THINK INDIA JOURNAL

ISSN:0971-1260
Vol-22- Issue-14-December-2019

Impact Of Various Threats Responsible For The Enhancement Of Cybercrime And Understanding The Effectiveness Of Security Technologies To Consolidate The Cybercrime Incidents Associated With Networked Information Systems

[1]Dr. Pallavi Rani, [2]Dr. Vikas Sharma,
[1, 2] Assistant Professor,
Department of Computer Science,
Govt. PG College, Ambala Cantt
E-mail : pallavimalik56@gmail.com, vsvikas22@gmail.com

ABSTRACT

This research study is based on analysis of the responses to the survey questionnaire, which was Internet based delivery via e-mail as well as information collected personally through Information technology professionals. Moreover, to authenticate the analytical results & findings, data has been collected from the National Technology Readiness Survey, Business Software Alliance, Electronic Privacy Information Center (EPIC), The e-commerce firm, CERT-CC (Computer Emergency Response Team Coordination Center), the Software & Information Industry Association (SIIA), Computer Security Institute, CCRDU, Delhi; Cyber Crime Research Center, and visiting various authentic statistics sites and going through various cybercrime reports. As well researcher interviewed & discussed personally various organizations and individuals/ households who access the internet during the period of research. This paper discusses current and emerging forms of computer-related illegality. It reviews various factors and vulnerabilities responsible for the enhancement of cybercrime that affects the different organization which is related with network systems and to identify and consolidate the cybercrime incidents associated with networked information systems, and to formulate an approach to evaluate illegality involving information systems as instruments or as targets of crime.

1. INTRODUCTION

While there is already a considerable volume of collected works on cybercrime research but still needs to be done to get a sufficient representation of cybercrime, and in particular how we can effectively and competently control it. There has hardly been any organized empirical or investigative work involving long-drawn-out data analysis or modelling although there is now data available on reported cybercrimes and also some data from surveys. Nor has there been any organized exploration of the existing data sources to evaluate their validity and expediency for analysis, or to improve decision making models for policy analysis to reduce cybercrime. Unless we precisely analyze and model cybercrime for this purpose, we shall not be able to get a satisfactorily in depth indulgent of the phenomena that is needed for developing operative policies to counter cybercrime. Therefore, it is perilous that we have more and better statistics and analyses

ISSN:0971-1260
Vol-22- Issue-14-December-2019

to arrive at a well-judged view of cybercrime and a reasonable, effective and resourceful policy to control it. Further, this research paper is distributed in following sections. Requirement of the study provides the introductory information about the research and a brief analysis of the problem was presented in this part. After this we have shown objective of the study & briefly explained research design and methodology. The next to it is exploration of the responses to the survey questionnaire & interpretation of tabular analytical data. The final module of this research paper focuses on the findings & conclusive analysis based on present research.

2. OBJECTIVE OF THE STUDY

The main purpose of the research is to show the various factors and vulnerabilities responsible for the enhancement of cybercrime that affects the different organization which is related with network systems and to identify and consolidate the cybercrime incidents associated with networked information systems, and to formulate a methodology to evaluation of cybercrime incidents Associated with Networked Information Systems. In this paper, the following objectives are matter of concern

- To collect the information about the various threats and their impact related to cybercrime on the Network Information
- Go through the various aspects of cybercrime.
- Analyzing the various data related to cybercrime and security in the network information.
- To suggest how to protect the data information and network resources from threats and to deal with the situation like cyber crime
- Explaining the kind of security technologies are used to decrease the vulnerabilities and to evaluate the effectiveness of Security Technology in cybercrime world.

3. RESEARCH METHODOLOGY

The research was conducted in different phases with development of a questionnaire, sample identification and selection. The researcher poses a series of questions to willing participants; summarizes their responses with percentages, frequency counts, or more sophisticated statistical indexes; and then draws inferences about a particular population from the responses of the sample. The main data collection techniques used in this research study was a questionnaire and secondary source analysis and historical surveys. A random sampling method was used, through the use of a database of e-mail addresses of representatives from different organizations and few individuals interviewed personally. This was done so that the appropriate participant may receive the e-mail and participate in the computer-delivered survey. Another benefit to using e-mail and the computer delivered survey was to enable the researcher to contact participants who might otherwise be unreachable. A random sampling method was used, to achieve the outcomes of an almost precise and accurate statistical result. A sample size of various organizations and individuals were randomly identified and selected those are having internet access. Participants were asked to report on events that they have personally experienced, the reply needs to be assessed carefully. As mentioned in the previous section organizations selected were from different industry sectors, with

ISSN:0971-1260
Vol-22- Issue-14-December-2019

different staff size compliments and income turnovers. The individual participants from the 25 organizations targeted to participate in this research project were mainly people who represented the organisations at management level. The type of organizations, the positions of people who were targeted to participate and the number of questionnaires sent, with the number of respondents. The questionnaire, so that participants can respond to questions with assurance that their responses will be anonymous, and so they may be more truthful than they would be in a personal interview, particularly when they are asked to answer about sensitive or controversial issues. Furthermore, closed-response questions were appropriate as there was a clear frame of reference, the research question in relation to the cybercrime and its effects in information security. The participant's level of information was predictable and the researcher believed that the participant understood the topic. The 't' test was applied to analyze the percentage & prepare statistics.

4. DATA ANALYSIS

The purpose of this part is to present and analyse the research data obtained by means of the secondary sources and the questionnaire used during the survey. The data has been analysed and interpreted to address the above mentioned research objectives.

5.1 Respondents According To Their Designation/ Job Title

The percentages of respondents according to their designation/ job title are given as:

Table 1: percentages of respondents as per designations

Respondents With Designation	Percentage
Principal / Director	10%
Chief Operating Officer	17%
Organization Manager	15%
System analyst	8%
Information Security Officer	11%
IT Manager	18%
Network Administrator	12%
QM Security Manager	13%
Personal Service Advisor	12%
IT Consultant	7%
Others	10%

4.2 Organizations To Which The Respondents Normally Belongs

Table 2: Respondents Organizations

Health	1%
Information Technology	30%
Manufacturing	2%
Education	7%
Banking	10%
Consulting / Business Services	7%
Telecomm/Communication	31%
Financial /Insurance	8%
Real Estate / Social and Personal Services	3%
Business Services	1%

ISSN:0971-1260
Vol-22- Issue-14-December-2019

4.3 Use Of Computer Network Systems To Maintain Data & Keeping The Records

There is a different type of sensitive information regarding customer identification numbers, financial records, personal records, information regarding the scale models, business and marketing plans etc. The chart below shows how important is the kind of information.

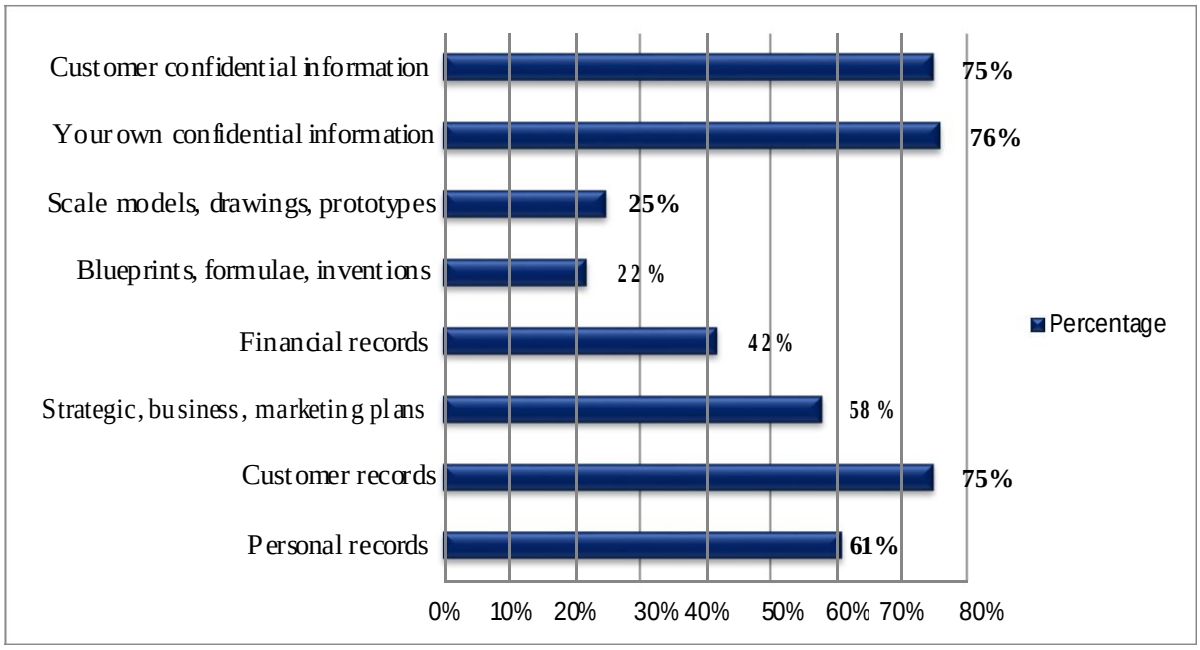
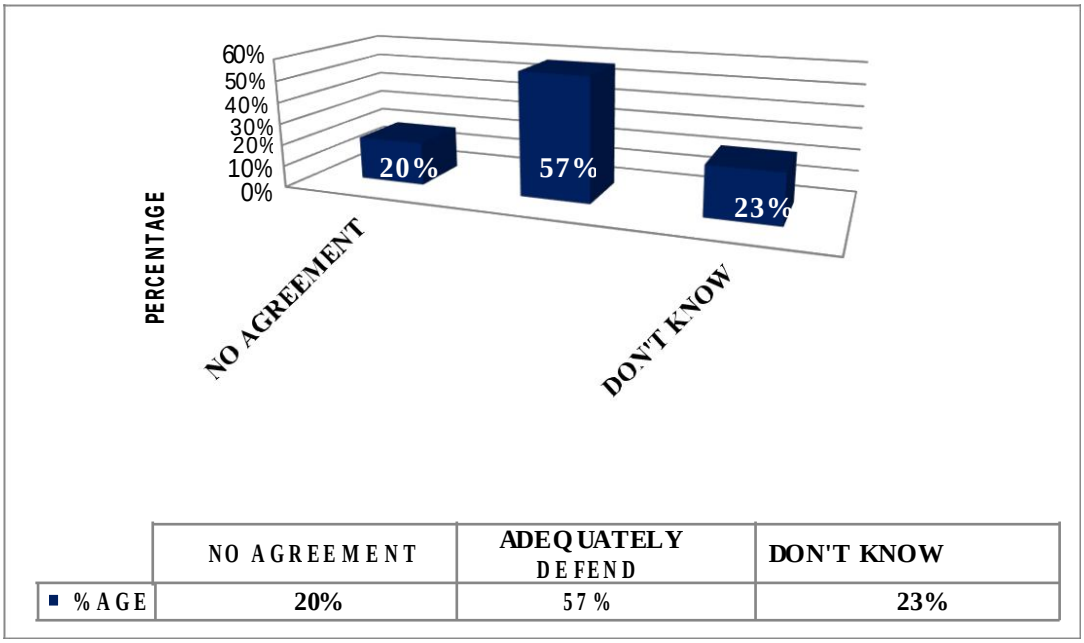


Figure 1: Use of computer network systems to maintain data & keeping the records

4.4 Do Existing Multilateral International Agreements And Efforts Adequately Defend Your Country Against Cyber Violations



	NO AGREEMENT	ADEQUATELY DEFEND	DON'T KNOW
%AGE	20%	57%	23%

Figure 2: Information about Existing Multilateral International Agreements

ISSN:0971-1260
Vol-22- Issue-14-December-2019

4.5 WhatAre The Network Security Standards/Techniques Organisations Have Implemented

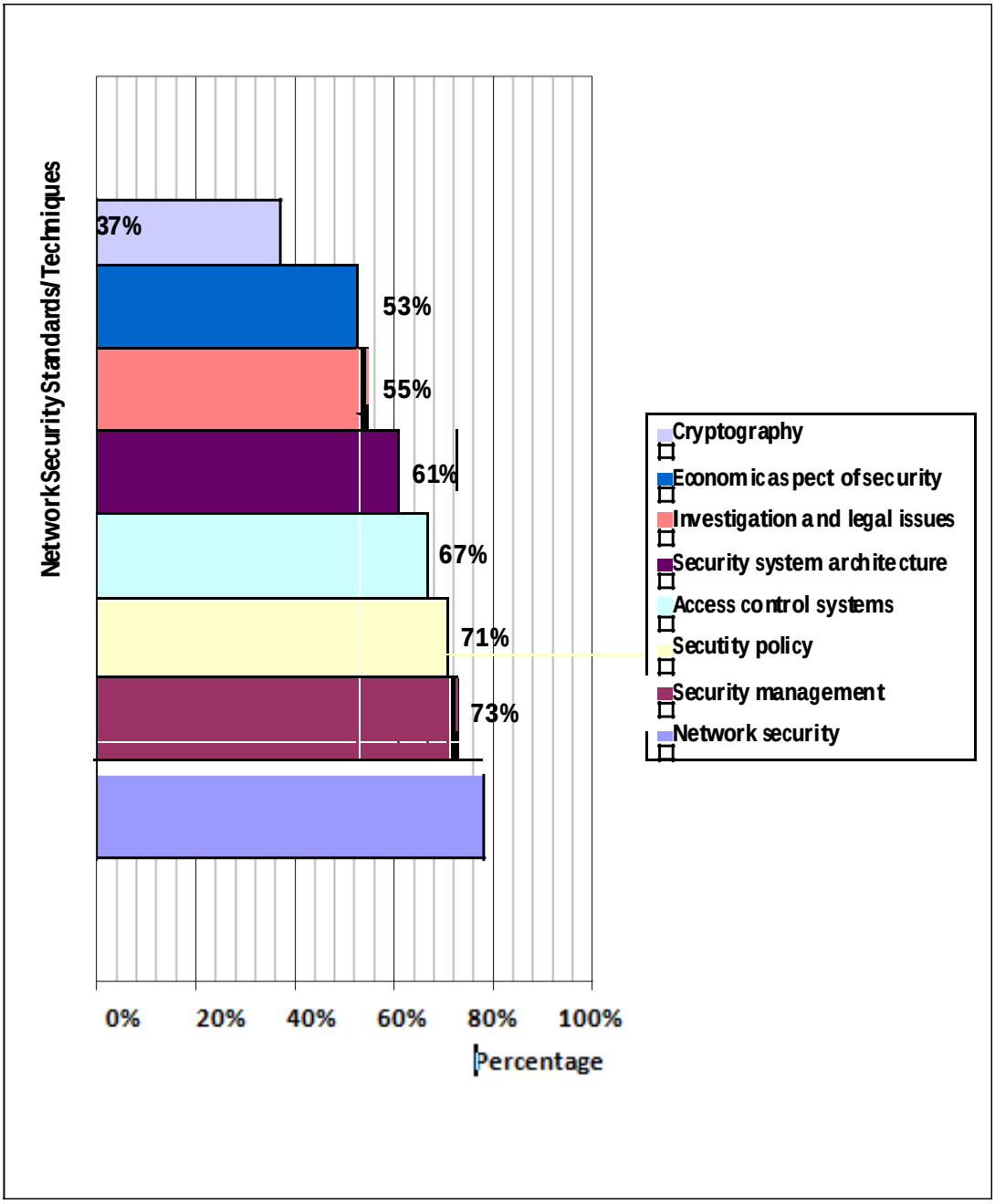


Figure 3: Implementation of network security standards/Techniques

ISSN:0971-1260
Vol-22- Issue-14-December-2019

By asking this question it can be analyzed that how many organizations has implemented the information security standard. From the figure 3 it is clear that 100% of organizations are aware of information security standards and they believe that it is important for every organization to have some information security standards.

5.6 Organisations Experienced Security Incidents in the Past 12 Months?

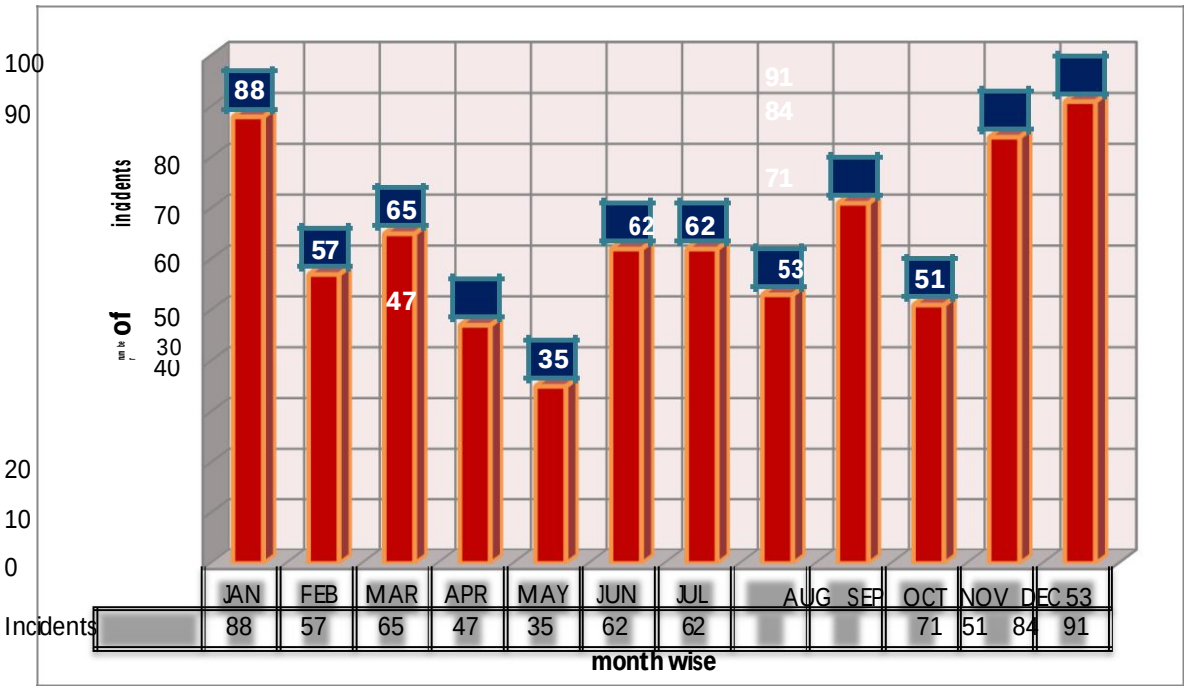


Figure 4: Information Security incidents (Month wise)

4.6 Different Types Of Cyber Security Attacks Faced By Individuals

Cyber Security Attacks	Percentage
Violations against privacy	62%
Insider abuse of Net Access	58%
Virus	55%
Device theft	42%
Phishing	41%
Instant Messaging Misuse	43%
Denial of Service	23%
Unauthorized Access to information	25%
Bots with in the organization	21%
Theft of customer/employee data	23%
Financial Fraud	19%
Password Sniffing	17%
Website Defacement	19%
Theft of Proprietary Information	21%
Misuse of public web application	11%
Exploit of the organization's DNS server	8%
Telecom Fraud	8%
Sabotage	4%
Abuse Of wireless network	16%
System Penetration	13%
Computer-mediated espionage	12%
Worms/ Spams	39%

ISSN:0971-1260
Vol-22- Issue-14-December-2019

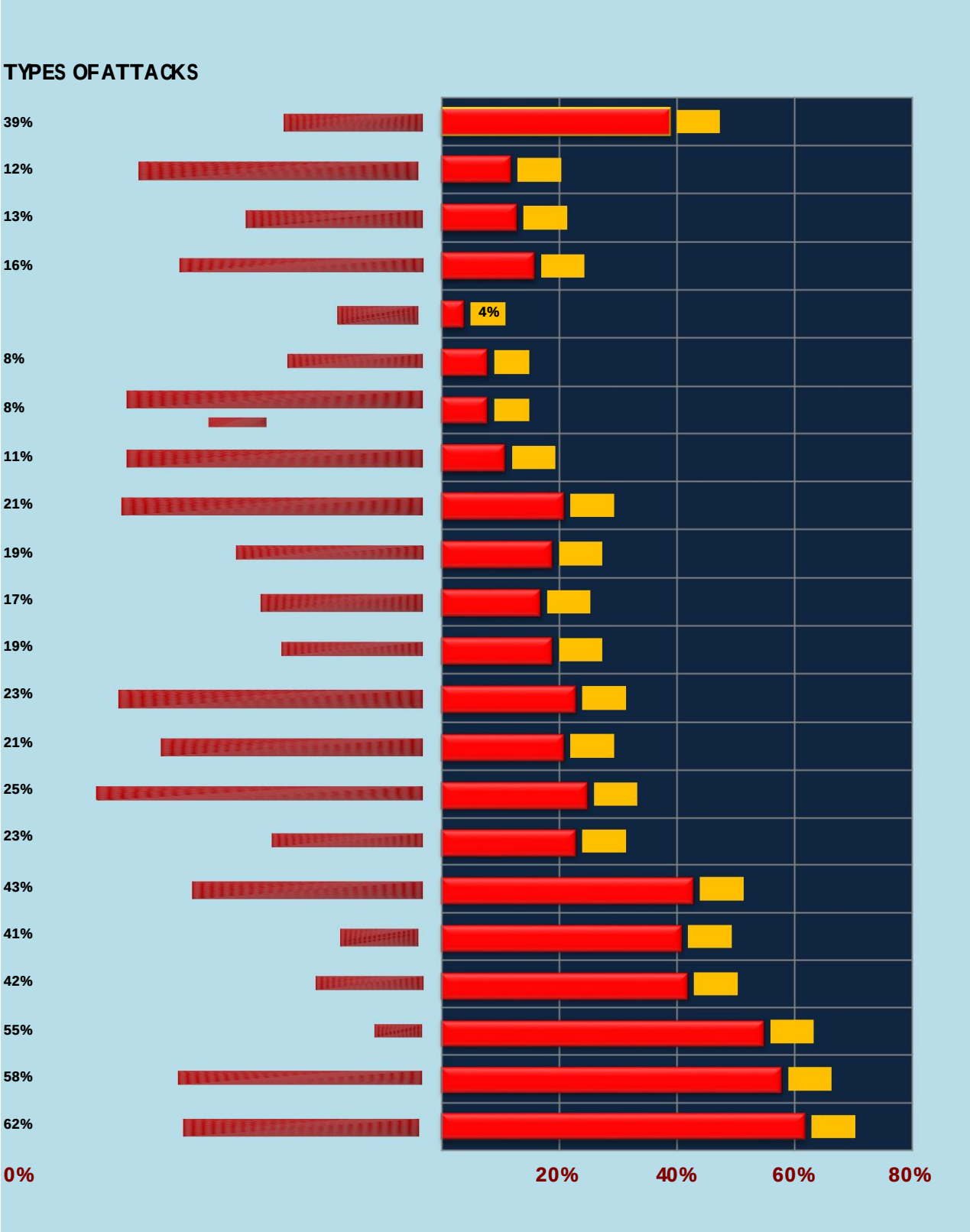


Figure 6: Cyber Security Attacks Faced By Individuals

ISSN:0971-1260
Vol-22- Issue-14-December-2019

4.7 Loss Due To Different Cyber Types Of Cyber Attacks

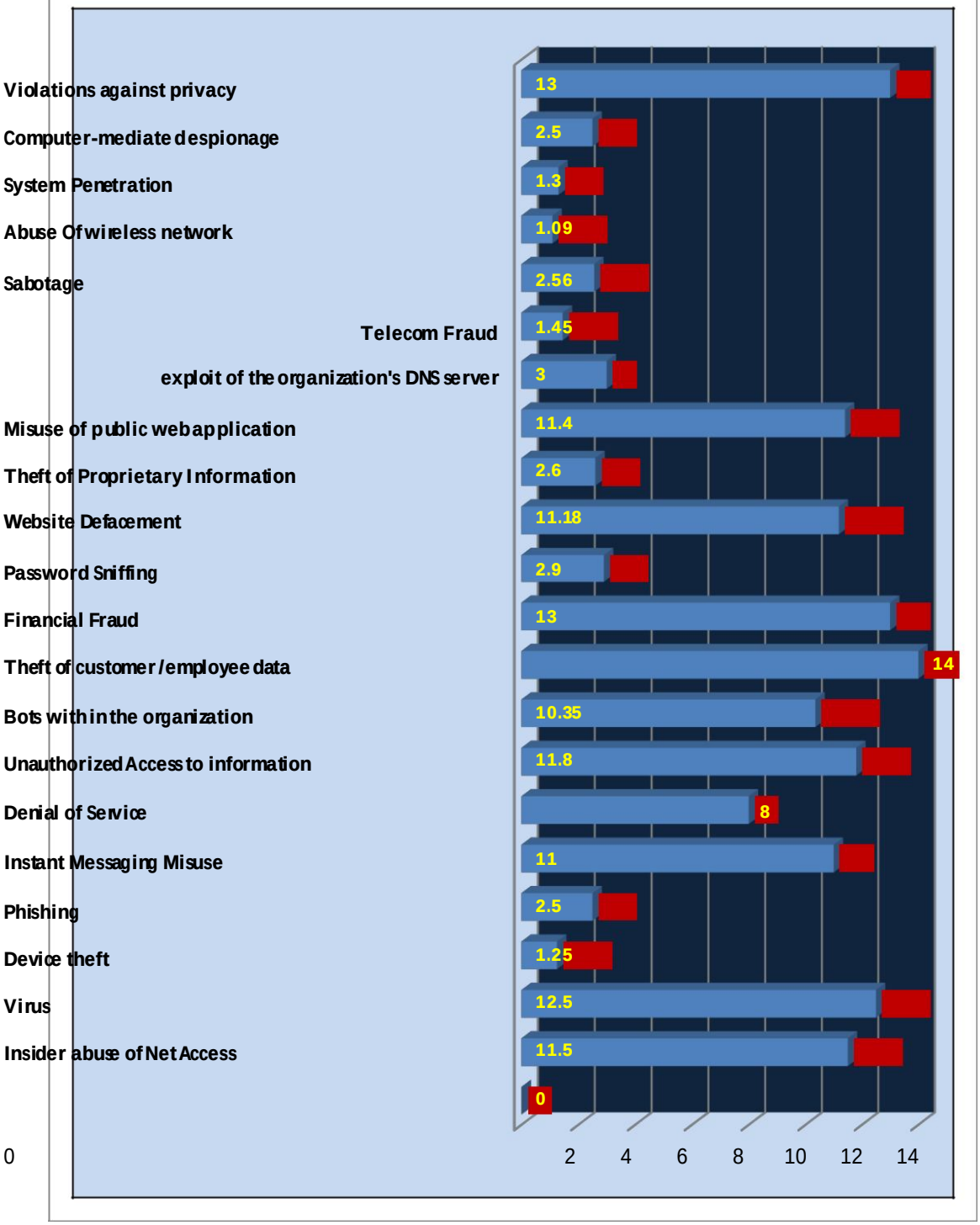
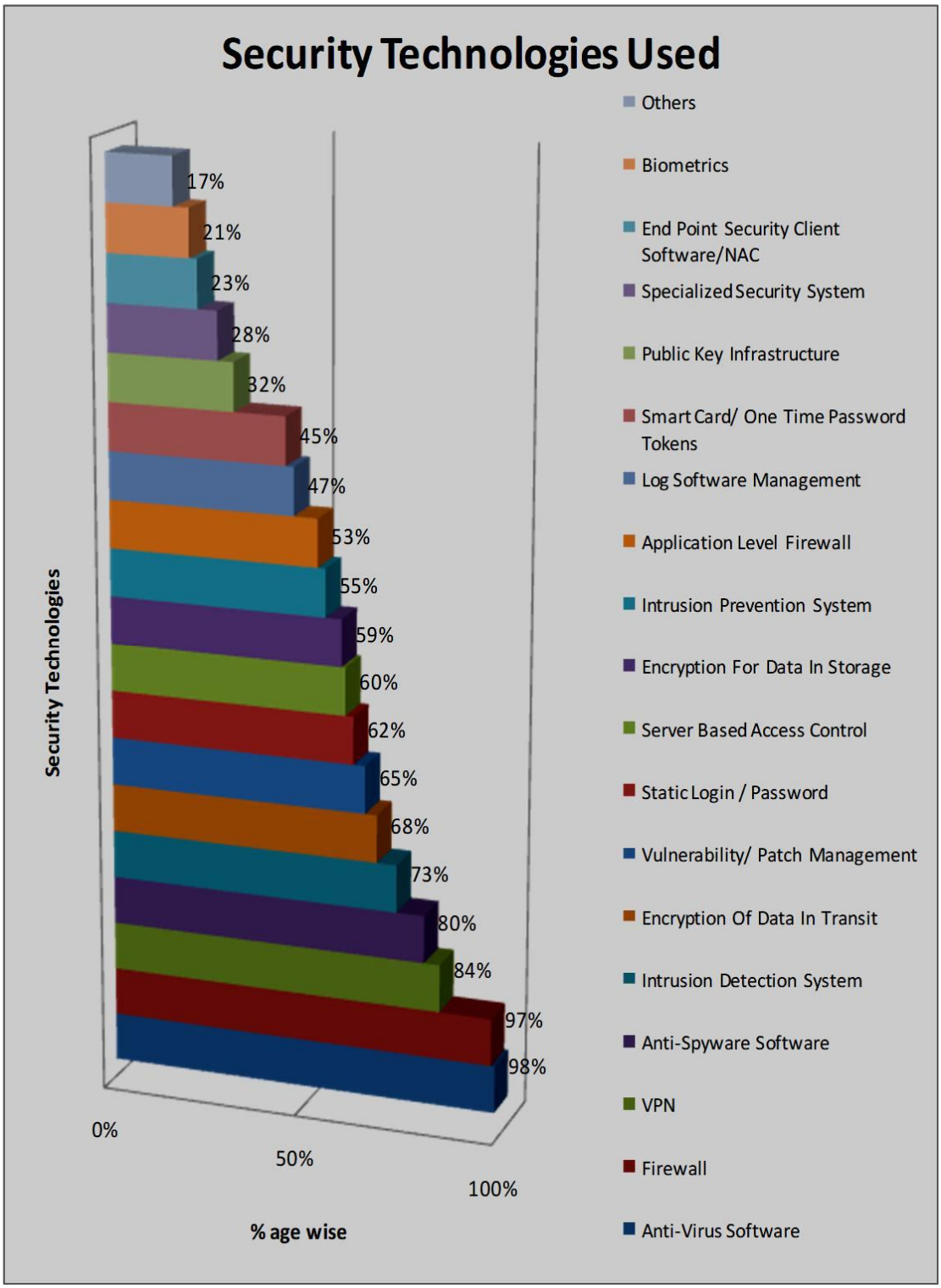


Figure 7: Estimated loss

ISSN:0971-1260
Vol-22- Issue-14-December-2019

5.8 What are the various cyber security technologies used to prevent cyber attacks



4.8 What Kind Of Actions Has Been Taken For The Reported Incidents

ISSN:0971-1260
Vol-22- Issue-14-December-2019

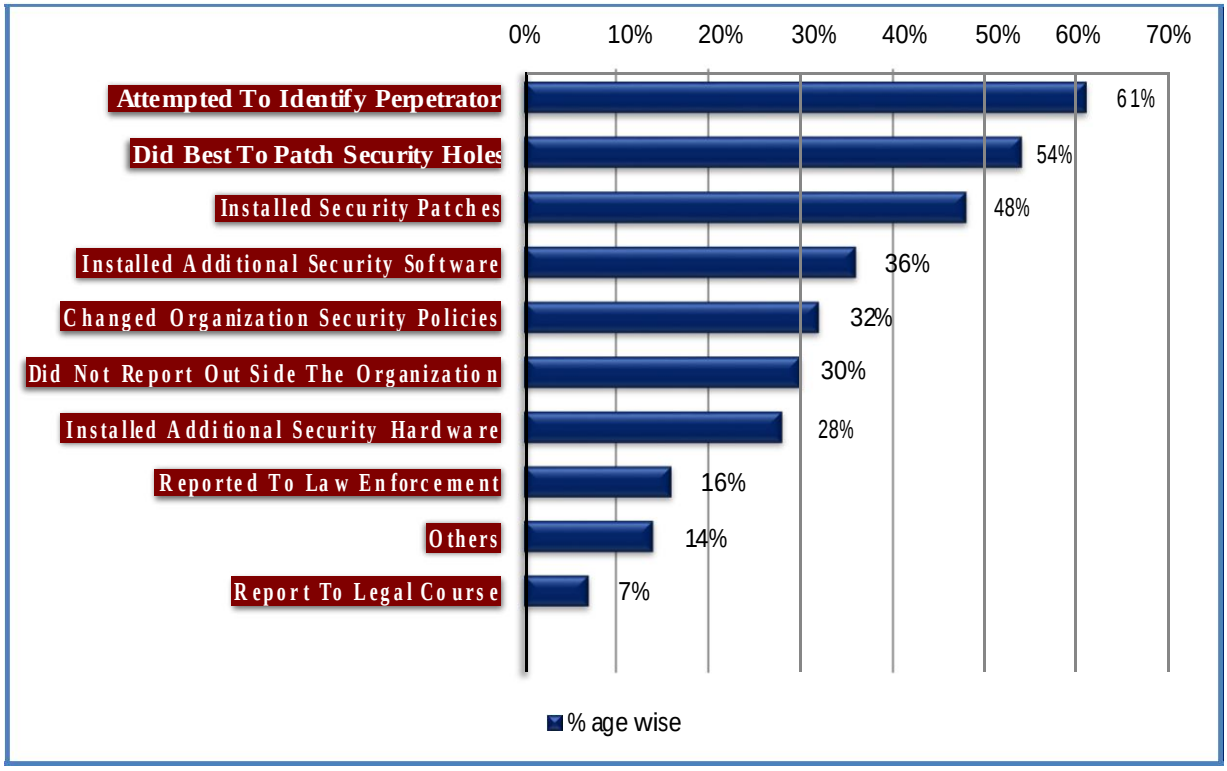


Figure 9: Kind Of Actions Has Been Taken For The Reported Incidents

5. IMPORTANT OUTCOMES

The Table 1 &Table 2, shows the percentage of number of participants as well as to which organization they belongs. It can be seen clearly that 22% respondents belongs telecom/communication sector 19% respondents belongs to IT sector, 12% from education sector, 10% from banking sector, 8% from financial / Insurance as well as Business services & 7 % from consulting services. Only 1 -2 % from health & manufacturing sectors. Figure 1 analysed that whether the organizations are aware of security awareness methods or not. It also rates the important security awareness training which is important for organizations to control cybercrime. It shows the percentages of respondents indicating that which security awareness is important as per there requirements. This chart shows how important is networked information system to store various kind of data. Also, as per the respondent's %age has been calculated. Chart 6 shows the different kind of attacks and their percentage. Such narrowly targeted attacks are becoming more popular than ever. Very close to one-third (32 percent) of those who answered the question about targeted attacks said that at least some of those incidents involved targeted attacks under this definition. It is probably more accurate to compare the number reporting some number of targeted attacks to the number of respondents reporting security incidents overall (asked in the prior question), in which case the result drops to 18 percent. Whatever the costs of identity theft, most of them are not paid by the company that lost the data in the first place, so it's even possible that cybercrime losses could be shooting upward due to costs placed on consumers while enterprise losses were falling. Notwithstanding all the points made above, security professionals observing the state of the "hacker" underworld have long been very concerned about several significant factors likely to change the face of cybercrime within organizations. Additionally, the security measures that organization have taken against their attackers, such as the anti-virus and firewall components discussed above, are fundamentally imperfect. This is because much of the defensive posture of a typical

ISSN:0971-1260
Vol-22- Issue-14-December-2019

organization relies on technologies that attempt to identify known, broadly distributed attacks that have easily recognizable "patterns" in them. This approach of looking for the "signatures" of known threats can often be highly practical, but over time developers of malware (viruses and their ilk) have been gradually increasing the sophistication of their methods and are arriving at points where it is possible to bypass an anti-virus package more or less at will, at least within a limited time frame. Targeted attacks are much harder to detect than conventional mass attacks. This no doubt means that many penetrations of network defenses will go unnoticed either for a very long time or, practically speaking, forever. The survey asks about attacks in two different ways, first in Terms of whether they have occurred at all, and second in terms of financial damages to the organizations where the respondents work.

Chart 7 shows the percentage of loss approximately bears by organizations & respondents calculative. It can be seen that as per the kind of cybercrime the loss varies. It can be seen that people are aware of security technologies. Maximum respondents are aware of anti-Virus software. Most of above 98 % respondents are aware of this. Modernized & high level organizations are having latest technology to cope with cybercrime. Chart 8 shows the actions taken against incidents. Perhaps the most interesting finding among these new answers is that only about one-third of respondents said that their security policies didn't change in the wake of incidents, suggesting that there was no need to create or amend policy, but rather that the policies had been broken or that inside, policy-governed behavior was not a factor in the incident. Among answers that have long been available with this question, one of particular interest has been the percentage that report to law enforcement. Exactly 61% said they have attempted to identify Perpetrator. About 48% to 54% installed security patches. While some have installed additional security software and made change in their security policies. Only 16% has reported to law enforcement. Respondents tell us that they lost more money to cybercrime on average than last year. It is very difficult to predict whether that signals increasing losses in the years ahead, in no small measure because information security professionals won't sit idly by. They will react to shore up their defenses. Nevertheless, the stakes are high and the outlook isn't necessarily comforting. Where will the balance between vulnerabilities and safeguards lie in a year's time? If no more than the status quo of firewalls and anti-virus are maintained, it's hard to foresee anything other than the erosion of enterprise security. Time, of course, will tell. Meanwhile, regardless of the threats and the opportunities, those responsible for computer security have to make their case within their respective organizations: security professionals are increasingly being asked to develop detailed business cases to justify new investments in technologies they need to address the constantly evolving threat. As with any other problem, the more knowledge we have about the causes and consequences, in this case of computer security breaches, as well as the way organizations address computer security issues, the more likely it is that organizations will be able to improve their computer security.

6. CONCLUSION

Technology grounded crimes have been emerging with the passage of each day. And they must be grip with utmost priority. These crimes are not restricted to computers but other electronic devices are made its means such as financial operation machines, telecommunication equipment's and so on. The legislative reforms will be more effective if they would be done according to nature of cybercrime done, so that maximum convictions are possible and no one escapes from the hands of law and courts just due to unavailability of specific law. Developing countries are fighting against cybercrime according to their means but developed countries must feel their responsibility being advanced in technology, and must share the burden of developing countries and

ISSN:0971-1260
Vol-22- Issue-14-December-2019

facilitate them as much as possible because if these crimes are not controlled now it will affect the whole world with a single click. Countries should adopt the corresponding technologymeasures to regulate the investigation of these crimesto gather the evidence of any crime as much as possible.

7. REFERENCES

[1] Furnell, S. (2002). Cybercrime: Vandalizing the information society. London, England: Addison Wesley.
[2] Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. In D. Wall (Ed.), Crime and the Internet (pp. 23–45). London, England: Routledge.
[3] Internet Fraud Complaint Center. (2003). IFCC 2002 Internet fraud report.
[4] Washington, DC: Government Printing Office. Retrieved from http://www.ic3.gov/media/annualreport/2002_ifccreport.pdf
[5] Kabay, M. E. (2001). Studies and surveys of computer crime. Retrieved from http://www.mekabay.com/methodology/crime_stats_methods.pdf
[6] Kaplan, D. (2000). Structural equation modeling: Foundations and extensions.
[7] Kennedy, L. W., & Forde, D. R. (1990). Routine activities and crime: An analysis of victimization in Canada. Criminology, 28, 137–151.
[8] Kowalski, M. (2002). Cyber-crime: Issues, data sources, and feasibility of collecting police-reportedstatistics. Ottawa, Ontario, Canada: Statistics Canada.
[9] Lyng, S. (1990). Edgework: A social psychological analysis of voluntary risk taking. The American Journal of Sociology 95, 851–886.
[10] A. D. Smith, and W. T. Rupp, "Issues in cybersecurity: understanding the potential risks associated with hackers/crackers," Information Management and Computer Security, vol. 10, no. 4, pp. 178-83, 2002.
[11] D. Thomas, and B. D. Loader, "Introduction - Cybercrime: Law Enforcement, Security and Surveillance inthe Information Age," In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Taylor & Francis Group, New York, 2000