COMPARATIVE STUDY OF CYBERCRIME AND ITS PREVENTIVE MEASURE ACROSS DIFFERENTCOUNTRY

[1]Deepanayaki.M, [2]Ashokkumar.P
[1]Associate Professor, [2]II Year MCA
[1 2]Department of Computer Applications,
[1 2]Priyadarshini Engineering College, Vaniyambadi, Vellore, Tamilnadu, India

Abstract: Cybercrimes are responsible for the interruption of normal computer functions and has been known to cause the downfall of many companies and personal entities. This research paper aims to discuss following aspects of Cybercrimes: the definition, why they occur, laws governing them, methods of committing cybercrimes, who they affect, and cybercrime prevention procedures. More specifically, this paper will delve into one main example of cybercrime "hacking". This paper will delay into one main example of cybercrime "

I. INTRODUCTION

In our modern technology-driven age, keeping our personal information private is becoming more difficult. The truth is, highly classified details are becoming more available to public databases, because we are more interconnected than ever. Our data is available for almost anyone to sift throu5gh due to this interconnectivity. This creates a negative stigma that the use of technology is dangerous because practically anyone can access one's private information for a price. Technology continues to promise to ease our daily lives; however, there are dangers of using technology. .

IMPLEMENTATION

By khamla sounnalat. acting Director general national CERT of Laos. ministry of post and telecommunication cybercrime. Legislation and implementation. Octopus conference 2016. 16-18 Nov, 2016 Zstrasbourg, France.

LAW OF CYBER CRIME

In this section of this paper well discusses law and legislation. That governs cybercrime in the united states will highlight some laws and let people know some has that out there to protect amendments to these law keep up with different advancement in technology

Which country

- Japan – 2.25%
- France – 2.35%
- Russia – 3.07%
- Germany – 3.35%
- India – 5.11%

ADVANTAGE

- Improved security of cyberspace.
- Increase in cyber defence.
- Increase in cyber speed.
- Allows more options to save data

DIS-ADVANTAGE

- Improved hacker speed and ability.
- Interconnected computers.
- Improved viruses, malware and worms.
- Increase in "cyberwarefare"possibly.
- More annomitty between hackers.

CYBER LAWS IN INDIA

2012 and 2013, respectively. A total of 422, 601 and 1,337 cases were registered under cyber-crime related sections of In INDIA information technology act 2000 deals with the Indian Penal Code in 2011, 2012 and 2013, respectively. the cybercrime activities /problems. It act 2000 has There has been an annual increase of more than 40 per cent both positive and.

PREPARE YOUR PAPER BEFORE STYLING

Beforeyoubegintoformatyourpaper,firstwriteandsavethecontentasaseparatetextfile.Keepyourtextandgraphicfilesseparateuntilafterthetexthasbeenformattedandstyled.Donotusehardtabs,andlimituseofhardreturnstoonlyonereturnattheendofaparagraph.Donotaddanykindofpaginationanywhereinthepaper.Donotnumbertextheads—thetemplatewilldothatforyou.

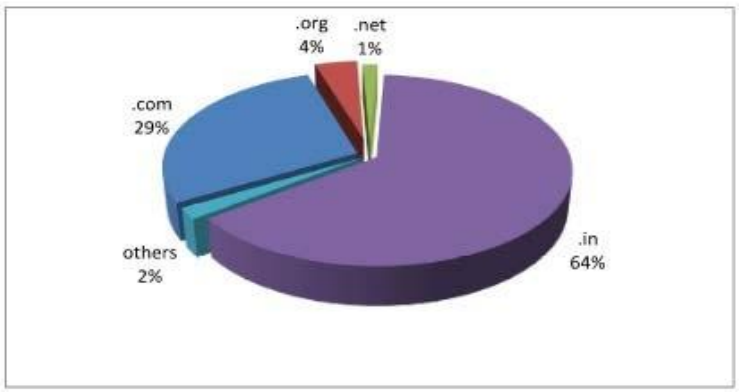
3.1Population and Sample

KSE-100 index is an index of 100 companies selected from 580 companies on the basis of sector leading and market capitalization. It represents almost 80% weight of the total market capitalization of KSE. It reflects different sector company's performance and productivity. It is the performance indicator or benchmark of all listed companies of KSE. So it can be regarded as universe of the study.Non-financial firms listed at KSE-100 Index (74 companies according to the page of KSE visited on 20.5.2015) are treated as universe of the study and the study have selected sample from these companies.

The study comprised of non-financial companies listed at KSE-100 Index and 30 actively traded companies are selected on the bases of market capitalization. And 2015 is taken as base year for KSE-100 index.

3.2 Data and Sources of Data

For this study secondary data has been collected. From the website of KSE the monthly stock prices for the sample firms are obtained from Jan 2010 to Dec 2014. And from the website of SBP the data for the macroeconomic variables are collected for



Period of five years. The time series monthly data is collected on stock prices for sample firmsand relative macroeconomic variables for the period of 5 years. The data collection period is ranging from January 2010 to Dec 2014. Monthly prices of KSE - negative aspects as well. Therefore. 2008. And referred as ITAA 2008.

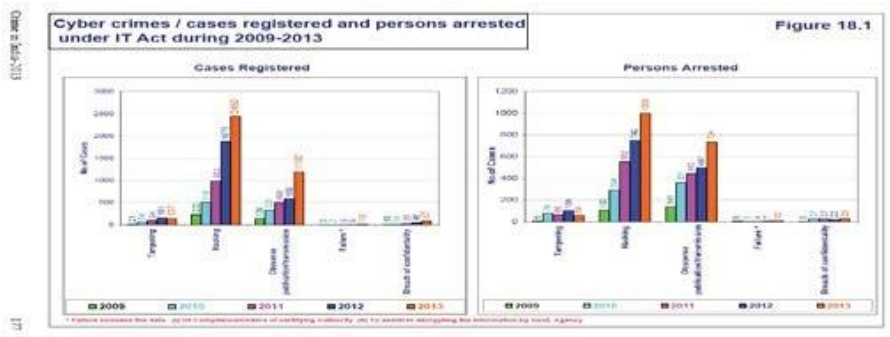
PRESENT TRENDS OF CYBERCRIME IN INDIA

India is trying to implement the Digital India project to the best of its capabilities. The success of Digital India project would depend upon maximum connectivity with minimum cyber security risks. This is also a problem for India as India has a poor track record of cyber security. According to Home Ministry statistics, as many as 71,780 cyber frauds were reported in 2013, while 22,060 such cases were reported in 2012. There have been 62,189 incidents of cyber frauds till June 2014.

In 2013, a total of 28,481 Indian websites were hacked by various hacker groups spread across the globe. The numbers of hacking incidents were 27,605 in 2012 and 21,699 in 2011.

US Cyber Crime Laws: An Exordium

The Wire Fraud Statute being the first law used to prosecute computer criminals in the USA. It was seen that the communication wires were used in international commerce to commit fraud. To overcome such US passed the Law so as to prohibit the use of communication wires.



This was an effective statute as it was to overcome defrauders trying to obtain money, property by false representation or promise; modus operandi being radio or television communication, signs or signals

Criminal Wrong

Section 65 –Tampering with computer Source Documents, imprisonment up to 3 years or fine which may extend to two lakh rupees or both.	Sec 66E – Punishment for violation of privacy, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees or both.
Sec 66 – Computer Related Offences with reference to section 43, punishable with imprisonment for a term which may extend to 3 years or with fine which may extend to five lakh rupees or both. This section has reference to IPC for some definitions.	Sec 66F – Punishment for cyber terrorism, shall be punishable with imprisonment which may extend to imprisonment for life.

- **Criminal Intimidation by E-Mail or Chat**

  Sec 506 – Punishment for criminal intimidation
  Sec 507- Criminal Intimidation by an anonymous communication

- Online Sale of Drugs, NDPS Act
- Online Sale of Arms Act
- Piracy – In Copyright Act

Children and adolescents between the age group of 6 – 18 years

The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other children in their group. Further the reasons may be psychological even. E.g. the Bal Bharati (Delhi) case was the outcome of harassment of the delinquent by his friends.

Types of criminal conduct in cyberspace

Cybercrimes on Social Media Sector

In Nigeria, Social networks have gained a very high ground in every sector. The banking industry, government, business, universities use this platform to promote and communicate with each other. Social networking sites such as Facebook, Twitter, LinkedIn and Instagram serve as a fertile ground for cybercriminals to launch new attacks. Users create semi-public profiles and can directly communicate with friends without restriction (Michael, 2014).

CYBER ETHICS

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way?

The South African effort in combatting cyber attacks

Since the mid-1990s, South Africa has taken the first steps to protect its information. It has passed legislation such as the *South African Constitution of 1996* to protect privacy. In 2000, the *PAIA (Promotion of Access to Information Act) No 2 as amended* was passed to give effect to Section 32 of the Constitution, subject to justifiable limitations (PAIA Act 2000). These limitations are aimed at the reasonable protection of privacy, commercial confidentiality and good governance in a manner that balances the right of access to information with any other rights, including the rights in the Bill of Rights in Chapter 2 of the Constitution (SA Constitution 1996). Linked to this Act is the PAIA Reg 187 Regulations regarding the promotion of information of access to information (Government Gazette 2003).

The collaborative international cyber defense effort

Cyber warfare is an emerging form of warfare not explicitly addressed by existing international law. While most agree that legal restrictions should apply to cyber warfare, the international community has yet to reach consensus on how International Humanitarian Law (IHL) applies to this new form of conflict (Kelsey 2008). In particular, there is a need for an international consensus on the due diligence criteria which have to be fulfilled by a State in order to avoid international responsibility for failing to protecting other sovereigns from cyber-attacks conducted from its territory

ROLE OF SOCIAL MEDIA IN CYBER SECURITY

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack.

CYBER SECURITY TECHNIQUES

Access control and password security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

Authentication of data

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti virus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.

Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

Firewalls

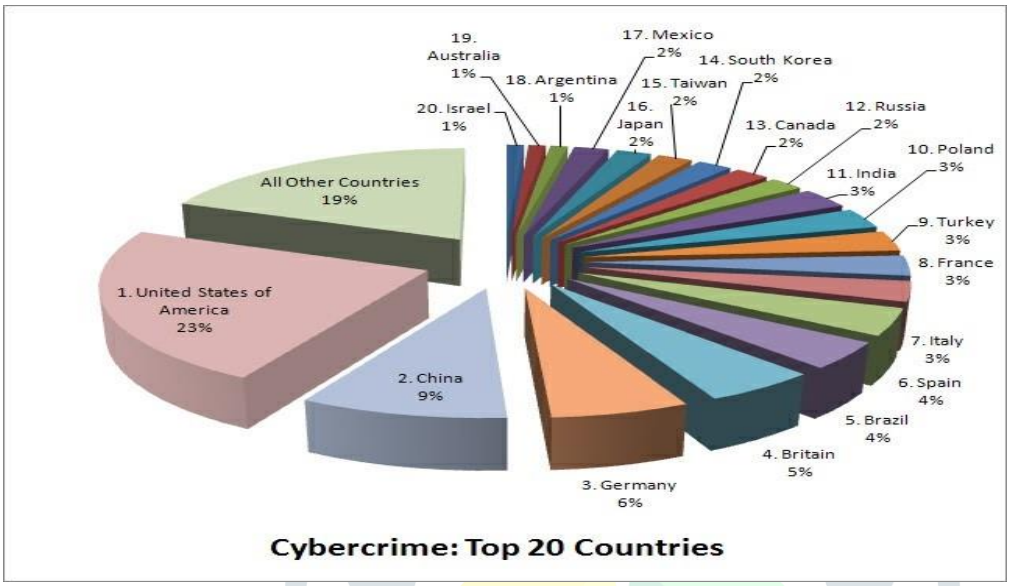
A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

Anti-virus software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software program.

LIST OF TOP 20 COUNTRIES WITH THE HIGHEST RATE OF CYBERCRIME

Each country lists 6 contributing factors, share of malicious computer activity, malicious code rank, spam zombies rank, phishing web site hosts rank, bot rank and attack origin, to substantiate its cybercrime ranking



INDIA

Share of malicious computer activity: 3%
Malicious code rank: 3
Spam zombies rank: 11
Phishing web site hosts rank: 22
Bot rank: 20
Attack origin rank: 19

RUSSIA

Share of malicious computer activity: 2%
Malicious code rank: 18
Spam zombies rank: 7
Phishing web site hosts rank: 7
Bot rank: 17
Attack origin rank: 14

BRAZIL

Share of malicious computer activity: 4%
Malicious code rank: 16
Spam zombies rank: 1
Phishing web site hosts rank: 16
Bot rank: 5
Attack origin rank: 9

SPAIN

Share of malicious computer activity: 4%
Malicious code rank: 10
Spam zombies rank: 8

Phishing web site hosts rank: 13

ITALY

Share of malicious computer activity: 3%
Malicious code rank: 11
Spam zombies rank: 6
Phishing web site hosts rank: 14
Bot rank: 6
Attack origin rank: 8

FRANCE

Share of malicious computer activity: 3%
Malicious code rank: 8
Spam zombies rank: 14
Phishing web site hosts rank: 9
Bot rank: 10
Attack origin rank: 5

International Responses to Cyber Crime

1.E-mail correspondence with Susan Brenner, March 6, 2000.
2.The alternative is for a state court to rely upon federal statutes, such as 18 U.S.C. § 1030, to prosecute computer crimes occurring wholly within its territory.
3.Brenner notes, for example, that Oklahoma state law was used in the federal court prosecution of Terry Nichols, one of the suspected perpetrators of the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City.

CONCLUSION

Cybercrimes will always be an ongoing challenge despite the advancements being made by numerous countries.Cybercrimeswill always be an ongoing challenge despite the advancements being made by numerous countries. Most countries have their own laws to combat cybercrimes, but some doesn't have any new laws but solely relies on standard terrestrial law to prosecute these crimes. Along with outdated laws to combat cybercrime, there are still feeble penalties set in place to punish criminals, thus doing no major prevention of cybercrimes' which affect the economy and people's social lives on a large scale by those criminals. Consequently, there is a desperate need for countries on a global scale to come together and decide on what constitute a cybercrime, and develop ways in which to persecute criminals across different countries.

REFERENCES

[1] Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India,New Delhi, India.

[2] Cyber Law & Information Technology (2011) by Talwant Singh, Additional District & Sessions Judge, New Delhi, India.

[3] Introduction to Indian Cyber Law (2008) by Rohas Nagpal, Asian School of Cyber Laws, Pune, India

[4] Cyber Crime (2003) by R.K. Suri and T.N. Chhabra, Pentagon Press, New Delhi, India. [5] http://en.wikipedia.org/wiki/Computer_crime

Hassan, A. B. Lass F. D. and Makinde J. (2012) Cybercrime in Nigeria: Causes, Effects and the Way Out, ARPN Journal of Science and Technology, vol. VOL. 2(7), 626 – 631. Lakshmi P. andIshwarya M. (2015), Cyber Crime: Prevention & Detection," International Journal of Advanced Research in Computer and Communication Engineering, vol. Vol. 4(3). Maitanmi, O. Ogunlere, S. andAyinde S. (2013), Impact of Cyber Crimes on Nigerian Economy, The International Journal of Engineering and Science (IJES, vol. vol 2(4), 45–51.

6]. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.

[7]. CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar. Crow, K. (2002). Collaboration. Available from: http://www.npd-solutions.com/ collaboration.html (Accessed 23 May 2011). Da Silva, I. S. (2011). Cybercrime increase worries, vulnerable groups targeted. Available from: http://m.bizcommunity.com/Article/196/19/64855.html (Accessed 1 February 2012) Dhlamini IZ. Cyber Security Awareness Initiatives in South Africa: A Synergy Approach. Avalable from http://researchspace.csir.co.za/dspace/bitstream/10204/5941 /1/Dlamini_2012.pdf (Accessed 12 June 2013)

Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 IJSER © 2012 [2] Abraham D. Sofaer, David Clark, Whitfield Diffie ,Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/catalog/12997.htmlCyber Security and International Agreements ,Internet Corporation for Assigned Names and Numbers pg185-205