CHAPTER – VI

IMPACT OF CYBER CRIMES

Computer crime can affect the personal records of the individual. It can be an impediment in the financial resources fit of bank, causing confusion and potentially, affecting customer accounts. It can result in confidential information being compromised affecting the price of the victim’s publicly traded shares. It can be an attack on a corporation’s marketing information causing misinformation to be communicated to the sales force. The cyber maneuvering person can break into a system, steal sensitive information, cover his or her tracks and leave to return another day. If the intruder is skilful and safeguards are not in place, one will never know that the theft has occurred. Theft of computer data does not leave a void where the stolen item once resided.¹

Technology Trends

The risks associated with current and anticipated vulnerabilities of threats to, and attacks against the IT infrastructure provide the rationale for this strategy. Fast-shifting trends in both technologies and threats make it likely that the security issues of the IT infrastructure will intensify in the coming years.²

The Internet has the potential to impact human life in a way that surpasses other inventions of the 20th century. It is expected to outdo the other inventions both in terms of magnitude of impact and the speed with which the transformation takes place. A combination of repeated declines in the price of computing power and the increase in the value of a network with the increase in the number of users

² www.cactusblog.files.wordpress.com browsed on 30th September 2013.
has ensured that cost of access continuously declines and the rate of Internet penetration continuously increases.3

**Cyber murder**

A hacker breaks into hospital medical records and maliciously alters prescriptions. If a patient is allergic to penicillin, the hacker adds 500 mg of penicillin to his usual dose of medication and cyber murder would be committed. The nurse administers the drug causing immediate health hazards and then flood gates are open to bring cheap publicity to the hospital and its credibility will be in stake. For example, one mafia don was shot by his rivals in America, he did not die of bullets, but he was injured and admitted to hospital. Now his enemy group hacked computer, changed the prescription of the medical and included the medicines to which he was allergic. Nurse gave him the medicine and the person died. Many cases like these have taken place in America.4

The obvious effect of cyber crime on business is the evolving threat landscape. The motive of the attacks has changed over time. Earlier, the intent of the attacker was to gain fame although the motivation was criminal attitude. Cyber crime economics are too compelling to subside.

**EFFECTS OF HACKING ON SOCIETY**

Hacking effects can be categorised into three types; effects on individuals, organizations, economy and effects on countries. The most important issue to recognise is that victims are the only ones who feel the threat and effects of hacking attacks, and our duty is to inform other people about the danger of

---


4 [http://ensaiosjuridicos.files.wordpress.com](http://ensaiosjuridicos.files.wordpress.com) browsed on 1st January 2015.
hacking to be cautious and alert which helps in preventing hacking attacks from happening. The effects are as following:

1. Effects on individuals: There are cases where individual information is sold and used for bad purposes like usurping their accounts. The focuses on the psychology of individuals after being hacked and that they will always have the fear of being monitored when accessing internet and information, added to that the privacy of users can be easily penetrated. Credit card details and passwords can be stolen causing financial damage to individuals added to that computer systems can be hacked causing the machine to stop working as usual or stealing your data.

2. Effects on organisations and economy: Hacking is said to have cost the global economy at an estimated $1.2 Billion. Hacking has caused bankruptcy and financial crisis to plenty of companies, leading to the loss of customer confidence, liquidity problem in the security capabilities of the company. It is believed that companies are a main target for hackers who break into their systems to steal trade information or customer’s payment details. The company server will be broken due to huge traffic causing customer frustration and immensely hurt the company reputation. Software theft that causes bankruptcy to companies which spend millions to develop and create software. The main problem is that some companies hire or use hackers to break into other competitor systems to steal precious information. In respect of the effect of
hacking on E-commerce by means of web sites for online selling are being hacked for the sake of getting customer and company information which are then used for despicable purposes.\textsuperscript{5}

3. Effects on countries: Since we are living in information society where all our daily activities are controlled by technology, there will be irrepairable damage if a vital system was broken by hacking attacks. Breaking main system might result in collapse and disaster for countries. The cyber attacks on computer systems aim to steal vital information of the countries decisions regarding foreign policies and strategies, this result in causing countries to reconsider their policies that were taken after long analysis. It might also cause disturbance due to the attack of precious and top secret information. This approach caused a lot of controversy and opened the door for other countries to hack different systems and retrieve any source of data using the excuse of tracking criminals which might lead to destroying the principle of information owning and security and then turn the world into a chaos and open the door to a new cold war.

Results of Hacking

At the risk of stating the obvious, hacking—computer crime—which will culminate in massive financial losses for companies, governments, and individuals alike. The costs associated with computer crime can manifest themselves in various ways, which may range from the obscure to a clear hit to the bottom line.

\textsuperscript{5} http://pdf.usaid.gov browsed on 21\textsuperscript{st} February 2014.
Digital assets where costs from hackers can manifest themselves fall into four major categories: resources, information, time, and reputation.\(^6\)

1. **Resources**: Resources are computer-related services that perform actions or tasks on the user’s behalf.

2. **Information**: Information can represent an enormous cost if destroyed or altered without authorization. Data can be affected in several ways that will have voluminous cost related to the type of effect: loss, disclosure, and integrity.
   a. **Loss**: The loss of data is relatively easy to measure when compared to disclosure and integrity. Information takes time to collect or produce, requires resources to be managed, and will certainly (to some degree) have value.
   b. **Disclosure**: Nearly every entity that uses information has the potential to be negatively affected by its uncontrolled disclosure. Although the impact of an unauthorized disclosure is one of the most difficult to measure, such a breach is noteworthy because it represents the traditional fear of hacking: proprietary information theft.
   c. **Integrity**: The ensuring information is accurate and complete is necessary for any organization. If data were to be manipulated it could become a loss to the owner.

---

3. **Time:** The loss of time can be related to costs in the form of payroll, not meeting critical deadlines, or an unavailable E-commerce site that would normally produce thousands of dollars in revenue if it were available.

4. **Brand and Reputation:** There are many companies who have very recognizable and reputed brands, so much so that the color alone will promote images of the company.

Effects that hacking has caused to the society cannot be sidelined. Hacking nowadays is taking new phases and the danger is increasing because we are now living in a society that runs by Information and Communication Technology (I.C.T.), and any attack on this field especially in advanced countries will cause vital consequences.  

**The Economics of Computer Hacking**

In the digital age, cyber security is perhaps the most important form of security individuals must be concerned with. Banks, schools, hospitals, businesses, governments and virtually every other modern institution you can think of stores and organises it electronically. This means that all of our most sensitive information – from credit card numbers and checking accounts, to medical records and phone bills – is accessible for viewing, stealing, maneuvering or manipulating to anyone with a PC, an Internet connection, and some computer know-how. The increasingly computer-based world is increasingly vulnerable to malevolent computer hackers. 

---

7 [www.fanews.co.za](http://www.fanews.co.za) browsed on 1st March 2015.
8 [www.peterleeson.com](http://www.peterleeson.com) – e-Article on “The Economics of Computer Hacking” submitted by Peter T.Leeson and Christopher J.Coyne, p.2.
Growth of the Underground Cyber Crime Economy

A major threat that may hamper the fight against cyber crime is the growth of an underground economy, which, for cyber criminals can be a lucrative venture which will cause peril to the saturated and accomplished economy. The underground economy attracts many digital experts and talented individuals with a specialty around cyber initiative. In the cyber underworld, the hackers and organized crime rings operate by selling confidential stolen intelligence.9

The mobile devices takes the concept of anywhere banking to the next level and presents a whole host of new product opportunities for banks to make available to their customers. Much like a double-edged sword, mobile banking also presents a threat to those banks that ignore it. Payments for small value purchases is one such area where the available value can be competed away by nimble-footed groups of mobile telecom companies and banks acting in unison.10

Loss of Banks towards Cyber Crime

In the year 2009, total cyber crimes reported in Scheduled Commercial Banks was 21,966 with the amount involved as Rs.72,33,31,000/-. Likewise in 2009, a total of cyber crimes reported in Public Sector Banks was 97 with the amount involved as 1,05,81,000/- (Punjab National Bank alone had 33 crimes with Rs.50,15,000/-), in 2010. There were 156 with Rs.3,70,12,000/- (Punjab National Bank alone was 108 crimes with Rs.2,48,64,000/-), in 2011 there were 128 with 6,72,48,000/- (IDBI Bank Limited alone was 50 crimes and amount involved by Indian Overseas Bank was

---

Rs.1,76,03,000/-) and in 2011 was 214 crimes with the amount involved as Rs.8,28,63,000/- (IDBI Bank Limited alone was 87 crimes with Rs.2,03,04,000/-).

In 2009, the total number of cyber crimes reported in Private Sector Banks was 16,100 with the amount involved as Rs.42,32,61,000/- (ICICI Bank Limited alone was 15,666 crimes with Rs.37,31,95,000/-), in 2010 there were 10,129 with Rs.22,25,94,000/- (ICICI Bank Limited alone was 9,811 crimes with Rs.19,20,28,000/-), in 2011 was 6,527 with 16,70,72,000/- (ICICI Bank Limited alone was 6,013 crimes with Rs.10,96,67,000/-) and in the year 2011 there were 4,144 crimes with the amount involved as Rs.25,06,47,000/- (ICICI Bank Limited alone was 3,428 crimes and amount involved by Axis Bank Limited was Rs.12,25,41,000/-).

In 2009, total cyber crimes reported in Foreign Banks were 5,769 with the amount involved as Rs.28,94,89,000/-, in 2010 there were 4,733 with Rs.14,52,88,000/-, in 2011 was 2,933 with 13,28,99,000/- and in 2011 there were 3,964 crimes with the amount involved as Rs.19,31,85,000/-.

However, overall a declining trend has been observed in cyber frauds in private sector bank. ICICI Bank had a highest position in cyber frauds during this four years period showing voluminous number of cases and large money involved.11

Impact of Operation of Modern Equipments of I.T. by the Children

According to a survey conducted by the ASSOCEM, “Cell Phones, Tablet Personal Computers and Ipods are operated by 85% of the juveniles in the metropolitan cities like Chennai in our country.”

This survey was conducted in the cities of Chennai, Delhi, Kolkata, Mumbai, Bangalore, Hyderabad, Pune, Ahmedabad, Lucknow and Jaipur. In this, it shows that 63% of the juveniles are operating computers and 60% of them are browsing the internet daily. One out of ten children are having the own mobile phone from the age of 5 to 12 and they are considering this as social status.

The Chief Secretary of ASSOCEM Dr.R.S.Rawad has given a clarion call to the parents that modern technology instruments are handled by the children, the failure of parents to monitor their children while operating these instruments will pave the way to make addict the children. Hence, parents have to take care in this regard. He has also cautioned that with handling of these modern equipments by the children, they are supposed to be alienated from the society. Apart from that, they are being affected by way of sleeplessness, mental disorder, mental sorrow, obesity and mental distress.12

Polluting Youth/Dissemination of obscene material/Indecent exposure

1. Pornography (basically child pornography)/Polluting through indecent exposure which corrupts the mind and psychology of juveniles.

2. Pornographic materials can be reproduced more quickly and cheaply on new media like hard disks, floppy discs and CD-Roms. The new

technology is not merely an extension of the existing forms like text, photographs and images.

3. Apart from still pictures and images, full motion video clips and complete movies are also used.

4. Another great disadvantage with an internet is that its easy availability and accessibility to children who can now log on to pornographic websites from their own houses in relative anonymity and the social and legal deterrents associated with physically purchasing an adult magazine surfing the net.

5. Furthermore, there are more serious offences which have universal disapproval like child pornography and far easier for offenders to hide and propagate through the medium of the Internet.13

The Internet’s Impact on Law and Regulation

The Internet has affected law and regulation in two, often overlapping, ways. First, the technical design of the Internet has allowed for genuinely new ways of interaction and new activities which is not to deny the existence of some remotely analogous activities in the offline world. These have diversified and raised myriad genuinely new legal issues. For example, the process of linking on the Internet is novel, and one legal issue which it has raised is whether a link from one website to an inner webpage of another website constitutes copyright infringement. Another new legal problem arises from the ability to sign up to software packages with ongoing updates: for taxation purposes are these packages goods or services? The use of domain names has raised the question whether they

should be treated like trademarks and, if so, how the different allocation bases can be made compatible.\textsuperscript{14}

**Challenges Faced by Governments**

Although governments are actively focused on fighting and preventing cyber criminals from damaging infrastructure, the very nature of cyber space poses a number of challenges to the implementation of cyber regulations in any country. Within cyberspace it is often difficult to determine political borders and culprits. Furthermore, the cyber criminal community and their techniques are continuously evolving and they improvised a lot, making it more challenging for governments and companies to keep up with ever-changing techniques.\textsuperscript{15}

Companies face two kinds of cyber crimes… one in which the company or its assets are the target and the other in which company’s assets is used as tools for a cyber crime either by its employees or others.\textsuperscript{16}

The annual losses globally estimated were around $388 billion (Rs.1,83,60,15,98,81,591/-) on financial losses and time lost due to cyber crime which was significantly higher than time spent in black-marketing drugs.\textsuperscript{17}

**NASA Shut their Offices for 21 Days Due to Hacking by Juvenile**

A juvenile hacked into the official site of NASA and through that he could access the main server breaking the security code. NASA had to shut their offices all over the U.S. for 21 days to rectify and construct a new code.

\textsuperscript{16} www.naavi.org browsed on 4\textsuperscript{th} October 2013.
\textsuperscript{17} www.dnaindia.com browsed on 29\textsuperscript{th} May 2014.
Similarly a group of software engineers hacked into the main server of the Cyber Police Station of Mumbai and deleted a lot of details pertaining to criminals. Sensitive Government departments are vulnerable to such cyber criminals. By this, the society for a fault of it will be in the receiver end.  

**The Economic Impact of the Internet in the UK**

Nearly three-quarters (73%) of households in the UK had Internet access. The Internet usage was more than twice as large as the UK hotel and restaurant market and nearly as big as the financial services sector, which accounted for 9% of GDP in 2009.

It is uncommon for a person to return from vacation and find his email box 90% full with spam messages. Nevertheless, there are some practical steps that can be taken to minimize the volume of spam. More than 95% of daily global mail traffic is spam.  

**Drawbacks of Ethical Hacking**

As with all types of activities which have a darker side, there will be dishonest people presenting drawbacks. They are the parasites. The possible drawbacks of ethical hacking include:

- The ethical hacker using the knowledge they gain to do malicious hacking activities.
- Allowing the company’s financial and banking details to be porous.
- The possibility that the ethical hacker will send and/or place malicious code, viruses, malware and other destructive and harmful things on a computer system.
- Massive security breach.  

---

19 [www.iod.com](http://www.iod.com) browsed on 20th June 2014.  
These are not common. However, they are something all company should consider when using the services of an ethical hacker.

In a report of expressindia.com, it was said that internet was becoming a boon for the terrorist organisations. According to Mr.A.K.Gupta, Deputy Director (Co-ordination), CBI, terrorist outfits are increasingly using internet to communicate and move funds. Lashker-e-Toiba, a highly professional illegal militant group is collecting contributions online from its sympathizers all over the world. During the investigation of the Red Fort shootout in December 2000, the accused Ashfaq Ahmed of this terrorist group revealed that the militants are making extensive use of the internet to communicate with the operatives and the sympathizers and also using the medium for intra-bank transfer of funds. They do this discretely.\(^{21}\)

**400 Million SMS Fraud**

The alleged mastermind behind a Rs.400 million SMS fraud that duped at least 50,000 people has been arrested along with an associate more than two months after the scam was unearthed. Jayanand Nadar, 30, and Ramesh Gala, 26, were arrested in February 2007. They had allegedly duped at least 50,000 people of Rs.400 million, said officials in the city police’s Economic Offences Wing (EOW). The two brothers along with Gala allegedly took help of SMS technology and launched a salvo which was first-of-its kind SMS fraud in India. According to EOW sources, in August 2006 the duo launched an aggressive and catchy advertisement campaign in the print media that read: “Nothing is impossible. The word itself is: I M Possible.”

\(^{21}\) http://in.answers@yahoo.com browsed on 22\(^{nd}\) June 2014.
As part of the attractive scheme, the Nadar brothers messaged random numbers, asking people interested in ‘earning Rs.10,000 per month’ to contact them. The “interested ‘subscribers’ were asked to deposit Rs.500 each, the duo claimed to be working with a US-based company which wanted to market its client’s products through SMS. The brothers even put up a website through http://www.getpaid4sms.com/ to promote their scheme. Subscribers who registered with them and came to their fold by receiving about 10 SMS’ every day about various products and were promised to pay Rs.10,000/- over 16 months to the investors. The amount was to be paid in instalments of Rs.1,000/- every few months. The brothers are said to ensure the subscribers by luring them in the guise that their American clients wanted to conduct a study about local response to their advertisement and were using SMS as it was the latest medium of communication.

The duo invited people to become agents and get more members for the scheme. Gala reportedly looked after the accounts. Initially, the brothers paid up small amounts. But when cheques and pay orders of larger sums issued by the duo were not honoured, the agents got worried. The SMSs too suddenly stopped. On November 30, one of the duped agents approached police and lodged a complaint after a bank failed to honour a pay order amounting Rs.2.17 million issued by the Nadar brothers. Then suddenly, Nadars and Gala disappeared, leaving their agents and investors in the lurch.
By December, the police were flooded with similar complaints. The police registered a case against the brothers and Gala and later transferred it to the EOW.

By December 2006, the scheme had over 50,000 membership in Mumbai alone. And it was suspected that hundreds of thousands from across the country were also hooked to the scheme.²²