ISSN: 2321-7782 (Online)

Volume 4, Issue 1, January 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Study of Information Technology Security Threats and Security Practices Adopted in Co-operative Credit Society With reference to Karad and Patan Taluka

Manisha G. Patil[1]
Assistant Professor, MCA Department
Krishna Institute of Computer Application & Management
Wathar, Karad, Satara, Maharashtra, India

Dr. R. D. Kumbhar[2]
Assistant Professor, MBA Department
Karmeveer Bhaurao Patil Institute of Management Studies and Research
Satara, Maharashtra, India

Abstract: Due to globalization the credit societies adopt the change in their manipulation and maintenance of data. Information Technology implementation has brought about significant changes in the way the co-operative credit society's process and store data. By implementation a information system in co-operative credit society the organization face some security related problems which is harmful to society as well as stakeholders for their financial transactions. This study seeks to identify the security threats occurred in cooperative credit society and various security practices adopted by cooperative credit societies for minimizing the risks occurred because of security threats. Researcher studied the total 68 cooperative credit societies from Karad and Patan taluka. Out of these 47 cooperative credit societies are from Karad Taluka and 21 cooperative credit societies are from Patan Taluka. Researcher has taken 68 technical persons and 68 information system users using census method. Researcher has found that the number of security threats occurred to the information system are large and the number of security practices adopted by societies are less.

Key words: Security threats, information system, security practices, information technology.

I. INTRODUCTION

The 21st century brings an embracing convergence of computing, information and knowledge. It causes the growth of high speed networks as well as accurate computing power. This explosion of technology is changing the co-operative credit society from paper to computerized services. Some of the co-operative credit societies in India are using information technology based systems since 1995 for performing different transaction processing activities.

The various functional areas in credit societies where information technology affects are following:

1. Deposits
   - Saving
   - Current
   - Fixed
   - Recurring
   - Pygmy deposit
2. Loans
   - Housing
   - Personal

- Agricultural
- Loan against deposits

Information security means protecting information and information systems from unauthorized access, use, disruption, or destruction. There are some goals of information system they are-

- Confidentiality: -Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems
- Integrity: - In information security, integrity means that data cannot be modified undetectably
- Availability: - For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.
- Non-repudiation: Non-repudiation is the prevention of either the sender or the receiver denying a transmitted message.
- Authentication: Authentication involves confirming the identity of a person. Information system security has evolved significantly and grown even more important in recent years.

II. Objectives

1. To examine the information system security threats observed in credit societies.
2. To study present information system security practices adopted in cooperative credit societies.

III. Review of Relevant Literature

James D. Harris, Felix F. Dreher, Maeve L. Cummings (2005) in their research article explains that credit unions are offering more services that depend on information technology. But these services offer more security threats to the confidentiality and integrity of member information. It is likely that the person with specific responsibilities for planning, oversight, and operational management of the computer information services will hold a position such as CEO, CFO, or Vice President rather than a more technically oriented position such as system administrator or IS manager. Since information assurance and computer security concerns have grown rapidly in recent years the security posture of the organization could potentially be enhanced by providing key leaders with training regarding relevant threats to information resources along with appropriate countermeasures.

Michael Kimwele,Waweru Mwangi, Stephen Kimani (Journal of Theoretical and Applied Information Technology volume 18 No.2,2005-2010)said in their research article that after implementation of Information Technology in SMEs in Kennya they are not aware about any security policy. To minimize threats the SMEs should have to follow security policies such as create more awareness programs amongst SMEs and offer them related products to help in protection, Education on the topic of Internet Security, Hold vulnerability seminars to try and show SMEs what goes wrong in their day to day operations.SMEs are depending more on their information technology infrastructure but they lack the means to secure it appropriately due to inadequate know-how. SMEs can be made adequately aware of information technology security issues through regular education and training.

Paul Jeffery Marshall (International Journal of Scientific & Engineering Research, Volume 1, Issue 1, October-2010 ISSN 2229-5518) in this paper researcher gives four scenarios regarding cyber crimes in financial institutions. After the study and research, researcher concluded that there should be awareness of increased activity of cyber crime in financial institutions and gives some cardinal rules of information security as

1. Unprotected Information Systems is a Business Crime
2. Lack of Information Security Policy is Unacceptable
3. Audit and Compliance routinely to Identify Information Security Shortfalls
4. Risk Management Analysis Strengthens Information and System Security
5. Strong Virus Protection Policy help protect against Network Vulnerabilities and Threats

Benjamin Tomhave in Information Security Technologies (November 10, 2004) this research paper provides analysis of 13 information system security control measures it includes Access Control Management, Antivirus, Audit Data Reduction, Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Anomaly Detection Systems (ADS), Event Correlation Systems (ECS), Network Mapping, Password Cracking, Public Key Infrastructure, Virtual Private Network, and Vulnerability Scanning Systems. This paper provides basic overview information about each technology, but primarily focuses on analyzing each technology within the modern information security and business context, looking at how it meets business needs while addressing Confidentiality, Integrity and Availability as a Countermeasure that Detects, Corrects and/or Protects.

IV. RESEARCH METHODOLOGY

The study is inferential descriptive (diagnostic) in nature based on systematic collection, analysis, and interpretation of the data related to information technology asset and information system security practices used in co-operative credit societies.

Sample Design :- The method used for selection of sample is stratified proportionate random sampling method in which units are divided into two stratums. Each taluka is considered as stratum.In every sample unit there is one technical person who look after information system and IT assets and one to two information system users performing IT related tasks. Researcher has taken 68 technical persons and 68 information system users using census method.

Data Sources

The data is collected for the research by using two different sources –

Primary data sources –

The primary data is collected through a well structured schedule from users of information system and technical personals of a sample credit society.

Secondary data Sources –

The necessary secondary data is collected from sources like societies documents, reference books, reports, various publications, journals, articles and reports.

Instrument: Two different structured schedules are used for collecting the data from information system users and technical staff.

V. RESULTS

TABLE 1 SECURITY THREATS

Below table shows various security threats observed in sample units and their intensity.

Sr.No.	Security Threats		Intensity of Security Threats.				Total
			Frequently	Moderately	Rarely	Never	
1	Hacking	Count	8	12	30	18	68
		%	11.76%	17.65%	44.12%	26.47%	100%
2	Password Misuse	Count	23	19	17	9	68

		%	33.82%	27.94%	25.00%	13.24%	100%
3	Power Fluctuation	Count	14	22	17	15	68
		%	20.59%	32.35%	25.00%	22.06%	100%
4	Malware attacks (malicious virus, worm, Trojan horses, spyware and adware)	Count	15	29	24	0	68
		%	22.06%	42.65%	35.29%	0.00%	100%
5	Denial of Service Attack	Count	5	3	3	57	68
		%	7.35%	4.41%	4.41%	83.82%	100%
6	Theft of Information	Count	5	9	23	31	68
		%	7.35%	13.24%	33.82%	45.59%	100%
7	Software Theft	Count	0	2	3	63	68
		%	0%	2.94%	4.41 %	92.65%	100%
8	Hardware Theft	Count	4	9	11	44	68
		%	5.88%	13.24%	16.18%	64.71%	100%
9	Sabotage	Count	10	15	18	25	68
		%	14.71%	22.06%	26.47%	36.76%	100%
10	Natural Disasters	Count	11	10	9	38	68
		%	16.18%	14.71%	13.24%	55.88%	100%

From above table it reveals that majority of the security threats are observed due to malware attacks and security threats are observed in all units but they differ in their intensity.

TABLE 2. STATUS OF SECURITY PRACTICES

Following table shows various security practices and their implementation status in sample units.

Sr.No	Security Practices	Fully	Partially	Not Implemented	Total Respondents (%)
1.	Access control Management	3 4.42%	16 23.53%	49 72.05%	68 100%
2.	Real Time Monitoring	0 0%	15 22.05%	53 77.94%	68 100%
3.	Physical security	30 44.11%	32 47.05%	6 8.82%	68 100%
4.	Encryption	0 0%	0 0%	68 100%	68 100%
5.	Authentication and authorization	7 10.29%	10 14.72%	51 74.99%	68 100%

6.	Employees Hiring policies	9 13.23%	12 17.65	47 69.12%	68 100%
7.	Back Up	50 73.53%	12 17.65%	6 8.82%	68 100%
8.	Auditing of information system	0 0%	8 11.77%	60 88.23%	68 100%

Above table reveals that in 4.42% sample units access control management security practice is fully adopted, in 23.53% sample units it is partially implemented and 72.05% sample units are not implemented access control management system.

Real time monitoring of IS security practice is partially implemented in 22.05% sample units partially whereas 74.94% sample units are lagging in this regard.

Maintaining the physical security of IT asset is an important part of information system security but in 44.11% sample units have provided full security to their physical assets by making locking system and hidden camera vigilance. 47.05% sample units partially implemented physical security measures whereas 8.82% sample units have not taken initiative for physical security.

Encryption system is not adopted by any unit to protect their data and software from misuse.

In 10.29% sample units authentication and authorization security practice is fully adopted, in 14.72% sample units it is partially adopted and in 74.99% sample units authentication and authorization security practice is not adopted.

Hiring new employees will have some risks. For reducing the risk the employee hiring policies are useful to increase the chances of finding more reliable employees. Therefore this hiring policies of employees are adopted in 13.23% sample units fully, in 17.65% sample units it is adopted partially and in 69.12% sample units it is not adopted.

Backup security practice is a common practice used by majority of the organizations. Therefore 73.53% sample units are adopted regular and systematic backup practice, 17.65% sample units are taking backup but systematic practice is not adopted and 8.82% sample units are lagging in adopting proper backup system.

Information system audit is conducted partially in 11.77% sample units and in 88.23% sample units have not gone for system audit.

From above interpretation it has been concluded that majority of the sample units are not serious about implementation of security practices.

TABLE 3 STATUS OF INFORMATION SYSTEM SECURITY AUDIT

Following table shows the status of information system security audit in sample units.

Sr.No.	Response	Number of Societies	Percentage
1	Yes	0	0
2	No	60	88.2
3	Upto some extent	8	11.80
	Total	68	100

(Source :Primary Data)

Above table reveals that 11.80% sample units are conducting system audit up to some extent whereas 88.2% sample units are lagging in this regard.

From above interpretation it has been concluded that no any sample unit conducts the IS audit as per standard guidelines.

TABLE 4 FREQUENCY OF IS AUDIT

Following table shows frequency of information system audit conducted in sample units

Sr.No.	Parameter	Once in a year	Once in 2 year	Arbitrarily	Never at all	Total
1	IS audit conducted	0	0	8	60	68
	Total	0	0	11.80%	88.2%	100%

(Source: Primary Data)

Above table reveals that 11.80% units are conducting system audit arbitrarily.

From above table & interpretation it has been concluded that cooperative credit societies under study are not serious about system audit even it is mandatory.

VI. FINDINGS

The status of information system security practices is analyzed for 68 selected units. It has been observed that no any sample unit has adopted information system for all functional areas.

1) All sample units are facing the problem of information system security threats but with different intensity.

2) Standard information system implementation practices are not following in all sample units.

3) All sample units have not done security risk analysis and also not adopted standard security practices.

4) Information system auditing is not done by majority of the units.

VII. CONCLUSION

There are various conclusions are drawn from findings. Cooperative credit societies are not serious about security threats arise in their units and their impacts on information system. They have to develop standard security practice for security of information system and design a standard security policy.

ACKNOWLEDGEMENT

I would like to acknowledge this research paper to my husband Mr. Ajit K. Patil and my research guide Dr. R. D. Kumbhar for their constant support and inspiration. It is the duty of the researchers to remember their parents whose blessings are always with them .Thank you.

References

1. Department of Co-operative(2007), "Report on 'As-Is' studies on IT usage & level of computerization and IT E-goverance Roadmap" , PricewaterhouseCoopers Private Limited
2. James D. Harris, Felix F. Dreher, Maeve L. Cummings (2005) ,"The CEO's View Of The Impact Of It Security Requirements Within Credit Unions", Journal of Information Technology Management, Volume XVI, Number 2.
3. Paul Jeffery Marshall(2010) ,"Online Banking: Information Security vs.Hackers Research Paper" , International Journal of Scientific & Engineering Research, Volume 1, Issue 1, October-2010
4. Angel Javier Salazar Alvarez (2004) ,"Challenges of information system implementation and organizational change management :Insights from health sector in Ecuador"
5. Valerie Abend, Brian Peretti, C Warren Axlerod, Andrew Bach(2008),'Cyber security for banking and finacial sector'.
6. Isabel Maria Lopes (University of Minho),"Information Security Policies: A Content Analysis".

Author(s) Profile

Ms. Manisha G. Patil, I have done MCA from Bharati Vidyapeeth Pune in 2011.I am now pursuing M.Phil from shivaji University, Kolhapur. Currently working as an Assistant Professor at Krishna Institute of Computer Application and Management, Wathar, Karad. My teaching experience is 4 years.

Dr. Rajendra D. Kumbhar, is woking as an Assistant Professor at Karmeveer Bhaurao Patil Institute of Management Studies and Research, Satara. He has 10 years teaching experience, he awarded with Ph.D.degree from Shivaji University Kolhapur in 2011. He also works as a research guide for Ph.D. as well as M.phil students of Shivaji University.He is member of DRC, worked on various BOS subcommittees, worked on LIC , scrutiny committee and selection committee of Shivaji University Kolhapur