International Journal of Cyber Criminology
Vol 7 Issue 1 January - June 2013

Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector

Atul Bamrara[1]
HNB Garhwal University, India

Gajendra Singh[2]
Doon University, India

Mamta Bhatt[3]
HNB Garhwal University, India

Abstract

Organizations cannot sustain without communication networks linking the vast sources of information spread all over the globe and information technology experts are struggling to design the high performance hardware and software which can cater the needs of today's' hi tech firms. The potential threat to secure enormous volume of data with a varied community of cyber criminals is a challenge in the current digital era. The present study is an attempt to reveal the varied cyber attack strategies adopted by cyber criminals to target the selected banks in India where spoofing, brute force attack, buffer overflow and cross side scripting are found positively correlated with public and private sector banks. Further, the findings show a positive correlation between Intruder Detection and cyber attacks, i.e., online identify theft, hacking, malicious code, DOS attack and credit card/ATM frauds as well as online identify theft, DOS attack & credit card/ ATM fraud are found positively correlated with System Monitoring.

Keywords: Cyber criminals, Banking sector, PHP remote file inclusion, Cross site scripting, Brute force attack, SQL injection vulnerability, Buffer overflow.

Introduction

Cyber crime is emerging as a challenge for national and economic security. Many industries, institutions and public and private sector organizations (particularly those within the critical infrastructure) are at significant risk. Comparatively some organizations have

[1]Assistant Professor and Head, Department of Management Studies, BFIT Technical Campus, HNB Garhwal University (A Central University), Srinagar Garhwal, Uttarakhand-246174, India. E-Mail: atulbamrara@gmail.com
[2]Associate Professor and Head, School of Management, Doon University, Uttarakhand-248001, India.
[3]Assistant Professor, School of Commerce, HNB Garhwal University (A Central University), Srinagar Garhwal, Uttarakhand-246174, India.

identified organized cyber criminal networks as its most potential cyber security threat and some are ready to defend such security threats.

The complexity of modern enterprises, their reliance on technology and the heightened interconnectivity among organizations have created widespread opportunities for theft, fraud and other forms of exploitation by offenders both outside and inside an organization. With the growth of e-business, internal and external perpetrators can exploit traditional vulnerabilities in seconds. They can also take advantage of new weaknesses in the software and hardware architectures that now form the backbone of most organizations (KPMG, 2000, p. 2). In a networked environment, such crimes can be committed on a global basis from almost any location in the world, and they can significantly affect an organization's overall work culture. Network and computer attacks have become common issues in today's world (KPMG, 2000, p. 2). Any computer connected online is under threat from viruses, worms and attacks from hackers. Public users as well as business users are attacked on a regular basis. As organizations develop and refine their e-business strategies, they need to consider the issues that influence the Confidentiality, Integrity and Availability of their data. In this context, they need to know how they can be affected by the new risks of e-crime and how inadequate preparation could leave them open to an attack that could easily degrade the value of their businesses. Thus, the need to fight computer and network challenges in form of cyber attacks is becoming gradually more essential for security professionals (Hansman & Hunt, 2005, p. 32).

Electronic banking, with its inherent advantages for the banking industry as well as the customer, is an area with tremendous growth potential. This field has also seen a corresponding rise in network security breaches, data thefts, data losses, identity thefts and other white collar crimes resulting in huge losses to the banking industry. Losses by the banking industry worldwide due to white collar crimes are in huge amounts and far outstrip conventional methods of bank robbery. The exponential speed at which internet banking has evolved, the ubiquitous and global nature of open networks and the overwhelming reliance on IT has all added up to provide a platform for enhanced security challenges. Amendments in the IT act, banking regulations and the various wireless networking issues that need to be taken into account by the industry.

When a bank's system is connected to the internet or intranet, an attack could originate anytime, anywhere. Some essential level of security must be established before business on the internet can be reliably conducted. An attack might be in the form of unauthorized access, destruction, corruption or alteration of data or any type of malicious procedure to cause network failure, reboot or hang. Modern security techniques have made cracking very tedious but not impossible. Furthermore, if the system is not configured properly or the updated patches are not installed then hackers may crack the system using security hole. A wide array of information regarding security hole and their fixes is freely available on the web.

Hertzum et al. (2004) analyzed six Danish web-based electronic banking systems which indicated that the systems have serious weaknesses with respect to ease of use which suggested that security requirements are among their causes and the weaknesses might result in low level security (p. 52). They viewed the conflict between ease of use and security in the context of usable security, a concept that is intended to match security principles and demands against user knowledge and motivation. Rudasill and Moyer (2004) reviewed the possible cyber-security threats to today's military and civilian

populations. The study alerted the organizations to possible compromise in the systems with which they work, and provided some understanding of the process by which the government was reacting to threats (p. 248). Web Services are growing at a rapid rate and new security issues are evolving in web security.

Hansman and Hunt's (2005) proposed taxonomy consisted of four dimensions which provided a holistic taxonomy in order to deal with inherent problems in the computer and network attack field (p. 32). One covers the attack vector and the main behaviour that how attacks happen. Second classifies the attack targets. Third dimension focuses on taxonomy of vulnerabilities, where fourth dimension deals with payloads. Various cases of thefts were caused by companies' inability to determine risks associated with the protection of their data and these companies lack of planning to properly manage a security breach when it occurs (Polstra III, 2005, p. 135). The study further revealed that organizations need to realize that the theft of information is a management issue as well as a technology one, and most of security breach incidents caused by managerial decisions and not by technology implementations.

Wueest (2005) studied that malicious applications employ two kinds of attack vector – local attacks which occur on the local computer, and remote attacks, which redirect the victim to a remote site (p. 4). Some attacks may be foiled by adopting security measures such as transaction numbers (TAN) and public key infrastructure (PKI) methods. A description of attack scenarios over a two-year period illustrated several key security issues with Internet banking systems in Norway (Hole et al., 2006, p. 14). 29% of the attack methods target web servers and are not directly applicable to distributed agent technology. These methods are directory traversal, PHP remote file inclusion, cross-site scripting, SQL injection, and web cache poisoning. Of the remaining methods, three emerged as most likely to affect agent-based control of power distribution: crafted input, buffer overflow, and direct access to restricted resources (Simmons et al., 2006, p. 184). Crafted input and buffer overflow accounted for 24% of the attack methods and direct access to restricted resources contributed almost 10%.

Kjaerland (2006) analyzed the data from CERT/CC of 838 attacks towards the commercial sector and 559 attacks towards the government sector, for a total of 1397 attacks through the multidimensional scaling (MDS) technique, smallest space analysis (SSA) and found that the government `Target Sector` commonly experiences `Web Compromise` from a `User` source, resulting in file change (`Distort`) while the Commercial `Target Sector` experiences `Virus` and `Root` attacks with the consequence of access change (`Disrupt`) from other commercial institutions (p. 522). Choo (2009) examined the technology-related risks associated with the NII and provided examples of existing incidents and areas in which new threats might emerge (p. 3). The `Commercial Sector` more commonly experiences `Virus` and `DoS`, whereas the `Government Sector` more commonly experiences `Web Compromise` and `User Compromise` (Kjalerland, 2006, p. 522). The attacks towards the `Commercial Sector` more often come from a `Commercial` source, and the attacks towards the `Government Sector` more often come from a `User` source.

Hibbs (2008) focused the methods and techniques used in cyber crime, cyber terrorism and discussed the ideas of cracking, denial of service, unauthorized intrusions, and man-in-the-middle attacks, as well as defenses against these attacks (p. 2). E-business applications can be susceptible to attacks or unauthorized activity without proper protection (Akhter & Kaya, 2008, p. 1474). A large majority of independent media sites subject to DDoS attacks

were also subject to filtering, intrusions, or defacement. The results suggested that DDoS needed to be considered in conjunction with other vectors of attack, and that these attacks can have synergistic effects that can be difficult to mitigate individually (Zuckerman et al., 2010, p. 56).

The number of casual hackers far exceeds the number of cyber terrorist organizations and their targets may be much less predictable and at the same time the impact of any individual attack is likely to be less severe while Cyber terrorists operate with a political agenda which meant that these types of attacks will be more specifically targeted and aimed at more critical systems (Furnelb & Warren, 1999, p. 33). They described the difficulties that attend the measurement and quantification of cyber-risk. The major obstacle is the lack of data on the frequency and severity of cyber-attacks (Cashell et al., 2004, p. 34). It further focused on how to improve quantification of risk and costs in the face of this complexity and proposed three major market forces at work that will lead to improvements in cyber-risk management, i. e., competition, liability, and insurance.

Most of the prior studies were built on western data. Almost nil researches were done in Indian context and specifically in banking sector. The previous studies related to the e-Services, cyber threats, information security, cyber-crime and its impact on financial institutions are not sufficient to identify the cyber-attack and cyber defense strategies in private and public sector banks (Hole et al., 2006; Simmons et al., 2006; Choo, 2009), and it does not clearly depict the cyber threat scenario with electronic banking (and e-Services). The present study will add to further understanding of the extent to which the results in Indian context will be similar to prior studies and will fill the gap in the literature.

Methodology

Objectives of the Study

1. To assess the various cyber-attack strategies in public and private sector banks.
2. To assess the various cyber defense strategies and their correlation with cyber attacks.

Universe and Sampling Design

The geographical region is divided on the basis of different districts of Uttarakhand, India. The total number of sample size is 100 for cyber crime victims and 50 for bank executives respectively. In this research, the sample size selected randomly on the basis of cyber crime victims and number of banks operating in Uttarakhand. The entire Universe includes population of people in the selected districts on which the study is focused. Dehradun, Haridwar, Chamoli, Nainital and Pauri districts have been selected for study purpose on the basis of electronic services usage and cyber crime victimization.

In this research, probability sampling procedure has been used. In this study, we have applied Stratified Random sampling. Since Uttarakhand is a newly born state and most of the population reside in remote areas where the concentration of electronic banking is either nil or not distributed uniformly, hence the universe is heterogeneous. In this case, stratified random sampling is used to stratify the sample on the basis of name of bank, age, gender, highest qualification, income, job type and dealing with bank/ experience with bank.

Data Collection

The present study pertains to the study of impact of cyber crime on e-services in public and private sector banks in Uttarakhand. Survey methodology is used to collect the primary data. The primary data was collected on the basis of questionnaires administered to various respondents in the State of Uttarakhand. The customers who had been the victim of cyber crime and the bank's technical staff have been chosen as the respondents of the survey. The secondary data was collected from various published reports available nationally or internationally. It also includes portals of Reserve Bank of India, Anti Phishing Working Group, Deloitte, KPMG, Ministry of Information Technology (Government of India), Cert-in, State bank of India, Punjab National bank, Union Bank of India, ICICI and HDFC.

The data were collected by means of a structured questionnaire with five point Likert scale (1-5). It was based on literature review and developed in a close cooperation with experts from different research fields. The instrument was divided into two types: first, bank customers who had been the victim of cyber crime and second, the technical staff involved with bank. The questionnaire is divided in three sections viz., Respondent's Details, Cyber Crime Handling (further subdivided in Database Management, Cyber Crime Occurrence, Complaint Handling, Feasibility and Support) and Organizational Strategy (further subdivided in Employee Training, Customer Awareness Program, Security Policy, Data Classification Policy, Access Control Policy, Virus Prevention Policy, Intrusion Detection Policy, System Security, Acceptable Use Policy, Government Policy).

Tools for Analysis

The data has been analyzed keeping the objective of the study in view. The analysis is based on the data on several aspects in tabulated form, besides making use of simple descriptive tools of statistics such as mean, percentage and standard deviation, possible relationship have been brought out through cross sectional analysis wherever necessary feasible. These relationships have been highlighted by computing the Chi-square and Karl Pearson coefficient of correlation.

Analysis of results

Hypothesis 1 (H1): There is no significant difference between cyber-attack strategies identified by public and private sector banks

Buffer Overflow (BO): It is evident from Table 1 that the value of Karl Pearson coefficient of correlation is 0.055, which concludes that there is a positive correlation between identification of BO and types of bank. Calculated value of χ^2 for 4 degrees of freedom at 5% level of significance is 1.74 and tabulated value of χ^2 is 9.488. Hence null hypothesis is accepted or it can be concluded that there is no significant difference between types of bank and identification of BO.

Spoofing (SP): The value of Karl Pearson coefficient of correlation is 0.1 which concludes that there is a positive correlation between identification of SP and types of bank. Calculated value of χ^2 for 4 degrees of freedom at 5% level of significance is 1.91 and tabulated value of χ^2 is 9.488, which shows that there is no significant difference between types of bank and identification of SP (Table 1).

Brute force (BF): The value of Karl Pearson coefficient of correlation is 0.013 which shows a positive correlation between identification of brute force attack and types of bank

(Table 1). Calculated value of χ^2 for 4 degrees of freedom at 5% level of significance is 1.65 and tabulated value of χ^2 is 9.488. Hence, null hypothesis is accepted or it can be concluded that there is no significant difference between types of bank and BF.

PHP remote file inclusion (PH): The Karl Pearson coefficient of correlation is -0.14 which concludes that there is a negative correlation between identification of PH and types of bank. Calculated value of χ^2 for 4 degrees of freedom at 5% level of significance is 1.11 and tabulated value of χ^2 is 9.488. Since calculated value of chi-square is less than tabulated value therefore null hypothesis is accepted or it can be concluded that there is no significant difference between types of bank and identification of PH (Table 1).

Cross-site scripting (CS): The coefficient of correlation 0.271 shows a positive correlation between identification of CS and types of bank. Calculated value of χ^2 for 4 degrees of freedom at 5% level of significance is 3.94 and tabulated value of χ^2 is 9.488. Hence, null hypothesis is accepted or it can be concluded that there is no significant difference between types of bank and identification of CS (Table 1).

SQL injection vulnerability (SQ): The coefficient of correlation -0.014 shows that there is a negative correlation between identification of SQ and types of bank. Calculated value of χ^2 for 4 degrees of freedom at 5% level of significance is 4.35 and tabulated value of χ^2 is 9.488. Hence, null hypothesis is accepted or it can be concluded that there is no significant difference between types of bank and identification of SQ (Table 1).

The variables `BO`, `SP`, `BF` and `CS` are positively correlated with government and private sector banks while the variables `PH` & `SQ` are negatively correlated with government and private sector banks. On the basis of chi square results it can be concluded that (Table 4) there is no significant difference between cyber-attack strategies identified by public and private sector banks.

Hypothesis 2 (H2): There is no significant difference between cyber defense strategies and cyber-attacks on banks

Online Identify Theft (OI): The value of Karl Pearson coefficient of correlation 0.088 shows that there is a positive correlation between OI and SM. Calculated value of χ^2 for 16 degrees of freedom at 5% level of significance is 14.97 and tabulated value of χ^2 is 26.296. The value shows that there is no significant difference between OI and SM (Table 2).

Malicious Code (MC): The value of Karl Pearson coefficient of correlation is -0.044 which concludes that there is a negative correlation between MC & SM. Calculated value of χ^2 for 16 degrees of freedom at 5% level of significance is 15.06 and tabulated value of χ^2 is 26.296. Therefore, it is no significant difference between MC and SM (Table 2).

DOS Attack (DA): There is a positive correlation between DA & SM (Table 2). Calculated value of χ^2 for 16 degrees of freedom at 5% level of significance is 13.22, which concludes that there is no significant difference between DA and SM.

Credit Card/ ATM Frauds (CC): The value of Karl Pearson coefficient of correlation is 0.086 which concludes that there is a positive correlation between CC and SM. The value of χ^2 for 16 degrees of freedom at 5% level of significance is 18.36 (Table 2), which clearly depicts that there is no significant difference between CC and SM.

Phishing (PV): The value of Karl Pearson coefficient of correlation is -0.088 which concludes that there is a negative correlation between PV & SM. Calculated value of χ^2 for 16 degrees of freedom at 5% level of significance is 21.58, while tabulated value of χ^2 is 26.296. It shows that there is no significant difference between PV and SM (Table 2).

Table 1. Cross tabulation of cyber attack strategies and types of bank

			Type of bank			
			Government	Private	Total	Value
Buffer Overflow (BO)	Agree	Count	21	5	26	χ^2 = 1.74
		%	42%	10%	52%	
	Undecided	Count	11	3	14	
		%	22%	6%	28%	
	Disagree	Count	8	2	10	R= 0.055
		%	16%	4%	20%	
	Total	Count	40	10	50	
		%	80%	20%	100%	
Spoofing (SP)	Agree	Count	32	8	40	χ^2 = 1.91
		%	64%	16%	80%	
	Undecided	Count	7	1	8	
		%	14%	2%	16%	
	Disagree	Count	1	1	2	R= 0.1
		%	2%	2%	4%	
	Total	Count	40	10	50	
		%	80%	20%	100%	
Brute force (BF)	Agree	Count	27	6	33	χ^2 = 1.65
		%	54%	12%	66%	
	Undecided	Count	4	2	6	
		%	8%	4%	12%	
	Disagree	Count	9	2	11	R= 0.013
		%	18%	4%	22%	
	Total	Count	40	10	50	
		%	80%	20%	100%	
PHP remote file inclusion (PH)	Agree	Count	19	6	25	χ^2 = 1.11
		%	38%	12%	50%	
	Undecided	Count	12	3	15	
		%	24%	6%	30%	
	Disagree	Count	9	1	10	R= -0.14
		%	18%	2%	20%	
	Total	Count	40	10	50	
		%	80%	20%	100%	
Cross-site scripting (CS)	Agree	Count	26	9	35	χ^2 = 3.94
		%	52%	18%	70%	
	Undecided	Count	5	1	6	
		%	10%	2%	12%	
	Disagree	Count	9	0	9	R= 0.271
		%	18%	0%	18%	
	Total	Count	40	10	50	
		%	80%	20%	100%	
SQL injection vulnerability (SQ)	Agree	Count	26	5	31	χ^2 = 4.35
		%	52%	10%	62%	
	Undecided	Count	4	3	7	
		%	8%	6%	14%	
	Disagree	Count	10	2	12	R= - 0.014
		%	20%	4%	24%	
	Total	Count	40	10	50	
		%	80%	20%	100%	
Agree = Strongly Agree + Quite Agree; Disagree = Strongly Disagree + Quite Disagree						

Table 2. Cross tabulation of cyber attacks and system monitoring

			System Monitoring				
			Agree	Undecided	Disagree	Total	Value
Online Identify Theft (OI)	Agree	Count	25	3	2	30	$\chi^2_=$ 14.97
		%	50%	6%	4%	60%	
	Undecided	Count	4	1	2	7	
		%	8%	2%	4%	14%	
	Disagree	Count	8	5	0	13	R= 0.088
		%	16%	10%	0%	26%	
	Total	Count	37	9	4	50	
		%	74%	18%	8%	100%	
Hacking (HK)	Agree	Count	24	5	4	33	$\chi^2_=$ 15.13
		%	48%	10%	8%	66%	
	Undecided	Count	4	1	0	5	
		%	8%	2%	0%	10%	
	Disagree	Count	9	3	0	12	R= -0.057
		%	18%	6%	0%	24%	
	Total	Count	37	9	4	50	
		%	74%	18%	8%	100%	
Malicious Code (MC)	Agree	Count	21	3	3	27	$\chi^2_=$ 15.06
		%	42%	6%	6%	54%	
	Undecided	Count	6	1	1	8	
		%	12%	2%	2%	16%	
	Disagree	Count	10	5	0	15	R= -0.044
		%	20%	10%	0%	30%	
	Total	Count	37	9	4	50	
		%	74%	18%	8%	100%	
DOS Attack (DA)	Agree	Count	21	4	2	27	$\chi^2_=$ 13.22
		%	42%	8%	4%	54%	
	Undecided	Count	3	2	1	6	
		%	6%	4%	2%	12%	
	Disagree	Count	13	3	1	17	R= 0.018
		%	26%	6%	2%	34%	
	Total	Count	37	9	4	50	
		%	74%	18%	8%	100%	
Credit Card/ ATM Frauds (CC)	Agree	Count	18	3	1	22	$\chi^2_=$ 18.36
		%	36%	6%	2%	44%	
	Undecided	Count	1	1	1	3	
		%	2%	2%	2%	6%	
	Disagree	Count	18	5	2	25	R= 0.086
		%	36%	10%	4%	50%	
	Total	Count	37	9	4	50	
		%	74%	18%	8%	100%	
Phishing/ Vishing/ Spoofing (PV)	Agree	Count	28	8	2	38	$\chi^2_=$ 21.58
		%	56%	16%	4%	76%	
	Undecided	Count	3	0	1	4	
		%	6%	0%	2%	8%	
	Disagree	Count	6	1	1	8	R= -0.088
		%	12%	2%	2%	16%	
	Total	Count	37	9	4	50	
		%	74%	18%	8%	100%	
Agree = Strongly Agree + Quite Agree; Disagree = Strongly Disagree + Quite Disagree							

Table 3 Cross tabulation of cyber attacks and intruder detection

			Intruder Detection				
			Agree	Undecided	Disagree	Total	Value
Online Identify Theft (OI)	Agree	Count	17	8	5	30	χ^2 = 11.6
		%	34%	16%	10%	60%	
	Undecided	Count	4	3	0	7	
		%	8%	6%	0%	14%	
	Disagree	Count	7	4	2	13	R= 0.013
		%	14%	8%	4%	26%	
	Total	Count	28	15	7	50	
		%	56%	30%	14%	100%	
Hacking (HK)	Agree	Count	21	8	4	33	χ^2 = 24.7
		%	42%	16%	8%	66%	
	Undecided	Count	1	3	1	5	
		%	2%	6%	2%	10%	
	Disagree	Count	6	4	2	12	R= 0.155
		%	12%	8%	4%	24%	
	Total	Count	28	15	7	50	
		%	56%	30%	14%	100%	
Malicious Code (MC)	Agree	Count	17	7	3	27	χ^2 = 12.3
		%	34%	14%	6%	54%	
	Undecided	Count	5	2	1	8	
		%	10%	4%	2%	16%	
	Disagree	Count	6	6	3	15	R= 0.212
		%	12%	12%	6%	30%	
	Total	Count	28	15	7	50	
		%	56%	30%	14%	100%	
DOS Attack (DA)	Agree	Count	16	7	4	27	χ^2 = 12.05
		%	32%	14%	8%	54%	
	Undecided	Count	3	3	0	6	
		%	6%	6%	0%	12%	
	Disagree	Count	9	5	3	17	R= 0.013
		%	18%	10%	6%	34%	
	Total	Count	28	15	7	50	
		%	56%	30%	14%	100%	
Credit Card/ ATM Frauds (CC)	Agree	Count	11	9	2	22	χ^2 = 18.26
		%	22%	18%	4%	44%	
	Undecided	Count	3	0	0	3	
		%	6%	0%	0%	6%	
	Disagree	Count	14	6	5	25	R= 0.016
		%	28%	12%	10%	50%	
	Total	Count	28	15	7	50	
		%	56%	30%	14%	100%	
Phishing/ Vishing/ Spoofing (PV)	Agree	Count	20	11	7	38	χ^2 = 16.28
		%	40%	22%	14%	76%	
	Undecided	Count	3	1	0	4	
		%	6%	2%	0%	8%	
	Disagree	Count	5	3	0	8	R= -0.259
		%	10%	6%	0%	16%	
	Total	Count	28	15	7	50	
		%	56%	30%	14%	100%	
Agree = Strongly Agree + Quite Agree; Disagree = Strongly Disagree + Quite Disagree							

Table 4 Summary of results for Hypothesis 1

SN	Proposed Relationship	Results
1	Type of bank - Buffer Overflow	+ve, Accepted
2	Type of bank - Spoofing	+ve, Accepted
3	Type of bank - Brute Force attack	+ve, Accepted
4	Type of bank - PHP remote file inclusion	-ve, Accepted
5	Type of bank - Cross Site Scripting	+ve, Accepted
6	Type of bank - SQL injection vulnerability	-ve, Accepted

Table 5 Summary of results for Hypothesis 2

SN	Proposed Relationship	Results
1	System Monitoring – Online identify theft	+ve, Accepted
2	System Monitoring – Hacking	-ve, Accepted
3	System Monitoring – Malicious code	-ve, Accepted
4	System Monitoring – DOS attack	+ve, Accepted
5	System Monitoring – Credit card/ ATM frauds	+ve, Accepted
6	System Monitoring – Phishing/ Vishing/ Spoofing	-ve, Accepted
7	Intruder Detection – Online identify theft	+ve, Accepted
8	Intruder Detection – Hacking	+ve, Accepted
9	Intruder Detection – Malicious code	+ve, Accepted
10	Intruder Detection – DOS attack	+ve, Accepted
11	Intruder Detection – Credit card/ ATM frauds	+ve, Accepted
12	Intruder Detection – Phishing/ Vishing/ Spoofing	-ve, Accepted

Online Identify Theft (OI): The value of Karl Pearson coefficient of correlation 0.013 concludes that there is a positive correlation between OI and ID. The value of χ^2 for 16 degrees of freedom at 5% level of significance is 11.6, which is less than tabulated value of χ^2, therefore null hypothesis is accepted or it can be concluded that there is no significant difference between OI and ID (Table 3).

Hacking (HK): There is a positive correlation between HA and ID (Table 4). Calculated value of χ^2 for 16 degrees of freedom at 5% level of significance is 24.7 and tabulated value of χ^2 is 26.296, i.e., there is no significant difference between HA and ID (Table 3).

Malicious Code (MC): The value of Karl Pearson coefficient of correlation is 0.212, i.e., there is a positive correlation between MC and ID. The χ^2 value for 16 degrees of freedom at 5% level of significance is 12.3, while tabulated value of χ^2 is 26.296. Hence, null hypothesis is accepted or it can be concluded that there is no significant difference between MC and ID (Table 3).

DOS Attack (DA): There is a positive correlation between DA and ID. Calculated value of χ^2 for 16 degrees of freedom at 5% level of significance is 12.05 and tabulated value of χ^2 is 26.296, i.e., there is no significant difference between DA and ID.

Credit Card/ ATM Frauds (CC): A positive correlation has been found between CC and ID (0.016). The χ^2 value for 16 degrees of freedom at 5% level of significance is 18.26, which concludes that there is no significant difference between CC and ID (Table 3).

Phishing (PV): The value of Karl Pearson coefficient of correlation is -0.259 which concludes that there is a negative correlation between PV and ID. Calculated value of χ^2 for 16 degrees of freedom at 5% level of significance is 16.28, which shows that there is no significant difference between PV and ID.

The variables `OI`, `DA` and `CC` are positively correlated with System Monitoring (SM) while the variables `HK`, `MC` & `PV` are negatively correlated with SM. The variables `OI`, `HK`, `MC` `DA` and `CC` are positively correlated with Intruder Detection (ID) while `PV` is negatively correlated with ID (Table 5). On the basis of chi square results shown in Table 5, it can be concluded that there is no significant difference between cyber defense strategies (intruder detection and system monitoring) and cyber-attacks on banks.

Discussion and Conclusion

The study reveals that 60% bank executives agree that online identify theft has been identified by their bank. Attacks through malicious code and Denial of Service attack have been agreed upon by 54% of the executives. Denial of service attacks are increasing with a rapid pace as seen in the wake of the recent Wiki Leaks incidents. In fact, the Wiki Leaks inspired attacks against leading e-commerce sites have fueled interest among fraudsters. The cases of hacking as well as credit card or ATM frauds have also been identified or reported in the banks. Sophistication in phishing, vishing and spoofing attacks are also identified and confirmed by 76% of the bank executives.

Various cyber-crime strategies have been identified by the bank executives. 52% of them identified that extraneous data can overflow into adjacent storage causing software failure. 80% agreed that identity deception had been used to gain access to the database or other resources available on the network. Instead of intellectual strategies, 66% executives agreed that cyber attacker uses an exhaustive search technique based on trial and error approach. PHP remote file inclusion has been agreed upon by half of the executives which allow a remote user to upload and possibly execute an arbitrary file on a web server. Scripts embedded in HTML requests tricking an unsuspecting surfer into executing the scripts are identified by 70% executives while processing cyber-attack patterns. Structured Query Language injection vulnerability has been detected by 62% executives. Considering the statistics, it is clearly understood that spoofing, cross side scripting, SQL injection vulnerability and brute force attacking strategies are the preferred way of attackers to assault the victims. Financial Institutions should adopt adequate security measures during financial transactions from internal databases. Confidential and high risk data should be encrypted during transmitting over insecure channels.

Information security policies strengthen the security and well-being of information resources. They are the foundation and bottom line of information security within the organization. 66% of the bank executives agreed that sufficient granularity of data is allowed for appropriate authorized access. Access to the network and servers is achieved by unique logins and requires authentication, which includes passwords, smartcards, biometrics etc. is agreed upon by 92% executives, whereas 74% agreed that monitoring is implemented on all systems including recording log on attempts and failures, successful logons and date and time of logon and logoff. All connections of the internet travel through a secure connection point to ensure the network protection is agreed upon by 90% executives. The installation of an approved, licensed antivirus software product with regular updates is also confirmed by 86% of the executives. The statistics show that banks have adopted the best security measures as far as software and hardware is concerned. But if we closely study the data collected from the survey, it reveals that in some specific areas much focus is required.

Where possible and financially feasible, more than one person must have full rights to any bank owned server storing or transmitting high risk data. The branches and top level administration must have a standard policy that applies to user access rights. Data custodians may apply strict policies and authentications for end user accessibility. Further, various logging activities may be reviewed either frequently or in a timely manner to inspect the data access. End users may be facilitated through specific provisions in the application software to find alerts when a serious intrusion is identified. Intrusion tools should be installed where feasible and reviewed on a regular basis. Operating system and application software logging processes must be enabled on all host and server systems.

Phishing, vishing, spoofing, hacking and online identify theft are some of the major challenges for banks to safeguard their customers and itself. To fight these attacks, inroads in consumer education should be made in collaboration with government and other private agencies. Education should be implemented to ensure that users understand data sensitivity issues, level of confidentiality and the mechanisms to make the transaction secure.

References

Akhter, F., & Kaya, L. (2008, March 16-20). Building secure e-business systems: Technology and culture in the UAE. SAC'08, Fortaleza, Ceara, Brazil, *ACM*, 1474-1475.

Armstrong, I. (2000). Computer forensics: Investigators focus on foiling cybercriminals, *SC Magazine*.

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks, CRS Report for Congress. Congressional Research Service, The Library of Congress, 1-41.

Choo, K. R. (2009). High tech criminal threats to the national information infrastructure. *Information Security Technical Report*, XXX, 1-8.

Cyber Crime. Retrieved November 10, 2010, from http://www.techterms.com/definition/cybercrime.

Cyber Crimes. Retrieved January 17, 2010, from http://www.cybercellmumbai.com/cyber-crimes.

Furnelb, S. M. & Warren, M. J. (1999). Computer hacking and cyber terrorism: the real threats in the new millennium. *Computers & Security, 18(1),* 28-34.

Future trends in net banking security, Retrieved January 11, 2011, from http://www.financialexpress.com/news/future-trends-in-net-banking-security/154138/0.

Hansman, S. & Hunt, R. (2005). A taxonomy of network and computer attacks, *Computers & Security, 24,* 31-43.

Hertzum, M., Juul, N. C., Jorgensen, N. & Norgaard, M. (2004). Usable security and ebanking: ease of use vis a-vis security. *Australasian Journal of Information Systems, 11*, 52-65.

Hibbs, J. (2008, June 02). Cybercrime & cyberterrorism against corporate America. Retrieved February 27, 2011, from http://www.infosecwriters.com/text_resources/pdf/JHibbs_Cybercrime.pdf

Hole, K. J., Moen, V. & Tjostheim, T. (2006). Case Study: Online Banking Security, *IEEE Security & Privacy,* 14-20.

Hole, K. J., Moen, V. & Tjostheim, T. (2006). Case Study: Online Banking Security, *IEEE Security & Privacy,* 14-20.

IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Standards, 2004-07-23. Retrieved October 04, 2010 from http://standards.ieee.org/getieee802/download/802.11i-2004.pdf, p.43.

Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security, 25,* 522-538.

KPMG (2000). *E-Commerce and cyber crime: New strategies for managing the risks of exploitation.* Forensic and Litigation Services, KPMG LLP.

Meyers, M. (2004). *Managing and Troubleshooting Networks.* Network+. McGraw Hill.

Polstra III, R. M. (2005, 23-24 September). A case study on how to manage the theft of information. Information Security Curriculum Development (InfoSecCD) Conference '05, Kennesaw, GA, USA, ACM, 135-138.

Rudasill, L. & Moyer, J. (2004). Cyber-security, cyber-attack, and the development of governmental response: the librarian's view. *New Library World, 105,* 248-255.

Simmons, S., Edwards, D. & Wilde, N. (April 2006). Preventing unauthorized islanding: cyber-threat analysis, Proceedings of the 2006 IEEE/SMC International Conference on System of Systems Engineering, Los Angeles, CA, USA, 184-188.

Wueest, C. (2005). *Threats to online banking.* Symantec Security Response, Dublin, 4-9.

Zuckerman, E., Roberts, H., McGrady, R., York, J. & Palfrey, J. (2010). *Distributed denial of service attacks against independent media and human rights sites.* The Berkman Center for Internet & Society at Harvard University.