Journal of Scientific Research and Development 2 (6): 75-80, 2015
Available online at www.jsrad.org
ISSN 1115-7569

Feasibility of creating SOC in Agricultural Bank of Iran

Sajjad Daliri *

Network Department, Keshavarz Hi-Tec Solution Company, Agricultural Bank of Iran

Abstract: Reliable security is essential for information systems. Considering the extent and speed of utilizing e-banking, banks require more up-to-date and sophisticated mechanisms than others. Security Operations Center (SOC) is a safe mechanism capable of providing such security for all pertinent functions of a bank. The purpose of this study was to evaluate the feasibility of using the SOC for enhancing the reliability of the security system at the Agricultural Bank of Iran at all levels. In this study, the relevance of the SOC to the Agriculture Bank of Iran is assessed from a multidimensional viewpoint that includes structures, people, processes, and price.

Key words: Security Operations Center (SOC); Network security; Banking network; Security-process; Access control; ISMS

1. Introduction

Reliability and security of information have been of concern within the banking system. In mid-1970s, the Information Security Management System (ISMS) was introduced as a policy, articulating matters regarding information security (Humphreys, 2011; Dhillon and Backhouse, 2000). Since then numerous efforts have been made to assure the reliability and security of information systems by designing new security systems and introducing new standards for enhancing security (PCI DSS 3.0, 2014).

One of the more promising structures known as the Security Operations Center (SOC) is a centrally located unit, technically and organizationally, in charge of all information security matters of the entire organization (Managed Services at the Tactical FLEX, 2014).

As an all-in-one structure, SOC offers a comprehensive and systematic approach in continuously (24/7) monitoring and controlling the entry and exit of the data, confronting information security issues with an attitude of spontaneous security-threat-detection with immediate response, leaving no room for further deterioration of the process. It is especially the latter, plus the centrality of SOC and its non-stop operation that make it one of the better choices for ensuring information security for the banks "(Transaction Monitoring for HMG Online Service Providers, 2014).

Banks have been among the first to embrace the new technology and offer electronic banking (Majidpour and Setareh, 2011). The velocity of exchanging financial information electronically, across the globe, by the banks, enhances the need for a fast and flawless information system that secures the data (Liao and Cheung, 2002). Similarly, the Agricultural Bank of Iran has been one of the first Iranian banks to embrace the new technology and offer electronic banking.

Research indicates that the SOC is capable of satisfying this need, for banks in general and the Agricultural Bank of Iran in particular.

1.1. Necessity of SOC in banks

At the first step in securing electronic or online banking, bank prompts its customer to use its equipment or tools (Moghadas, 2010), but this is not enough lonely. Deployment of security solutions such as Firewalls, Anti-malware, IDS†, IPS‡, Access-control and Authentication-systems can somewhat rescue the network from its passive and without supervision mode. Using this equipment leads generating a huge amount of security incidents in different formats (Scarfone and Mell, 2007). But with network integrated and comprehensive security observation in SOC, managers can have a detailed analysis of network security situation and its risk, in addition that it provides the permission to have the best reaction against the threats. The main reasons for the necessity of SOC in the bank are as follows (Gholipour and Imani, 2010):

- Prevention of failures albeit small and short
- Notification and registration of attacks and threats revealed in the banking system
- Avoiding the traffic increase in accessing to data centers
- Prevention of multiple configuration problems in firewall, IDS, and routers
- Optimal management of events

* Corresponding Author.

† Intrusion Detection System
‡ Intrusion Prevention System

- Removing duplicate events and the correlation between events
- Protecting and responding to different types of attacks
- Creating security patches to correct applications and network equipment
- The exact knowledge of the managers of the network security risks

1.2. Definition

SOC is a place for 24-hour monitor and control the security of entry and exit the data in the realm of information exchange with the attitude of security threats detections.

1.3. Purposes

SOC produces an immediate report of what is happening on the network with data collection by various tools deployed throughout the network and then the integration of this information and integration of them. Network operator can manage and response to the attacks before they harm the network using this information (FAVA Passive Defense Center, 2009; FAVA Passive Defense Center. 2013). Determination and correction and timely reaction are the main reason for setting up the SOC and one of the most important issues in its design should have these public following features (FAVA Passive Defense Center. 2013):

- Scalability: Do its duty with the increase in production of events
- Modularity: Can add or change the new analysis and correlation algorithms and resources to the system.
- High efficiency: Have a complete coverage of the relevant infrastructure
- Security: Collection of events from different sources must be through secure channels.
- Connection with computer rescue centers: In order to update and comprehension their knowledge base, they use output of the computer relief and rescue centers (FAVA Passive Defense Center, 2009).

1.4. Overall structure

Security incidents are produced in an information infrastructure by the sensors. Security events are collected and stored in the same format in the events database. The collected events are analyzed by the analyst and then attacks and security threats related to the information infrastructure will be announced after evaluating the correlation between events (HP Enterprise Security Business Whitepaper, 2011). In the following, performance of each of the major parts of the system will be examined (Gholipour and Imani, 2010; FAVA Passive Defense Center, 2009).

- Sensors: The resources are the collected security events. The most important sensors are IPS, IDS, firewall, switches and routers, operating systems, Internet services, anti-malware, etc. (Abdullah et al., 2006).
- Aggregation unit of events: This unit collects events using related protocols and stores them after preprocessing operation and monitoring these events in the database.
- Correlation analysis and detection unit of events: Responses for analyzing the collected events across the information infrastructure.
- Patch management and configuration review: It improves attacks and threats in the process of analyzing events and respond to events generated by security managers.
- SOC portal and console: Have duties such as immediate notification of security events, adjusting parameters for each of the following systems and preparing a variety of reports on the status of network security, and generated security events and also analysis and reporting of security risks.

1.5. Advantages

Threat management, vulnerability assessment, security device management, online security dashboard, trouble ticket system, reporting system.

2. A review of past works

2.1. SOC in non-bank organizations

- Transportation Security Administration (TSA) is an agency of the Department of Homeland Security United States of America that has deployed SOC in most airports in the country (TSA, 2014).
- Microsoft has provided solutions for the establishment of the SOC. The company has created centers in America, Britain, and India and provide services in the field of duties through seven hundred websites [Microsoft in Public Safety and National Security].
- IBM Company has provided managed security services under the web security tools and provides them to the applicant organization (SOC).
- HP Company describes the best way for the creation and growth of the SOC in a paper that can be useful for those organizations that are building new SOC or optimize their existing SOC (HP Enterprise Security Business Whitepaper, 2011).
- Infrastructure Communications Company: It is the subset of Ministry of Communications and Technology in 2014 that is implementing its own SOC project (Ministry of Communications and Information Technology, Infrastructure communications Company, 2011).

2.2. SOC in banks:

- SOC was inaugurated at the Central Bank of India in June 2012. The purpose of its establishment was to integrate security activities.
- Central Bank of South Africa is established in 2013 (UBA).

- The first phase of bank emergency and network security control center has been launched in 2012 in the country and its future plans of this center announce becoming a bank SOC (Iran e-banking news website, 2012).

3. Presentation of the proposed model

Using a Security Operations Center is the solution to all problems. The implementation possibility of this center should be provided in both forms of software and hardware (Leon and Sixto, 1976). SOC shows the status of what is currently happening in the network through a central console. This center simultaneously suggests or implements appropriate solutions tailored to each event (Nadel and Barbara, 2004; Bidou, 2011).

3.1. Proposed plan

The notable point in this design is the flexibility in methodology, in which certain solutions can be offered to clients according to their specific required services to manage network security. All services offered by the SOC are monitored and managed (McAfee® Foundstone® Professional Services, 2013). The plan should be designed in such a way that it has a comprehensive approach to the various aspects of this center.

Provable services by a safety relief group can be divided into three general categories: Preventive block, reaction block and quality security management block.

3.1.1. Preventive block

All actions in preventive block are done in order to prevent cyber threats. The following occurs in SOC empowering block: Individuals, tools (software), protocols, equipment (hardware).

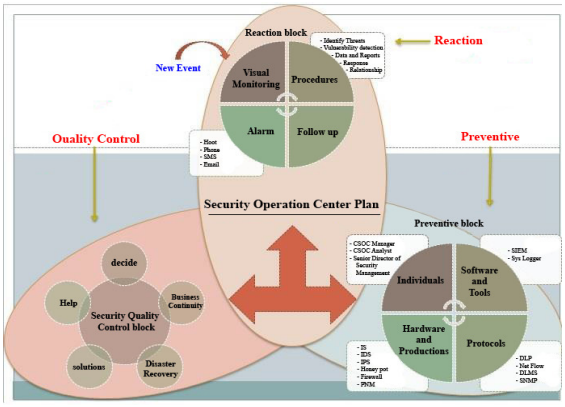

Fig. 1: Architecture of proposed plan

Table 1: Preventive block details

Name	Details	Dependence
CSOC manager	It has coordinating and managing role on all activities (McAfee® Foundstone® Professional Services, 2013)	Individuals
CSOC analyst	It analyzes the events and records them in certain forms (McAfee® Foundstone® Professional Services, 2013)	Individuals
SIEM tool	It is used to reduce errors in IDS diagnosis (Swift, 2014).	Tools
Sys logger	It is a standard for logs. Windows operating system logs are saved in binary format in evt files (Neysi and Madhaj, 2011)	Tools
DLP Protocol	It is able to detect and block leakage of information in web security gateways (Websense, 2010)	Protocols
Net Flow Protocol	It sends the flow data to the server that pass from the router or switch (http://www.cisco.org)	Protocols
SNMP Protocol	The seventh layer protocol that allows the transfer of management information between network elements. It is part TCP/IP protocol (Douglas et al., 2001)	Protocols
IDS	It identifies and detects any unauthorized use of the system, abuse or harm by both internal and external users (Darrin, 2003)	Equipment
IPS	Its tasks are identifying malicious activities, recording information about them, action to stop them and recording reports (Engin et al., 2009)	Equipment
Firewall	Probably already have a firewall and there is no need to re-install it on the system (Raj, 2000)	Equipment
PNM	It monitors services, servers and hardware (PNM, 2010)	Equipment
Honey pot	It is an information system that uses its resources to detect and collect unauthorized activity on the network (Kaushik and Tyagi, 2012)	Equipment

3.1.2. Reaction block

These services are not limited to the security group and they are designed with the aim of enhancing the overall security of the IT system. These services include risk analysis, continuity of operations and disaster recovery plans, security consulting, information, education, and assessment. This block includes the following processes: Monitoring, procedures, follow-up, warning (Khalilipour and Nouralivand, 2012).

3.1.3. Security Quality Management block

This block contains the following: Decision making, business continuity, disaster recovery, problem-solving, and relief.

3.2. Proposed cycle

Deming cycle consists of four stages: Planning, implementation, control, and review that are raised by Dr. Deming§. Deming PDCA cycle is a simple and effective method to solve the problem and change management (Shewhart and Walter, 1980). Continuous model proposed in this center is as follows:

Fig. 2: Security Operations Center in the PDCA cycle

PDCA cycle is repeatedly executed in different time intervals T. With the implementation of the cycle, designing is done first at each stage. Then, this design is implemented on the bank's IT platform. This implementation is reviewed and evaluated and finally, the design will work on it.

3.3. Evaluation the status of the proposed SOC in the framework of security architecture

SABSA is a layered model for organizational security architecture. SABSA model is composed of six layers and the general characteristics of each layer is shown in the following table.

Table 2: Various levels of SABSA security architecture

Skill view	Contextual architecture of security
Architect view	Conceptual architecture of security
Designer view	Logical architecture of security
Constructer view	Physical architecture of security
Supplier view	Architecture of security component
Service manager view	Security services management architecture

One of the features of SABSA is using the best practices and standards of information security. SABSA framework unlike other frameworks that are more abstract is more functional and with presenting methodology. In the view of the above mentioned security architecture, six questions of what, with what motivation, how, who, where must be answered.

3.4. Structural aspects of the proposed model to the Agricultural Bank

Before the creation of SOC, organizations need time for its planning to design it in the following way before the implementation of the structure.

3.4.1. Physical structure

Includes facilities, workforce, support staff, training and practice, sharing threat intelligence, surveillance technology and additional technologies

3.4.2. Training

Training courses should include:

SANS**, Intrusion Detection In-depth, and GCIA††. For security information and event management (SIEM) organizations, training program spins around ArcSight and ACSA ‡‡(Communication Vally Reply, 2011).

3.4.3. Power supply planning

There should be at least ten analyst among manpower employed in SOC 24×7×365 (24 hours Day 7 days a week, every day of the year) Best timing for these four is a twelve-hour shift per week. Two of the more experienced analysts who are known as second level analysts work in 8×5 work shift (Tanenbaum and David 2010).

3.4.4. Structure of processes and procedures

The evolution of process management initially is achieved by repeatability and continuous improvement processes. Capability Maturity Model Integration (CMMI) belonged to Software Engineering Institute (SEI) Carnegie Mellon® proposed an excellent method for continuous improvement process: CMMI provides the essential elements of effective processes in organizations. This model can be used during implementation of the project and a portion or all of the organization and in order to improve the process. It also helps to integrate separate categories such as organizational duties, set of purposes and development processes priorities, guidance of high-quality processes and also providing a reference point to assess current processes (Paulk, 2002).

SOC processes are divided into four main categories:

- Commercial processes: It is the documentation of all management components, which is required for practical implementation.
- Technology processes: Maintenance information that include system management, configuration management and conceptual design.
- Operational processes: Machine documentation of daily operations such as scheduling work shifts and turn-over procedure.

§ Dr. William Edwards Deming (October 14, 1900 – December 20, 1993)

** System Administration and Network Security

†† GIAC Certified Intrusion Analyst

‡‡ ArcSight certified security analyst

- Analytical processes: Includes all activities designed to identify and understand the devastating events.

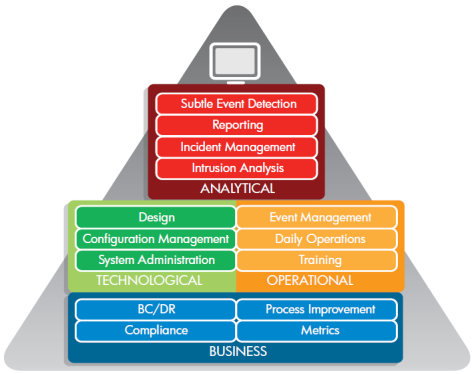

Fig. 3: Hierarchy of SOC

3.5. Technology

Arc Sight solutions are the better solution for monitoring, evaluation, and response to malicious events. ESM is a step beyond the storage and preparation, monitoring and communication. Its characteristics are analysis based on the historical event and automatic reaction and a high level of risk management in relation to trade in today's digital world. Arc Sight manages the event in real-time and does legal works and creates warning event source preparation time with caution exercise.

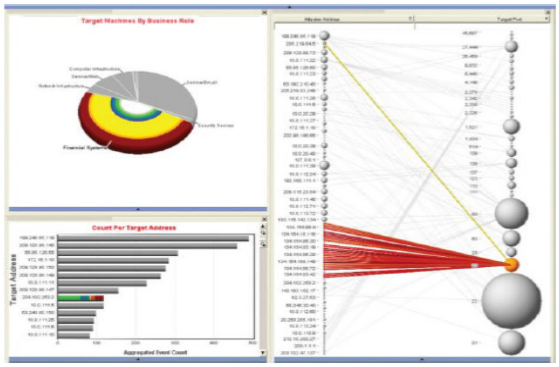

Fig. 3: Effective analysis using ESM

4. Conclusions and recommendations

Based on the software lifecycle, it can be said that assessment of the quality of SOC is a process that should be done during a cycle.

4.1. Methodology

Key performance indicators are different depending on the type and strategy and strategy. Key performance indicators help measure the progress of the organization, but they have problems for measurement the knowledge-based activities. A key performance indicator is a key part of a measurable objective that is made of a path, index, benchmarks, targets and time frame (Taylor and Gibbon, 1990). Therefore; the proposed should be assessed with qualitative factors. Key performance indicators are classified in categories named control purposes and represent goals that each category is responsible for it (Tanenbaum and David 2010; Manzuk, 2006). We should inevitably collect all key performance indicators that must be fulfilled in SOC to evaluate this proposed model. This set of indicators can also be viewed and explained as a basis for evaluating the performance of each SOC. This index was reviewed in the proposed model and it can be seen that the proposed model can meet all these indicators. These indicators are supported by proactive and reactive block. Similarly, IPS and VPN with protocols of SSL VPN and PPTP, L2TP over IPsec, IPsec also including indicators that are supported by proactive and reactive block.

4.2. Recommendations

The obtained results in this paper cover different aspects. On the one side, the most important achievement is presenting an inclusive plan, which observes different perspectives of the Agricultural Bank's cyber security issues and will demonstrate appropriate action in the event of any problem. Another important extracted aspect of this paper is the presentation and suggesting SOC lifecycle that works based on the PDCA model and it makes the deployed SOC on cyber banking system to move towards technological maturity by continuously planning, performing, evaluating and action.

4.3. Future works

Due to the ongoing nature of subversive activities in cyberspace banking, it is expected that SOC adapt itself to the new conditions and dynamically respond to different circumstances to protect the property of the people. Items that can be recommended for future works are as follows:

- Providing a more detailed conceptual model to describe the life cycle of SOC
- Providing a conceptual model to describe the maturity of the centers
- Providing and developing the organizational structures and Follow Diagram
- Explaining the organizational field activities (WBS) in Bank's administrative system

Codification of structured and precise key performance indicators to access.

References

Abdullah K, Lee Ch, Conti G, Copeland J, Stasko J. 2006. IDS Rainstorm: Visualizing IDS Alarms. IEEE,10.1109/VIZSEC.2005.1532060, ISBN: 0-7803-9477-1, P 1-10.

Astan Ghods Razavi, Department of Development Management and Support. 2013. SOC.

Bidou R. 2011. Security Operation Center. citeseerx.ist.psu.edu, 10.1.1.93.8577.

Communication Vally Reply. 2011. Security Operation Center, http://www.reply.eu/

Darrin W. 2003. Intrusion Detection Systems: An Overview of Real Secure, SANS Institute, October, 2003.

Dhillon G, Backhouse j. 2000. Information system security management in the new millennium. Communications of the ACM Magazine. NY USA. Pages 125-128. Doi>10.1145/341852.341877.

Douglas R. Mauro & Kevin J. Schmid T. 2001. Essential SNMP (1st Ed.). Sebastopol, CA: O'Reilly & Associates.

Engin K, Somesh J, Davide B. 2010. Recent Advances in Intrusion Detection, 12th International Symposium, RAID 2009, Saint-Malo, France, September 23–25, 2009, Proceedings. Springer. pp. 162–. ISBN 978-3-642-04341-3. Retrieved 29 June 2010.

FAVA Passive Defense Center. 2009. Project of architecture and design domestic SOC based on open source solutions.

FAVA Passive Defense Center. 2013. Necessity of creating SOC from the perspective of passive defense.

Gholipour A, Imani S. 2010. Technology process in Banking. Management Bimonthly, No 159; P 22-25.

HP Enterprise Security Business Whitepaper. 2011. Building a Successful Security Operation Center. Hewlett-Packard Development Company. ESP-BWP014-052809-09.

Humphreys, Edward (8 March 2011). "Information security management system standards". Datenschutz und Datensicherheit - Dud 35 (1): 7–11. Doi: 10.1007/s11623-011-0004-3.

Iran e-banking news website. 2012. Conversion Kashef to banking SOC within a year.

Kaushik G, Tyagi R, Honeypot. 2012. Decoy Server or System Setup Together Information Regarding an Attacker. VSRD International Journal of Computer Science & Information Technology 2: 155–166.

Khalilipour A. Nouralivand Y. 2012. Cyber threats and its impact on national security. The journal of strategy studies. No 56. P 167-196.

Leon D, Sixto O. 1976 Security: Defense against Crime. Manila: National Book Store. P17.

Liao Z, Cheung MT. 2002. Internet-Based E-Banking and Consumer Attitudes: An Empirical Study. Information & Management, Vol 39, P 283-295

Majidpour, M; Setareh, F. 2011. Electronic Payment – Evolution and Current Techniques. Electronic Banking. No 37; P 30 – 41.

Managed Services at the Tactical FLEX, Inc. Network Security Operations Center (NSOC)". Tactical FLEX, Inc. Retrieved 20 September 2014.

Manzuk S, etl. 2006. Network Security Assessment: From Vulnerability to Patch. Syngress, ISBN: 1597491012, edition 2006.

McAfee® Foundstone® Professional Services. 2013. Creating and Maintaining a SOC, The details behind successful Security Operations Centers.

Ministry of Communications and Information Technology, Infrastructure communications Company. 2011. Implementation of the SOC project.

Moghadasi A. **20**10. Variety of payment methods in e-banking, Age IT Magazine. No 58; P 71-75.

Nadel J, Barbara A. 2004. Building Security: Handbook for Architectural Planning and Design. McGraw-Hill. p. 2.20. ISBN 978-0-07-141171-4.

Neysi J. Madhaj N. 2011. Investigation privacy and protection of cyberspace data in Iran criminal provisionswith comparative look on Germany, England and Italy criminal provisions. The first regional conference on new approaches in computer engineering and IT. Ramsar. May 26-28. P 662-669.

Paulk M. 2002. Capability Maturity Model for Software. Copyright © 2002 by JohnWiley & Sons, Inc. All rights reserved. DOI: 0.1002/0471028959.sof589

PCI DSS 3.0: The Impact on Your Security Operations". Security Week. 31 December 2013. Retrieved 22 June 2014.

Public Network Monitoring (PNM). 2010. Sun Cluster 2.2 System Administration Guide, ORACLE.

Raj J. 2000. Network Security, the Ohio State University.

Scarfone K, Mell P. 2007. Guide to Intrusion Detection and Prevention Systems (IDPS). Computer Security Resource Center (National Institute of Standards and Technology) Retrieved 1 January 2010: P 94-800.

Shariatia M, Bahmania F, Shamsa F. 2011. Enterprise information security, a review of architectures and frameworks from interoperability perspective. Procedia Computer Science, Elsevier.

Sherwood J, Clark A, Lynas D. 2009. Enterprise Security Architecture. SABSA.

Shewhart T, Walter A. 1980. Economic Control of Quality of Manufactured Product/50th Anniversary Commemorative Issue. American Society for Quality. ISBN 0-87389-076-0.

Swift, David. 2014. "A Practical Application ofSIM/SEM/SIEM,AutomatingThreat Identification" (PDF). SANS Institute. p. 3. Retrieved 14 May 2014 .

Tanenbaum AS, David J. 2010. Computer Networks. Wetherall, 5th Edition, ISBN-10: 0132126958.

Taylor C, Gibbon F. 1990. Performance indicators. BERA Dialogues (2), ISBN 978-**1**-85359-092-4.

Transaction Monitoring for HMG Online Service Providers". CESG. Retrieved 22 June 2014.

Transportation Security Administration (TSA).2014. Agency of the U.S. Department of Homeland Security, United States, "www.tsa.gov", last visited on 2014.

United Bank for Africa (UBA), UBA Commissions State-Of-The-Art Security Operations Centre For More E-Banking Security, 2013

United Bank of India, Public Relations Division , Head Office, Kolkata , 2012

Websense. 2010. Websense Web Security Gateway: Integrating the Content Gateway component with Third Party Data Loss Prevention Applications.