Cybercrime and its impact on international business

Business

Cyber crime can be referred to any illegal activity that is executed with the help of a computer. Such kinds of crimes have always been executed ever since the computertechnologywas introduced (Cross, F 2007). With the advent of Internet, these crimes have gained an even faster pace. These thefts are not limited to enclosed vicinity. Accessing to data of an organization while sitting in another part of the world through internet has now become extremely effortless. This has drastic affects on organizations.

Stealing sensitive information such as data of the stock exchange, profits of a financial institution and even identities of individuals (Cross, F 2007) to access into their personal accounts are crimes that are increasing rapidly. This has led to many connotations for businesses worldwide; taking better security measures. Cyber crimes committed are unique in such a way that no physical existence of material or equipment is needed. Everything is done through the use of a computer (Nag, D & Bajaj, K 2005). This has made these crimes even more dangerous and difficult to control. Opportunities for cyber criminals

The increasingglobalizationhas led to the merger of activities all over the world. Banks, stock markets, multi nationals all have become connected with each other and technology has become the life and blood for all organizations. Used for various purposes such as enhancedcommunicationmediums and information sharing, technological advancements have also made businesses worldwide more susceptible to frauds and misuse of information (Grabosky, P 2005). Amongst all technological developments of the 20th century the internet is a widely used instrument for information sharing all over the world.

Between the year 2001 and 2002 there has been an increase of $6501 billion revenue being generated from business executed online (Grabosky, P2005). This means there are greater chances for individuals to commit cyber crimes that are both dangerous and risky to the business and also illegal in nature (ibid). Businesses worldwide make use of electronic communication means particularly those in the Western World and hence computer and cyber crimes have exploded after the 1990's (Chamely, H 2003).

The use of internet has fuelled the globalization process and hence the world has become smaller. People across the globe can now connect to each other easily though electronic means. However this advantage also carries perils to security. Issues such as fraud over the internet and piracy have been facilitated with the internet development (ibid). Multinationals have offices all over the world that are connected providing cyber criminals with the opportunity to act. It could be someone from within the employees or even a third party criminal.

With the pace of technological development, e-commerce has come into existence and businesses are shifting not only their single operations online but transferring their complete business processes online (Edin, M 2002). Bank for instances have started to offer international fund transfers from branches in two different parts of the worlds through internet which provides criminal opportunity for fund embezzlement which could mean loss of huge amounts ofmoneyfor the banks. Online businesses such as Amazon. com deal in online shopping and purchasing of goods without dealing in any brick and mortar business.

All such organizations function globally and hence are at a greater chance of cyber fraud then a business that only has one office in a single country and hence a smaller network and system. Impact of cyber crimes on business activities All businesses internationally have started to rely on electronic means of doing work and hence dependence on internet and technological sources has gained immense importance. Break down or illegal access to business information system and data base can have severe repercussions:

• Hindrance in day to day operations of a business like communication with employees across the borders. Some companies function internationally with employees connected through means of video conferencing or emails etc (Grabosky, P 2005). • A complete shutdown of business for instance organizations such as Wal-Mart function on a real time inventory management system and illegal access gained by a competitor means sharing of sensitive inventory data and customer preferences. • E commerce business entails developing of relation online with suppliers as well.

This affect is multiplied when cyber crimes not only gives access to financial data of the targeted organization but even its suppliers who may be functioning in another part of the world (Grabosky, P 2005). • Another great loss that the company might face is the declining confidence level of customers. Consumer have less trust in the business functions especially online retailing like online shopping, purchases and electronic banking. And with the increasing rate of such crimes companies might lose on their customers.

Thus companies must ensure that they do not loose on any important customers due lack of trust in the company’s system (Smith, A 2004). •

Economic losses to business resultant of frauds have also increased. These are measured in terms of declining profits or fraudulent transactions. An example could be the Russian TOC efforts to steal $10 million dollars from Citi Bank in the USA through forty unlawful fund usage (Jones, DM 2004). Another institution which has had to face the impact of cyber crimes in terms of economic losses is the stock market where traders trade online.

Company information (functioning in L. A.) available to individuals has been misused where wrong information was posted onto the internet leading to stock price increase and hence investors all over the world were affected (ibid). Types of cyber crimes and their impacts According to David Carter’s research (Grabosky, P 2005), there are three acts which can be labeled as cyber crime; entering into some one’s computer through illegal means and mishandling or damaging data, doing something illegal through means of the net or computer like piracy and thirdly, usage of computers to store some illegal information.

Cyber crimes that generally take place within an organization take place through emails, viruses transferred through email or through software being used by the company, access to company database for employee or customer information (Nag, D & Bajaj, K 2005). Further detailed classifications of cyber crimes and how they affect organizations is explained below: Fraud in telecom services: Such a crime is committed by gaining access to the organizations switchboard and making use of call time.

Not only does this cause the organization to be expensed with the bill worth the talk time used, is also a hassle for the individual subscribers using that particular service for instance an engineer in India was caught thieving

hundred Internet hours from a particular customer (Grabosky, P 2005). Criminals of such sort also gain access to calling card data for customers and hence they can make their calls on the expense of the customers who then have to pay larger bills and in return blame the company for poor device (ibid).

Hacking into computers to gain access to data: Hacking into company data which is password protected is another form of cyber crime that is very common. This has caused the most extensive damage to organizations especially organizations which mostly deal in financial data example banks. For instance, the accountant of a bank who is computer literate can gain access to finances of the bank and transfer funds in his name causing economic losses to the his organization (Cross, F 2007)

Cyber Terrorists: There work is very much similar to the terrorists that are a threat to national and international security of an individual nation and global relations. Cyber terrorists pose a threat to the national security of organizations by accessing into the central processing system (Cross, F 2007). This is particularly useful for business competitors to gain access to their competitors' financial or future plans and monitor their activities to gain competitive edge (ibid).

Piracy issues and counterfeiting: Reproducing products or services of various businesses without legal rights is another classic case of cyber crime. This is most extensively found in the media industry where movies are pirated without any legal rights and sold at even lower prices This has served as a problem for media producers example the movie " The world is not enough" starring James Bond was distributed over the internet even before it was

available for public by the officials (Grabosky, P 2005). Implications for businesses: what businesses need to do?

Cyber crime activities have caused losses of millions of dollars for companies however many companies do not prefer to report such incidents due to protection of their reputation and hence the data on cyber crimes is still incomplete (Grabosky, P 2005). The massive exploitation of these crimes has led businesses to take action. Global organization are making use of further technology to strengthen their systems of information sharing such as their data bases which contains customer information and financial data.

Focus is now on IT itself to develop such products, services and solutions that do not promote the risk of cyber thefts and frauds (Edin, M 2002) Along with the governments of various nations coupled with investments from individual organizations in the corporate world, efforts are being made create more secure systems that could prevent cyber crimes (ibid). Venture in IT infrastructure and security According to a report of the Internet association Industry in Australia, on an average thirty five different cyber crime attempts are made on an individual organization’s system (Grabosky, P 2005).

One of the greatest actions that companies have now started to take is focus on their IT teams in order to build a strong and secure network and data base. This team must not only focus on building an internal secure system but also focus on cross border security as most businesses now function globally (ibid). Investing money in infrastructure and training related to IT development against cybercrime protection is becoming a necessity for all organizations and this investment is no longer considered to be an expense (Edin, M 2002).

Such work was once and still is considered by some organizations as a function of purely IT engineers however this is not the case. As discussed how threatening the consequences of cyber frauds can be for any business, whether functioning online in a physicalenvironment, it is important that a collaborative effort of all members of the organization is made to avoid these risks (Edin, M 2002).

With this, development of a new concept has emerged; " cyber space security" (Smith, A 2004) which focuses on protecting not only business systems but also consumer information. Access to consumer information like their pin number and account information in a bank means risk of losing their money if their personal information is lost. Assessing financial impact of cyber frauds Another important analysis being conducted by companies across the world is the cost of security frauds being carried out within their organizations (Cashell, B et.

Al. 2004). Such an analysis provides the companies with the facts of how risky such crime attacks can be for them in terms of risks of information sharing with competitors, risk of alteration of consumer perceptions (Smith, A 2004) and risk of economic losses (Miller, R 2007) being incurred by the firm I case of the system being damaged and information extracted. The fact that these frauds and thefts have led to losses in monetary terms has generated the focus of the organizations in this regard.

According to survey conducted by a computerscienceinstitute, there has been an increase in financial losses reported by organizations due to cyber fraud in US in the past three consecutive years. Every year the percentage increase in frauds rises. According to that survey, corporations are not able

to comprehend the danger that such frauds expose the organizations to and hence they misjudge the consequences (“ Cyber crime bleeds US corporations: Financial losses from attacks climb for three years in a row” as reported in Koletar, J 2003).

The increase in such acts has not only forced businesses but also government of individual nations to act to promote business especially that of e-commerce. The IT Act introduced in India in the year 2000, also incorporated certain activities related to cyber crime in e-commerce business and activities such as hacking into computer systems, affecting privacy of consumer information and disrupting computer system encryptions and codes (Nag, D & Bajaj, K 2005). The basic reason was to instill trust amongst customers of e-commerce.

The use of Internet is a two way tunnel for organizations. They must it to enhance relations with business partners, suppliers and customers. At the same time, it has given a chance to hackers for committing crimes of mass scale that require the attention of policymakers in the organization and individual employees too (Salifu, A 2008). Thus internet frauds have become a problem not only for the developing nations who face a shortage of technological skills but en the developed world (ibid). Conclusion

Summing up the former discussion leads us to a conclusion that cyber frauds and risks have increased with the level of globalization and thus pose major threats to international business in the form of information loss, access of grave information by the wrong hands, threats to intellectual property right and to business operations, financial losses and wrong information being leaked out regarding a certain company (Edin, M 2002). With the

development of global business, more data is transferred and shared online through electronic means and hence cyber fraud has been motivated to a dangerous level.

The threat of such risks has lead businesses and even governments to develop solutions ensuring that customer and company information I not leaked out and does not reach the wrong hands. Companies are focusing on developing risk management solutions and are “ digitizing” (Edin, M, 2002, p. 17) their systems introducing stronger security checks and encryptions to protect the company against cyber frauds. Bibliography Cashell, B, Jackson, WD & Jickling, M, Webel, B 2004, Economic Impact of Cyber attacks, Congressional Research Service, Retrieved from scholar.

google. com, Retrieved on 8th April 2010 Chamely, H 2003, Cybercrime and Society, Geo-Sciences, Environment and Man, Retrieved from books. google. com, Retrieved on 8th April 2010 Cross, F & Miller, R 2007, West’s legal environment of business, 6th edition, Cengage Learning, Thomson West, USA Edin, M, Smith, B & Chiozza, E 2002, Challenges and Achievements in E-business and E-work, IOS Press, Netherlands Gobrasky, P & Broadhurst, R 2005 (eds), Cyber Crime: The challenge in Asia, Hong Kong University Press Jones, DM 2004 (ed.

), Globalization and the new terror, Edward Elgar Publishing Limited, UK Koletar, J 2003, Fraud exposed, John Wiley and Sons Inc , New Jersey. Miller, R and Jentz, G 2007, Fundamentals of business law, 2nd edition, South Western Cengage Learning, USA Nag, D & Kamlesh, B 2005, E-commerce, the cutting edge of business, Tata McGraw Hill, India Salifu, A, 2008, The impact of internet crime on development, Journal of Financial Crime, Vol. 15,

No. 4, pp. 432-443. Smith, A 2004, Cybercriminal impacts on online business and consumer confidence, Online Information Review, Vol. 28, No. 3, pp. 224-234.