using PCI-DSS standard checklist could have prevented costs in business disruption as well as monetary fines and makes the financial sectors competitor in the international market by enabling them to provide international card services such as VISA International, MasterCard, Union Pay and the like. PCI-DSS security standard reduce the risk of electronic payment including debit card, credit card and internet banking data loss by preventing, detecting, and reacting to potential breaches or hacks that lead to an account data compromise since one of the goal of PCI-DSS is to protect electronic payment system from risk and threats and minimize data breach risk. Electronic banking has many security issues which includes fraud, data loss and lacks information security in general (Arif Shaikh, 2014). To address all these information security issues related to the card banking security, this study is made using PCI-DSS security standard check list to assess the effectiveness of information security practice and management of the card banking security in the financial sector and to identify the factors that prohibits the Ethiopian financial sectors from PCI-DSS security standard compliance.

3. Methods

The researchers used purposive sampling technique and selected two private banks and one electronic payment processor to conduct this research. The selected two private banks and the electronic payment processor issue electronic payment card at their premises. Since, among the seventeen commercial banks in Ethiopia, only four banks print electronic payment card and PIN (Personal Identification Number) at their premises to transact money using payment terminals such as ATM and POS machine. And from the four banks that have electronic card issuing service for the electronic payment services, two banks were selected using purposive sampling technique. The researchers used purposive sampling technique as it provides the deliberate choice based on the qualities of the participant possesses to address the objective of the research. In this regard, the researchers can decide the sample based on what to be studied as per the study objective (Etikan et al., 2015). Since, purposive sampling techniques involve selecting certain cases based on a specific purpose rather than random selection (Teddlie and Yu, 2009). In addition to the four banks with card banking services, there are two electronic card payment service providers sectors that are established under the Ethiopian national bank license to provide the electronic payment service which serves as a switch among the banks and print the electronic payment card (debit card) and PIN. The researchers also selected one electronic payment processor among the two financial sectors using purposive sampling. Hence, 50% of the banks that issues electronic card and PIN, and 50% of the electronic payment processors are selected for this study using purposive sampling method. Regarding the target population, all the IT executives and IT staff in the IT department were selected to answer the questioners.

4. Results

4.1 Security Scoping

The security scoping questions provided to the financial sectors comprises of how their inventory device are updated, and whether it included all the necessary information regarding the devices information such as model of devise, location of device, serial number asset identification tag and classification of item type . In addition to this, it verified if there is a detailed network diagram covering all boundaries in scope including network segmentation, if there are boundaries between trusted and un-trusted networks, wireless and wired networks, type of devices, device interfaces, protocols and security controls in the scope.

Table 1: Security scoping of hardware and software inventory

	Frequency	Percent
Less Secure	8	32.0
Partially Secure	6	24.0
Fully Secure	11	44.0
Total	25	100

The result in Table 1 shows that hardware and software asset inventory has been maintained in the organizations but the existing inventory is not updated to include all the essential assets which should be under the security scope. Furthermore, the existing inventory didn't have detailed description and function of use. Regarding the network diagram, there is a detailed network diagrams which covers boundaries in scope including network segmentation and boundaries between trusted and un-trusted networks. However, the Network diagram was not updated with cardholder data components of the organizations since the following was not well illustrated within the diagram:

- The Card Data Environment (CDE) and non-Card Data Environment (Non CDE) data flow is not well mentioned in the network diagram.
- DMZ (Demilitarized Zone) is configured in the premises however; there are components which aren't included in the DMZ zone.
- ATM and POS (Point of Sale) transaction connectivity (Type of connection, systems involved within operation) is not clearly defined to include the end to end connectivity for storing, processing and transmission of transaction data.

4.2 Media and Facilities Security

The media and facility security part of the questioners includes how the removable media that contains sensitive information is properly labeled to protect the information from an authorized access, how the medias are destroyed using procedures supported by legal reasons such as retention period based on business justification, how onsite personnel are identified from visitor and the entry control security as a whole using different technologies such as CCTV and Access control.

Table 2: Media and Facility Security

	Frequency	Percent
Less Secure	9	24.0
Partially Secure	10	40.0
Fully Secure	6	36.0
Total	25	100.0

The result in Table 2 shows that there is no documented procedure which is existed in the organization to include the below requirements:

- Maintaining a list of media devices periodically.
- Periodic inspection of media devices to look for tampering or substitution.
- Training personnel to be aware of suspicious thing and to report tampering or substitution of devices.

4.3 Network and Security

The network and security category consists of both wired and wireless network security on top of the technologies applied to protect the premises from unauthorized access and periodic vulnerability assessment and penetration test.

Table 3: Network and Security

	Frequency	Percent
Less Secure	2	8.0
Partially Secure	11	44.0
Fully Secure	12	48.0
Total	25	100.0

As shown in Table 3, there is notable gap in network and security. Internet connection is separated from the internal network through firewall and router and there is no direct connection between internet and internal network of the organizations. Furthermore, production and test environment is segmented to protect production environment from any security risk using VLAN technology however, the firewall and router configuration standard has not been documented to include roles, responsibilities and access privileges to the network components. Further to this, services and ports are not restricted for inbound (incoming) and outbound (outgoing) traffic in the card data environment. There is no successive quarterly wireless scanning and analysis activity that identifies unauthorized access point at the premises. In addition to that, there is no all-inclusive vulnerability assessment and penetration test conducted regularly to verify the security of the whole perimeter and the security system to monitors and responds to networks intrusions, vulnerabilities and irregularities behaviors are not monitored on a 24/7 basis hence, it will not be easier to take immediate action if any internal or external incident occurs.

4.4 Application Security

In relation to application security, it is tried to evaluate the software development process, security patches management, application log monitoring and application change detection mechanisms. As evidenced in Table 4, not all system components were installed with the latest patches on time to fix the application from recent virus definitions. There is no application vulnerability assessment and application penetration test conducted periodically or at the time of significant change, and application firewall is not deployed on perimeter location.

Table 4: Application Security

	Frequency	Percent
Less Secure	6	24.0
Partially Secure	9	36.0
Fully Secure	10	40.0
Total	25	100.0

Furthermore, the file integrity and log monitoring tool is not fully integrated with all the application systems to alert unauthorized access and modification. It is examined that cardholder data components including Windows servers, Linux servers, Oracle Database, Application, Cisco firewall, Router and Switch are configured to enable audit track and send all logs to centralized system which are file integrity monitoring and log monitoring to monitor the system components. However, not all the component in the scope is integrated and configured to send logs to the log monitoring system. Moreover, logs are not analyzed periodically to examine the security status of the system components.

4.5 Card Data Security and Encryption

The card data security and encryption questioners include both card holder data security and the encryption technology used to protect the sensitive data from being exposed to an authorized access.

Table 5: Card Data Security and Encryption

	Frequency	Percent
Less Secure	6	24.0
Partially Secure	13	52.0
Fully Secure	6	24.0
Total	25	100.0

While data is transmitted over the public network, security protocols such as IPSEC (IP Security) and SSH (Secure Shell) is used to secure the end to end connectivity nevertheless, it is not fully implemented (as revealed in Table 5) with all the connections and some of the application components don’t use cryptography technologies such as SSH (Secure Socket Shell). Access to sensitive areas are not strictly limited to individuals that there job requires to visit this area and there is no formal and periodic security awareness training though, there is security briefing up on the hiring on new staffs. Regarding the network diagram that identifies the connections between cardholder data environment and other networks, all the cardholder components are included in the network diagram however, the network diagram doesn’t show the cardholder data flows across systems and networks.

4.6 Logging and Monitoring

As shown in Table 6, the logging and monitoring category consist of time synchronization technology (NTP), password management, access management, user management process and account management.

Table 6: Logging and Monitoring

	Frequency	Percent
Less Secure	10	40.0
Partially Secure	10	40.0
Fully Secure	5	20.0
Total	25	100.0

- There are users who have not logged in for more than 60 days and are not disabled and removed from the system.
- Account lockout has not been configured on some of the components (Servers and Network) based on requirement.
- It is verified that there are system components not configured with minimum password length.
- Some system components are not configured with password complexity enabled (alphanumeric characters).
- There are system components which are not configured with password history
- In some of the components, Password is not interactive to enforce strong password.

4.7 Policy and Procedure

The organizations aren't providing security training and don't provide refresher training every year as it is documented in the information security policy. Information classification policy is not defined within the organization to maintain proper control of all assets identified with the correct classification and Table 7 magnifies this issue.

Table 7: Policy and Procedure

	Frequency	Percent
Less Secure	5	20.0
Partially Secure	11	44.0
Fully Secure	9	36.0
Total	25	100.0

As a part of the recruitment and training policy, all employees sign on commitment form, which mentioned that they understood the policy and procedures. Non-Disclosure agreements with all employees are maintained. Changes are not being routed through change management. Access rules are being modified based on specific request from different department however, structured formal change management was not followed for systems, firewall and router configuration changes.

4.8 Anti-Malware

As indicated in Table 8, antivirus has been installed on most of the components including servers and client machines but it may not protect all the machines from all type of malicious software since the antivirus is not updated in some components with new virus definitions and new updates.

Table 8 Anti-Malware

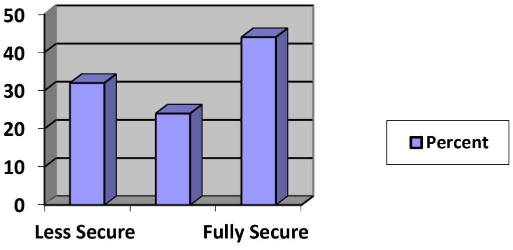
	Frequency	Percent
Less Secure	5	20.0
Partially Secure	8	32.0
Fully Secure	12	48.0
Total	25	100.0

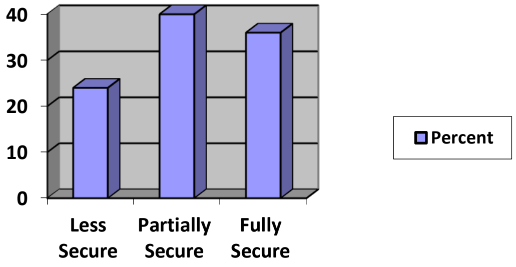
The Antivirus has not been enabled and configured to generate logs to store log files since it is not configured to be integrated with the log monitoring server. Moreover, there was no antimalware procedure or virus prevention procedure documented to make the action easier while such kind of attack happens in the premises.

5. Discussion

According to Bradley and Dent (2010), organizations have struggled to adequately protect their most sensitive information assets, leading in many cases to breaches of security and the loss or disclosure of sensitive data. Many widely publicized incidents of high-profile data losses occurred across the globe in recent years in which of the 90% confirmed breaches that investigated, 285 million records were compromised and that 80% of these records involved payment card data. The report confirmed that fraudulent use of this payment card data occurred in 83% of these cases. Thus, financial organizations should work hard in securing their premises from an unauthorized access and protect their sensitive information and business as well. Periodic vulnerability scanning, which is every quarter is mandatory for the financial organizations to identify gaps and mitigate on time before the occurrence of any damage. As Lokhande and Meshram (2013), vulnerability is a weakness which allows an attacker to reduce a system's information assurance by intersecting the system flaw, access to the flaw, and exploit the flaw.

As per PCI-DSS Reference Guide (2010), security vulnerabilities in applications systems may allow criminals to access PAN and other cardholder data. Many of these vulnerabilities are eliminated by installing security patches, which perform a quick repair job for a specific piece of programming code. All critical systems must have the most recently released software patches to prevent exploitation. Entities should apply patches to less-critical systems as soon as possible, based on a risk-based vulnerability management program. Secure coding practices for developing applications, change control procedures and other secure software development practices protects the application system if it is properly followed.

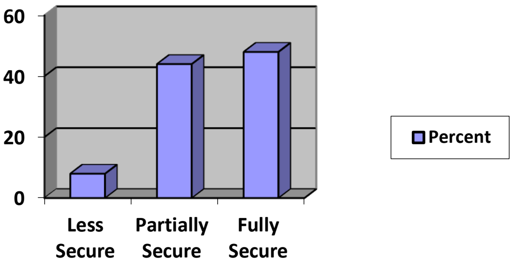


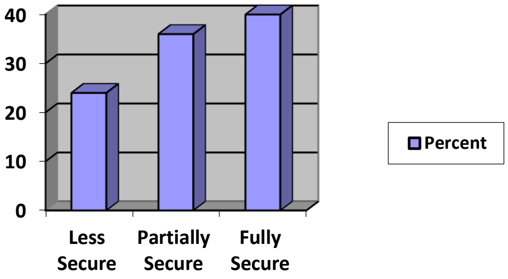


Security scoping of hardware and software inventory

Media and Facility Security

One of the key success factors in analyzing and measuring the effectiveness of information security is to ensure that the organization has a thorough understanding of the assets which are most valuable to them, and those assets have been allocated an appropriate level of classification based on criticality of the asset relative to prioritized risk (Khan, 2010). If all the valuable assets are not included in the scope for security management, there will not be effective information security management in the organization. As Liu et al., (2010), the media inventory should be stored securely and while those media are useless for legal or business reasons, they must be destroyed permanently.

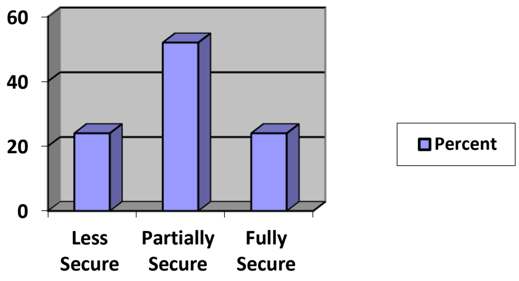




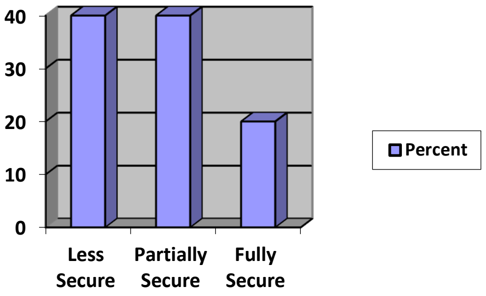
Network and Security

Application Security

For the network devices, security policy was not defined properly and default services were allowed for inbound and outbound traffic. In addition to this, personal firewalls were disabled by users. According to Omariba et al., (2012), when a computer is connected to the network, it becomes vulnerable to attack. A personal firewall helps to protect the computer by limiting the types of malicious traffic initiated.



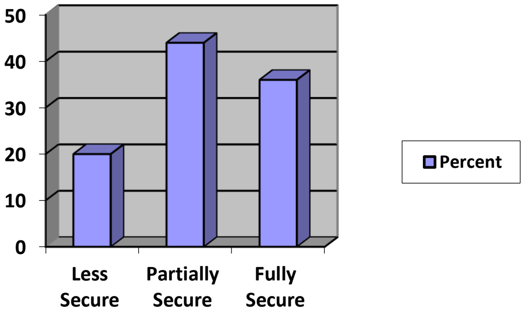
Card Data Security and Encryption



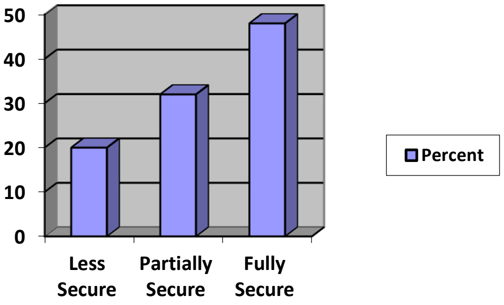
Logging and Monitoring

Data retention and disposal policy and procedure have not been well documented in the organizations, and the practice is not exercised properly. Hence, data retention requirement such as secure deletion of cardholder data was not addressed descriptively in the security policy and there are some system components where full PAN (Primary Account Number) was displayed.

One of the major security protections for organization is password security. Since common types of attack is occurred by week password management practice in the organizations. As Liu et al., (2010), passwords should be changed every 90 days, and the minimum length should be seven characters, where alphabetic and numeric characters are both required and the user whose repeated access attempts are over six times should be locked out from accessing the system.



Policy and Procedure



Anti-Malware

Information security policies and procedures are in place but it is not carried out in a day to day activities. The organizations weren't providing security awareness training for its employees periodically as per the information security policy. As Shi-Ming et al (2006) noted, if organizations follow the guidelines and standards to set up their security policy, they could own a tighter and more complete IT environment.

Antivirus wasn't installed on some of the components including servers and clients and antivirus wasn't updated on some critical components with up-to-date signature. Malicious software like viruses, worms, and trojans can give access to unauthorized and malicious people by entering into computer system and antivirus software is capable of removing or quarantining known malware, and it is able to generate audit logs actively (Susanto et al., 2011).

In addition to these, sensitive information should be encrypted while it is transmitted internally or externally for business need. Encrypted data is intrinsically protected because it is unreadable. This is the major reason that it is required in so many compliance guidelines and industry standards (Lokhande and Meshram, 2013). And the use of IPSEC (IP Security) encryption ensures secure private communication over the IP networks by facilitating direct IP connectivity between sensitive hosts through untrusted networks (Singh et al., 2014). Since, as Desisa and Beshah (2014), layered security control in the communication channel is recommended for the financial sector while using the public network like the Internet. Cryptography technology should also be used to protect sensitive information in the financial sectors. According to Singh et al., (2014), cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit or in storage. Information security uses cryptography technology to transform usable information into a form that is unusable by anyone other than an authorized user. One of the major security protections for organization is password security. Since common types of attack is occurred by week password management practice in the organizations. Organization should have a password management policy that is adhered by all the staffs and there should be password enforcement on every system components. Hackers can guess passwords locally or remotely using either a manual or automated approach as there are many tools available which can automate the process of typing password after password. Password cracking methods also capture password hash and convert it to its plaintext original. For password cracking, an attacker uses tools like extractors for hash guessing, rainbow tables for looking up plaintext passwords, and password sniffers to extract authentication information. Password crackers sniff authentication traffic between a client and server and extract password hashes or enough authentication information to begin the cracking process (Lokhande and Meshram 2013).

Change and release management policies ensure adequate testing and roll back policies (Liu et al., 2010). It defines the authorization and escalation processes, incident classification, and exception management with centralized log management, reviews, and continuous monitoring with appropriate audits. The information security policy should also include the basic requirements such as assigning risk ranking to vulnerabilities including high, medium and critical risk status in addition to that; there should be clearly stated incident management procedure to be followed. As Susanto et al., (2011) stated, information Security incident management involves identification of resources which are needed for incident handling. Good incident management will help with the prevention and awareness of incidents.

Antivirus software is capable of removing or quarantining known malware, and it is able to generate audit logs actively (Susanto et al., 2011). Periodic wireless scan is also mandatory for organizations to identify insecure connections availability in the premises and take action accordingly. As Lokhande and Meshram (2013), many people may think about logging in to a random and unprotected wireless network just to get some work done. That's all it takes for someone with ill intent to capture a user's login credentials and work his way onto the wireless network. There are security policies and procedures prepared and documented to manage and control the organizations information security from unauthorized internal and external access but the policies and the procedures are not maintained to be executed in the day to day activities of the organizations. In general, information security management and practices in the Ethiopian financial sectors are not well addressed and maintained in regard to the current security threat and risks associated with the financial sectors. In this study, in addition to assessing the effectiveness of information security management in the Ethiopian financial sectors focusing on the card banking security, the factors prohibiting the effectiveness of information security management towards Payment Card Industry Data Security Standard (PCI-DSS) are identified. As the result implies, the effectiveness of information security management and practice focusing on the card banking security is below the acceptable level. On top of this, the factors that are prohibiting the financial sectors from security standard compliance are identified.

6. Conclusion

Absence of one vital asset from the security scoping implies that the organization has not used its resources to best advantage in addressing security risk exposure (Zhi Xian Ng et al., 2013). If certain assets were not considered in the risk assessment, then they may be unprotected which in turn lead the organization to adverse consequences such as leakage of sensitive information and interruption or destruction of critical IT services. In addition to including all the vital assets in the scope, devices inventory need to be updated with detail description and function to identify and classify assets easily and protect from loss and unauthorized access. Device security operation procedure needs to be documented to include requirement as maintaining a list of devices, periodic inspection of devices to look for tampering or substitution and training personnel to be aware of suspicious behavior and to report tampering or substitution of device.

Media inventory should be stored securely and while those media are useless for legal or business reasons, they must be destroyed permanently (Liu et al., 2010). Regarding the physical security, there should be entry controls to limit and monitor physical access to systems using video cameras and access control mechanisms that monitors individual physical access to sensitive areas such as data center, card printing room and PIN printing room. As (Susanto et al., 2011) mentions, physical and environmental security are used to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment, buildings and rooms to protect the environment and to avoid damage or unauthorized access to information and systems. All network device configuration need to be changed using a defined change management. This change management should include testing and approval of new access rule and connection before it is implemented on the production system. Organizations should develop change management forms which include detailed business justification for the requested change such as which ports and protocols are required and for what purpose and a roll back procedure should also be maintained. According to Pinder (2006), risk initiated by unexpected events and changes will be mitigated by adequate change management processes. When a computer is connected to the network, it becomes vulnerable to attack. A personal firewall helps to protect the computer by limiting the types of traffic initiated by and directed to the computer. The intruder can also scan the hard drive to detect any stored passwords (Omariba et al., 2012).

Organization must have a formal process to approve and test external connections and changes to firewall configurations. The standard demands a justified documentation of unapproved or risky protocols, a description of network managing groups, roles and their responsibilities, and lists of services and ports needed to operate the business. It also requires a review of the firewalls and router settings on a quarterly basis. Every connection from an un-trusted area must be blocked by the firewall (Liu et al., 2010). System components in the organization should be configured with secured services such as SSH, RDP-SSL, IPSEC VPN and strong encryption technology such as VPN and RDP-SSL. In general, to protect sensitive cardholder data during transmission, strong cryptographic and security protocols like Internet Protocol Security (IPSEC) and SSL/TLS must be used (Susanto et al., 2011). According to Lokhande and Meshram (2013), it is not considered logging onto a random and unprotected wireless network to get some work done. That's all it takes for someone with ill intent to capture a user's login credentials and work his way onto the wireless network. Patch management procedure should be documented to include installation of critical vendor patch within one month and all applicable patches should be installed within vendor defined timeframe. As Susanto et al., (2011) stated, security patches fix the majority of bugs by installing the latest official security patches no later than one month after the release. Moreover, all of the patches must be tested before deployment.

In the software development process, development and test environments should be separated and there should be a separation of duties between personnel assigned to the development or test environments and those assigned to the production environment. Furthermore, production data should not be used for testing and test data and accounts should be removed before a production system becomes active. Generally, there should be a separate environments and duties for development, testing, and production in the organization (Susanto et al., 2011) and the databases and applications must have a production environment that is physically and logically separated from the test and development environment (Liu et al., 2010). Card data encryption policy and procedures should be documented to include Full PAN to only be displayed to specific roles and users with business need. And no PAN data should be stored without encryption in addition to this, SSL/TLS or other cryptography method should be used for cardholder data transmission since insecure channel should not be used for cardholder data transmission. According (Susanto et al., 2011), organization should render the Primary Account Number (PAN) into an unreadable form when stored via using pads, index tokens, truncation, and should use strong hash functions or a strong cryptography with an appropriate key-management procedure. Cardholder data should be encrypted while sending it over end user messaging technologies. And no clear text PAN data should be shared over email or any end user messaging technology. In addition to this, all unnecessary default ids, user account need to be disabled or removed. This includes all system components (Firewall, Router, switch, application, and database). All accesses to network resources should be tracked and monitored using log files or audit trails, critical activities can be tracked and analyzed in a further step if something goes wrong. Without the log files and audit trails, it would be difficult to determine the cause of any problem (Liu et al., 2010).

References

Bradley, M. and Dent, A. (2010). Payment Card Industry Data Security Standard (PCI DSS) –What it is and its impact on retail merchants, Royal Holloway Series, pp.16-19.

Choobineh, J., Dhillon, G., Michael R. Grimaila, Jackie Rees (2007). Management of Information Security: Challenges and Research Directions, Communications of the Association for Information Systems Volume 20, pp.958-971.

Desisa, A. and Beshah, T. (2014), Internet Banking Security Framework: The case of Ethiopian Banking Industry, HiLCoE, Computer Science College, Addis Ababa, Ethiopia pp.8-13.

Etikan, I., Musa, S., and Alkassim, R. (2015). Comparison of Convenience Sampling and Purposive Sampling, American Journal of Theoretical and Applied Statistics, Department of Biostatistics, Near East University, Nicosia-TRNC, Cyprus, p.p1-4

Heru, S., Almunawar, M. N. and Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five, International Journal of Electrical & Computer Sciences Vol: 11, pp.21-27

Liu, J., Xiao, Y., Hui Chen, Suat Ozdemir, Srinivas Dodle and Vikas Singh (2010). A Survey of Payment Card Industry Data Security Standard, pp.287-303

Lokhande, P. S., and Meshram, B. B., (2013). E-Commerce Applications: Vulnerabilities, Attacks and Countermeasures, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, pp.499-509

Omariba, Z. B., and Wanyembi, G. (2012). Security and privacy of electronic banking, International Journal of Computer Science Issues, Vol. 9, pp. 432-446

PCI DSS Quick Reference Guide 2010. Understanding the Payment Card Industry Data Security Standard version 2.0, PCI Security Standard Council, pp.1-34.

Pinder, P. (2006). Preparing Information Security for legal and regulatory compliance information security technical report, pp.32-38

Shaikh, M. A. (2014), Ethiopian Banker's Perception of Electronic Banking in Ethiopia – A Case of Adama City, International Journal of Scientific and Research Publications, Volume 4, pp.1-7

Shi-Ming, H., Lee, C., and Kao, A. (2006). Balancing performance measures for information security management, Industrial Management & Data Systems, Vol. 106, pp. 242-255

Spremic, M. (2011). Standards and Frameworks for Information System Security Auditing and Assurance, Proceedings of the World Congress on Engineering Vol I London, U.K.pp.978-988.

Teddlie, C. and Yu, F. (2007). Mixed Methods Sampling: A Typology with Examples, Journal of Mixed Methods Research, p.p77-100

Ula, M., Ismail, Z. and Sidek, Z. M. (2011). A Framework for the Governance of Information Security in Banking System, Journal of Information Assurance & Cyber security, pp.1-12.

Zachary B. Omariba, Zachary B. Omariba, Dr. G. Wanyembi (2012). Security and privacy of electronic banking, International Journal of Computer Science Issues, Vol. 9, pp. 432-446.

Zhi Xian Ng, Atif Ahmad, Sean B. Maynard (2013). Information Security Management: Factors that Influence Security Investments in SMES, Australian Information Security Management Conference, Edith Cowan University, pp.60-73

Biographies

Daniel G.hawariat has MSc degree in Information Science from Addis Ababa University, Ethiopia and a BSc Degree from RMIT University and Addis Ababa University, through a joint venture program hosted at Addis Ababa University, Ethiopia. He is also a certified ISO/IEC 27001 Lead Implementer. Currently he is an IT infrastructure and System Security Division Manager at Bunna International Bank, a private commercial bank in Ethiopia. Previously he worked at Premier Switch Solutions one of the Electronic Payment Switch service providers in Ethiopia as a Network and Security Section Head for about six years, and served as a PCI-DSS Compliance Project Manager in the same company for more than four consecutive years. Daniel also worked at ZTE Corporation, a Chinese giant telecom solution provider, for more than five years. His interest area is Cyber Security.

Lemma Lessa is an assistant professor of Information Systems at School of Information Science, Addis Ababa University (AAU), Ethiopia. He received his doctorate in Information Technology (specializing in Information Systems) in 2016, Master of Science degree in Information Science in 2003, and BSc degree in Library Science (Computer Science minor) in 1995 from AAU, Ethiopia. Dr. Lemma has completed research projects in ICT for Sustainable Development and Application of Blockchain Technology for e-Government services. His teaching interest is on the social and management aspects of Information Systems. His postgraduate teaching includes Information Systems Security Management, Information Systems Strategy & Management, Enterprise Systems, Information Systems Project Management among others. His research interest is on behavioral, socio-cultural, and organizational aspects of Information Systems in general and the adoption and evaluation of e-Government in particular. He is member of Association for Information Systems (AIS) and current president for the Ethiopian chapter of AIS. He is serving as editor and reviewer for African Journal of Information Systems, reviewer for reputable conferences such as the International Conference on eDemocracy & e-Government, International Conference on Digital Transformations and Global Society, Hawaii International Conference on System Sciences, and International Conference on Electronic Governance and Open Society.