Journal of Internet Banking and Commerce

An open access Internet journal (http://www.icommercecentral.com)

Journal of Internet Banking and Commerce, August 2015, vol. 20, no. 2

Evaluating Database Security and Cyber Attacks: A Relational Approach

BAMRARA A

Academic Counselor, School of Computer and Information Sciences, Indira Gandhi National Open University, Uttarakhand, India, Tel: +917500941108

Email: **atulbamrara@gmail.com**

Abstract

With a mounting number of enterprises become reliant on access to its data over the web, the need for ample security measures is becoming more and more significant. Security of the databases has become a multifarious concern for enterprises. More complex the database is additional security measures have to come into action. Huge internet penetration and enormous capability of computer networks have posed the security concerns of the enterprise databases more complicated for Database Specialists. Significant business information is an evident target for cyber criminals; therefore, ensuring the Confidentiality, Integrity and Authority of data are the major issues for business houses. In this paper, we survey the information system specialists of the banks to explore the facts and figures associated with information associated risks, and discuss the role of central data warehouse to deal with such risks. Further, it highlights on various cyber-attack methodologies and its correlation with data warehouse operations.

Keywords: **Cyber-crime; Database security; DoS attack; Malicious code; Online identity theft**

INTRODUCTION

Noteworthy emphasis has been placed in recent times on the hardening of databases. Data centers dealing with sensitive data and mission-critical systems, particularly centers which belong to government agencies, have been under great pressure to protect its databases in conformity with numerous security guidelines. This in turn has been putting great pressure on database administrators who are already besieged by the tasks of installing, properly maintaining, and configuring the enterprise systems. Nonetheless, it is becoming enormously challenging, time consuming, and resource intensive to deal with security demands under fixed budgets and timelines. Therefore, it may be advantageous to apply robotic features into database systems to tackle a few facets of this challenge [1].

Electronic banking, with its intrinsic advantages for the banking industry as well as the customer, is an area with incredible growth possibilities. This field has also seen an analogous boost in network security breaches, data losses, identity thefts and other white collar crimes resulting in enormous losses to the banking industry as well as its clientele. Losses by the banking industry are global due to white collar crimes are in billions of dollars and far outstrip conventional techniques of bank robbery. The extraordinary speed at which net banking has evolved, the everywhere and global nature of open networks and the mounting reliance on information technology have all added up to offer an environment of improved security challenges. Amendments in Information Technology Act, banking regulations and the coming detonation in WAP are issues that need to be taken into consideration by the industry.

Strategies to overcome cyber threats

When a bank's system is connected to the internet or intranet, an attack could originate anytime, anywhere. Some acceptable level of security must be established before business on the internet can be reliably conducted. An attack could be any form like

a. The intruder may gain unofficial access.
b. The intruder can destroy, corrupt or otherwise alter data.
c. The intruder does not gain right of entry, but instead fakes messages from user system.

d. The intruder does not gain access, but instead implements malicious procedures that cause the network to fail, reboot or hang.

Modern security techniques have made cracking very difficult but not unfeasible. In addition, if the system is not configured properly or the updated patches are not installed then hackers may crack the system using security loophole. A wide range of information regarding security hole and their fixes is freely available on the internet.

Authentication techniques: Authentication is the act of establishing genuineness or originality of a subject. It can be divided into many types depending on how it is performed. Authentication techniques evolved and got strengthened by continuous refinements so as to lessen attacks on private domains.

Single factor authentication: A well-known and trusted solution in the initial days of computerization was validation by a single attribute. It was effective in the days of localized processing and single user environments. But as networking and Internet based applications spread everywhere, and users were required to maintain passwords for many sites and different applications, they tended to use a single password for all applications on different websites. There are several reported cases where attackers broke into low security websites and retrieved thousands of username/password pairs and directly try to use them by trial and error methods to enter high security e-commerce sites such as eBay with the intention of committing frauds.

Web password hashing: PwdHash is a browser extension that transparently converts a user's password into a domain explicit password. PwdHash mechanically replaces the contents of these password fields with a one-way hash of the pair (domain name with password). This makes the program on the website process only the domain-specific hash of the password, and not the password itself. A break-in at a little security website exposes password hashes rather than an actual password. Nevertheless, this was a very effective technique, but it requires extensions to be added to the browsers. This feature if embedded into every browser will avoid the need to install any extensions.

Two stage authentication: All users cannot be expected to load extensions to their passwords as it requires some knowledge of processing and also as password-stealing attacks have become so common that the software industry observed that the two stage authentication may control the ID theft only to some extent. Businesses chose different methods for second stage authentication apart from passwords. The second input for authentication should preferably be dynamic and possessed by the authorized user. Single time passwords given through tokens, transaction numbers over mobile telephones, grids printed on the back of cards, dynamic digits from ATM card numbers, etc., all are entered as a

second input for authentication and come in the increasing order of complexity and cost [2]. Though these methods are loosely termed as second-factor authentication in reality these get used as knowledge based inputs and thus can be stolen or shared.

Multifactor authentication: Federal Financial Institutions Examination Council issued supplemental guidance on authentication in 2006, in which they explained, “By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors”. Using several solutions of the identical group, would not qualify as a multifactor authentication.
Cryptography: Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian inscribe used non-standard hieroglyphs in a writing. Some experts disagree that cryptography appeared instinctively a short time after writing was invented, with applications ranging from ambassadorial missives to war-time encounter plans. It is no surprise, then, that new types of cryptography came soon after the extensive development of computer communications. In data transmission, cryptography is essential when communicating over any insecure medium, which includes just about any network, particularly the Internet (Figure 1). An array of cryptographic methods may include Public Key Cryptography, Secret Key Cryptography, or Hash Functions [3].

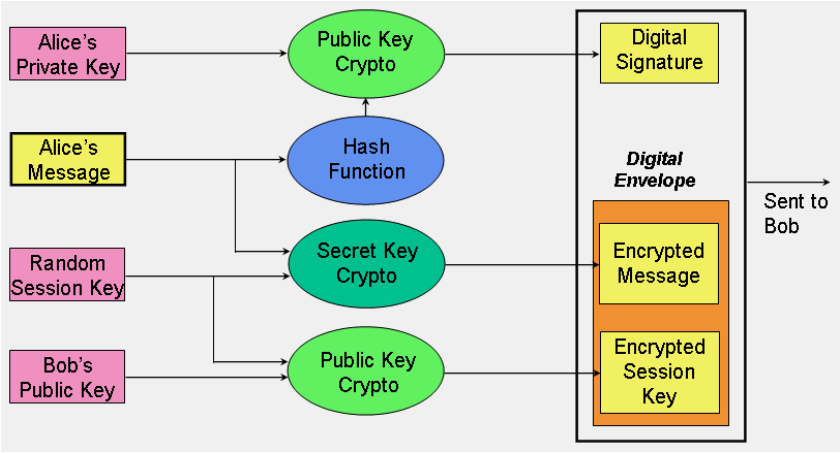

Figure 1: Sample applications of the three cryptographic techniques for secure communication.

Database security: Data base Management Systems are increasingly being used to store information about all aspects of an enterprise. The data stored in a DBMS is often imperative to the business interests of the organization and is regarded as a commercial asset. In addition to protecting the inherent value of the data, financial institutions must consider ways to ensure privacy and to control access to data that must not be revealed to certain users’ group for

various reasons. A database of the bank contains a great deal of information and usually has several groups of users. Most users require accessing only a small part of the database to carry out their jobs. Allowing users unrestricted access to all the data can be undesirable and a DBMS should provide mechanisms to control access to data. A DBMS uses two major approaches to access control.

Discretionary access control: Discretionary access control is the standard of restricting access to objects based on the identity of the subject (the user or the group to which the user fits in). DAC is implemented using access control lists. A resource profile holds an access control list that identifies the users who can access the resource and the authority (such as read or update) the end-user is allowed in referencing the resource. The security officer defines a profile for each object (a resource or group of resources), and revises the access control list for the profile. This kind of control is discretionary in the sense that subjects can maneuver it, because the owner of a resource, adding to the security administrator, can recognize who can access the resource and with what authority.

Mandatory access control (MAC): Mandatory Access Control guarantees that the enforcement of enterprise's security policy does not bank on voluntary web application user compliance. MAC secures information by allocating sensitivity labels on information and matching it to the level of sensitivity a user is operating at. Normally, Mandatory Access Control mechanisms are more protected than Discretionary Access Control yet have tradeoffs in performance and expediency to users. MAC mechanisms assign a security level to all the information; assign a security clearance to every user, and guarantees that all users only have access to that data for which they have authentications. MAC is usually suitable for extremely secure systems with multilevel secure military applications or mission critical data applications.

Network security: Experts opine that a network is secure if the connection obeys CIA property. To provide security in a network many security protocols are being designed by Internet Authority time to time. Web came into being in early 90s; researchers started thinking about to provide security to web and web transaction.

IPSEC: Internet Protocol Security is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. It includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. It is an end-to-end security scheme operating in the Internet Layer of the IP Suite. It can be exercised in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or amid a security gateway and a host (network-to-host).

SSL: The Secure Sockets Layer (SSL) protocol was developed by Netscape Communications to provide application-independent secure communication over the Internet for protocols such as the Hypertext Transfer Protocol (HTTP). SSL employs RSA and X.509 certificates during an initial handshake used to authenticate the server (client authentication is optional). The client and server then are in agreement upon an encryption scheme; SSL v2 supports RC2 and RC4 with 40-bit keys, while SSL v3 adds support for DES, RC4 with a 128-bit key and 3DES with a 168-bit key, all along with either MD5 or SHA-1 message hashes.

DNSSEC (DNS security extension): DNSSEC was designed to shield the Internet from definite attacks, such as DNS cache poisoning. It is a set of extensions to DNS, which offers
a. Origin authentication of DNS data
b. Data integrity and.
c. Authenticated denial of existence.

These mechanisms require changes to the DNS protocol. DNSSEC includes four resource record types: Resource Record Signature (RRSIG), DNS Public Key (DNSKEY), Delegation Signer (DS), and Next Secure (NSEC).

WEP: Wired Equivalent Privacy is the encryption algorithm built into the 802.11 (Wi-Fi) standards. WEP encryption uses the RC4 stream cipher with 40 or 104 bit keys and a 24 bit initialization vector. Most 802.11 devices allow WEP keys to be entered using an ASCII passphrase or in hexadecimal format. The conversion between these two formats is an industry standard which is shared by almost all vendors.

WPA: Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless networks. The WPA protocol realizes the mainstream of the IEEE 802.11i standard. The Wi- Fi Alliance proposed WPA as a midway measure to take the place of WEP pending the grounding of 802.11i. Explicitly, the Temporal Key Integrity Protocol (TKIP) was brought into WPA. TKIP encryption restores WEP's small 40-bit encryption key that must be manually entered on wireless access points and devices and does not modify. TKIP is a 128-bit per-packet key which dynamically generates a new key for each packet and thus prevents collisions.

RSN (Robust security network): The RSN is a security network that only permits the creation of robust security network associations (RSNAs), which are a type of association used by a pair of stations (STAs) if the method to establish authentication or association between them includes the 4-Way Handshake. It also provides two RSNA data confidentiality and integrity protocols, TKIP and

CCMP, with implementation of CCMP being mandatory.

REVIEW OF LITERATURE

The protection of enterprise databases has received substantial concentration in the literature in past few years. It can be attributed to instantaneous raise in volumes of data being stored in databases, the analysis of such data, and the need to protect confidential information. The study made by Muralidhar et al. [4] described a General Additive Data Perturbation approach that does not change relationships between attributes. All accessible methods of additive data perturbation are shown to be special cases of this technique. When the database has a multivariate normal distribution, the current technique provides maximum protection and minimum bias. As a mounting number of enterprises become dependent on access to their data over the Web, the need for ample security measures is becoming more and more serious. The most trendy security measure nowadays is the firewall. Nevertheless, a firewall is not immune to penetration, and it does not provide any defense from insiders and successful intruders [5]. Managers of database security must ensure that data access does not compromise the confidentiality afforded data providers, whether individuals or establishments [6]. Due to a variety of requirements for user access control to huge databases in enterprises, database security has been put emphasis on. There are numerous security models for database systems using a wide array of policy-based access control techniques. Jeong et al. [7] proposed a database security system that can independently control user access to data groups of numerous sizes and is appropriate for the situation where a user's access opportunity to arbitrary data is altered regularly. Access control mechanisms are usually used to offer control over who can access susceptible information. Nevertheless, malicious users can utilize the correlation among the data and infer susceptible information from an array of seemingly inoffensive data access [8]. The first stage is composed of a modified MAC (mandatory access control) model and RBAC (role-based access control) model. A user may access any information that has lower or equal security points, and which is accessible by the roles to which the user is assigned. In the next stage, a modified Discretionary Access Control model is used to re-control the read mode by filtering out the non-accessible information from the output obtained at the initial phase. With this security arrangement, more complex read access to numerous data sizes for individual users can be supplely controlled, though other access mode may be controlled as usual Jeong et al. [7].

Data centers have been under remarkable pressure to protect its databases in conformity with numerous security guidelines. Jabbour et al. [1] proposed a structure that embeds autonomic capabilities into database systems to offer auto-secure features in case of illicit, unintended, or deliberate change in safety parameters. They achieved it by embedding into the database the potential to evaluate each safety configuration parameter change effort with an inbuilt

security policy before permitting or declining the variation. SQL injection assaults have posed a severe security risk to Web databases. To tackle this risk, Haixia et al. [9] presented a scheme of database protection testing. They studied how to sense latent input points of SQL injection repeatedly design test cases and locate susceptibility of databases by running these test cases to develop a simulation attack to an application. Database encryption is a vital practice in the security mechanisms of databases. It is extensively recognized as one of the key issues of data protection. Existing methods of sharing the keys and the encrypted data for databases are neither expedient nor flexible in the genuine applications. Inspired by the Pretty Good Privacy technique, Chen et al. [10] proposed a novel database encryption format for improved data sharing within a database, which offers safe storage for defense related information and effective key organization, which permits the encrypted data to be allocated properly. Johnsten et al. [11] investigated issues pertaining to the evaluation of the impact of categorization mining on database protection. They proposed a set of security measures to be applied in context of decision-region based categorization mining algorithms along with the implementation and specification of a security risk measure which permits for the realization of a subset of the planned measures.

OBJECTIVES OF THE STUDY

a. To study the role of Central Data Warehouse in defending Cyber Attacks.
b. To study the correlation between Data Warehouse Maintenance and Cyber Attacks.

RESEARCH METHODOLOGY

The present study relates to the study of central data warehousing operations of banks in view of various cyber attacks posed on it. Survey (interview and schedules) methodology is adopted to collect the primary information regarding the associated issues from the bank officials working with information systems in one of the States (Uttarakhand) in India. The secondary data was collected from various published reports available nationally or internationally. It also includes portals of Reserve Bank of India, Antiphishing 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. 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 research probability sampling procedure has been used. Further, stratified random sampling is used to stratify the sample on the basis of name of bank, designation, job type, work experience, data warehouse and cyber threats' issues.

Geographical region is divided on the basis of different districts of Uttarakhand. In this research, sample size is selected randomly on the basis of number of banks operating in Uttarakhand constitutes to a sample of fifty bank officials

dealing with IS issues. Based on review of literature and available gaps in research, a testing instrument has generated in close co-operation with experts from concerned research areas and finalized for final survey after Pilot Testing. A set of schedules is distributed among the respondents to fetch responses of each question. The data has been analyzed keeping the objective of the study in view. The analysis is finally based on 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 Pearson coefficient of correlation.

Null Hypothesis (H0): There is no association between database management of banks and cyber-attacks (Table 1).

Table 1: Cross tabulation of cyber-attack and proper display of information from data warehouse.

	A central data warehouse or data repository has been maintained for proper display of information and to avoid conflicts (CDW)						
			Agree	**Undecided**	**Disagree**	**Total**	**Value**
Online Identity Theft (OIT)	Agree	Count	28	1	1	30	χ^2 = 14.4
		%	56%	2%	2%	60%	
	Undecided	Count	5	2	0	7	
		%	10%	4%	0%	14%	
	Disagree	Count	9	2	2	13	ρ= 0.296
		%	18%	4%	4%	26%	
	Total	Count	42	5	3	50	
		%	84%	10%	6%	100%	
Hacking (HCK)	Agree	Count	28	3	2	33	χ^2 = 9.98
		%	56%	6%	4%	66%	
	Undecided	Count	4	1	0	5	
		%	8%	2%	0%	10%	
	Disagre	Coun	10	1	1	12	ρ = -

	e	t					0.031
		%	20%	2%	2%	24%	
	Total	Count	42	5	3	50	
		%	84%	10%	6%	100%	
Malicious Code (MCO)	Agree	Count	22	2	3	27	$\chi^2 =$ 10.44
		%	44%	4%	6%	54%	
	Undecided	Count	6	2	0	8	
		%	12%	4%	0%	16%	
	Disagree	Count	14	1	0	15	ρ = -0.2
		%	28%	2%	0%	30%	
	Total	Count	42	5	3	50	
		%	84%	10%	6%	100%	
DOS Attack (DOS)	Agree	Count	23	1	3	27	$\chi^2 =$ 14.78
		%	46%	2%	6%	54%	
	Undecided	Count	5	1	0	6	
		%	10%	2%	0%	12%	
	Disagree	Count	14	3	0	17	ρ = -0.044
		%	28%	6%	0%	34%	
	Total	Count	42	5	3	50	
		%	84%	10%	6%	100%	
Credit Card/ ATM Frauds (CAT)	Agree	Count	19	2	1	22	$\chi^2 =$ 6.78
		%	38%	4%	2%	44%	
	Undecided	Count	3	0	0	3	
		%	6%	0%	0%	6%	
	Disagree	Count	20	3	2	25	ρ = 0.159
		%	40%	6%	4%	50%	
	Total	Count	42	5	3	50	
		%	84%	10%	6%	100%	
Phishing/ Vishing/ Spoofing	Agree	Count	32	4	2	38	$\chi^2 =$ 19.32
		%	64%	8%	4%	76%	

(PVS)	Undecided	Count	4	0	0	4	
		%	8%	0%	0%	8%	
	Disagree	Count	6	1	1	8	
		%	12%	2%	2%	16%	ρ = 0.051
	Total	Count	42	5	3	50	
		%	84%	10%	6%	100%	

OIT (CDW- central data warehouse)

The value of Pearson coefficient of correlation shows that there is a positive correlation between online identity theft attack and maintaining a data warehouse. Calculated value of $\chi 2$ at 5% level of significance is 14.4 and which is less than tabulated value therefore null hypothesis is accepted or it can be concluded that there is no significant association between online identity theft attack and maintaining a data warehouse.

HCK (CDW)

There is a negative correlation between hacking attack and maintaining a data warehouse (ρ = - 0.031). The value of $\chi 2$ for is 9.98 and tabulated value of $\chi 2$ is 26.3, which shows that there is no significant association between hacking attack and maintaining a data warehouse.

MCO (CDW)

A negative correlation has been observed between malicious code attack and maintaining a data warehouse ($\rho = -0.2$). There is no significant association between malicious code attack and maintaining a data warehouse ($\chi 2$calculated = 10.44).

DOS (CDW)

Pearson coefficient of correlation is found - 0.044 concluding that there is a negative correlation between DOS attack and maintaining a data warehouse. The calculated value of $\chi 2$ for the observed data is 14.78 and tabulated value of $\chi 2$ is 26.3, which shows that there is no significant association between DOS attack and maintaining a data warehouse.

CAT (CDW)

There is a positive correlation between Credit Card/ ATM frauds and maintaining a data warehouse (ρ = 0.159). Calculated value of $\chi 2$ at 95% level of significance

is observed as 6.78 which is less than the tabulated one, therefore null hypothesis is accepted and it can be concluded that there is no significant association between Credit Card/ ATM frauds and maintaining a data warehouse.

PVS (CDW)

A positive correlation has been observed between Phishing/ Vishing/ Spoofing and maintaining a data warehouse ($\rho = 0.051$). There is no significant association between PVS and maintaining a data warehouse ($\chi 2_{calculated} = 6.78$)

OIT (DWD- data warehouse defend systems)

The value of Pearson coefficient of correlation ($\rho = 0.081$) shows that there is a positive correlation between online identity theft attack and vital role of data warehouse to defend systems from cyber threats. Calculated value of $\chi 2$ at 5% level of significance is 13.37 and which is less than tabulated value therefore null hypothesis is accepted or it can be concluded that there is no significant association between online identity theft attack and vital role of data warehouse to defend systems from cyber threats.

HCK (DWD)

There is a negative correlation between hacking attack and vital role of data warehouse to defend systems from cyber threats ($\rho = - 0.072$). The value of $\chi 2$ for is 15.3 and tabulated value of $\chi 2$ is 26.3, which shows that there is no significant association between hacking attack and vital role of data warehouse to defend systems from cyber threats.

MCO (DWD)

A positive correlation has been observed between malicious code attack and vital role of data warehouse to defend systems from cyber threats ($\rho = 0.133$). There is no significant association between malicious code attack and vital role of data warehouse to defend systems from cyber threats ($\chi 2_{calculated} = 10.73$).

DOS (DWD)

Pearson coefficient of correlation is found - 0.074 concluding that there is a negative correlation between DOS attack and vital role of data warehouse to defend systems from cyber threats. The calculated value of $\chi 2$ for the observed data is 28.8 and tabulated value of $\chi 2$ is 26.3, which shows that there is a significant association between DOS attack and vital role of data warehouse to defend systems from cyber threats.

CAT (DWD)

There is a negative correlation between Credit Card/ ATM frauds and vital role of data warehouse to defend systems from cyber threats (ρ = - 0.177). Calculated value of χ2 at 95% level of significance is observed as 13.95 which is less than the tabulated one, therefore null hypothesis is accepted and it can be concluded that there is no significant association between Credit Card/ ATM frauds and vital role of data warehouse to defend systems from cyber threats.

PVS (DWD)

A positive correlation has been observed between Phishing/ Vishing/ Spoofing and vital role of data warehouse to defend systems from cyber threats (ρ = 0.054). There is no significant association between PVS and vital role of data warehouse to defend systems from cyber threats (χ2calculated = 6.78) (Table 2).

Table 2: Cross tabulation of cyber-attacks and role of data warehouse to defend systems

	The data ware house plays a vital role to defend the systems from cyber threats and intruders (DWD)						
			Agree	**Undecided**	**Disagree**	**Total**	**Value**
Online Identify Theft (OIT)	Agree	Count	22	2	6	30	χ^2 = 13.37
		%	44%	4%	12%	60%	
	Undecided	Count	4	3	0	7	
		%	8%	6%	0%	14%	
	Disagree	Count	9	1	3	13	ρ = 0.081
		%	18%	2%	6%	26%	
	Total	Count	35	6	9	50	
		%	70%	12%	18%	100%	
Hacking (HCK)	Agree	Count	24	2	7	33	χ^2 = 15.3
		%	48%	4%	14%	66%	
	Undecided	Count	2	2	1	5	
		%	4%	4%	2%	10%	

	Disagree	Count	9	2	1	12	ρ = -0.072
		%	18%	4%	2%	24%	
	Total	Count	35	6	9	50	
		%	70%	12%	18%	100%	
Malicious Code (MCO)	Agree	Count	19	4	4	27	χ^2 = 10.73
		%	38%	8%	8%	54%	
	Undecided	Count	6	1	1	8	
		%	12%	2%	2%	16%	
	Disagree	Count	10	1	4	15	ρ = 0.133
		%	20%	2%	8%	30%	
	Total	Count	35	6	9	50	
		%	70%	12%	18%	100%	
DOS Attack (DOS)	Agree	Count	19	2	6	27	χ^2 = 28.8
		%	38%	4%	12%	54%	
	Undecided	Count	2	4	0	6	
		%	4%	8%	0%	12%	
	Disagree	Count	14	0	3	17	ρ = -0.074
		%	28%	0%	6%	34%	
	Total	Count	35	6	9	50	
		%	70%	12%	18%	100%	
Credit Card/ ATM Frauds (CAT)	Agree	Count	14	2	6	22	χ^2 = 13.95
		%	28%	4%	12%	44%	
	Undecided	Count	2	1	0	3	
		%	4%	2%	0%	6%	
	Disagree	Count	19	3	3	25	ρ = -0.177
		%	38%	6%	6%	50%	
	Total	Count	35	6	9	50	
		%	70%	12%	18%	100%	
Phishing/ Vishing/	Agree	Count	27	5	6	38%	χ^2 = 25.77

Spoofing (PVS)		%	54%	10%	12%	76	
	Undecided	Count	3	0	1	4	
		%	6%	0%	1%	8%	
	Disagree	Count	5	1	2	8	
		%	10%	2%	4%	16%	ρ = 0.054
	Total	Count	35	6	9	50	
		%	70%	12%	18%	100%	

CONCLUSION AND RECOMMENDATIONS

It has been observed that the variables 'OIT', 'MCO', 'CAT' and 'PVS' are positively correlated with proper display of information from data warehouse (CDW), while the variables 'HCK', and 'DOS' are negatively correlated with proper display of information from data warehouse.

The variables 'OIT', 'MCO' and 'PVS' are positively correlated with vital role of data warehouse to defend systems from cyber threat (DWD), while the variables 'HCK', 'DOS' and 'CAT' are negatively correlated (Table 3). On the basis of chi square results shown in Table 3, there is a significant association between DOS attack and vital role of data warehouse to defend systems (DWD), while other cyber attacks have no significant association between database management of banks and cyber attacks. So, it can be concluded that there is no significant association between database management of banks and cyber-attacks except DOS attack.

Table 3: Summary of results for Hypothesis 1.

	Proposed relationship	**Results**
1	CDW – OIT	+ve, Accepted
2	CDW – HCK	-ve, Accepted
3	CDW – MCO	-ve, Accepted
4	CDW – DOS	-ve, Accepted
5	CDW – CAT	+ve, Accepted

6	CDW – PVS	+ve, Accepted
7	DWD – OIT	+ve, Accepted
8	DWD – HCK	-ve, Accepted
9	DWD – MCO	+ve, Accepted
10	DWD – DOS	-ve, Rejected
11	DWD – CAT	-ve, Accepted
12	DWD – PVS	+ve, Accepted

The study reveals that 60% bank executives agree that online identify theft has been identified by their bank. While attack 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. 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

1. Jabbour GG, Menasee DA (2008) Policy-based enforcement of database security configuration through autonomic capabilities. Proceedings of the Fourth International Conference on Autonomic and Autonomous Systems 1:188-197.

2. Radha V (2010) Digital Identity-Issues. Fast Forward. 13: 5-10.

3. Kessler GC (2011)An overview of cryptography.

4. Muralidhar K, Parsa R, Sarathy R (1999) A general additive data perturbation method for database security. Management Science 45: 1390-1415.

5. Bertino E, Jajodia S, Samarati P (1995) Data security: Research and practice. Information Systems 20:537-556.

6. Duncan GT, Keller-McNulty SA, Stokes SL (2004) Database security and confidentiality: Examining disclosure risk vs. data utility through the R-U confidentiality map. National Institute of Statistical Sciences, Technical Report 142: 1-24.

7. Jeong M, Kim J, Won Y (2003)A flexible database security system using multiple access control policies. Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies 7: 236-240.

8. Chen Y, Chu WW (2006) Database security protection via inference detection. Intelligence and Security Informatics. 3975: 452-458.

9. Haixia Y, Zhihong N (2009) A database security testing scheme of web application. Proceedings of the Fourth International Conference on Computer Science & Education 3: 953-955.

10. Chen G, Chen K,Dong J (2006)Adatabase encryption scheme for enhanced security and easy sharing. Proceedings of the 10th International Conference on Computer Supported Cooperative Work in Design 8: 1-6.

11. Johnsten T,Raghavan VV (2000) Impact of Decision-Region Based Classification Mining Algorithms on Database Security.