"A STUDY OF INFORMATION TECHNOLOGY SECURITY IMPLEMENTATION AND USER AWARENESS IN URBAN COOPERATIVE BANKS "

Dr.RajeshreeKhande, Associate Professor
Singhad Institute of Management, Vadgaon (Bk)Pune, Maharashtra
rajeshree.khande@gmail.com

Dr. Y. S. Patil ,Associate Professor
Head, Center for Information Technology
Vaikunth Mehta National Institute of Cooperative Management, Pune
yspatil@vamnicom.gov.in

ABSTRACT

In today's competitive environment , banks and financial institutions operate in highly complex and interconnected environments with a critical responsibility of ensuring the privacy and security of their customers' information. Information assurance is certainly not taken seriously except few large size urban cooperative banks. Urban cooperative banks need to keep in step with technological advancements while maintaining protected and secured assets and information systems. The authors have undertaken the study of urban cooperative banks in Maharashtra, India. The study discusses the IT security requirements and its implementation by the urban cooperative banks and the awareness amongst users of the bank at various levels of management. The study is survey based and aims to throw light on the various steps taken by the bank for information technology security in order to protect their IT assets and also to assess the IT security awareness. The ultimate objective of the study is to see how the benefit of deploying IT security controls and level of risk varies from bank to bank.

Keywords : Information Security, Information system, Information Technology

I. Introduction : Urban cooperative banks (UCBs) and its role in development:

There are over 1,650 UCBs with close to 7,000 branches in the country. Yet they form a tiny part of the banking system accounting for less than 3% of the total banking assets and deposits and less than 3.5% of total advances. They also follow the 80-20 rule. The top 20% of UCBs accounts for almost 80% of its deposits.

In spite of being present in 25 states, much (almost 80%) of the action happens in the five states of Gujarat, Maharashtra, Andhra Pradesh, Karnataka and Tamil Nadu with the largest share going to Maharashtra. There are almost half of all UCB branches, around 60% of total extension counters of UCBs and more than 85% of all its automated teller machines (ATMs) are in Maharashtra. As a result more than 60%of the total banking business of the UCBs sector was concentrated in Maharashtra but their numbers have been decreasing in recent years. During 2000-2010, 132 banks licenses were cancelled and 62 merged with other banks. In this scenario, it is perhaps understandable why this sector does not exactly steal the limelight in banking policy.

As far as financial inclusion is concerned, ignoring the value of this sector would be a serious mistake. By their nature, UCBs in India can play a critical role in this area. They have traditionally played an important role in mobilizing resources from lower and middle-income groups and in providing direct finance to small entrepreneurs and traders. The UCBs, with their deep-rooted connections with specific communities, can easily inspire the trust of small savers and borrowers. By being local in nature and intricately interwoven with the local community, the UCBs have a clear advantage over commercial banks. It is easier for the UCBs to break the psychological barrier that proves prohibitive in the last mile of financial inclusion – create trust for the bank among its target community and bring customers within its fold. Today, when large commercial banks are working hard to set up branches and employing technology to reach out to thus far untouched regions of the country, it is time for the UCBs to step into the game that is naturally theirs.[1]

II. Role of technology in development of UCBs:

Technological innovation has not only enabled a broader reach for consumer banking and financial services, but has enhanced its capacity for continued and comprehensive growth. Banks and financial institutions rely on gathering, processing, analyzing information in order to improve its service and fulfill the expectation of customers. The visible benefits of IT in day-to-day banking in India are quite well known. The 'Anywhere Banking' is now possible as 'Anytime Banking' with the help of core banking system solution, through new, 24 by 7 by 365 days delivery channels such as Automated Teller Machines (ATMs), net banking and mobile banking etc. and are also becoming gradually more as an integral part of the services provided by the UCBs. In addition, IT has enabled for the efficient, accurate and timely management of the increased transaction volume that comes with a larger customer base.

Another important aspect with regard to technology implementation for internal purpose in UCBs is the Management Information System (MIS). The MIS reports generated help the top management as an effective risk management and a strategic decision making tool. Use of IT reduces the costs of financial transactions, improves the allocation of financial resource and increase the competitiveness and efficiency of banks.

The challenge now lies in taking greater advantage of new technologies and information-based systems and expanding the coverage of Indian banking and financial system to serve the potential market in rural and semi-urban areas. The use of Smart Card technology, ATMs, Electronic payments networks in remote areas could play significant role in providing financial services to people. The technology based solution would go a long way for achieving inclusive growth in India.

However, the expansion of such capabilities must be accompanied by a minimum level of information security features and continued compliance with established covenants and international standards relating to privacy of customers transaction in order to enhance the customer's confidence in the advanced technology based delivery channels like internet banking .mobile banking by controlling the fraudulent transactions.[2]

III. Need of Information Security for Urban Cooperative Banks

Today globally all types of businesses (large and small), are using information systems, networks, and Internet technology to conduct their business electronically, achieving new levels of efficiency and competitiveness. Information systems have both technical and behavioral perspectives. The growth of the rapid technology itself is responsible for the rising risks and threats. The cyber attacks can be represented by the relation among the threats, vulnerability and damage. A threat is an object, person, or other entity that represents a constant danger to an asset. Information Technology security is designed to protect the Confidentiality, Integrity and Availability of data from those with malicious intentions.

The purpose of information technology security is to ensure business continuity and reduce business damage by preventing and minimizing the impact of security incidents. An Information Security System enables information to be shared, as ensuring the protection of information and computing assets.

Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more striving and increasingly complicated. The internet exposes organizations to an increased threat if networks are accessed improperly, data corrupted and viruses introduced. Not all breaches are the result of crime; misuse and human errors play a role in damaging business. The virus infections are still the single most prevalent form of abuse. More common and just as destructive as crime, are threats like fire, system crashes, and power cuts. The poor supervision of staffs and lack of proper authorization procedures are the main causes of security incidents in all types of organisations line service or manufacturing.

According to RBI, complaints related to unauthorised fund transfers, fraudulent withdrawals from ATMs using duplicate cards, phishing e-mails aimed at extracting personal information have registered significant increase in recent times for all types of banks in the country.

IV. Need for Training and awareness of information Technology Security

The rationale of continuous security awareness training is to develop necessary competencies, new techniques and methods that are so important in facing possible security issues. The training and awareness programmes provide a great way to train employees and keep the organization information technology security policy in their brain. The idea behind training and awareness programmes is to motivate people to take information security seriously and respond accordingly. Any technological protection would be ineffective if the staff is not aware of information technology security and cyber security . A good security program is one where in everyone gets involved by staying updated with new technologies and understanding the common types of threats or attacks that are attached with these technologies that can affect banking business operations.

V. Background of the Study:

India is a home for large number of cooperative banks in general and urban cooperative banks in particular . The cooperatives, as economic enterprises and as self-help organizations, play a meaningful role in uplifting the socio-economic conditions of their members and their local communities. Over the years, cooperative enterprises have successfully operated locally-owned people-centered businesses.

Many of the cooperative banks and regional rural banks have gone for CORE Banking facility due to mandatory compliance imposed to deploy CBS by Reserve Bank of India (RBI) and National Bank for Agriculture and Rural Development Bank (NABARD for cooperative banks in the country . The cooperative banks in India are therefore deploying core banking solutions (CBS) and are introducing various payment channels in order to improve customer's services. While many UCB's have already deployed CBS, and some more are in the process of automation, they are often faced with issues of initial capital requirement.

As the technology is getting evolving new challenges faced by the banks are increasing and one of the major challenges is information security. If bank's customer's adopts the secure banking services of core banking, there are chances of relying on these services. Following types of risk must be minimized by cooperative banks to maintain the confidentiality, integrity and availability of data and information. Hence the cooperative banks role is to implement globally accepted information security standard to minimize the risk.

- **Regulatory risk:** As the Internet allows services to be provided from anywhere in the world, there is a threat that banks will try to avoid regulation and supervision.
- **Legal risk**: Online banking carries considerable legal risks for banks. Banks can potentially expand the geographical scope of their services faster through online banking than through traditional banking.
- **Operational risk:** The dependence on new technology to provide services makes security and system availability the central operational risk of core banking. The security threats can come from inside or outside of the system, so banking regulators and supervisors must ensure that banks have appropriate practices in place to guarantee the confidentiality of data, as well as the integrity of the system and the data
- **Reputational risk:** The breaches of security and disruptions to the system's availability can damage a bank's reputation. The more banks relies on electronic delivery channels, the greater the potential for reputational risks. The solution is customer's education- a process in which regulators and supervisors can assist.

  Information Technology security enables a financial institution to meet its business objectives by implementing business systems with due consideration of information technology (IT). The banks meet this goal by striving to accomplish the following objectives.

- **Availability** -For any information system to serve its purpose, the information must be available when it is needed. The high availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.
- **Integrity of data or systems** - Ensure that information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.
- **Confidentiality** - Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals.

The six major activities involved in information security are:

1. Policy development.
2. Specification of roles and responsibilities.
3. Designing and developing a security control framework.
4. Implementing a solution.
5. Monitoring and awareness.
6. Training and education

VI. Research Methodology:

a. Objective of the Study

The main objective of the study is to evaluate information technology security implementation in core banking environment of urban cooperative banks in Pune and Mumbai cities. This study is carried out to understand present status of information technology security implementation of urban cooperative banks (UCBs) and the training and awareness amongst the employees. This study aims to achieve objective viz.,

1. To study the training and awareness of information security amongst the end users of UCB's.

b. Hypothesis of study

1. End users of UCB's have positive attitude towards training and awareness program conducted by UCB's.

2. The password security awareness at all level of management is high in all UCBs under study

c. Scope of the Study

The present study focuses on information security system in CBS environment of selected urban cooperative banks in Pune and Mumbai cities. The present study is conducted for UCBs who have implemented core banking solution.

d. Primary Data

The primary data is collected from 18 urban cooperative bank’s management members, Information Security Officer (IT heads), and employees by a structured questionnaire. The researcher has also interviewed the Heads of the IT department of the respective urban cooperative banks in Pune and Mumbai cities.

e. Sampling Design And Sample Size

The simple random sampling has been used for selection of target population. There are total 46 urban cooperative banks in Pune and Mumbai cities who have implemented core banking solution as on March 2014. The probability sampling method is used for the selection of individuals from the population so that they are representative of the population. The universe of the study is urban cooperative banks and the researcher has selected 18 (40%) UCB’s out of 46 urban cooperative banks from Pune and Mumbai cities using simple random sampling method as shown in Table No. 1.0. The random sampling is a scientific and most important method among all types of sampling methods. It is simplest possible sampling method and it is most appropriate when the population is more or less homogeneous with respect to the characteristics under study.

Table No. 1.0: Selection of Sample

Population: Total Number Of UCB in Pune and Mumbai Cities implemented CBS	Sample : Number of selected UCB for the Study	% of Population Sample	Sampling Technique
46	18	40%	Probability simple random sampling

VII. Data analysis and interpretation of present status of Information Technology Security Training and awareness level of Urban Cooperative Banks

The data analysis for the present study was done quantitatively with the help of both descriptive statistics and inferential statistics. The statistical techniques adopted are frequency, means and standard deviation, percentage, Pearson's Correlation. The SPSS 16.0, statistical software, has been used to conduct various statistical analysis. The results obtained thereby are presented and interpreted.

The objective of this analysis is to evaluate the level of information Technology Security awareness in the urban cooperative banks to preserve confidentiality, integrity and availability of the bank's data.

1. Assessment of the training and awareness program on information security amongst the end users (Employees) :

As per Reserve Bank of India guidelines urban cooperative banks should provide the periodic training in computer and information security awareness and accepted information security practices for all employees who are involved with the management, use, or operation of a urban cooperative banks information system. The data was collected by self administrated questionnaire from end users (employees) by survey method to assess the training programmes based on questions like

- Do the management conduct training programmes?
- Which topics of information security are included as part of training programmes?
- Did the training programmes gives better idea of importance of computer and information security?

- Does they are satisfied with the training programmes organized by the bank?

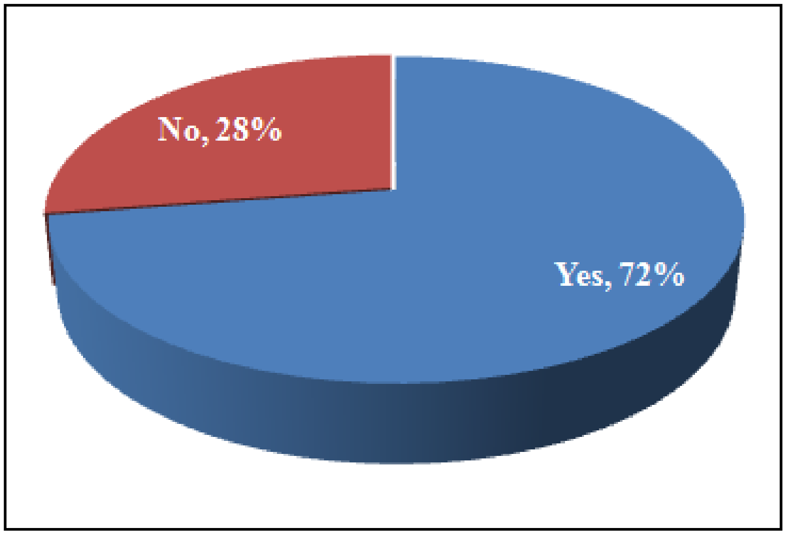
1. **Conduct of Awareness Training Programmes on IT Security**

The respondents views are recorded for above defined questionnaire for awareness programmes on information security and the respondents views are summarized as below in Table No. 1.1

Table No. 1.1 : Percentage of UCB's for conduct of Awareness Training programmes on Information Security

Management conducts awareness training programmes	No. of Respondents	Percentage (%)
Yes	342	72.5%
No	130	27.5%
Total	472	100%

As indicated in the Table No. 1.1 and Graph No. 1.0, 72.5% respondents indicated that management conducts awareness training programmes on information security. However, 27.5% stated that their management does not conduct awareness training programmes on information security.



Graph No 1.0 : Percentage of UCB's for conduct of Training programmes

Therefore, it is observed that most of the respondents agreed upon that management of the bank conducts training programmes on information security to reduce the operational and technical risk in CBS environment.

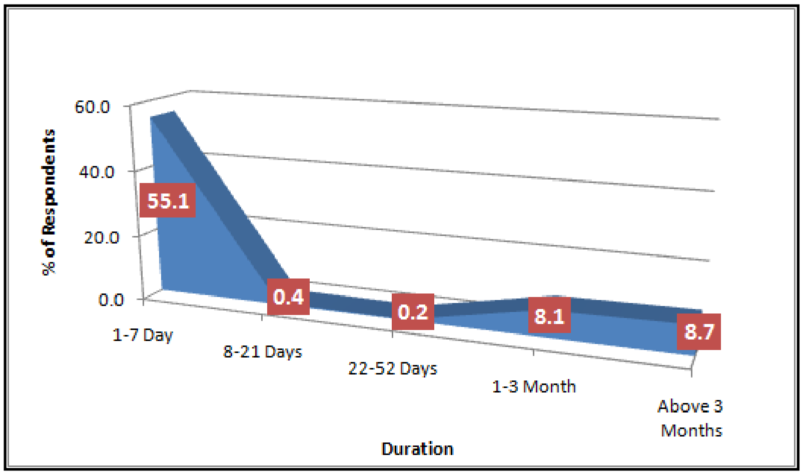
2. **Duration of training programmes :**

The respondents views are recorded for duration of training and awareness programmes on information security through self administrated questionnaire and the respondents views are summarized as below in Table No. 1.2

Table No. 1.2: Training program duration wise percentile of respondents

Duration	**No. of Respondents**	**Percentage (%)**
1-7 Days	260	55.1%
8-21 Days	2	0.4%
22-52 Days	1	0.2%
1-3 Months	38	8.1%
Above 3 Months	41	8.7%
Total	342	100%

On assessing the frequency of duration of training and training program on awareness on information security , 55.1% respondents stated that the training programmes duration is one to seven days, while 0.4% respondents stated that it is between 8 to 21 days. Furthermore 8.1% of the respondents stated that duration of such programmes organized by bank are above 3 months. Moreover a similar percentage 8.7% is supported for 1 to 3 months duration of training programmes. Only one respondent stated that the training program is of 22 to 52 days as indicated in Table No. 1.2 and Graph No. 1.1



Graph No. 1.1: Training program duration wise percentile of respondents

3. Topics included as a part of awareness and training program:

The following were indicated by bank employees (End User) as topics included for training programmes ;

- IS policies/procedures
- Usage of IT assets
- Standards relating to passwords and authentication, Physical protection
- Safe handling of sensitive data/information
- Network Security and Reporting of any security incidents

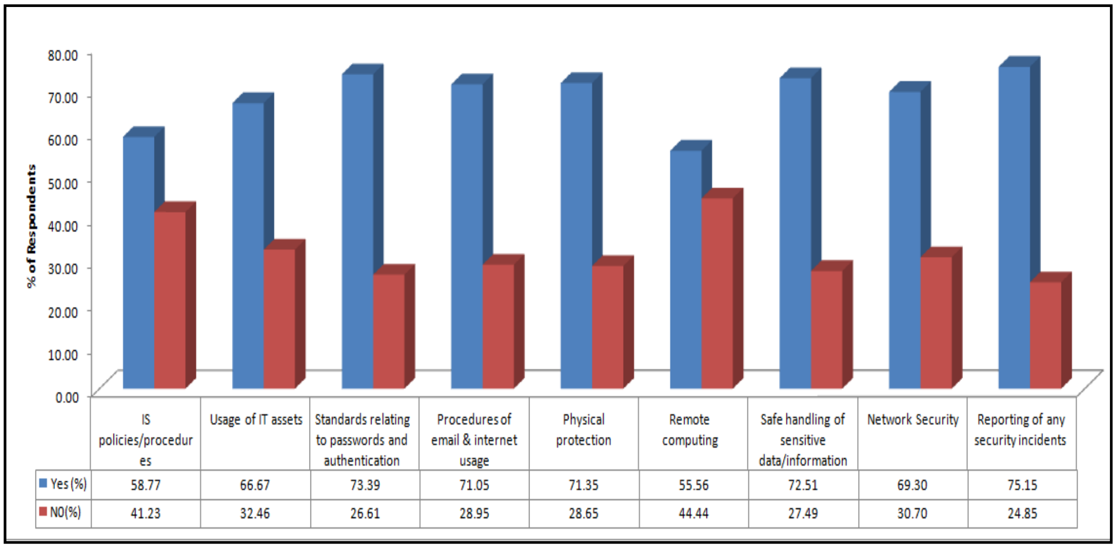
A compilation of responses from end users of bank is shown in Table No. 1.3 and Graph No.1.2

Table No. 1.3 : Training programmes on Awareness - Topic wise percentile of respondents

Sr. No	**Topic Included in Training Programmes**	**Response**	**Yes**	**No**	**Total**
1	IS policies/procedures	R (Count)	201	141	342
		%	58.77%	41.23%	100%
2	Usage of IT assets	R (Count)	228	115	342
		%	66.67%	32.46%	100%
3	Standards relating to passwords and	R (Count)	251	91	342
		%	73.39%	26.61%	100%

	authentication				
4	Procedures of email & internet usage	R (Count)	243	99	342
		%	71.05%	28.95%	100%
5	Physical protection	R (Count)	244	98	342
		%	71.35%	28.65%	100%
6	Remote computing	R (Count)	190	152	342
		%	55.56%	44.44%	100%
7	Safe handling of sensitive data/information	R (Count)	248	94	342
		R%	72.51%	27.49%	100
8	Network Security	R (Count)	237	105	342
		%	69.30%	30.70%	100%
9	Reporting of any security incidents	R (Count)	257	85	342
		%	75.15%	24.85%	100%

According to 58.77% of the respondents policies/procedures included as part of training program, while 66.67% of the respondents stated usage of IT assets. Furthermore 73.39% of the respondents indicated that training and awareness program also i the standards relating to passwords and authentication. 71.05% respondents stated that Procedures of email & internet usage is also a part of training program, while 71.35% of the respondents indicated Physical protection. Furthermore 55.56% of the respondents revealed that training programmes also focuses on remote computing, likewise 72.51% of the respondents indicated Safe handling of sensitive data/information. 69.30% of the respondents rated for Network security and 75.15% respondents stated that training is also imparted on how to report on occurred security incidents .



Graph No. 1.2: Awareness and Training Program topic wise percentile of respondents

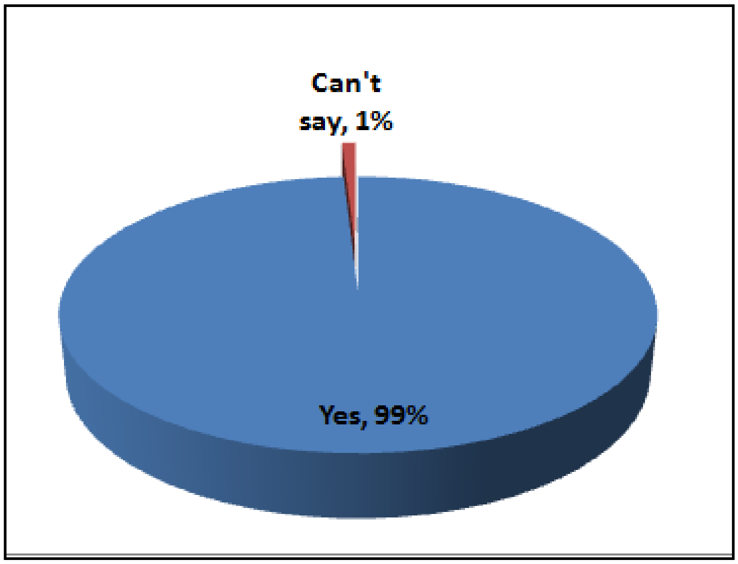
4. Training gives better ides of information security:

The respondents were requested through questionnaires to clarify that whether the training and awareness program provides better idea on information security? The findings are as summarized in below Table No. 1.4

Table No. 1.4 : Percentile of respondents for Training gives better ides of information security

Training gives better ides of information security	No. of Respondents	Percentage (%)
Yes	339	99.12%
No	0	0%
Can't say	3	0.88%
Total	342	100%

From the Table No. 1.4 and Graph No 1.3, it has been observed that, 99.12% respondents stated that the training programmes imparted enables for better idea of information security, while 0.88% respondents responded negatively.



Graph No 1.3:

Statics of respondents for training enables for better ides of information security

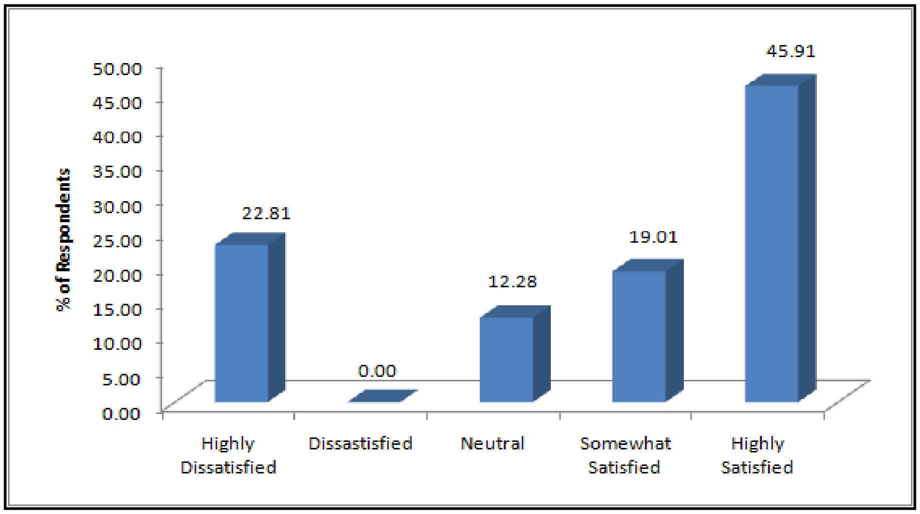
5. **Satisfaction level about the training programmes on information security :**

The respondents views are recorded for satisfaction level of training and awareness program on information security through self administrated questionnaire and the respondents feedback is summarized as below in Table No. 1.5

Table No. 1.5: Satisfaction level wise percentile of Respondents for Training programmes

Satisfaction Level	**No. of respondents**	**Percentage (%)**
Highly Dissatisfied	78	22.80%
Somewhat Dissatisfied	0	0.00%
Neutral	42	12.28%
Somewhat Satisfied	65	19.00%
Highly Satisfied	157	45.91%
Total	342	100%

When the respondents were requested to judge their satisfaction level for the training and awareness programmes on Information security, 45.91% of the respondents rated that they were highly satisfied. As shown in Table No.1.5 and Graph No. 1.4 22.80% of the respondents stated that they are highly dissatisfied with training programmes , 19% of the respondents stated that they were somewhat satisfied, 12.28% were neutral in their feedback. The result shows that respondents were generally satisfied with training programmes as the percentage is high.



Graph No 1.4: Satisfaction level wise percentile of respondents for training programmes

6. Awareness about password security:

To study the respondent's awareness on Password Security , the primary data was collected using five point Likert scale method. The collected data was presented in following Table No. 5.60. (SD: Strongly Disagree, D: Disagree, N: Neutral A: Agree, SA: Strongly Agree)

Table No. 1.6: Password security wise percentile of respondents

Sr. No	**Password Security**	**Response**	**SD**	**D**	**N**	**A**	**SA**
1	Password protects System, service or programs	R (Count)	5	0	27	144	296
		%	1.1%	0%	5.7%	30.5 %	62.7 %

		R%	1.1%		5.7%	93.2%	
2	Longer password is more secure	R (Count)	6	35	49	159	223
		%	1.3%	7.4%	10.4%	33.7%	47.2%
		R%	8.7%		10.4%	80.9%	
3	Use a combination of uppercase, lowercase letters, including special characters difficult to crack the password	R (Count)	105	21	28	86	232
		%	22.2%	4.4%	5.9%	18.2%	49.2%
		R%	26.6%		5.9%	67.4%	
4	Change password regularly, then chances of password being cracked is less.	R (Count)	109	8	5	149	201
		%	23.1%	1.7%	1.1%	31.6%	42.6%
		R%	24.8%		1.1%	74.2%	
5	Hacker will take a very long time to crack a long, complex password.	R (Count)	76	21	60	132	183
		%	16.1%	4.4%	12.7%	28%	38.8%
		R%	20.5%		12.7%	66.8%	
6	Never record your password anywhere	R (Count)	90	3	2	127	250
		%	19.1%	0.6%	0.4%	26.9%	53%
		R%	19.7%		0.4%	79.9%	
7	Never open attachments sent by a stranger.	R (Count)	115	52	41	143	121
		%	24.4	11%	8.7%	30.3	25.6

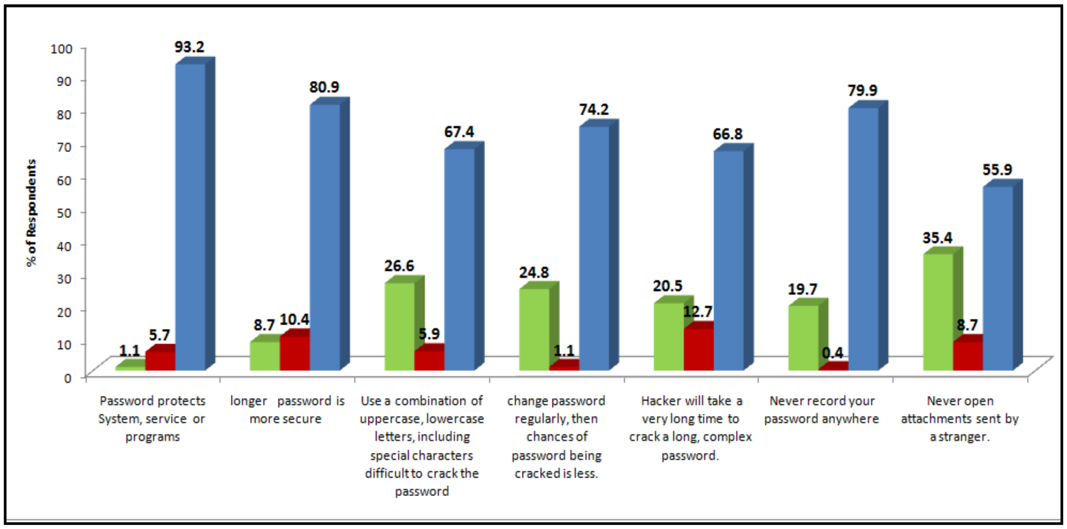
			%			%	%
		R%	35.4%		8.7%	55.9%	

The statistical findings from the Table No. 1.6 shown that majority of the respondents 93.3% stated that password protects system, service or programs, while very few respondents 1.1% do not agreed with the statement and 5.7% of the respondents were neutral . Furthermore, 80.9% respondents stated that longer password is more secure, while 8.7% of the respondents stated that they do not agree with this statement and 10.4% of the respondents were neutral.

On the other hand , 66.4% of the respondents reported they are aware on the use of combination of uppercase, lowercase letters, including special characters difficult to crack the password, at the same time 26.6% of the respondents are not aware of such password security guidelines. According to 74.2% of the respondents, password should procedure should be followed regularly so that a chance of password being cracked is less, while 24.8% of the respondents did not agree with this statement of password security. At the same time 12.7% of the respondents were neutral on the same.

On password security awareness, 68.8% of the respondents agreed that hacker will take a very long time to crack a long, complex password, while 20.5% respondents did not agree. At the same time 12.7% of the respondents were neutral. 79.9% of the respondents agreed that never record your password anywhere so that unauthorized access is prevented, while 19.7% of the respondents did not agree and 0.4% respondents were neutral .

In addition, 55.9% of the respondents agreed for the statement never open attachments sent by a stranger, at the same time 35.4% of the respondents said they did not agree with this statement and 8.7% of the respondents were neutral in their response. The Graph 5.62 shows the pictorial representation of the same statistical findings.



Graph No. 1.5: Password security wise percentile of respondents

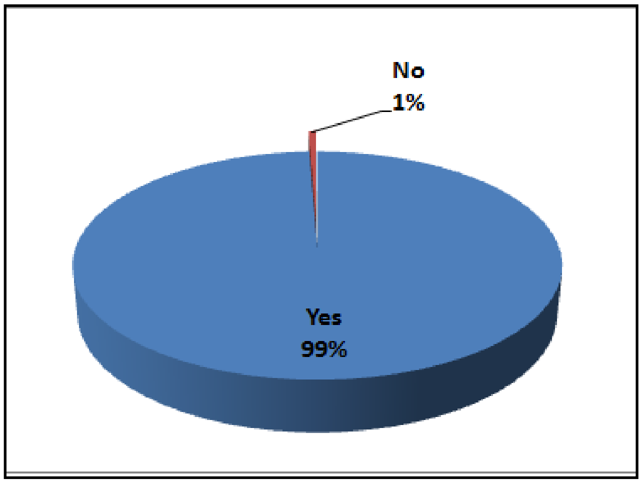
7. Regular password updation:

The respondents were requested whether they change the password on regular interval and the details obtained are as summarized in below Table No. 1.7

Table No. 1.7: Percentage of respondents for regular password updation

Updating of Password	No. of Respondents	Percentage (%)
Yes	469	99.4%
No	3	0.6%
Total	472	100%

From the Table No. 1.7 and Graph No 1.6, it has been observed that, 99.4% respondents stated that they change their password regularly, while 0.60% respondents stated negative response.



Graph No 1.6: Percentage of respondents for regular password updation

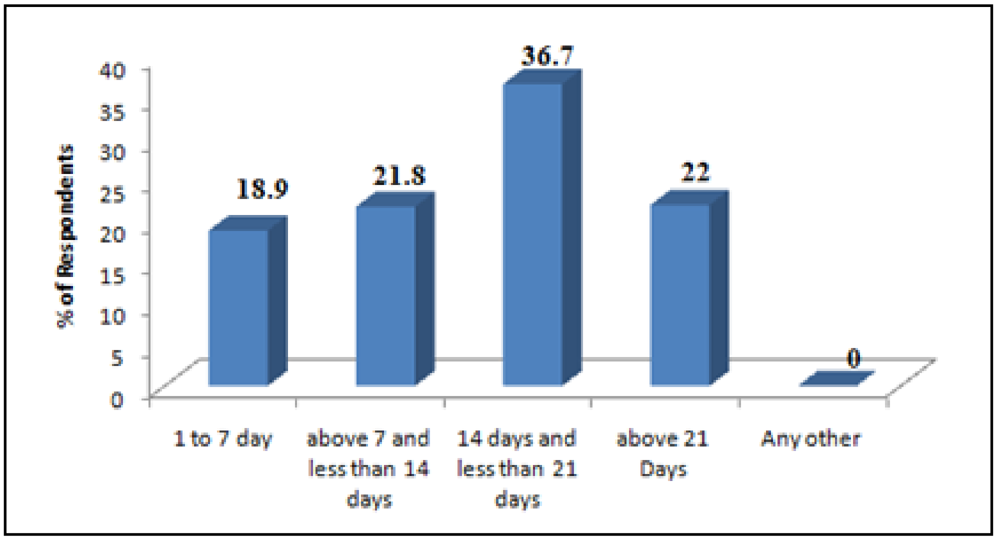
8. Duration of Password updation:

The respondents were requested to response the duration of password updation and the details obtained are as summarized in below Table No. 1.8

Table No. 1.8: Password updation duration wise percentile of respondents

Duration of Password Updation	No. of Respondents	Percentage (%)
1 to 7 days	89	18.9%
above 7 and less than 14 days	103	21.8%
14 days and less than 21 days	173	36.7%
above 21 Days	104	22%
Any other	0	0%
Total	469	100%

On assessing the frequency of duration for password updation, 36.7% of the respondents indicated that they update their password between 14 to 21days, whilst 22% between 7 to 14 days. Similar percentage of the respondents said that they change password above 21 days. However about 19% of the respondents indicated that they change their password between 1 to 7 days as indicated in Table No. 1.8 and Graph No 1.7



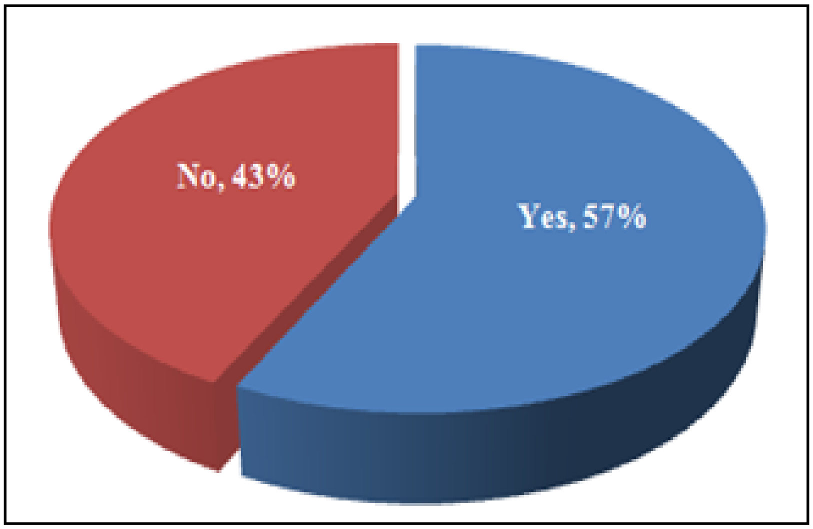
Graph No 1.7: Password updation duration wise percentile of respondents

Furthermore the respondents were asked whether frequent changes in password will be difficult to recall or remember and details obtained are summarized as in below Table No. 5.63**.**

Table No. 1.9: Percentage of respondents for frequent changes in password difficult to recall

Changes in password difficult to recall	**No. of Respondents**	**Percentage (%)**
Yes	269	57.35%
No	200	42.64%
Total	469	100%

From the Table No. 1.9 and Graph No 1.8, it has been observed that almost for 43% respondents it is difficult to remember the password if changed regularly, while 57% of the respondents indicated that they do not face such problem.



Graph No. 1.8: Percentage of respondents for frequent changes in password difficult to recall

9. **Awareness about Physical and logical Security:**

Table No. 1.10: Physical and Application Security awareness wise percentile of respondents

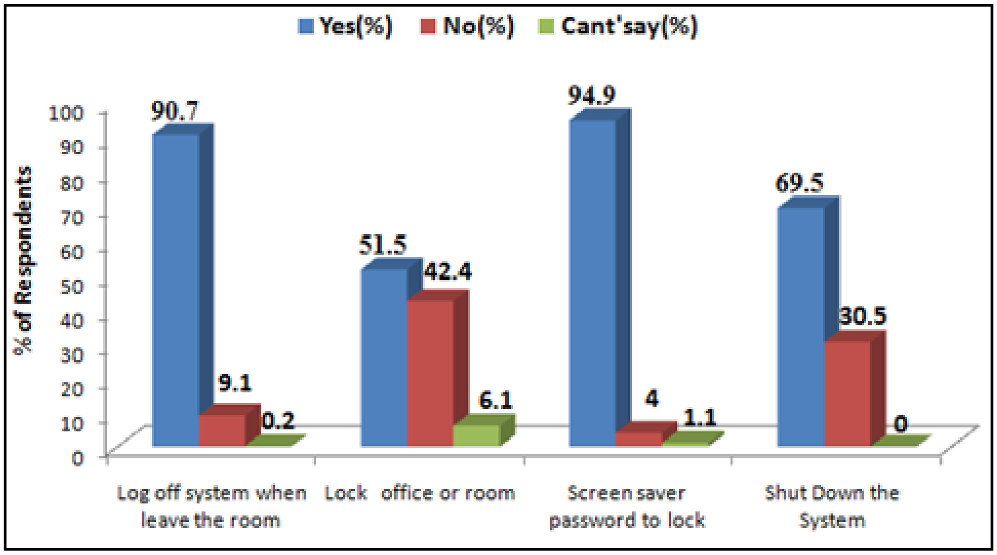
Sr. No	**Physical and Application Security awareness**	**Response**	**Yes**	**No**	**Can't Say**	**Total**
1	Log off system when leave the room	R (Count)	428	43	1	472
		%	90.7%	9.1%	0.2%	100%
2	Lock office or room	R (Count)	243	200	29	472
		%	51.5%	42.4%	6.1%	100%
3	Screen saver password to lock	R (Count)	448	19	5	472
		%	94.9%	4%	1.1%	100%
4	Shut Down the System	R (Count)	328	144	0	472
		%	69.5%	30.5%	0%	100%

From the Table No. 1.10 and Graph No 1.9 it is revealed that the 90.7% of the respondents stated that they log off the system when they leave the room or terminal, while only 9.1% of the respondents reported that they do not follow such security measures and 0.2% respondents were unable to respond.

Furthermore 51.5% of the respondents said that they lock the office or room when they leave the terminal. At the same time 42.4% of the respondents said that they do not lock the room or office and very few respondents 6.1% not able to respond.

On the other hand, 94.9% respondents stated that each computer was provided with a screen saver locked with a password.

According to 69.5% of the respondents, they shut down the system while they were not around or not using the CBS solution, and 35.5% of the respondents recorded that they do not shut down the system.



Graph No 1.9: Physical and Application Security awareness wise percentile of respondents

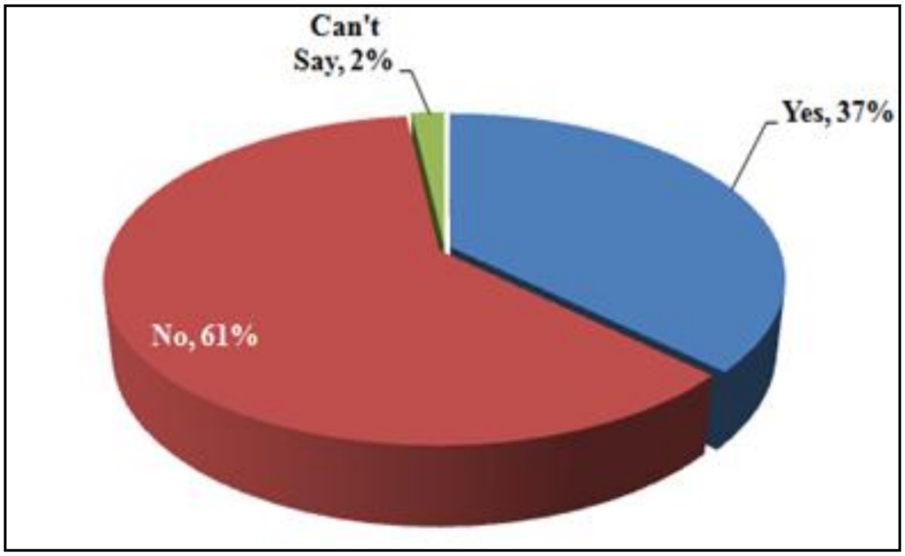
10. Access to transfer the CBS system data to external storage devices (like pen drive, CD etc)?

To assess the authorized access or copying of data respondents were requested to clarify whether they have access to transfer the data in external storage device like pen drive or CD and details of which are as summarized in Table No. 1.11.

Table No. 1.11: Respondents percentage for transferring data to external storage device

Access to transfer the CBS system data in external storage devices	No. of Respondents	Percentage (%)
Yes	175	37.1%
No	288	61%
Can't Say	9	1.9%
Total	472	100%

From the Table No. 1.11 and Graph No 1.10, it was observed that 61% respondents stated that they do not have access to transfer the data to external storage device; while 37.1% of the respondents stated that they have access to transfer data to external storage device and 1.9% of the respondents were unable to answer.



Graph No. 1.10: Respondents percentage for transferring data to external storage device

VIII. Testing Of Hypothesis

Testing Of Hypothesis 1:

The first hypothesis of the study is **"End users of UCB's have positive attitude towards training and awareness program conducted by UCB."**

H0 Null Hypothesis: 73% or more employees (End Users) have positive attitude towards training and awareness program conducted by UCBs. (H0: p=0.73)

H1 Alternate Hypothesis: < 73% employees (End Users) do not have positive attitude towards training and awareness program conducted by UCBs**.** (H1 <0.73)

This hypothesis has been tested by using the training and awareness program organized by UCB's on information security for employee using percentage. It has been observed from the statistical analysis that the majority of the respondents i.e. 72.5 percent are positive attitude towards training programmes organized by UCBs (Table No. 5.55).

As the sample sizes is >= 30, normal approximations is satisfied. In this case to test the hypothesis parametric Z-test is used at 5% level of significance.

Respondents: End Users(Employees)			
Sample Size (N)	**Proportion of responses Yes**	**Std. Error**	**Z-statistics**
472	**0.725**	**2.043489**	**0.2446796**

Table value of Z for one tail test at 5% level of significance is 1.64. Calculated value of Z(0.24) is less than the table value of z-statistics i.e. Zcal (0.24) < Ztable(1.64), hence accept H0 which means more than 73 percent respondents have a positive attitude towards Management conducts training programmes on information security. Hence hypothesis of the study "End users of UCB's have positive attitude towards training and awareness program conducted by UCB" is accepted.

Testing of Hypothesis 2:

The second hypothesis of the study **"The password security awareness at all levels of management is high in UCBs."**

H0 Null Hypothesis: The password security awareness at all level of management is low in UCBs.

H1 Alternate Hypothesis: The password security awareness at all levels of management is high in UCBs.

As sample size is large , the chi-square Goodness of fit (One Sample Test) was used to test Hypothesis. This hypothesis has been tested by using Chi-square for password security awareness at all levels of management .The Password security awareness is tested by checking the knowledge of end users regarding the password security standards, practices and guidelines. The frequency analysis of the same is shown in Table No. 1.12. The chi square calculation for the same is shown as below

oi	**ei**	**(oi-ei)**	**$(oi-ei)^2$**	**$(oi-ei)^2/oi$**
440	349.43	90.57	8203.18	23.476
382	349.43	32.57	1060.9	3.036
318	349.43	-31.43	987.76	2.827
350	349.43	0.57	0.33	0.001
315	349.43	-34.43	1185.33	3.392
377	349.43	27.57	760.18	2.175
264	349.43	-85.43	7298.04	20.886
32	122.57	-90.57	8203.18	66.926
90	122.57	-32.57	1060.9	8.655
154	122.57	31.43	987.76	8.059
122	122.57	-0.57	0.33	0.003
157	122.57	34.43	1185.33	9.671
95	122.57	-27.57	760.18	6.202
208	122.57	85.43	7298.04	59.542
			$\sum\chi^2$ =	**214.851**

At the 5% level of significance , calculated value of χ^2 (214.851) is greater than Table value of Chi-square (12.592) i.e. χ^2cal (214.851) < χ^2tab (12.592), hence Null hypothesis is rejected and alternative hypothesis is accepted. This means that the password security awareness at all levels of management is high in UCBs.

Hence hypothesis of the study is accepted.

IX. Conclusion and Suggestions

The findings of the study reveals that the respondents were satisfied with training programmes organised by UCBs as the percentage of respondents is high. It is also observed that most of the important topics related to information security are covered as a part of Information security awareness training programmes. Though the study reveals positive results ,the usage of CBS for managerial and top level is very low and users at these levels need to understand the derived benefits of the CBS software solution and increase the utilization of the software for managerial and strategic decisions at middle and top levels of management by interfacing dashboard for routine decisions and also for policy decisions. On deployment of such interface ,the information security needs to be assessed for these levels by administrating questionnaire.

Bibliography

1. http://www.rbi.org.in/scripts/PublicationsView.aspx
2. http://rbidocs.rbi.org.in/rdocs/Bulletin/PDFs/
3. Internet Banking in India – Guidelines, June 14, 2001
4. Information systems audit policy for the banking and financial sector, Working group for information systems security for the banking and financial sector Department of Information Technology, Reserve Bank Of India, Mumbai, October, 2001
5. Report of Working Group on IT Support for Urban Cooperative Banks, Reserve Bank Of India, December 19, 2007.
6. Genesis And Architecture Of Urban Cooperative Banks, Reserve Bank Of India, Mumbai, August 2008
7. Report On Information Security, Electronic Banking, Technology Risk Management And Cyber Frauds, Reserve Bank Of India, Mumbai, January 2011
8. Report Of The High Level Committee For Preparation Of The Information Technology Vision Document 2011-2017, Reserve Bank Of India, Mumbai, 2011
9. ISO/IEC 27001(ISO 27001): Series of Standard for implementing and maintaining information security program(ISMS) available on http://www.iso.org & http://en.wikipedia.org/wiki/ISO/IEC_27001:2005
10. An Introduction to the Business Model for Information Security, ISACA, 2009
11. An Overview Of Information Security Standards, The Government Of The Hong Kong Special Administrative Region, February 2008
12. Ashutosh Saxena, V. P. Gulat (2007), Framework of IT Security Policy, IDRBT’s, Institute for Development and Research in Banking Technology (Established by Reserve Bank of India), Working Paper No. 7

13. B. Munirajasekhar and B Sudheer (2013), Core Banking Solutions in Urban Cooperative Banks- Issues and Challenges, B Munirajasekhar et al./ Elixir Fin. Mgmt. 55 (2013) 12820-12824
14. Deepshikha Jamwal & Devanand Padha (2009), Internet Banking Systems in India: Analysis of Security Issues, Proceedings of the 3rd National Conference; INDIACom-2009 Computing For Nation Development, Bharati Vidyapeeth‟s Institute of Computer Applications and Management, New Delhi, February 26 – 27, 2009
15. Diwakar H., Naik A.(2008), Investigation of Information Security Management Practices in Indian Pubic Sector Banks, IEEE 8th International Conference, Page(s): 276 – 281, E-ISBN : 978-0-7695-3239-1 Print ISBN: 978-0-7695-3242-4, July 2008.
16. Dr. K. C. Chakrabarty (2013), Frauds in the Banking Sector: Causes, Concerns and Cures Inaugural address, Deputy Governor, Reserve Bank of India on July 26th 2013 during the National Conference on Financial Fraud organized by ASSOCHAM at New Delhi
17. Dr. S. S. Satchidananda, Sanat Rao, Rahul Wadhavkar(2013) , Core Banking Solutions: An Assessment, International Institute of Information Technology – Bangalore, CBIT-CBIT Centre of Banking and Information Technology, IIITB- International Institute of Information Technology Working Paper WP-2006-8, June 2013
18. Hiltgen A.(2006), Secure Internet banking authentication, Security & Privacy, IEEE, Volume:4, Issue:2, Pages: 21-29, ISSN : 1540-7993, April 2006
19. Hisamatsu A., Pishva D., Nishantha G.G.D.(2010), Online banking and modern approaches toward its enhanced security, Advanced Communication Technology (ICACT), 2010, The 12th International Conference , IEEE, Volume:2, Page(s):1459 – 1463, ISSN :1738-9445, ISBN:978-1-4244-5427-3
20. Julie J. C H. Ryan (2001), Information Security Practices and Experiences in Small Businesses, Center for Information Policy Research, Harvard University, ISBN 1-879716-75-5 I-01-2, 2001
21. Michael Kimwele, Waweru Mwangi, Stephen Kimani (2010), Adoption Of Information Technology Security Policies: Case Study Of Kenyan Small And Medium Enterprises (SMES), Journal of Theoretical and Applied Information Technology, 2010