An Overview of Corporate Cybercrime in India and US
Tanya Syngle
Sacred Heart Senior Secondary School, Chandigarh, India
#111, Sector 23-A, Chandigarh 160023, India
tanyasyngle@gmail.com

Abstract
Cybercrime perpetrated by pockets of citizens is posing a serious threat to international security and economy. Recognizing the lack of any global cooperation on this issue, this paper provides a comprehensive comparative analysis of cyber crime in the corporate sector of the East with India serving as the prototype, and the West, with United States of America (US) being the prototype using an interpretive qualitative research design. Such an analysis would facilitate better understanding of the cybercrime scenario, highlight the differences between the two countries and explore the probable reasons behind them and provides a policy framework for international cooperation in combating cybercrime. The frequency of cybercrime in the two countries is similar despite more enterprises in the US making it a board priority and allocating huge resources for cyber security. There is a vastly different make-up of cyber crime in the two countries in terms of frequency of cyber crime and demography of cyber criminals. The variance in the profile of the cyber minds could be an important factor for the identified differences in cybercrime in the two countries. These differences are helpful in developing such a policy environment that will act as an effective deterrent to the menace of cybercrime.

Keywords:
Comparative analysis; Cyber attacks; Cyber crime pattern; Corporate sector; Cyber criminal

1. INTRODUCTION
In the twenty first century, technology has progressed by leaps and bounds with technology becoming an inseparable unit in all sectors. In corporate sector especially technology has facilitated ease of function, accuracy, optimal time utilization and massive reduction in human labor [1]. However, cyber crime, a negative consequence of this technological advancement, now threatens to overshadow its benefits. Cybercrime is a broad range of illegal digital activities to target an individual or an organization in order to cause harm ranging from mere web site defacements to grave activities such as service disruptions that impact business revenues and misappropriate funds. The high level of insecurity on the Internet is leading to loss of confidence in online transactions. Cyber security incidents are not only increasing in number, they are also becoming progressively destructive and target a broadening array of information and attack vectors [2]. It is clear that adversaries continue to advance their threats, techniques, and targets. New research suggests that cyber crime will cost businesses over $2
trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015 [3]. Hence, Cyber-security is no longer a consideration but a compulsion. Cyber-security assures protection of assets, which include data, computers and computer networks.

India enjoys the dubious distinction of being the favorite among cybercriminals, mostly hackers and other malicious users who use the internet to commit crimes such as identity theft, spamming, phishing and other types of fraud [4]. The situation is not any different in the West either. Cybercrime is the top national security threat, higher than that of terrorism, espionage, and weapons of mass destruction in US [5]. This paper provides a comparison of the current published evidence on cyber crime in India and US. This paper:

- Juxtaposes a comprehensive database regarding cyber crime in India and US.
- Analyses the difference in patterns and trend of the two countries.
- Explores probable causes behind the patterns.

This would help us to become forewarned, forearmed and develop effective collaborative strategies and policies to provide a strong deterrent to the menace of cybercrime.

2. RESEARCH METHOD

The search was based on secondary data accumulation. The data was obtained from various journals, articles, surveys and reports. Secondary research depicts information obtained from literature, broadcast media, publications, and other nonhuman origins. The data analysis done in this study was based on an interpretive qualitative research design. The relevance of the research topic and year of publishing of the literature were taken into consideration for choosing the literature. Three types of searches were carried out.

**High-Level General Searches:** These were carried out to quickly gather literature relating to the cybercrime scenario in the two countries.

**Directed searches:** These searches were carried out in both public and private libraries as well as online databases like Springer, Elsevier, SAGE and so on and search engines like Google and Yahoo by using the following keywords: (cyber crime survey, US, 2015), (cyber crime survey, India, 2015), (global cyber crime survey 2015) and (cyber crime surveys, 2015).

**Snowball’ Searches:** In these searches, the reference lists of retrieved articles were studied for additional information to identify other potential sources of information.

3. RESULTS

After analyzing the data based on India and US, comparisons were drawn on the parameters judged to be essential in the process of understanding and combating cybercrime. First, the three main factors of understanding cybercrime pattern of a particular region under consideration in the present study i.e., frequency of cyber attacks, nature of attacks and profile of cyber mind, were determined after which the response of business organizations was analyzed (table 1).
Table 1. Cybercrime Pattern & Response of Organization in India & US (2015)

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Parameters of comparison</th>
<th>India (%)</th>
<th>US (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Frequency Of Cyber Attacks</td>
<td>72</td>
<td>79</td>
</tr>
<tr>
<td>2</td>
<td>Nature of Attacks Faced By Companies</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Malware</td>
<td>61</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>• Social Engineering</td>
<td>41</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>• Exploits of Vulnerability</td>
<td>39</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>• Cyber Espionage</td>
<td>26</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>• Distributed Denial of Service (DDoS)</td>
<td>19</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>• Wire fraud</td>
<td>-</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>• Phishing</td>
<td>-</td>
<td>&gt;31</td>
</tr>
<tr>
<td></td>
<td>• Others</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Profile of Cyber mind</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• External perpetrators</td>
<td>27</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>• Internal perpetrators</td>
<td>17</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>• Both external and internal perpetrators</td>
<td>56</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>• Unidentified perpetrators</td>
<td>0</td>
<td>23</td>
</tr>
<tr>
<td>4</td>
<td>Response of Organizations</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Priority of Board</td>
<td>23</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>• Board Engagement in Cyber Risks</td>
<td>41</td>
<td>15-25</td>
</tr>
<tr>
<td></td>
<td>• Annual Cybercrime Risk Assessment</td>
<td>26</td>
<td>26-30</td>
</tr>
<tr>
<td></td>
<td>• Allocation of Funds To Combat Cyber Crime</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>➢ Organizations allocating funds</td>
<td>2-58</td>
<td>69</td>
</tr>
<tr>
<td></td>
<td>➢ Amount allocated</td>
<td>5-20</td>
<td>-</td>
</tr>
</tbody>
</table>

Source: [6], [7]

3.1 Frequency Of Cyber Attacks

Over the years, the frequency of cyber attacks has increased all over the world. In India, 72% companies faced a cyber attack within 12 months while in US, 79% companies were attacked within the time duration [6]. Also in both countries, many attacks go unreported because of lack of detection by the attacked party so the real tally is expected to be higher than this [7].
3.2 Nature of Attacks Faced By Companies

There are various forms of cybercrimes with varying modus operandi and intentions. In India, the most frequent form is Malware (61%) followed by Social Engineering (41%), Exploits of Vulnerability (39%), Cyber Espionage (26%) and Distributed Denial of Service (DDoS) (19%). Other forms make up 10% of the nature of cybercrimes faced in India [6]. In US, in 2014, the most reported form was Phishing (31%) and other common forms are wire fraud (21%), DDoS (18%), Ransomware, a type of malware (13%)[7].

3.3 Profile of Cybermind

There are various intentions behind a cyber attack. The profile of the cyber criminal is a big factor in determining the intent and form of cyber attack. In India, 17% are internal perpetrators whereas 27% are external perpetrators. However, 56% believe that both internal and external perpetrators are guilty. The external perpetrators in India include Script kiddies, Professional hackers/hackers for hire, Hacktivist, Cyber terrorist, Malware engineers, Spammers, phishers and online scamsters. The internal perpetrators include but are not limited to disgruntled employees or employees with malicious or criminal intent [6]. In contrast in US, the greatest cyber threat to organizations is from external perpetrators (49%) while internal perpetrators (12%) account for a smaller number. However, a large number of organizations have yet to identify the perpetrators (23%). The external perpetrators in US include Hackers (25%), Organized crime (10%), Foreign nation states (8%) and Hactivists (6%). The internal perpetrators include current employees [7].

3.4 Priority of Board

Cyber crime is an all-encompassing threat that needs to be taken seriously. Only by prioritizing cyber security can the issue of cyber crime be dealt with seriously.

In India, only 23% companies put cyber risk management on The Board of Directors’ top 10
organizational priorities [6]. Contrary to this, 75% of US chief executives (respondent) ranked cyber security solutions as “very important” to the company’s business strategy [8].

3.5 Board Engagement in Cyber Risks
Cyber crime risk management needs to be recognized as an all encompassing risk and hence should be included in board agenda. In India, Cybercrime risk management is part of board agenda in some organizations (41%) [6]. In US, the full Board of directors is engaged in cyber risk management in only 25% organizations. It is a part of the Audit Committee in 15% and part of the Risk Committee in only 24%. But in 30% it is not a part of any Board Committee [7].

3.6 Annual Cybercrime Risk Assessment
Annual cyber crime risk assessment is an important strategy for combating cyber threat. However in India, 26% companies carry out a detailed annual cyber risk assessment [6]. In US, in 26% companies Chief Information Security Officer (CISO) or Chief Security Officer (CSO) makes a security presentation to the Board annually, in 30% Senior security executive makes quarterly security presentations and in 28% no such presentations are made [7].

3.7 Allocation of Funds To Combat Cyber Crime
After recognizing this threat and its pattern, the next important step is to combat this issue. This requires a lot of commitment, experience, resources and funds. In India, 58% organizations spend less than 5% of information technology (IT), 31% spend 5-10% of IT, 9% spend 11-20% of IT and only 2% spend more than 11-20% of IT [6]. Majority of the US firms (69%) have allocated more funds towards investment in cyber security technologies more than any other spending category [8]. US information security budgets have grown at a rate almost double of that of IT budgets over the last two years [9]. Further the cyber risk management spending priorities are predetermined in US. For 47% of the organizations adding new technologies is a priority, for 40% auditing and assessments, for 33% harnessing new skills and capabilities, for 24% redesigning cyber security strategy, for 15% redesigning processes and for 15% participating in knowledge sharing is a priority [7].

3.8 Adequacy of Cybercrime Response Organizations
Adequacy and efficiency of cyber crime response of organizations is also an important factor in combating this threat. In India, 72% companies think that there are not enough cybercrime response organizations in the country to tackle cyber-related issues while 28% companies think that there are enough cybercrime response organizations in the country [6]. In US, only 25% organizations are involved with Information Sharing and Analysis Centers (ISACs)[10].

4 DISCUSSION
Over the past few years, the global cyber crime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security. In general, cyber crime reported to law enforcement authorities is merely 5 - 10%, which is just the tip of the iceberg [2]. There are several reasons as to why cyber crime is not reported varying from ignorance of a cyber incident to preventing its public exposure. Computers and the Internet are now an integral part of our lives. We may not see them often, but they are involved in some way in almost all our daily activities like healthcare, communications, entertainment, business, education, governance, etc. Without the support of any of these tools, we would not be able to handle the overwhelming amount of information that seems to characterize our society. However, the cyber security limits the integrity of information and computer systems. Security of the cyberspace is threatened by cyber crime. The frequency of cyber attacks appears to be similar in East vs. West (72% versus 79%). Hence, there is gross underreporting and underestimation of the true picture of cyber crime scenario in both countries. It is surprising that despite the similar frequency of cyber attacks in India and US, there is vast difference in the nature of attacks faced by companies in the two regions. The most frequent nature of attack in India is malware (61%) whereas the most reported from US is phishing (31%). Other forms of cybercrime in India are social engineering (41%), exploits of vulnerability (34%), cyber espionage (26%) while the other common attacks faced in US are wire fraud (21%) and ransomware (13%). Malware is software that takes control of any individual’s computer to spread a bug to other people’s devices or social networking profiles [11]. Social engineering is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures [12]. Vulnerability is a flaw in a system, or in some software in a system that could provide an attacker with a way to bypass the security infrastructure of the host operating system or of the software itself. Exploiting is the act of trying to turn vulnerability into an actual way to breach a system [13]. Cyber espionage is the act of engaging in an attack or series of attacks that let an unauthorized user or users view classified material. The goal is typically to acquire intellectual property or government secrets [14]. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason [15]. Mail and wire fraud is any fraudulent scheme for obtaining money or property by means of false or fraudulent pretenses via mail or wire communication [16]. Ransomware is malware for data kidnapping, an exploit in which the attacker encrypts the victim's data and demands payment for the decryption key [17]. A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources [18]. DDoS
appears to be the only common nature of attack faced by the two countries that too in similar frequencies (18% & 19%). Also while US is targeted by phishing attacks, a type of social engineering attack, India, on the other hand, is subject to a broad spectrum of social engineering attacks. In India, 17% of the attacks are carried out by internal perpetrators, 27% by external perpetrators and in 56% both internal and external perpetrators work in collaboration. The internal perpetrator will supply the required information about the weakness or confidential data while the external perpetrator might provide the resources but most importantly motivate and lure the internal perpetrator to become his partner in crime. However, in US external perpetrators pose the biggest threat (49%) while internal perpetrators constitute 12% and 23% are unidentifiable perpetrators. The internal perpetrators in both the cases are the employees. The external perpetrators are similar in both countries but foreign nation states and organized crime are more likely to perpetrate in the US.

To understand the nature of attacks it is imperative to know the intent behind the cyber incident. The profile of the cybercriminal is an important factor in determining the nature & intention of attack. A relationship between the nature of attacks and the nature of cybercriminals appears to emerge from the current analysis. It appears as if the nature of attacks perpetrated in an area is influenced by the demographic of cyber minds present locally. The nature of the attack is chosen keeping in mind the benefits enjoyed by a particular cyber mind.

In US, the population of cyber criminals consists of hackers, activists, organized crime and foreign nation states. The nature of attacks i.e., phishing, wire fraud, DDoS and ransomware are chosen according to their motives like stealing funds and information from the organization, money extortion, killing competition, taking revenge with resultant weakening of the targeted organization and sometimes even posing a national security threat. The nature of attacks chosen benefit hackers and hactivists (in the form of personal gain through money or fame), organized crime (in the form of monetary gain through extortion or blackmailing and by selling confidential information in the black market) and foreign states (in the form of gain through money or by obtaining confidential information which might reveal the weaknesses of a nation).

In India, the demographic of cyber minds consists of script kiddies, professional hackers, hactivist, cyber terrorist, malware engineers, spammers, phishers and online scamsters. The nature of attacks perpetrated in India i.e., malware, social engineering, exploits of vulnerability, cyber espionage and DDoS are varied according to the diverse profile of cyber minds. The nature of the attack is decided by benefit reaped by script kiddies (in the form of personal gain through fame), hackers and hactivists (in the form of personal gain through money or fame), cyber terrorist (in the form of political or ideological gain by extortion or blackmail after obtaining confidential information), malware engineers (in the form of personal gain through fame and money) and
spammers, phishers and online scamsters (in the form of personal gain through fame or money) [19]. That explains the difference in the nature of attacks perpetrated in India and US. Since there are many differences in the profile of the cyber mind, accordingly the nature of attacks perpetrated varies. Since the profile of cyber mind is more diverse in India, hence it faces a broader spectrum of cyber attacks.

Given the enormity of cyber crime, it is important to analyze the strategy to combat cyber crime. In India, despite the high frequency of cyber crime, only 23% companies put cyber risk management on The Board of Directors’ top 10 organizational priorities. In stark contrast, 75% of US chief executives ranked cyber security solutions as “very important” to the company’s business strategy. In India, cyber risk management is part of the board agenda in 41% organizations as compared to US where it is part of at least some board or committee in 64% organizations. In India, annual cyber risk assessment is carried out in 26% companies while in US more than double the number (56%) of organizations carry out this exercise. Also in US, in 30% organizations, cyber risk management is not a part of any board agenda and in 25% organizations no cyber risk assessment is carried out making them high-risk targets and also potential candidates for cyber security breach.

Commitment, resources and funds are required to combat the menace of cyber crime. Analysis of funds allocated for this purpose reveals that in India 58% organizations spend less than 5% of IT, 31% spend 5-10% of IT, 9% spend 11-20% of IT and only 2% spend more than 11-20% of IT. Contrary to this, 69% of American firms have allocated more funds towards investment in cyber security technologies more than any other spending category clearly demonstrating the high priority given to cyber security. There appears to be a significant relation between the amount of funds allocated for cyber security and the number of attacks detected [20]. The more an organization spends, the more cyber incidents it detects. Majority of Indian organizations spend less than 5% of IT as compared to USA where the portion of budget allocated to cyber security is much higher. Hence, more cyber incidents are detected in US (79%) than in in India (72%). Relatively comparable detection rates with huge difference in organization spend is another glaring difference between the two countries. Also a very surprising observation is that despite investing significant resources in cyber security, the frequency of cyber crime in US is similar to that in India where majority of the firms have minimal cyber security. This may be because funds and resources are being allocated without a strategy in place or proper research [20]. Cyber security spending will be most productive when the allocation of resources is based on specific business risks while taking into account individual plan unique to each business. Adequacy of efficient cyber crime response in organizations is a necessity to combat cybercrime. In India, 72% companies think that the current number of cyber crime response organizations is not enough. In US, a mere 25%
of the organizations are involved with Information Sharing and Analysis Centers (ISACs) which are set up with the objective of combating cybercrime through information sharing. In India, there appears to be a paucity of cyber crime response organizations whereas, in US the organizations set up to combat cyber crime surprisingly do not receive active participation from American firms. The reason for this could be that the current cyber crime response organizations might not have a sound foundation coupled with disorganization and lack of strategizing. Hence, there exists a need to establish efficient cyber crime response organizations in US and elsewhere as well or to improve the existing ones.

5 CONCLUSIONS
In conclusion, though many similarities in frequency of cyber attacks exist between east and west there are vast differences in nature of attacks, type and intent of perpetrators, cyber criminal profile, priority and resources for cyber risk management, adequacy of cyber risk response and the paradoxes of cyber crime response organizations. It is interesting to understand how the nature of cyber attack is determined by the demographic profile and motive of cyber criminals. The economic growth of any nation and its security whether internal or external and competitiveness depends on how well is its cyberspace secured and protected. The present study could provide a window of opportunity to address the spiraling menace of cybercrime.

6 POLICY IMPLICATIONS
Despite the difference in the effort expended by the organizations in the two countries, the situation of cybercrime is similar in India and US. Cybercrime remains a big obstacle in the corporate world in India due to lack of prioritization of cyber crime by organizations. Only a few organizations spend the appropriate amount resources in detecting and combating cyber crime. This lax attitude towards cybercrime has not helped in controlling the frequency of cyber attacks. On the other hand the situation in the US seems almost paradoxical. Despite majority of organizations making cyber crime a priority and allocating resources in cyber security, the frequency of cyber in the US is quite high. The main reason behind this could be improper and inappropriate planning and ineffective allocation of resources. Hence, despite the huge effort being expended in combating cyber crime there appears to be no respite from cyber crime.

The creation of a well-planned policy environment will prove to useful in fulfilling the gaps in the respective nations. This strategy should focus on:
- A centralized cyberspace security response system,
- A centralized cyberspace security threat and vulnerability reduction program,
- A centralized cyberspace security awareness and training program,
- Securing organizational cyberspace, and
- Inter-organizational cyberspace security cooperation [21].

Such a through policy environment will address the menace of cybercrime in its broader context. This will aid organizations in prioritizing
- Improvement of response rate and time
- Reducing the potential damage caused by cyber attacks
- Preventing future breaches in security
- Protecting classified information

However, an actual difference can only come about if a serious commitment is made by the top management and effectively and efficiently implemented by employees and workers.

ACKNOWLEDGEMENT
I would like to express my heartfelt gratitude to my parents, especially my father without whom this research would have been impossible.

FUNDING
This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

REFERENCES
17. Whatis TechTarget: Ransomware, http://whatis.techtarget.com/definition/ransomware-cryptovirus-cryptotrojan-or-cryptoworm