Oversee Cyber Security as Hackers Seek to Infiltrate Even the Most Sophisticated Information Security Systems

Maryam Zafar
MPhil Scholar at IoBM, Karachi, Pakistan

Kashif Hashmi
Visiting Professor at IoBM, Karachi, Pakistan

Abstract

This report studies the impact of cyber security attacks its initial use and develop mechanisms for security of internet. There are numerous systems that are interconnected with internet and it is at risk and brief background of the cyber-attacks is outlined and our concentration in this report is on the impact of communication, positioning and implementing value delivery in order to increase productivity. It is concluded that the senior executives and government play major role in minimizing these risks and potential errors. In order to reduce them it is obligatory that IT professionals should take major responsibility of these issues and take productive measures. The research determines that cybersecurity threats also impacts Small and Medium Enterprises (SMEs), detecting just at the particulars for SMEs failing and the helping of IT inside the modern SME. The use of internet is becoming more often now a days and it is a major threat for SMEs due to oubsolete Microsoft versions technological systems therefore steps should be taken to mitigate these risks in order to minimize costs and boost performance by upgrading its software systems. The importance of cyber-intellienge should also be considerd due to vital practice to determine how firewalls coaching and detection structures work and compliance with risk management standards. There are different forms of attack such as viruses malware and these types of attacks create problem for initial users to have confidence and believe in technology. Such issue can be addressed by having antiviruses and it can eliminate financial as well as reputational losses for business in longrun.

Keywords: Cyber Security, SME, Information Security System.
JEL Classification: D80, L86

1. Introduction

Cyber security crime is increasing day by day due to the increasing number of users and activities on internet. It determines that there are different types of cyber security crimes such as breaches in information security, spam; information in to bids, Dos cyber-attacks and other types of attacks affects the performance of firm. It gives an overview of some of the growing cyber-risks and their latent influence in order to understand however the progress of the information society is actually at jeopardy. In additional reflects what the unalike investors can trigger to shape a safer and more secure information society and gives readers more refined considerate of the problems and challenges elaborated in developing confidence and safety in the use of IT systems. It provides an outline with amplified co-operation, teamwork, and information sharing, to join the distinct cyber security communities and one step wits, in order to permit investors to figure organized roadmap for cyber security.

Cloud computing, is one of the important element in defining an arrangement of remote servers on wi-fi system to allocate facilities in a nearby resources has developed most well-known method for governments in need of inexpensive,figuring on massive. Presently, the U.S officals has been on track to use its cloud computing structures, programme, and of cloud computing are uncountable risks that can take main effects on the data in raw form and services strengthened by this technology. The methodological innovation is often hindered by online risks. For instance, the relocation of information in raw form to third-party cloud providers has shaped a centralization of data and consequently more chances for offenders to steal critical info from a sole target attack (Paquette, S., & ., & Wilson, S. C., 2010). The supremacy of IT technology is the responsibility of board of directors, and comprises administrative infrastructures and measures that prove organizations IT endures company standards and includes organization aims. The investigation shows managements part is very significant in supervision threats of organizations, their portion in regulation of IT, their efficiency in transferring these threats and approaches through which that jeopardies can be shifted (Nolan, R., & F. W, 2005).

1.1 Purpose of the research

For the development and practice of the internet, developing trust and assurance is one of the key predictors. The goal is to evaluate some of the details for deteriorating trust, the varying landscape of cyber-risks, and intents to have closer glance at cyber security in the background of evolving nations and the exact difficulties these nations are going through when against increasing number of cyber-threats (Besnard D. A., Computer security impaired by legitimate users, 2004).

The purpose of this research is to show that director’s role is very important in overseeing risk of organizations, their part in control of IT, their efficiency in shifting IT risks and methods through which that risk can be migrated to or shared with others (Trautman & Altenbaumer-Price, 2011).

Many types of cybercrimes are not taken in to consideration but very little companies take responsibility on behalf of information available for losses. This is not new but it's a serious threat to company's reputation and those who are involved in cybercrime, there must be the presence of lawful act against those.

An important percentage of cyber-crime also undergoes unidentified, predominantly business intelligence where access to private papers and information in raw form is hard to discover. There is a risk that a corporation might craft at a weakness for months or even centuries as a consequence of an ongoing, but unobserved, safety breach. Cybercrime is first expected to rise, notwithstanding the greatest hard work of administration activities and cyber security authorities. Its development is reason for its existence due to the increasing amount of facilities existing online and the growing complexity of cyber offenders who are involved in a cruel inclination with security professionals (Abouzakhar, 2002).

2. Methodology

This article is actually a theoretical study of awareness of information security which is based on the psychological theories of behavior and awareness for instance theory of reasoned action which it illuminates that the goal of various campaigns of information security is to raise the knowledge of information security.

The research methodology gives an idea about the emerging cyber threats and their initial impact in order to understand whether or not growth of information society is actually is at threat. It also takes concern for different stakeholders; developing safe systems for them and gives person who reads outline about the good learning of future challenges.

It allows building a structure based on collaboration and sharing of information in order to link with individual cyber security groups and steps by permitting stakeholders to construct a strategy towards pertain to a goal for managing better cyber security issues.

3. Literature Review

Cyber security is considered as very important factor and its use is becoming more often. There are many systems that are allied with internet and it is at risk from hackers and other threats. These attacks are vulnerable to the system and are the root of instabilities which causes damage such as loss of financial information and security issues. With one powerful threat the entire systems remain at risk for number of hours and creates discrepancies, security or safety of computer has become very integral component of system alignment, sequence and growth. On past decades, safety from legitimate users is common issue that is brought in to light from hackers view point. The importance has been given to ends and means used to access systems and break analogous to bits. Looking at this side it means this research area has been and still is, it needs to identify the exact implication of authentic users (e.g. end-users, security officers, managers, designers) who are important part of cyber security systems (Besnard, 2004).

3.1 Human violations in contributing cyber security attacks

The previous studies are based on human blunders and defilements of end users and system management in computer and info safety. This information is brief in a theoretical outline for exploration of the human and structural issues regarding computer and information safety. This outline comprises human mistake classifications to define the labor circumstances that donate unfavorably to computer and info security, i.e. to security weaknesses and breaches. The subject of human error and defilement in computer and info security was discovered through a sequence of 16 meetings with system managers and security authorities. The interviews were acoustic recorded, and examined by coding exact refrains in a bulge structure. The consequence is a prolonged outline that classifies kinds of human error and classifies exact human and structural issues that donate to computer and information safety. System managers tended to view mistakes shaped by end users as more deliberate than accidental, while mistakes shaped by system managers as more accidental than deliberate. Structural issues, such as message, security code of conduct, strategy, and structural, were the greatest often cited factors related with internet and info safety (Kraemer, S., & Carayon, P. , 2007).

3.2 Act of Cybercrime

The propaganda about the knowledge of cyber terrorism and cybercrime is debauched triumph a point somewhere a little cynicism jeopardies being yelled miserable as deliberate illiteracy of the possibility of the problem. So, let's admit by confessing that cyber security is an honest existing challenge.

From current decades, progressively, cyber-attacks have become the topic of discussion. Closing down atomic equipment's, air protection structures, and electrical chart sheets, cyber-attacks stance is considered as a thoughtful risk to national security. As a consequence, cyber-crime must be preserved as items of war. Yet the occurrences appearance slight similar the equipped attacks that the law of war has usually controlled. The terms, “virtual-fighting,” and “cyber-war” are often secondhand with slight respect for pardon they are destined to comprise. This lack of clearness can provide variety of problems overall more problematic to project an expressive lawful reply (Hathaway & Levitz, 2012) .

3.3 Role of SMEs in Cyber Security

The study governs the portion of Small and Medium Enterprises (SMEs) in the UK economy,detecting exactly at the particulars for SMEs fading and the share of IT inside the modern SME. A complete valuation of cybercrimes is formerly assumed, intent on those dishonesties that are most appropriate to SMEs.Case study regarding businesses present primary indicator info on the mark of cybercrimes on SMEs. Now, greatest number of the small and medium enterprises is reliant on outdated technologies. There is inability in technical skills essential to yield good products. Most of the SMEs do not have information of advanced technological systems and prospects about their corporations. This difficulty is a key problem on the means to current technology founded SME system. It is related to the incapability of small and medium-sized enterprises to transport obligatory equipment and amenities for the drive of growth. This incapability may right or circuitously affect the competence and output of labor and henceforth may consequence in inferior efficiency as well as lesser financial competence at large.

The small Pakistani firms still used obsolete machines for organization and manufacturing in their corporations. This consequence in creating low-quality goods at maximum price vending it at minimum rates. There is a previous requirement to grow a structure to bond this gap and to discourse current technical breaches that can be recognized by emerging a system of manufacturing information net for SMEs mechanisms (Smith T. C., 2003/2004).

3.4 Increasing cyber security attacks by legitimate users

Cyber security is considered as a very important factor and its use is becoming more often, which sometimes contains problems in the system. There are many systems that are allied with internet and it is at risk from hackers and other threats. These attacks are vulnerable to the system and are the root of instabilities which causes damage such as loss of financial information and security issues. With one powerful threat the entire systems remain at risk for number of hours and creates discrepancies, security or safety of computer has become very integral component of system alignment, sequence and growth. There are so many problems and to counter this issue then necessary steps taken by management are not very effective as expected. There should be prevalent research and best tools adopted for proper understanding of different forms of attack, prevent and be ready against these security threats. On past decades, safety from legitimate users is common issue that is brought in to light from hackers view point who are central portion of computer safety structures (Besnard D. A., Computer security impaired by legitimate users., 2004).

3.5 Board of director’s responsibility for execution of efficient IT systems

It is important that top management should take responsibility at higher level and this specific topic is also significant in analyzing organizational procedures that consists of IT security systems in compliance with organizations strategies and objectives. Cyber security involves how board of directors oversees risks and develops systems to control them and implementing procedures through which these risks can be shared with others.

The information security has become significant and influences many administrations. Over the years, there has been a fast dissemination of e-commerce and a growing number of integrated systems, resulting in growth of safety risks (Abouzakhar, 2002).Today, various corporations see information as a vital strength and therefore it is important that the privacy, honesty and obtainability of this resource are kept undamaged. Thus, due to the increasing risks and worth of material, there has been a demand for better accountability to be accepted by the board of directors concerning information security problems (Von Solms, 2001).

3.6 Strategic alignment of IT systems raises technical competence

It has been noted that the business capabilities; combine organizations, reorganize businesses and facilitate worldwide competition. Concluding, it can be understood that with growing demand of technology and information within internal systems of an organization, managers are significantly being forced to adopt efficient security steps in order to safeguard their possessions. (Chan & Barclay, 1997). It can be divided in to three additional explanations for better board participation in information security development and regulation. The initial and maybe most noticeable motive is that executives are accountable, often officially, for their administration’s risk management system and inner control systems. For instance, the OECD (2004) Principles of Corporate Governance recommend that a firm’s board should have accountability for evolving a risk strategy and guaranteeing the honesty of organizations for monitoring risk.

3.7 Ethical compliance of IT governance with executive’s supervision

Furthermore, fraudulent behavior and lapses in organizational governance have forced the USA security and exchange commission to yield the Sarbanes-Oxley Act. The Act, like various in other countries, has a simple principle: "...good business governance and right professional practices are no longer elective particulars" (IT Governance Institute, 2004, p. 12). Its aim, consequently, is to improve corporate governance and reinforce internal payments. Hence, official stockholders are progressively having a detailed look to the governance practices of the businesses in which they invest or evade, looking for organizations with decent governance does as an optimistic sign of a shareholder-value focus (Witt, 2001).

The information technology governance practices belong to all of the processes of controlling whether launched by government network or informal organization and designs of authority for the core IT events in corporation's businesses, with use of IT structure either implementation of project management. During past decades, these key methods of IT governance have become dominant: central and distributed. For instance, detailed analysis on contingency theory in association with specific approach of IT governance, most of the hypothesis has been laid on particular effects of contingency issues. The underlying hypothesis is on these research states in reality; business firms are subject to the tugs and gravities of more than one contingency force. Therefore, study consists of discussion on the theory of multiple contingencies in order to inspect how contingency forces affect the particular approach of IT governance.

Most of the hypothesis determines that contingency forces interrelate with each other by also cumulative, diminishing, or superseding their common effects on the IT governance approach. There are three situations of multiple, interrelating contingencies have been acknowledged: strengthening, contradictory, and dominating. Each of these situations of multiple contingencies is assumed to affect a specific method of IT governance. (Sambamurthy, V., & & R. W. , 1999). There is last factor that states maximum board involvement in information security issues is that it could be number one factor that influences the victory of an organization's information security resourcefulness. There are other factors which contribute to a firm's success are applying standards which determine an information safety strategy that imitates business aims, an employment approach that is in compliance with an organization's philosophy, norms and the provision and promise from management. The increase of e-commerce has also drawn attention towards responsiveness amongst governments of the safety risks to which they are probable to be visible. Definitely, it has been described that safety risks, and fear of security pressures, establish the highest prevention to an extension in the acceptance of e-commerce (Ernst and Young Survey 2001:1).

4. Cyber security threats declines trust of internet users

Enlarged interconnectivity, is not though, the only issue manufacture computers, and the material stored therein, less protected (Baskerville, 1991).The final construction was also recognized as an achievement aspect of information security strategies in current investigation (Fulford, 2003).It is problematic to consider how these three dangerous success factors can be attained without vigorous board meeting. Therefore, it is authoritative that executives increase them participation in their firm's safety issues.

In comparison with the last two periods, the internet has changed many characteristics of recent lifestyle. There are 4 million international users at the end of year 2006, which constitutes that its use is increasing day by day. For couple of ages people across the world and from all spheres of life have been listening about the assured developments and variations, the internet will convey to their existence. This paper shows full adequacy of internet has not been understood. The major reasons beyond this approach are of keeping trust on the availability of internet and decreasing believes on its use. Its use is becoming prominent on daily basis which shows growth and open up new horizons for hackers and criminals to continue cyber-crime acts in order to damage online susceptibilities or even sensitively hack infrastructure for different states. Viruses, malware, fraudulent practice of sending emails, determine stealing of sensitive data, zero-theft exploits, denial of service and other attacks are weakness which risk cyberspace and imperiling the very imminent of the internet. With junk mail and other misuse secretarial for 90 per cent of the e-tailing over the internet, this is critical situation in this medium for future growth and progress of universal information society. Without significant development in structuring trust and safety in the use of ICTs, users' fading confidence on the internet might put boundary on its development and converting potential (ITU, 2006a). Reestablishing faith in the e-atmosphere and dealings, and straightforward online security, is important for the development and practice of the e-commerce.

4.1 Classifications of cybercrimes

The Cyber security problems are complicated and these are continually growing, So at the global level, synchronized policy act is required to discourse the trials and pressures to it that are developing. There are new forms of cybercrime have been introduced such as pop-ups as genuine notices from mail software in practice increasing use of computer as these are not recently selected by most of spam filters. The message in these files states: '' Caution concealed files might have been installed on computer from cookies or websites viewed''. The person is indicated as fraud or scam needs to put your finger receive and download a ''secure'' database to reject the hypothetical files from your pc. Image spam is another type of spam which shows sent messages implanted pictures which are disseminated quickly through email inboxes (security computing, 2006). Instead of using fixed pictures, or text messages are avoidable and detectable by anti-spam software which play crucial role on dependence of typing spam content, giving spammers a bigger choice of having their messages remain uncovered (Sund, Towards an international road-map for cybersecurity. , 2007).

4.2 Financial influence of IT security breaches

The internet safety is an influential concern for all the businesses that put heavy amounts of investments in IT security has been a particular trial because of shortly understanding and measuring the economic influence of breach. The IT security breach can be defined as any event that results in unauthorized access of data through this security laps.

The daily use and urgency of e-commerce requires the internet to be safe and protected but on ground reality differs as the internet is always the target of periodic attacks. Many internet reviews disclose that in between 36 and 90 percent of businesses; described computer safety breaches from past decades. A final conclusion on the results indicates degree of damages and losses as an incident on IT security MI commitment, dependence on self-reported company data undermined trustworthiness of results. Though the operating income and sales of breached companies didn't decline in the succeeding quarters after the breach, and in the third quarter, ROA (return on assets) declines. The market which has reaction on logical basis showed a loss of profits/cash flows etc. was a result of denial of service cyber-attack as opposite to web address disfigurements where no economic loss is determined (Garg, A., & Halper, H. , 2003).

4.3 Rules for cyber-warfare

The second part of research determines; go to investigative that in what manner, the rule of conflict force oversees cyber- attacks. For this purpose, it is analyzed that the way the law of war, utmost of which was established at a period when cyber-crime was unexpected, smears to this novel region of battle. In comparison year of 2010, Iran's nuclear database crushed to a stop, the topic of an urbane attack that directed nuclear machines that rotate around enthusiastically out of switch. The missile? Stuxnet, a processer "worm" that seems to have various writers about the environment and was probable verified by Americans and Israelis at the Israeli Dimona complex in the Negev desert. (1) A few periodicals advanced, a so-called "dispersed renunciation of facility" attack removed the entire people of Burma rotten the Internet directly previous the republic's first nationwide vote in twenty ages. (2) Spectators doubtful that the armed regime in Burma synchronized the bout to shut close the net and thus, limit the permitted movement of info, (3) but American community bureaucrats have fought censuring the attack on the management, even as they have disapproved the election. The United States could reinforce its national law by charitable national illegal laws addressing cyber-attacks additional regional result and by accepting incomplete, globally allowable countermeasures to battle cyber-crime that do not take room throughout a continuing equipped fight. Yet the test cannot be encountered by national improvements unaccompanied (Hathaway & Levitz, 2012) .

5. Conclusion and recommendations

Companies now days reflect security as one of the most significant subjects on their program, because the cumulative number of security openings pose a main risk to the faithful implementation of business policies and may have undesirable effects on corporate worth. In order to enjoy fruitful IT governance, there must be provision and promise from upper hierarchy. The context should discourse tactical arrangement, presentation organization, danger dimension, value distribution and resource supervision. There must be actual proposal of IT governance, spending of board of directors such as regulatory mechanisms for info and associated technology (COBIT) can be significant component in distrusting regulation and governance of complete information and systems that make, operate and accountable for recovery. The inspection team should have IT skill to discourse audit matters for prompt standby of board chair connected to cyber problems and treatment of damage of delicate info.

Risk management confirms the thought of all probable risks and weaknesses, as well as the appreciated possessions. Current methods such as best-practice strategies, information security standards, or field specialists and risk organization methods that are extremely acknowledged within the public come up with inadequacies. By working on a enduring defense pawn to malware is for small and medium size enterprises aganist a mainstream of occurrences. Therefore, small and medium size businesses should verify that they have normal contingency plan in situation of an attack and should be vital businesse's IT plan and moved to all employees inside the company. Large companies could act as an indicator that is an outcome to the IT department and the outcome would founded on their internal evidences and minor thought would be compensated to external issues. It should encompass theoretical study of responsiveness of information security which is completely based on the mental theories of conduct and disseminating awareness for instance theory of reasoned action.

The research signifies that theories of psychology constructed on knowledge, teaching and ecological transformation can be hired to make means well-organized for consciousness of information safety. Furthermore, it brightens that the goalmouth of various movements of information security is to increase the awareness of information security. All these security measures can reduce financial loss and increase financial performance in order to generate more revenue than losses.

Therefore it is concluded that there should be proper risk assesment of cyber internet analysis should be aware of triggring events,likelihood of occurance,ease of implementation,immediate impact and others.There should be penetration testing a major test used to determine system faults and weaknesses.The top management should support risk analysis in order to project and retriofy latest features software systems and anti-viruses placement of anti-malware,firewall and intrusion detection products and denial of service attacks (Sommer & Brown, 2011).

References

Abouzakhar, N. S. (2002). An intelligent approach to prevent distributed systems attacks. *Information management & computer security,*, 10(5), 203-209.

Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems,*, 1(2), 121-130.

Besnard, D. A. (2004). . Computer security impaired by legitimate users. . *Computers & Security, , 23(3), 253-264.*, 23(3), 253-264.

Besnard, D. A. (2004). Computer security impaired by legitimate users. *Computers & Security, ,*, 23(3), 253-264., 23(3), 253-264.

Besnard, D. A. (2004). Computer security impaired by legitimate users. *Computers & Security*, 23(3), 253-264., 23(3), 253-264.

Chan, Y. H., & Barclay, D. C. (1997). “Business strategic orientation, information systems strategic orientation, and strategic alignment ”. *, Information SystemsResearch,*, Vol. 8 No. 2, pp. 125-50.

Clark, M., E., H., & C. (2013). Unlike chess, everyone must continue playing after a cyber attack. *Journal of Investment Compliance*, 14(4) 5-12.

Fulford, H. &. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security,*, 11(3), 106-114.

Garg, A., , C., & Halper, H. . (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security,*, 11(2), 74-83.

Hathaway, R. O., & Levitz, P. N. (2012). The law of cyber-attack. *California Law Review,*, 817-885.

Khan, B., Alghathbar, K., Nabi, S., & Khan, M. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, 2(26) 10862.

Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: an empirical investigation. *Journal of information Technology Management*, 17(2), 13-22.

Kraemer, S., & Carayon, P. . (2007). Human errors and violations in computer and information seurity. *The viewpoint of network administrators and security specialists. Applied ergonomics,*, 38(2), 143-154.

McFadzean, E., Ezingeard, J., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online information Review*, 31(5), 622-660.

Nolan, R.,, M., & F. W. (2005). Information technology and the board of directors. *Harvard business review,*, 83(10), 96.

Paquette, S., , J., & ., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly,*, 27(3), 245-253.

Sambamurthy, V., & , Z., & R. W. . (1999). Arrangements for information technology governance. *A theory of multiple contingencies. MIS quarterly,*, 261-290.

Scott Paquette, P., & Susan C. Wilson. (13 April 2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, 27(3), 245-253.

Siegel, C., Sagalow, T., & Serritella, P. (2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security.

Smith, T. C. ((2003/2004)). Minimising the threat of cybercrimes to SMEs . *(Doctoral dissertation, University of Leeds, School of Computing).*, 65.

Smith, T. C. (2003/2004). Minimising the threat of cybercrimes to SMEs. *(Doctoral dissertation, University of Leeds, School of Computing).*, 65.

Sommer, P., & Brown, I. (2011). Reducing systematic cybersecurity risk. *Organization for Economic Cooperation and Development.*, 3.

Sund, C. (2007). Towards an international road-map for cyber-security. *Online information review*, 31(5) 566-582.

Sund, C. (2007). Towards an international road-map for cybersecurity. . *Online Information Review,* , 31(5), 566-582.

Trautman, L., & Altenbaumer-Price, K. (2011). The Board's Responsibility for Information Technology Governance. *John Marshall Journal of Computer and Information Law*, 29, 313.

Trim, P. (2005). Managing computer security issues: preventing and limiting future threats and disasters. *Disaster Prevention and Management: An international journal*, 14(4), 493-505.

Von Solms, B. .. (2001). Information security—a multidimensional discipline. *Computers & Security*, 20(6), 504-508.

Witt, P. S. (2001). How Directors View Their Roles and Responsibilities. *Boards at Work.*, pp. 243-245.