Appendix L

Cybercrimes Worldwide – Trends and Patterns

Introduction

Cybercrime is now the fastest growing activity in the connected world. In 2009, reported losses in the US stood at $560 million up from $265 million the previous year[1] (see Section 1.9, Chapter 1). Information and Communication Technology has been evolved as a revolutionary technological tool that enables efficient transfer of information on a global scale. This global information could be used for international trade, online digital libraries, online education, telemedicine, E-Government and many other applications that would solve vital problems in the developing world. Chapter 2 explains how cybercriminal plan cyberoffenses to steal this information and Chapter 5 explains about Phishing and ID Theft by stealing PII (Personally Identifiable Information) of an individual.

In Chapters 3, 4 and 5, we learned different cyberattacks which will help to understand the focus in this appendix, on understanding worldwide trends of cyberattacks and/or cybercrime. The discussion on trends and patterns of worldwide cybercrime will begin with the statistics about Internet Traffic followed by trends of cybercrime. It is much obvious to see the statistics about average losses incurred by an individual and percentage of losses due to insiders. This appendix is concluded with the small guideline on how to file an FIR (First Information Report) with law enforcement agencies.

Internet Usage and World Population Statistics for 30 June 2010 presented in Table L.1[2] shows phenomenal growth in the Internet users from 2000 to 2010. The Internet penetration rates [see column "Penetration (% Population)" in Table L.1] by geographic regions are quite found to be an eye opener and proves the importance about creating an awareness among the netizens, (*netizen* is someone who spends considerable time online and also has a considerable presence online through websites about the person, through his/her active blog contribution and/or also his/her participation in the online chat rooms.) about cybercrime and protection measures to be adopted to avoid being a victim (see Appendix D).

Table L.1 World Internet users and population

Regions	***Population (2010)***	***Internet Users (31 December 2000)***	***Internet Users (31 June 2010)***	***Penetration (% Population)***	**Growth (%) 2000–2010**
Australia	34,700,201	7,620,480	21,263,990	61.3	1.79
Middle East	2,12,336,924	3,284,800	63,240,946	29.8	18.253
Africa	10,13,779,050	4,514,400	1,10,931,700	10.9	23.573
South America	5,92,556,972	18,068,919	2,04,689,836	34.5	10.328
North America	3,44,124,450	1,08,096,800	2,66,224,500	77.4	1.463
Europe	8,13,319,511	1,05,096,093	4,75,069,448	58.4	3.52
Asia	38,34,792,852	1,14,304,000	8,25,094,396	21.5	6.218
Total	**68,45,609,960**	**3,60,985,492**	**19,66,514,816**	**28.7**	**4.448**

Source: http://www.internetworldstats.com/stats.htm (15 January 2011).

Table L.1 shows 28.7% as the average rate of Internet penetration, which might appear very low in comparison with Internet users and it is important to look into the volume of traffic on the Internet,[3] as mentioned below, to understand severity of cyberattacks:

1. Internet users saw a total of 107 trillion E-Mails in 2010, most of those being spam (Spam E-Mails are explained in Chapters 1 and 5).
2. There are 2.9 billion E-Mail accounts worldwide. About 480 million new E-Mail accounts were opened in 2010.
3. 294 billion E-Mail messages were sent per day on an average with 89% (i.e., about 262 billion) of those being Spam.
4. 255 million websites were running in 2010, increased by 21.4 million from the previous year. There were 88.8 million ".com" domain names, 13.2 million ".net" domains and 8.6 million ".org" domain names.
5. Facebook had a total of nearly 600 million registered users, with 250 million new users in 2010 and 70% of all Facebook users come from outside the US. As many as 20 million Facebook applications were installed each day in 2010.
6. Twitter added 100 million new accounts in 2010 and had a total of 175 million as of September 2010. Twitter users sent 25 billion "Tweets" during 2010.
7. 2 billion videos per day were watched on YouTube in 2010, and 35 hours of video were uploaded to YouTube every minute.
8. As of September 2010, more than 5 billion photos are hosted on Flickr, with 3,000+ images uploaded every minute on the site.

The Internet-enabled mobile devices (i.e., cell phones, PDAs, Laptops) turned a digital device into a global digital device and created a new playground for cyberattackers. (See Chapter 3 to understand different cyberattacks on mobile and wireless devices.) The phenomenal growth in mobile phone market can be seen, from the world statistics, by "number of mobile phones in use" available at http://en.wikipedia.org/wiki/List_of_countries_by_number_of_mobile_phones_in_use.

We have to describe "worldwide" pattern in this appendix, for example, India is the world's fastest growing wireless market, with 752 million mobile phone subscribers as of February 2011.[4] It is also the second largest telecommunication network in the world in terms of number of wireless connections after China. The Indian mobile subscriber base has increased in size by a factor of more than 100 since 2001 when the number of subscribers in the country was approximately 5 million to 752 million by February 2011. As the fastest growing telecommunications industry in the world, it is projected that India will have 1.159 billion mobile subscribers by 2013. Furthermore, projections by several leading global consultancies indicate that the total number of subscribers in India will exceed the total subscriber count in the China by 2013.

The Internet's ability to promote the efficient dissemination of information promises huge improvements to internal communications in and among developing countries. However, the fundamental commonality of cyberattacks is the realization that the developed nations have ICT (Internet and Communication Technology) in abundance, which the developing ones could use to solve some of their problems, but geographical, political, philosophical, ideological and cultural barriers exist that make it difficult or impossible for these solutions to be transferred effectively. The seven worst cyberattacks in the history are presented in Table L.2.

Table L.2 The seven worst cyberattacks in history

Sr. No.	***Attack***	***Target***	***Attacker***	***Description***
1	Titan Rain	US military intel	China	"Titan Rain" is the name given to these attacks by the FBI. During 2004, a Sandia National Laboratories employee, Shawn Carpenter, discovered a series of large "cyber raids" carried out by what is believed were government-supported cells in China. It was found that several sensitive computer networks were

				infiltrated by the attackers. The danger noticed is not only can the attackers make off with military intel and classified data, but also they can leave backdoors and "zombify" machines that make future cyberespionage easier. Titan Rain is considered as one of the largest cyberattacks in history.
2	Moonlight Maze	Military maps and schematics, US troop configurations	Russia (Denies involvement)	Much like Titan Rain, Moonlight Maze represents an operation in which attackers penetrated American computer systems. It was also one of the earlier major cyber infiltrations, starting in 1998 and continuing on for two whole years as military data was plundered from the Pentagon, NASA, Department of Energy and even from universities and research labs.
3	The Estonian Cyberwar	Estonia	The Nashi, a pro-Kremlin youth group in Transnistria	What happened to Estonia in 2007 is considered to be a model of how vulnerable a nation can be to cyberattacks during a conflict. In a very short period of time, a variety of methods were used to take down key government websites, news sites and generally flooded the Estonian network to a point that it was useless. The attack is one of the largest after Titan Rain, and was so complex that it is thought that the attackers must have gotten support from the Russian government and large telecom companies. Bronze Soldier of Tallinn, an important icon to the Russian people and the relocation of which played a part in triggering the attacks.
4	Presidential-level Espionage	Obama, McCain presidential campaigns	China or Russia (suspected)	No one wants to get a message from the FBI saying, "You have a problem way bigger than what you understand," but that's exactly what happened to both Obama and McCain during their run for the 2008 presidency. What was first thought of as simple cyberattacks on the computers used by both campaigns was discovered to be a more concentrated effort from a "foreign source" that accessed E-Mails and sensitive data. The FBI and secret service swooped in and confiscated all computers, phones and electronics from the campaigns and – with the kind of stuff that gets dug up on the

				campaign trail – there are probably plenty of folks hoping the FBI keeps them.
5	China's "7,50,000 American zombies"	US computer networks, all levels	Chinese hackers (Government-supported, organized crime-related, cyber gangs)	The worst fallout from a cyberattack can be what it leaves behind, such as malicious software that can be activated later. That compounded with ongoing efforts by attackers to infect as many machines as possible using bogus E-Mail offers, harmful website code to have a lot of "zombified" machines. Those machines can then be made into cyber weapons, which can overload a network, website or other machine with a deluge of data known as a DDoS (distributed denial-of-service) attack. Even back in 2007, former senior US information security official, Paul Strassmann, estimated that there were over 7,30,000 compromised computers "infested by Chinese zombies."
6	The Original Logic Bomb	Siberian gas pipeline in Soviet Russia	U.S. Central Intelligence Agency	One of the scariest implications of cyber warfare is that the damage is not always limited to networks and systems. It can get physical too. In 1982, the CIA showed just how dangerous a "logic bomb" – a piece of code that changes the workings of a system and can cause it to go haywire – can be. The agency caused a Soviet gas pipeline in Siberia to explode in what was described by an air force secretary as "the most monumental non-nuclear explosion and fire ever seen from space," without using a missile or bomb, but a string of computer code. Today, with the proliferation of computer control, the possible targets are virtually endless.
7	"The Most Serious Breach"	US military computer network	Foreign intelligence agency (unspecified)	A cyber attack can come in any shape or size – digitally or physically – and one of the worst on an American network happened in 2008. It was not involved thousands of zombie machines and the muscle of a national telecom giant. You could have held it in the palm of your own hand: a corrupt flash drive. Inserted into a military laptop in the Middle East, the Malicious Code on the drive created – a digital beachhead, from which data could be transferred to servers under foreign control. The

				attack acted as another reality check in security and prompted the Pentagon to form a special cyber military command.

Source: http://dvice.com/archives/2010/09/7-of-the-most-d.php (15 January 2011).

Cybercrimes Worldwide – Trends and Patterns

The survey results published by CSI (2009 CSI Computer Crime and Security Survey Report[5]) results are based on the responses of information security and information technology professionals in the US (6,100 US-based members of the CSI community) corporations, government agencies, financial institution, educational institutions, medical institutions and other organizations (see Fig. L.1). In today's Net-centric organizations operating in the global economy, information has become one of the most crucial assets of all the corporations. The global customer base expects assurance of data integrity, confidentiality and availability, and the organizations looked at a number of best practices in view of cybersecurity threats. See Chapter 9 to deal with this topic (Chapter 9 – cyber security with the perspective of organizational implications).

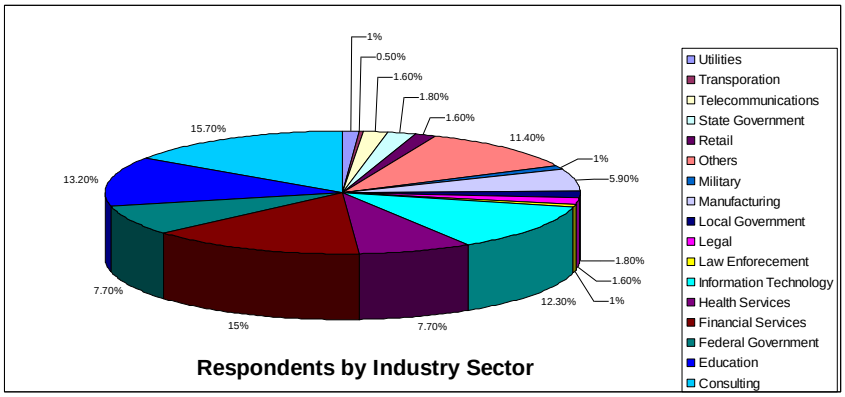

Figure L.1 Respondents by industry sector.
Source: Statistics based on 2009 – CSI Computer Crime and Security Survey – http://pathmaker-group.com/whitepapers/CSISurvey2009.pdf (15 January 2011).

The survey categorizes respondents by job title (see Section 12.2.1, Chapter 12 to understand the roles and responsibilities of these job titles). As Fig. L.2 shows, 31.5% of the respondents are senior executives, termed as C-Executives, that is, CEO, CIO, CSO and CISO. A sizeable 38.9% of respondents labeling themselves as "others" – found to be under the category of "security officer" as per the responses received from the respondents. However the "others" category also contained a variety of job roles that fell outside of information technology entirely, which may be evidence that the security function continues to expand into more business segments.

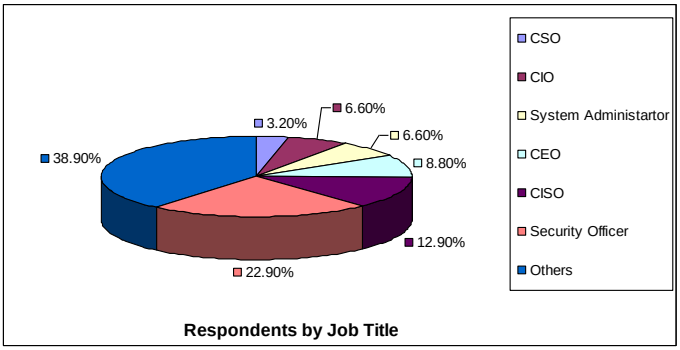

Figure L.2 Respondents by job title.
Source: Statistics based on 2009 – CSI Computer Crime and Security Survey – http://pathmaker-group.com/whitepapers/CSISurvey2009.pdf (15 January 2011).

Types of Cyberattacks Experienced

Cybercrime is a truly global criminal phenomenon which blurs the traditional distinction between threats to internal (criminality and terrorist activity – see Chapter 10) and external (i.e., military) security and does not respond to single jurisdiction approaches to policing. The liability of networks to exploitation for a number of different ends, and the ease with which individuals may move from one type of illegal activity to another suggests that territorialism in all its forms (both of nations and regions, and specific authorities within nations) hinders efforts to successfully combat the misuse of communications technology. Figure L.3 shows the most common attacks as stated below, launched since 2005 till 2009.

1. Denial of service (see Section 4.9, Chapter 4).
2. Exploit of wireless network (see Section 4.12, Chapter 4).
3. Financial fraud (see Section 3.4, Chapter 3 and Section 5.3.2, Chapter 5).
4. Insider abuse of Internet access or E-Mail (see Section 9.1.1, Chapter 9 to understand insider attacks).
5. Laptop or mobile hardware theft or loss (see Section 3.9.3, Chapter 3).
6. Malware infection (see Box 4.3, Chapter 4 and Section 9.3.1, Chapter 9).
7. Website defacement (see Section 1.5.11, Chapter 1).

Chapter 11 explains numerous illustrations, examples and mini-cases on the cyberattacks, discussed so far.

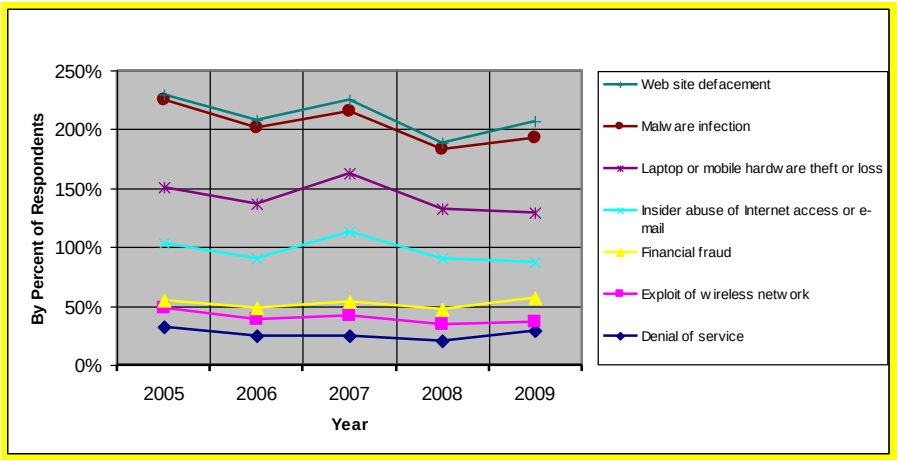

Figure L.3 Types of well-known cyberattacks.
Source: Statistics based on 2009 – CSI Computer Crime and Security Survey – http://pathmaker-group.com/whitepapers/CSISurvey2009.pdf (15 January 2011).

Malware infection leapt from 50% to 64.3%, making it easily the most prevalent incident; and specifically "Bots in the organization" increased modestly from 20% to 23%. Considering the rapidly increasing sophistication of malware – and the not-so-rapidly-increasing sophistication of anti-malware solutions – it would not be altogether surprising if malware infection makes another big jump during 2011.

The second-most prevalent incident is laptop and mobile hardware loss or theft, holding steady at 42%. The number of respondents that experienced data breaches occurred as a result of these hardware losses and thefts held level at 12%. To be specific, breach of PII (see Section 5.3.1, Chapter 5) or PHI (see Section 5.3.2, Chapter 5) dropped from 8% to 6%, and breach of proprietary information or intellectual property rose from 4% to 6%. Although mobile devices gone astray did lead to data breaches for 12% of respondents, 18% of respondents suffered data breaches for entirely different reasons like unauthorized access to PII or PHI and 8% reported theft of or unauthorized access to proprietary information or intellectual property due to other causes.

The third-most prevalent incident – reported by over one-third of respondents – was Phishing fraud (see Chapter 5), in which a victim organization is fraudulently represented as the sender of Phishing messages.

Fourth place was earned by insider abuse of Internet access or E-Mail – which principally means pornography (see Section 1.5.13, Chapter 1 and Section 6.2.2, Chapter 6), pirated software (see Section 9.2.2, Chapter 9) and the like – which was reported by 30% of respondents.

Next in line are DOS (denial-of-service) attacks, which jumped from 21% during 2008 (i.e., previous year) to 29% during 2009. DoS attacks are presumed to be far less profitable for attackers than those of data breaches and that DoS attacks receive far less press and attention than those of data breaches [unless, of course, the DDoS (see Section 4.9.5, Chapter 4) is experienced by a high-profile Web service].

Table L.3 Types of cyberattacks

Types of Cyberattacks Experienced	***2005***	***2006***	***2007***	***2008***	***2009***
Being fraudulently represented as sender of Phishing messages	Added in 2007		26%	31%	34%
Bots/zombies within the organization	Added in 2007		21%	20%	23%
Denial of service	32%	25%	25%	21%	29%
Exploit of client Web browser	Option altered in 2009				11%
Exploit of DNS server	Added in 2007		6%	8%	7%
Exploit of user's social network profile	Option altered in 2009				7%
Exploit of wireless network	16%	14%	17%	14%	8%
Extortion or blackmail associated with threat of attack or release of stolen data	Option altered in 2009				3%
Financial fraud	7%	9%	12%	12%	20%
Insider abuse of Internet access or E-Mail (i.e., pornography, pirated software, etc.)	48%	42%	59%	44%	30%
Instant messaging abuse	Added in 2007		25%	21%	8%
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	42%
Malware infection	74%	65%	52%	50%	64%
Other exploit of public-facing website	Option altered in 2009				6%
Password sniffing	Added in 2007		10%	9%	17%
System penetration by outsider	Option altered in 2009				14%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss	Option added in 2008			4%	6%
Theft of or unauthorized access to intellectual property due to all other causes	Option added in 2008			5%	8%
Theft of or unauthorized access to PII or PHI due to all other causes	Option added in 2008			8%	10%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss	Option added in 2008			8%	6%
Unauthorized access or privilege escalation by insider	Option altered in 2009				15%
Website defacement	5%	6%	10%	6%	14%

Source: Statistics based on 2009 – CSI Computer Crime and Security Survey – http://pathmaker-group.com/whitepapers/CSISurvey2009.pdf (15 January 2011).

Apart from the cyberattacks displayed under Fig. L.3, below are the cyberattacks which are on the verge of rise. The historical data since 2005 is not available for most of these attacks; however, exponential growth with regard to previous year is interesting to note.

1. Being fraudulently represented as sender of Phishing messages (see Section 5.2, Chapter 5).
2. Bots/zombies within the organization (see Section 2.6, Chapter 2).
3. Exploit of client Web browser (see Section 5.2.1, Chapter 5).

4. Exploit of DNS server (see Section 5.2.4, Chapter 5).
5. Exploit of user's social network profile (see Section 9.5, Chapter 9).
6. Extortion or blackmail associated with threat of attack or release of stolen data.
7. Instant messaging abuse.
8. Other exploit of public-facing website (see Sections 5.2.1 and 5.2.4, Chapter 5).
9. Password sniffing (see Section 4.4, Chapter 4).
10. System penetration by outsider (see Section 4.1, Chapter 4).
11. Theft of or unauthorized access to intellectual property due to mobile device theft/loss (see Section 10.2, Chapter 10).
12. Theft of or unauthorized access to intellectual property due to all other causes (see Section 10.2, Chapter 10).
13. Theft of or unauthorized access to PII (see Section 5.3.1, Chapter 5) or PHI (see Section 5.3.2, Chapter 5) due to all other causes.
14. Theft of or unauthorized access to PII (see Section 5.3.1, Chapter 5) or PHI (see Section 5.3.2, Chapter 5) due to mobile device theft/loss.
15. Unauthorized access or privilege escalation by insider (see Section 9.1.1, Chapter 9 to understand insider attacks).

Chapter 11 presents numerous illustrations, examples and mini-cases on the cyberattacks, discussed so far. The greatest concern is that financial fraud has been increased from only 12% to 19.5%. This is a reason for concern because financial fraud consistently causes victim organizations huge losses – almost US$ 450,000 per victim organization this year. Other notable changes are: password sniffing almost doubled, leaping from 9% to 17%, whereas wireless exploits were nearly sawed in half, dropping from 14% to 8%.

The CSI survey also reports the estimate of percentage of monetary losses (see Section 9.2.1, Chapter 9) that were attributable to actions and/or inactions by individuals within the organization (see Fig. L.4). Therefore, how did these attacks affect target organizations? According to Fig. L.4, respondents suffered, on average, US$ 234,000 in losses due to security incidents between July 2009 and June 2008. This is a 19% drop from 2008 average of US$ 289,000; which was a 16% drop from 2007's average of US$ 345,000.

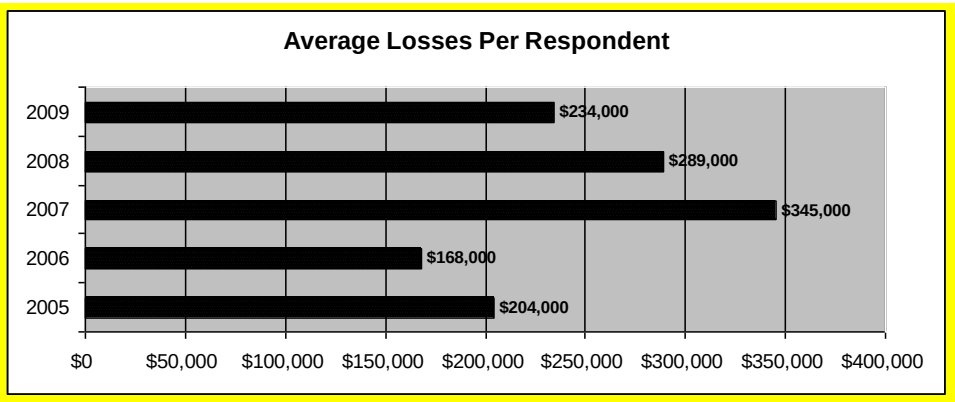

Figure L.4 Average losses per respondent.
Source: Statistics based on 2009 – CSI Computer Crime and Security Survey – http://pathmaker-group.com/whitepapers/CSISurvey2009.pdf (15 January 2011).

Much is made of "the insider threat." Insider threats are caused by human actions such as mistakes, negligence, reckless behavior, theft, fraud and even sabotage (see Section 9.1.1, Chapter 9 to understand insider attacks). The survey deals with two categories of insider threats:

1. Malicious.
2. Non-malicious.

Malicious employee are the ones who leverages their inside information to conduct a highly targeted attack with a big payoff and those posed by the average well-meaning user who discloses data to a social engineer (see Section 2.3, Chapter 2) because they just do not know anything better.

It is interesting to note that 43.2% of respondents stated that at least some of their losses were attributable to malicious insiders; but clearly non-malicious insiders are the greater problem (see Fig. L.5). The fact that 16.1% of respondents estimated that nearly all their losses were due to the non-malicious, merely careless behavior of insiders drives home the point that security awareness training for end-users plays an important role in organizations' security programs (see Section 9.1, Chapter 9 to understand different types of insiders).

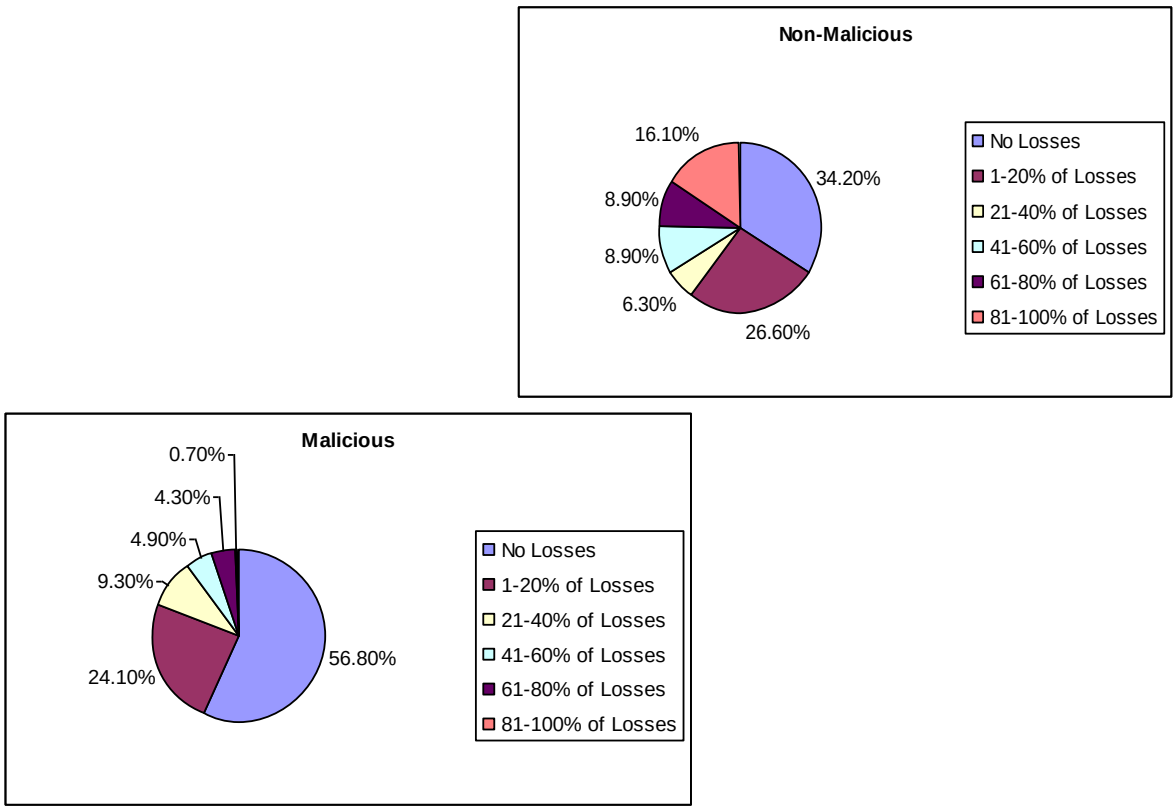

Figure L.5 Percentage of losses due to insiders.
Source: Statistics based on 2009 – CSI Computer Crime and Security Survey – http://pathmaker-group.com/whitepapers/CSISurvey2009.pdf (15 January 2011).

Reporting Cyberattacks and Cybercrimes

Cyber Cell of Mumbai Crime Branch reported that only 3% of the total complaints are turned out to be FIRs (see Box L.1) and most of the complaints are received from women.[6] Once the police trace the attacker, in most of the cases the victims/complainants do not want the accused/criminal to be booked since it may also affect their social life and as in many cases the offenders are minor and known to the victims. Besides, they also want to avoid any controversies fearing it will reflect negatively on their image in the society. Complainants/victims including teachers, students, professionals and film personalities approach law enforcement agencies (i.e., police department) to ensure that the harassment is stopped and defamatory messages or morphed pictures removed from the Internet.

Box L.1: FIR (First Information Report)

FIR means[7] First Information Report, made to police, about any event which can be categorized under a cognizable offence. In effect, it amounts to putting law and order into motion by giving information relating to the commission of a cognizable offence to an officer in charge of a police station and shall be signed by the person giving such information. It is mandatory to give a copy of the FIR, as recorded by police to the complainant or informant free of cost.

The discussions with Cyber Cell of Pune Police to understand evidence requirement while registering an FIR, resulted to understand below mentioned facts:

1. In case, you suspect about being a victim of cybercrime, it is important to ensure the same with few primary checks, before rushing to law enforcement agencies.
2. The victim should approach nearest cybercrime cell with the entire data and/or information about the event.
3. The police will help the victim about identifying whether the reported event is a cognizable offence and whether FIR can be registered.
4. Since every case is unique, the police will guide the victim about identifying the requirement of evidences.
5. The victim should provide all the required evidences to the police within the prescribed time period.
6. The victim should cooperate with police and their process of the investigation and should provide all the additional evidences (if any) within stipulated time.

Readers may want to visit http://mahapolice.gov.in/ to understand FAQs about FIR.

In summary, Internet security is not just limited to government, big business and law enforcers. The threat from cybercrime is multidimensional, targeting citizens, businesses and governments at a rapidly growing rate. It is an equally increasingly important concern for netizens as well as for technocrats. All of them just want to know that if they follow a few simple ground rules, they will be safe (see Appendix D). From the trends and patterns mentioned earlier in this appendix, the common challenges can be stated as mentioned below:

1. **Protecting netizens:** Cybercriminals have realized that it is easier to steal US$ from one in a million people, than to steal one million US$ from one person. Hence, they are becoming more and more organized so that the attack can remain undetected. When victim complains to the police about losing US$ 100 through cybercrime, or the theft of personal identity information, is rarely sufficient to elicit a response. It is difficult for law enforcement agencies, to reach to the attacker in case of cross-boarder attack (e.g., the attacker is residing out of India and the victim is in India).
2. **Data protection and privacy:** PII (Personally Identifiable Information) became as valuable as currency (cash). Awareness toward privacy of personal information should be created in the society.
3. **Bugs-free software:** The attacker always looks for security holes into the existing system. There is a clear need and opportunity for greater industry cooperation, standardization and testing of software products to reduce the opportunity for attackers.
4. **Rogue states:** On the Internet, a rogue state is not defined by its weapons (i.e., tools) or politics but by its laws and regulations. Without a common base level of data protection and computer misuse legislation, there will always be territories that provide a safe harbor for cybercriminals and attackers.

References

[1] To know more about Cybercrime, Cybersecurity and the Future of the Internet, visit: http://www.global-economic-symposium.org/solutions/the-global-polity/cybercrime-cybersecurity-and-the-future-of-the-internet (15 January 2011).

[2] To know more about World Internet Users and Population, visit: http://www.internetworldstats.com/stats.htm (15 January 2011).
[3] To know more about Traffic on the Internet, visit: http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/ (15 January 2011).
[4] To know more about Mobile Communications in India, visit: http://en.wikipedia.org/wiki/Communications_in_India (15 January 2011).
[5] To know more about 2009 – CSI Computer Crime and Security Survey, visit: http://pathmaker-group.com/whitepapers/CSISurvey2009.pdf (15 January 2011).
[6] Mumbai Cyber Crime Cell reveals the Cyber Crime and FIR ratio, to know more about this visit: http://www.cyberlawtimes.com/mumbai-cyber-crime-cell-reveals-the-cyber-crime-and-fir-ratio/ (15 February 2011).
[7] To know more about FIR FAQs, visit: http://mahapolice.gov.in/ (15 February 2011).

Further Reading

Additional Useful Web References

1. To know more about India (Internet Usage statistics), visit: http://www.indiabroadband.net/india-broadband-telecom-news/11169-some-statistics-about-internet-users-india.html (15 January 2011).
2. Read article *TOP 20 COUNTRIES WITH THE HIGHEST NUMBER OF INTERNET USERS* at: http://www.internetworldstats.com/top20.htm (15 January 2011).
3. To know more about *List of countries by number of Internet users*, visit: http://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users (15 January 2011).
4. To know more about Global Internet usage, visit: http://en.wikipedia.org/wiki/Global_Internet_usage (15 January 2011).
5. To know more about 2004 CSI/FBI – COMPUTER CRIME AND SECURITY SURVEY, visit: www.infragardphl.org/resources/FBI2004.pdf (15 January 2011).
6. To know more about 2005 CSI/FBI Computer Crime Survey, visit: www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf (15 January 2011).
7. To know more about 2006 CSI/FBI – COMPUTER CRIME AND SECURITY SURVEY at the link, visit: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf (15 January 2011).
8. To know more about 2007 – CSI Survey 2007 – The 12th Annual Computer Crime and Security Survey at the link, visit: http://www.computer-corner.com/pdf/CSISurvey2007.pdf (15 January 2011).
9. To know more about 2008 – CSI Computer Crime & Security Survey, visit: http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf (15 January 2011).
10. To know more about Trends in Cybercrime: Report, visit: http://www.esecurityplanet.com/trends/article.php/3874206/Trends-in-Cybercrime-Report.htm (15 February 2011).
11. To know more about Cyber Crime Trends and Internet Fraud Complaints on the Rise, visit: http://www.lawisgreek.com/cyber-crime-trends-and-internet-fraud-complaints-on-the-rise/ (15 February 2011).