Information Security: Exploring the Association between IT Receptivity and Cyber Crime Victimization

by Atul Bamrara, Lhato Jamba & Alka Rathore

Abstract

Cybercrime is a menace for all enterprises in the current digital age. Focusing on the consumer and financial services industry for several years, cybercrime definitively made the shift into the working patterns. The organizations are engaged in strong R&D and trying to manage secure transactions between clients and businesses. Although, cybercriminals are operational every moment to craft better strategies to intrude into the corporate networks, that leads to better payoffs. Our study is based on five Information Technology firms offering a range of electronic services globally. The survey based approach is applied to fetch responses from information specialists of the concerned enterprises to explore an association between cyber crime strategies identified.

Keywords

Brute Force Attack, SQL Injection Vulnerability, Cross Side Scripting, PHP Remote File Inclusion, Buffer Overflow

Introduction

Cyber-crime is an array of unlawful digital activities targeted at enterprises in order to cause damage. The term applies to an extensive range of targets and attack terminologies. It can range from web-site defacements to severe activities such as service disruptions that shock business revenues to e-banking scams (KPMG, 2014). 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. Electronic transactions, with its inherent advantages for the business firms as well as the customers are an area with remarkable growth potential. This field has also seen a analogous increase in network safety breaches, data thefts, identity thefts and other white collar crimes resulting in gigantic losses to the IT industry as well as its clientele. Losses by the IT industry worldwide due to white- collar crimes are in billions of dollars. The exceptional speed at which online businesses have evolved, the ubiquitous and global nature of open networks and the mounting dependence on information technology have all added up to present an environment of enhanced security challenges. Amendments in IT Laws, social media challenges, smart phone issues and cloud computing are among few of the areas which needed to be taken into account by the industry as well as Governments. Industry, government and indeed society are becoming critically dependent on IT (Anderson, 1994; Apt et al., 1997). This dependence is illustrated by the serious concerns which are now being caused by residual 'Year 2000' bugs. Seeing that even these conceptually-simple software errors are demanding massive resources and we must be concerned about the much more critical effects of cyber crime, malicious activities by hackers or organizations seeking to take advantage of an IT system, for trouble, financial gain, or more threatening motives (Benjamin, 1990).

Today's cyber criminals are increasingly practiced at gaining undetected access and maintaining an importunate, low-profile, long-term existence in IT environments. Temporarily, many organizations may be leaving themselves susceptible to cyber crime based on a false sense of defense. Cyber criminals are generally computer professionals or computer-literate people and not having any prior criminal record (Kumar, 2002). Studies also show that the threat is mostly from human resources or from those with access to the system, such as maintenance workforce, hardware and software vendors, etc. However, exterior threats via remote access have shown a mounting trend. The Internet is now available in over two hundred countries and because of its borderless nature, crimes may be committed through communications that are routed through a number of different countries (U. S. Department of Justice, 2000). Although cyber crimes cells have been set up in major cities of the nation but most cases of Spamming, Hacking, Phishing, Vishing stay unreported due to the lack of responsiveness among internet users and employees of monetary institutions. There are no policemen patrolling the information thruway, leaving it unlock to everything from Trojan horses and viruses to cyber stalking, trademark counterfeiting and defamation of brand names.

Data is more valuable than wealth as data can be used and reused to create more money again and again (Deloitte, 2010). The ability to reprocess data to access online applications, allow and activate credit cards or access firms' networks have enabled cyber criminals to engender an extensive archive of data for ongoing illegal activities. The world has not changed much since the early 1900's when Willie Sutton was asked why he robbed banks. He said - That's where the money is. Now, cyber criminals go where the data is since it gives them repeated access to the information, wherever it is. Cyber crimes may present the most potentially damaging threat to Information Technology based activities, transactions and assets. Deloitte sees this threat as under recognized and under rated among the risks that organizations encounter, and thus believe that many organizations are unprepared to sense, address, or protect themselves with these threats. One of the biggest challenges of cyber crime is that a criminal can commit a crime from any place; can target victims all over; hide its identity by transmitting communications through computer systems located in many overseas places and store evidence in remote locations. The ability to trace communications through diverse computer networks in different jurisdictions is a significant element in preventing, investigating and prosecuting cyber-crime (Ottawa Department of Justice, 2001). Thus, it is not shocking that initiatives for combating cyber crime largely rely on international collaboration. The first comprehensive international effort to deal with computer crime problems was initiated by OECD during the 1970's. Considerable attempts went into determining what was meant by computer crime and towards developing guidelines to encourage harmonization of global computer crime laws. It was recognized that global harmonization was necessary in order to have effective enforcement of what is largely a worldwide crime (Canadian Centre for Justice Statistics, 2002). Financial accountability requires the financial institutions so important in supporting and maintaining domestic and international commerce to take steps to defend their ability to carry out basic functions (Cashell et al., 2004).

The information security scene is continuously evolving. Private and public sector enterprises find it tricky to consider they could be a victimized by a cyber attack. As adversary complexity mounts, many enterprises react only after the event or the attack is imposed. Very few enterprises have the competence to foresee cyber threats and execute preventive strategies, despite anticipation being more cost effective and customer centric. As per the estimations of TrendLabs (September 2014).

> *"India posed for cybercriminal expansion with an average of 2.5 million malware detection in a single month. Also, 33 per cent more malicious apps were downloaded and network traffic from affected computers continued to rise"*

Cyber-crime may harm any enterprise, large or small, with an unpredictable degree of severity. Various incidents are not either publicly known or have not been reported by the media. Nevertheless, companies in United States are legally granted the accountability to report incidents to the higher officials. In the past, India used to be a target of cyber attacks for political motivation only.

Objectives of the Study

I. To assess the various cyber attack strategies in Information Technology Firms

ii. To assess the various cyber defense strategies and their correlation with cyber attacks

Review of Literature

The number and sophistication of cyber attacks continues to boost, but no national policy is in place to deal with. Critical systems need to be built on secure grounds, rather than the cheapest general purpose platforms. Spafford (2009) proposed that a program that combines education in cyber security, mounting resources for law enforcement, development of reliable systems for significant applications, and expanding research support in manifold areas of security and reliability is essential to combat cyber threats. Determining the appropriate level of security for a particular system should involve consideration of the magnitude of potential risks, the cost of implementing varying levels of safety, the impact on the functionality of the product and its implications for privacy. Hanacek (1998) studied that electronic money products have the potential to provide important benefits to payment systems if implemented with appropriate security. These systems cannot be made fully secure against all types of attack.

The Government officials and experts are often heard claiming that the world is unprepared for cyber-terrorism. Foltz (2004) examined the reasons for these disparate viewpoints and reviews the theoretical and actual forms in which cyber-terrorism may occur and refocused an existing model of computer security (Cyber-terrorism Computer Security Model) to help understand and defend against cyber-terrorism. The reasons for these disparate viewpoints review the theoretical and actual forms in which cyber-terrorism may occur and refocused an existing model of computer security (Cyber-terrorism Computer Security Model) to help understand and defend against cyber-terrorism. 80% of the security compromises are the result of the actions by an inside, one of the most overlooked threats in a corporate security program, i.e., the employee behavior (Gawde, 2004).

According to Furnelb et al. (1999), 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 additional critical systems. This collective action would do more destruction than the action of a single hacker. Nagpal (2002) examined the tools and methodologies of cyber terrorism such as viruses, worms, Trojans, denial of service attacks and cryptography. It discussed the proactive and reactive legislative measures undertaken by various countries to counter cyber crime in general and cyber terrorism in particular. Further, it focused on some of the major incidents of cyber terrorism that have ravaged the real and virtual worlds in the recent past. Gupta (2003) proposed that deceptive honey pots coupled with appropriate intrusion detection systems and firewalls may provide a means for providing much need forward intelligence about attackers and give defenders an increased reaction and countermeasure time window. Negative impacts such as banking scandals, closure programs due to poor management, and security problems with Internet banking are all undermining credit cardholders' trust in banks Hwang et al. (2003).

Theoretical security fears the level of security that is technically possible; for example, digital signatures offer strong authentication under the assumption that various difficult computational problems related to prime numbers will not be solved within a little time frame (Dourish et al., 2002). Effective security concerns the echelon of security achieved in practice and is usually lower than theoretical security, due to flaws with respect to algorithm implementations, protocol design and ease of use. Cashell et al. (2004) 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. 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. Cyber-terrorism is viewed as a threatening as well as frightening issue.

Rudasill et al. (2004) reviewed the possible cyber-security threats to current military and civilian masses. Analysis of the policy documents showed some similarities in the manner by which national and supra-national political agencies are reacting to the threat of cyber-attack. The study alerted the organizations to possible compromise in the systems with which they deal and provided some understanding of the practices by which the government was reacting to threats. Cybertrust (2005) argued that the problem of information security breaches is two-fold: firstly it is due to the increase in economic and political uncertainty and secondly to the pressure from consumers and regulatory bodies. Hansman et al. (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. The first aspect covers the attack vector and the key behaviour of the attack. The second aspect allows for categorization of the attack targets. Vulnerabilities are categorized in the third dimension and payloads in the fourth. Enamait (2006) addressed that information security must become ingrained into the culture of the organization to ensure security compliance in all facets of the organization. Organizations must begin to envision information security as an overall business problem and embrace the cultural change as well as information security in all aspects of a business by implementing the systems such as ITIL and ISO/IEC 17799 as a foundation for the development of a sound information security process (Enamait, 2006).

Any applications executing on a network have possible vulnerabilities that can be subjugated by system hackers. Developing safety solutions is an ongoing arms race between security professionals and hackers (Simmons et al., 2006). Attack methods are generally unique to the applications or targeted systems, but underlying strategies are common techniques. While the purposes or consequences of attacks varies and are usually meticulous to the domain, the classes of consequences are inadequate. Yeh et al. (2007) identified the gaps between manager perceptions of IS security threats and the security countermeasures adopted by firms by collecting empirical data from 109 Taiwanese organizations. Industry type and organizational use of Information Technology were seen as the two factors that affected the motivation of firms to adopt security countermeasures, but their execution did not necessarily affect the threat perceptions of the managers.

Most of the prior studies were built on western data. Very rare research was done in Indian context. With the advent of recent technology, there is a remarkable growth with array of cyber crime. The previous studies related to the e-Services, Cyber Threats, information security, Cyber Crime and its impact on Information Technology Firms and its businesses are not sufficient to categorize the cyber attack and it does not clearly depict the echelon of cyber crime. Thus, this study will add to further understanding of the extent to which the results in Indian context will be similar to prior studies.

Research Methodology

The present study pertains to the study of impact of cyber attack strategies identified by IT Firms operating in India, which include HCL Technologies, Infosys, L&T Infotech, Tata Consultancy Services and Tech Mahindra as these companies are top-rated among Global IT trade, operating from India (NASSCOM). Survey methodology is used to collect the primary data and it is collected on the basis of questionnaires administered to various respondents of the IT Firms who are looking after the Information Systems in the said organization at various levels. The secondary data was collected from various published reports available nationally or internationally. It also includes portals of Anti Phishing Working Group, KPMG, Accenture, Infosys, Tata Consultancy Services, Ministry of Information Technology (Government of India), Cert-in etc. Stratified Random sampling has been used to collect the primary data. The sample size is 200. The data were collected by means of a structured questionnaire with five point Likert scale. It was based on literature review and developed in a close cooperation with experts from different research fields. The entire Universe includes population of IT Executives working in the sample companies at various positions.

Hypotheses

H0: There is no significant association between cyber attack strategies identified by Information Technology Firms operating in India

H1: There is a significant association between cyber attack strategies identified by Information Technology Firms operating in India

Tools for Analysis

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, possible relationship have been brought out through cross sectional analysis wherever necessary feasible. These relationships have been highlighted by computing the Chi-square (as the data set is non parametric) & Karl Pearson coefficient of correlation.

Analysis of Results

The value of Karl Pearson coefficient of correlation is 0.94 which concludes that there is a positive correlation identified by various companies with Buffer overflow (Table1). Calculated value of χ^2 for 12 degrees of freedom at 5% level of significance is 5.99 and tabulated value of χ^2 is 21.026, which concludes that there is no significant association identified by IT Firms with respect to Buffer Overflow.

Name of the Company	Buffer overflow has been identified by our organization				Total
	Extremely Agree	Quite Agree	Und-ecided	Extremely Disagree	
HCL Technologies	6	9	7	10	32
Tata Consultancy Services	6	5	5	6	22
Infosys	13	15	8	10	46
L&T Infotech	15	13	10	11	49
Tech Mahindra	18	15	11	7	51
Total	58	57	41	44	200
Pearson Chi Square	5.99	Degrees of Freedom	12	Pearson Co-efficient of Correlation	0.94

Table 1 : Cross Tabulation : Company & Buffer Outflow Identification

The value of Karl Pearson coefficient of correlation is -0.112 which concludes that there is a negative correlation identified by various companies with Crafted Input Identification (Table 2).

Name of the Company	Crafted input has been identified by our organization			Total
	Agree	Undecided	Disagree	
HCL Technologies	7	18	7	32
Tata Consultancy Services	7	8	7	22
Infosys	6	15	25	46
L&T Infotech	28	13	8	49
Tech Mahindra	19	13	19	51
Total	77	77	56	200
Pearson Chi Square	34.11 Degrees of Freedom	8	Pearson Co-efficient of Correlation	0.112

Table 2 : Cross Tabulation : Company & Crafted Input Identification

Calculated value of χ^2 for 8 degrees of freedom at 5% level of significance is 34.11 and tabulated value of χ^2 is 15.50, which concludes that there is a significant association identified by IT Firms with respect to Crafted Input Identification (Table 2).

Name of the Company	Spoofing has been identified by our organization				Total
	Extremely Agree	Quite Agree	Undecided	Extremely Disagree	
HCL Technologies	8	8	9	7	32
Tata Consultancy Services	6	6	5	5	22
Infosys	19	10	10	7	46
L&T Infotech	30	7	7	5	49
Tech Mahindra	16	13	10	12	51
Total	79	44	41	36	200
Pearson Chi Square	16.45	Degrees of Freedom	12	Pearson Co-efficient of Correlation	0.152

Table 3 : Cross Tabulation : Company & Spoofing Identification

The value of Karl Pearson coefficient of correlation is -0.152 which concludes that there is a negative correlation identified by various companies with Spoofing (Table 3). Calculated value of χ^2 for 12 degrees of freedom at 5% level of significance is 16.45 and tabulated value of χ^2 is 21.026, which concludes that there is no significant association identified by IT Firms with respect to Spoofing.

Name of the Company	Directory traversal has been identified by our company			Total
	Agree	Undecided	Disagree	
HCL Technologies	10	16	6	32
Tata Consultancy Services	10	5	7	22
Infosys	9	20	17	46
L&T Infotech	17	15	17	49
Tech Mahindra	20	11	20	51
Total	66	67	67	200
Pearson Chi Square	14.02	Degrees of Freedom		8
Pearson Coefficient of Correlation	-0.023			

Table 4 : Cross Tabulation : Company & Directory Traversal Identification

The value of Karl Pearson coefficient of correlation is -0.023 which concludes that there is a negative correlation identified by various companies with Directory Traversal (Table 4). Calculated value of χ^2 for 8 degrees of freedom at 5% level of significance is 14.02 and tabulated value of χ^2 is 15.5, which concludes that there is no significant association identified by IT Firms with respect to Directory Traversal.

Name of the Company	Brute force attack has been identified by our company				Total
	Extremely Agree	Quite Agree	Undecided	Extremely Disagree	
HCL Technologies	13	7	5	7	32
Tata Consultancy Services	5	6	6	5	22
Infosys	27	6	6	7	46
L&T Infotech	16	11	9	13	49
Tech Mahindra	19	11	11	10	51
Total	80	41	37	42	200
Pearson Chi Square	11.9	Degrees of Freedom	12	Pearson Co-efficient of Correlation	-0.007

Table 5 : Cross Tabulation : Company & Brute Force Attack Identification

The value of Karl Pearson coefficient of correlation is -0.007 which concludes that there is anegative correlation identified by various companies with Brute Force Attack (Table 5). Calculated value of χ^2 for 12 degrees of freedom at 5% level of significance is 11.9 and tabulated value of χ^2 is 21.026, which concludes that there is no significant association identified by IT Firms with respect to Brute Force Attack.

Name of the Company	PHP remote file inclusion has been identified by our organization				Total
	Extremely Agree	Quite Agree	Und-ecided	Extremely Disagree	
HCL Technologies	11	5	9	7	32
Tata Consultancy Services	6	5	6	5	22
Infosys	13	10	12	11	46
L&T Infotech	12	8	10	10	40
Tech Mahindra	17	18	11	14	60
Total	59	46	48	47	200
Pearson Chi Square	3.89	Degrees of Freedom	12	Pearson Co-efficient of Correlation	-0.013

Table 6 : Cross Tabulation : Company & PHP Remote File Inclusion Identification

The value of Karl Pearson coefficient of correlation is -0.013 which concludes that there is a negative correlation identified by various companies with PHP Remote File Inclusion (Table 6). Calculated value of χ^2 for 12 degrees of freedom at 5% level of significance is 3.89 and tabulated value of χ^2 is 21.026, which concludes that there is no significant association identified by IT Firms with respect to PHP Remote File Inclusion.

Name of the Company	Cross side scripting has been identified by our organization				Total
	Extremely Agree	Quite Agree	Und-ecided	Extremely Disagree	
HCL Technologies	11	9	6	6	32
Tata Consultancy Services	6	6	5	5	22
Infosys	22	5	5	9	41
L&T Infotech	21	10	9	9	49
Tech Mahindra	15	15	13	13	56
Total	75	45	38	42	200
Pearson Chi Square	10.7	Degrees of Freedom	12	Pearson Co-efficient of Correlation	-0.106

Table 7 : Cross Tabulation : Company & Cross Side Scripting Identification

The value of Karl Pearson coefficient of correlation is -0.106 which concludes that there is a negative correlation identified by various companies with Cross Side Scripting (Table 7). Calculated value of $\chi2$ for 12 degrees of freedom at 5% level of significance is 10.7 and tabulated value of χ^2 is 21.026, which concludes that there is no significant association identified by IT Firms with respect to Cross Side Scripting.

Name of the Company	SQL injection vulnerability has been identified by our organization				Total
	Extremely Agree	Quite Agree	Und-ecided	Extremely Disagree	
HCL Technologies	6	7	10	9	32
Tata Consultancy Services	5	6	7	8	28
Infosys	19	11	5	7	42
L&T Infotech	15	10	8	10	43
Tech Mahindra	14	16	12	13	55
Total	64	50	42	47	200
Pearson Chi Square	11.2	Degrees of Freedom	12	Pearson Co-efficient of Correlation	-0.205

Table 8 : Cross Tabulation : Company & SQL Injection Vulnerability Identification

The value of Karl Pearson coefficient of correlation is -0.205 which concludes that there is a negative correlation identified by various companies with SQL Injection Vulnerability (Table 8). Calculated value of χ^2 for 12 degrees of freedom at 5% level of significance is 11.2 and tabulated value of χ^2 is 21.026, which concludes that there is no significant association identified by IT Firms with respect to SQL Injection Vulnerability.

SN	Proposed Relationship	Results
1	Company - Buffer Outflow	+ve, Accepted
2	Company – Crafted Input	-ve, Rejected
3	Company – Spoofing	-ve, Accepted
4	Company – Directory Traversal	-ve, Accepted
5	Company – Brute Force Attack	-ve, Accepted
6	Company – PHP Remote File Inclusion	-ve, Accepted
7	Company – Cross Side Scripting	-ve, Accepted
8	Company – SQL Injection Vulnerability	-ve, Accepted

Table 9 : Summary of Results for Hypothesis

The variables `Crafted Input`, `Spoofing`, `Directory Traversal`, `Brute Force Attack`, `PHP Remote File Inclusion `, `Cross Side Scripting` and `SQL Injection Vulnerability` are negatively correlated with the dealing of Information Technology firms (Table 9); While, `Buffer Overflow` is positively correlated.

On the basis of chi square results, it has been observed that there is no significant association between cyber crime strategies identified by various firms and `Buffer Overflow`, `Spoofing`, `Directory Traversal`, `Brute Force Attack`, `PHP Remote File Inclusion`, `Cross Side Scripting` and `SQL Injection Vulnerability`; while `Crafted Input` has a significant association. Hence, it can be concluded that there is no significant association between Cyber Crime Strategies identified by various Information Technology firms.

Findings

Today's cyber-criminals occupy numerous complex techniques to pass up detection as they creep quietly into corporate networks to filch intellectual property. Their threats are frequently encoded using multifarious complex algorithms to dodge detection by intrusion deterrence systems. Once they have exploited an object, attackers will try to download and install malware against the compromised system. In several instances, the applied malware is a recently evolved variant that conventional anti-virus solution doesn't yet know about. The various cyber crime strategies have been identified by the IT executives during the study. 61.5 % executives identified deceptions used to gain access to restricted resources (Spoofing). PHP remote file inclusion has been agreed upon by 52.5 % of the respondents which allows 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 60% executives while processing cyber attack patterns. Structured Query Language injection vulnerability has been detected by 50.5% executives. Considering the statistics, it is clearly understood that PHP Remote file inclusion, Spoofing, Cross side scripting, SQL injection vulnerability and brute force attacking strategies are the preferred way of attackers to assault the victims. Information Technology firms should adopt safety measures while processing the transactions, designing the databases & web portals. Confidential and high risk data should be encrypted during transmitting over insecure channels. Operating system and application software logging processes must be enabled on all host and server.

Implications for Academicians and Practitioners

Combating cyber-crime is an emblematic example of a rat race that is of course a challenge thorny to triumph. The least one can do, is to be as learned as achievable. To do so, enterprises need to assess their cyber-crime or IT risk through the eyes of the criminal, and settle on which segments of the enterprise signify the maximum value to the criminal. Therefore, security measures should be installed along the domains of deterrent, detective and response measures. Cyber attacks by their varying characteristics are multifaceted and multidimensional. As cyber-crime evolves into a structured action, the intentions of intruders are no longer restricted to stealing information only, but potentially to interrupt business or conduct espionage on behalf of contending enterprises. Though enterprises recognize the need to protect their Information Technology infrastructure, criminals have often been a step forward at exploiting new susceptibilities in information systems and processes of their target. Pointless to say, target enterprises have been observed wanting when it comes to countering these cyber attacks. With the dawn of hand held computing, intruders are now attacking beyond computers, and targeting mobile handheld devices, such as smart-phones and tablets. Cyber criminals have now taken benefits of the mounting reputation of cell-phone applications and games by implanting malware into them. Despite the growing cyber attack risks, various enterprises have no solutions to deal with these problems or attain acceptable answers. Often, this happens because the former question may be the most difficult to get replied. Cyber threats can be tough to enumerate in terms of likelihood and business impact. As a result, many enterprises do not fully recognize the nature of the risk and tend to inaccurately presume that information security is a technical issue.

Predicting the prospect becomes an assessment of possibilities—the possibility of enhanced defense and better international support compared to the possibility of increased expansion around the world. The latter is positive; the former remain an area for supplementary efforts. It seems secure to say that even if the echelon of loss from financial crime remains stable, the level of loss from IP theft can only boost. The circumstances are not beyond repair, nevertheless, and it is worth asking what would change this scenario. Improved technology measures and stronger defenses could diminish the loss from cyber attacks. Conformity, application of standards and best practices for cyber-security could also cut the cost of cyber attacks.

A Path Ahead...

As the proverb goes 'Prevention is better than cure' many enterprise could find improved value and defense by adopting a precautionary approach to deal with IT associated risks. Adopting a precautionary approach towards cyber-crime threat management, nevertheless, usually requires a cultural shift that starts with board level executives who can integrate cybercrime associated threats risks into the enterprise risk strategy. By doing so, strategic management can quickly initiate to recognize gaps in the existing IT risk management strategy and support an organization wide approach to counter cyber attacks. Further, numerous enterprises adopt a gradual approach towards IT risk management.

References and Links

— *Anderson, R. (1994). Why cryptosystems fail, Communications of the ACM, 37 (11), 32-40.*

— *Apt, K. R., & Olderog, E. R. (1997). Verification of sequential and concurrent programs (2nd Ed.), Springer-Verlag.*

— *Benjamin, R. (1990). Security considerations in communications systems and networks, Proc. IEE, 137, 1-2.*

— *Bryan Foltz, C. (2004). Cyberterrorism, computer crime, and reality. Information Management & Computer Security, 12(2), 154-166.*

— *Canadian Centre for Justice Statistics. (2002). Cyber-crime [electronic Resource]: Issues, Data Sources, and Feasibility of Collecting Police-reported Statistics. Canadian Centre for Justice Statistics.*

— *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.*

— *Cybertrust (2005). Justifying security spending: how to make a business case for information security. Retrieved from http://www.cybertrust.com/media/white_papers/cybertrust_wp_security_spending.pdf accessed on August 13, 2007.*

— *Deloitte (2010). Cyber crime: a clear and present danger combating the fastest growing cyber security threat. Center for Security & Privacy Solutions, Deloitte Development LLC, 1-15.*

— *Dourish, P. & Redmiles, D. (2002). An approach to usable security based on event monitoring and visualization. Proceedings of the 2002 Workshop on New Security Paradigms, ACM Press, New York, 75-81.*

— *Enamait, J. (2006). Information Security as a Business Practice, Retrieved from http://www.infosecwriters.com/text_resources/pdf/JEnamait_IS_Business_Practice.pdf accessed on February 27, 2011.*

— *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.*

— *Gawde, V. (2004). Information systems misuse - threats & countermeasures. Retrieved from http://infosecwriters.com/text_resources/pdf/information_systems_misuse.pdf accessed on February 27, 2011.*

— *Gupta, N. (2003). Improving the effectiveness of deceptive honey nets through an empirical learning approach. Retrieved from http://www.infosecwriters.com/text_resources/pdf/Gupta_Honeynets.pdf accessed on February 27, 2011.*

— *Hanáček, P. (1998). Security of electronic money. In SOFSEM'98: Theory and practice of informatics. Springer Berlin Heidelberg. 107-121.*

— *Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. Computers & Security, 24(1), 31-43.*

— *Hwang, J. J., Yeh, T. C., & Li, J. B. (2003). Securing on-line credit card payments without disclosing privacy information. Computer Standards & Interfaces, 25(2), 119-129.*

— *Kumar, A. (2002). Phishing- a new age weapon. Retrieved from http://www.infosecwriters.com/text_resources/pdf/Phishing-a_new_age_weapon.pdf accessed on February 27, 2011.*

— *Nagpal, R. (2002). Cyber terrorism in the context of globalization, Paper presented at II World Congress on Informatics and Law, Madrid, Spain.*

— *Ottawa Department of Justice (2001). Report to the coordinating committee of senior officials. Federal/Provincial/Territorial working group on illegal and offensive content on the internet.*

— *Simmons, S., Edwards, D., & Wilde, N. (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.*

— *Spafford, E. H. (2009). Cyber Security: Assessing Our Vulnerabilities and Developing an Effective Defense. In Protecting Persons While Protecting the People. Springer Berlin Heidelberg, 20-33.*

— *U.S. Department of Justice (2000). The electronic frontier: The challenge of unlawful conduct involving the use of the Internet. President's Working Group on Unlawful Conduct on the Internet. Retrieved from accessed on July 16, 2008.*

Author Profile

Dr. Atul Bamrara, a prolific author and eminent researcher, is currently Assistant Professor in Quantitative Techniques area at Royal University of Bhutan, Centre for Analytics & Research, Gaeddu College of Business Studies - Bhutan. In addition, he supervises postgraduate dissertations at various Indian Universities, which include Indira Gandhi National Open University, Uttarakhand Technical University and HNB Garhwal University etc. He earned his PhD in Cyber Crime from HNB Garhwal University, India and MBA in Operations Management. His doctoral thesis focused on impact of cyber-crime on electronic banking. Atul is delivering teaching, training and supervising Business and Computer Science students at Under Graduate, Post Graduate and PhD Level since last decade. His academic research interests and publications focus on electronic banking, cyber-crime, logistics and customer relationship management. He has published widely and presented research papers at various conferences and seminars in Asia and Europe.He can be reached at atulbamrara@gmail.com

Professor Lhato Jamba is currently Director General of the Gaeddu College of Business Studies, Gedu, Bhutan. Prior to this, he was Vice Principal of Sherubtse College, Kanglung. He has also served as Program Director of the College for a period of one year to work on the preparation and planning of the new College to enable its launch in July 2008. Under Director General Lhato Jamba's direction the College has developed into a progressive, innovative business and management centre consisting of qualified faculty, enthusiastic students and a community driven by learning environment. His research activities are focused on consumerism and Management Education. He is currently teaching Organizational Behaviour. He is currently the member of Academic Board and Program Quality Committee (PQC) of the Royal University of Bhutan. He can be reached at lhatoj@gmail.com

Professor Alka Rathore is a Senior Lecturer of Marketing at Royal University of Bhutan, Gaeddu College of Business Studies. She holds an MBA degree from UP Technical University and B Sc from Pune University. She has researched and published with Supply Chain Pulse and Bhutan Journal of Research & Development in the areas Women Participation and Supply Chain. Prof Rathore has been delivering lectures to Business and Commerce students at Under Graduate and Post Graduate standard. She also consults for a number of public and private sector organizations in Bhutan and India. She is actively involved in Conferences and publication to journals and books. Her area of expertise includes Business Environment, Marketing Management, International Marketing and Organization Behavior. She can be reached at alkarathore75@gmail.com