Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI:10.21474/IJAR01/2753
DOI URL: http://dx.doi.org/10.21474/IJAR01/2753
ISSN NO. 2320-5407

RESEARCH ARTICLE

INFORMATION SECURITY THREATS: COMPUTER HACKING.

[*]MunadhilAbduljabar Alsalim[1], Ahmed Munadhil Alsalim[2], Amr Hail Ghilan Al-madhagi[2] and Salah Mortada Shahen[2].

1. Cihan University/Sulaymaniyah.
2. Utara University Malaysia.

Manuscript Info

Manuscript History

Received: 15 November 2016
Final Accepted: 17 December 2016
Published: January 2017

Key words:-
Information security threats, information threat, security threats source and hackers.

Abstract

The purpose of this paper was to study information security threats, information threat, and security threats source with a threat agents. It focused on the meaning of hackers and perceptions of public against the word ‘‘hackers’’ with a special emphasis on different types of hackers within organizations and in the society. The empirical literatures provide the best way to prevent the problems of hacking in the society and shows that white hats, black hats and spy hackers motivation strategies are largely involved and effective to check organizations performance. It proposes quantitative approach with the design and descriptive for this study. The questionnaires will be used will be selected as a means to collect data with a simple random sample of the company's employees as observers / participants in the study.

Introduction:-

background of the study:-

Information is esteem, and more corporations have understood that information security dangers can impact business prepare coherence and open picture, relations, can bring about monetary misfortune, impact relations with customers and accomplices and their fulfillment, and additionally make the issues with lawful dominant presences if there should be an occurrence of non- compliance (marchewka, 2014).

The world has turned into a worldwide town because of the broad utilization of the web where with a tick of a mouse, a solitary thought can achieve billions of individuals over the globe. The advantages of information for corporations are obviously incomprehensible. Information is as of now the main thrust of organizations and economies because of the globalization of products and markets. The internet has empowered information accessibility in this manner making it a most important information source and a method for information transmission. The obstruction achieved by area is starting to die down as virtual organizations are as of now running round the clock. Increased dependency on information by organizations has consequently led to an increase on the dependence of the cia (confidentiality, integrity and availability) are the three main features of information security. The privacy guarantees that data is accessed only by those who have rights, information integrity serve as the state of being complete and uncorrupted and availability will enable users or other systems to access information(solms, &niekerk, 2013;shedden, smith, &ahmad, 2010;whitman &mattord, 2008). The paper presents a thorough details on information security threats, overviews of threats with the security threats source through the internal and external threats caused. This causes may likely to be the positive impacts to better identify threat’s characteristics in order to

Corresponding Author:-Munadhilabduljabaralsalim.
Address:-Cihan university/sulaymaniyah.

propose suitable measures to reduce risks. The succeeding of the paper is organized as follows. The next segment outlines information threats agents (accidental, contributory and deliberate). Section 3.1 discussed with word ‘‘hacker’’, 3.2 stated various types of hackers and the 3.3 section consider how the problems of hackers can be prevented in the society. While the last section 3.4 provide the recommendation and conclusion at the ends of the paper.

information security threats:-

'Information security is the assurance of data and its basic components' (whitman&mattord, 2008). Ferrari and thuraisingham (2006) portrayed information security as shielding information and frameworks from dangers, for example, unapproved access, unlawful use, exposure, interruption, alteration or destruction. According to ponemon institute (2014), and walters (2014) uncovered that information or security ruptures happen when information is not adequately secured and unapproved people can get to it.an information break can prompt to genuine outcomes. For organizations, a break regularly includes genuine budgetary misfortunes, expensive claims, reputational harm and in outrageous cases loss of business. Wholesale fraud, money related misfortune and harm shockingly appraising are a portion of the results of information crack for people. Information crack regain takes numerous years and the money related harms are cruel (ponemon institute, 2014).

Information security (infosec) is sweeping and incorporates specialized, behavioral, administrative, philosophical, and hierarchical methodologies that discourse the insurance and moderation of dangers to information resources (zafar&clark, 2009). Despite the fact that a portion of the information systems inquire about in the infosec field has considered socio-philosophical concerns or socio-authoritative concerns, it has basically cantered around specialized issues concerning the outline and usage of security subsystems (choo, 2011). For example, advanced technical approaches to deal with forestall interruption into authoritative frameworks (hansen, lowry, meservy, &mcdonald, 2007), discovery of denial of service attacks (zhi-jun, hai-tao, ming-hua, &bao-tune, 2012), and more advanced solutions for firewall protection (ayuso, gasca, &lefevre, 2012).

Although these technical, externally focused efforts are important, one zone that is an overwhelming shortcoming in legitimately securing information resources is the individual client inside an organizations (posey, bennett, &roberts, 2011; warkentin&willison, 2009; stanton, stam, mastrangelo&jolton, 2005). This is an especially critical problem since investigators evaluate that about half of intrusions and security violations happen from inside an organization by authoritative insiders (richardson, 2011; baker, goudie, hutton, hylender, niemantsverdriet, &novak, 2010). Until recently, research exploring the operational aspect of information security has been lacking.

However, the improvement of information and communication technologies and expanding availability to the internet, organizations get to be defenseless against different types of threats. Indeed, their information gets to be presented to digital assaults and their subsequent harms. Dangers originate from various sources, similar to representatives' exercises or programmer's assaults. The financial losses related misfortunes brought about by security ruptures, for the most part cannot definitely be distinguished, on the grounds that a critical number of misfortunes originate from smaller scale security episodes, created an underestimation of information framework security chance (shiu, baldwin, beres, mont, &duggan, 2011; farahmand, navathe, sharp, &enslow, 2005). Hence, managers need to know dangers that impact their advantages and recognize their effect to figure out what they have to do to counteract assaults by selecting suitable countermeasures.

To find these threats, threats sources and specific areas of the system that may be affected should be known, so the information security assets can be protected in advance (alhabeeb, almuhaideb, le, &srinivasan, 2010).

statement of the problems:-

As the modernity of cyber hackers intensifies keeps on expanding, their techniques and targets have likewise advanced. Rather than building the expansive internet worms that have turned out to be so well known, these offenders are presently investing more energy focusing on riches gathering violations, including misrepresentation and information theft (damico, 2009). Cyber-media india online ltd (2006), recommends that since home cuestas regularly have the poorest efforts to establish safety set up, they have turned into the most broadly focused on gathering. Cyber media reports that 86% of all hacking attackers are gone for home users. As attacks on homebased clients’ increment, new systems are surfacing, including the utilization of noxious code to attacks web programs and desktop applications.

Damico (2009) posists that by surveying that is efficient and effective in technique can limit the probability of been hacked. Although personal system users may not feel like they are associated with a system, any action on the internet can be considered "arranged action." therefore, security measures utilized by systems may likewise profit the home users. Switches and firewalls can regulate admission to a home computer, yet more particular strides might be used.

Top layer security (2008) considered the variance in network intrusion prevention and network detection systems. Its findings suggest that prevention systems "automatically detect and block malicious network and application traffic, while allowing legitimate traffic to continue through to its destination". It furthers stated that system that is detected may notice an unwarranted activity, but where is the protection from fast acting attacks? A system that is fully secured can stop and prevent malicious sites from entering or gaining access to a computer system. "the prevention system must operate with switch-like latency at all times". Due to advancement in technology old users of technology cannot be protected based on previous technology, they have to be up to date in other to beat malicious software.

a system that is prevented against virus and malicious software's must not block sites which are not dangerous to the system even if the system is at risk of an attack. It must have an extent to prevent malicious programs from damaging the system and must be up to date at regular intervals.

as a matter of facts, personal users of system must be known to various techniques which is been used in hacking and breaking in to a computer system.in hacking, the person can make use of various instrument to access information via the world wide web. We should bear in mind that system is not always stealing useful data but can also be used in saving content (such as pirated movie downloads) or a system could be recruited into an online 'bot army' (damico, 2009). In other to increase private owner's security against hackers, some steps can be taking such as making sure that his computer system anti-virus is updated. Computer users have always been attacked by malicious software due to negligence on their own part in updating the software which has been paid for by them. Virus data base needs to be constantly updated because of malicious threats always keep on transforming that is the reason why software updates are always available, in a situation where it is not updated then the user system might be infected with malicious software.

Hackingalert (2008) suggested a means through which users can get solutions by installing appropriate firewall. The firewall's acts as a shield in stopping unwarranted access to a computer system. However, a firewall does not erase data which is stored on the system. To be more secured an anti-virus subscription is needed in case it was able to bypass the firewall it will not be able to pass through an effective anti-virus. We have so many trogan and virus software in the market and running a different type will help in eliminating threats to a network or system.

Chapter two: literature review:-

Threats:-

A threat is the adversary's goal, or what an adversary might try to do to a system. It is also described as the capability of an adversary to attack a system (swiderski&snyder, 2004).

security threat source:-

A threat can be caused by internal, external or both external and internal entities.

- Internal threats is a situation when someone that has access to network with his details or credentials is negligent in his duties. A threat that is within the firm is usually because the worker failed to follow the due process or because he failed to report a specific threat (silowash,et al 2012).
- Jansen (2011) posits that threats outside the organization can be from outsiders not working for the organization. They have no access given to them by the firm in assessing there system or network. Organizations have to make sure that by pass by outsiders is cut off of natural disasters: hurricanes, fires, floods and earthquakes. External threats is done when network are intertwined together (wired and wireless), physical intrusion, or a partner network.

information threats agents:-

The threat agent is the on-screen character that forces the risk to the system. There are currently wide range of sorts of threats to information security that may achieve loss of loss of confidentiality, integrity or availability.this

studyidentified three categories of information threats such as accidental or unintentional, contributory or instrumental, and deliberate or intentional (greitzer, strozer, cohen, moore, mundie, &cowley, 2014; afyouni, 2006).

accidental or unintentional threats:-
Accidental or unintentional threats are those brought on by events outside the it hardware (i.e. Those that are outside human ability to control) such as natural disasters, technological disasters and human threats (bompard, huang, wu, &cremenescu, 2013).

natural disasters:-
Natural disasters are one of the primary dangers to information. The term 'environmental threats' is also used by some authors to depict these sorts of threats. Natural threats are dangers brought on by non-human agent. It comes, in the first place, from environmental threats like fire, lightning, flood, tidal waves, wind or water and likewise, due to animals and wildlife which cause extreme harm to information structures like lightning, tidal waves (like tsunami), floods and fire. Without a doubt, this class incorporates different dangers, for example, terrorist attacks, riots and wars (jouini, rabai, &aissa, 2014).
2.2.1.1.2technological threats

Innovative dangers are created by somatic and compound procedures on factual. Physical procedures incorporate the utilization of physical intends to pick up passage into confined ranges, for example, to build, compound room, or whatever other assigned territory like burglary or harm of equipment and programming. Be that as it may, synthetic procedures incorporate hardware and programming innovations. It, additionally, incorporates indirect system support equipment like power supplies (jouini, rabai, &aissa, 2014).

human threats:-
This class includes threats caused by human actions such as insiders or hackers which cause harm or risk in systems (abdulkadir, &dzarma, 2015; shaluf, 2007).

Contributory or instrumental:-
Contributory or instrumental intimidations are presented by the disaster or non-existence of adequate measures. Uncontrolled access to it equipment would constitute a procedural threat (alhabeeb et.al, 2010;poulsen, 2003). Hayes (2014) posits that technical disaster causes the main procedure to be hacked. For instance, someone who has no authority may have an access to a computer data if there are no necessary measures to check people. If there is no restricted access to key places then important information or data can be accessed to un authorized individuals. An organization that has control over it data and updates it regularly and usually amends it at interval bridges the gap of a potential hack. All computer operators that have unqualified system operators are usually prone to hacks. For these reason, administrators must make sure that only qualified people are employed and people who are trusted are in such seats or positions. Similarly, in case of leave or if an employee services are no longer needs, all organization id card or anything that can make him have access to the premises must be collected at the point of exit.

Contributory or instrumental threatss are presented by the disappointment or non-presence of satisfactory methods. Uncontrolled access to it hardware would constitute a procedural risk (alhabeeb et.al, 2010; poulsen, 2003). Hayes (2014) procedural threats cause the correct procedures to be by-passed. For instance, an unapproved individual may acquire access to computers hardware or media if there are insufficient checking systems. In the event that inadequate intelligent get to systems exist then information might be perused or overhauled by individuals with no power. Control over the advancement of new structures and the change of existing ones averts inaccurate projects being put into live utilize. All methods are at hazard through temperamental work force. Personnel routines ought to guarantee that exclusive respectable staff are utilized in places of trust. Exit systems ought to guarantee that staff leaving the organization do not hold their distinguishing proof or means of access.

Deliberate or intentional:-
Deliberate or intentional threats can be defined as the threats designed for either benign or malicious purposes to destroy or abuse targeted information. These include malware, hacks, intrusions, denial of service (dos) attacks, theft, fraud, espionage and arson (ateeq, 2012).

Malware:-
Malware is programming that is intended for a noxious reason. The software can contain viruses, trojan stallions and spyware (dezfouli, dehghantanha, mahmod, sani, shamsuddin, &daryabar, 2013). Solomon and chapple (2005) archived that viruses contain malevolent code intended to adjust documents to perform unapproved activities. Viruses are intentionally coursed to computer users with the expectation of spreading to different clients and harming or obliterating their information. The impact can be harmless (for instance, a screen message), or it can be a genuine defilement of either data or software (shim, qureshi, &siegel, 2013).

laptop theft:-
Laptop theft is a critical threats to users of laptop computers. Casualties of laptop theft can lose equipment, programming and key data that have not been moved down. Criminals may likewise access touchy information and individual data (brown, 2009).

Fraud:-
According to action fraud (2011), described fraud as any purposeful or consider act to deny another of property or cash by cleverness, fraud or other out of line means. It is one of the threats that can genuinely influence information. Misrepresentation or fraud is utilized as a part of numerous areas for various purposes, for example, internet misrepresentation and financial fraud. Internet fraud has gotten to be one of the most effortless courses for vandals to pick up cash or essential data utilizing strategies, for example, phishing tricks.

Intrusions:-
Vacca (2009) revealed that interruptions are assaults utilizing any strategy to increase unapproved access to a system. Denial of service (dos) attacks are intended to avoid honest to goodness access to systems and cause the inaccessibility of assets (desai, patel, somaiya, and vishwanathan, 2016). Hacking in to a computer software or data occurs when an individual is not giving the permission to handle such data. Hacking is a process of bypassing a network while to tab means to connect to a cable (easttom, 2006). Hacking is usually performed to prove the technical skill of the hacker but may destroy the confidentiality, integrity and availability of data.

Hacking and tapping happen when some person sets out, without power, to investigate pc held information. Hacking suggests breaking into a system while tapping infers truly partner into a connection (easttom, 2006). Hacking is commonly performed to show the particular mastery of the developer however may wreck the mystery, genuineness and openness of information.

Hackers can abuse information by inserting a piece of code into a program. This code operates at some future date to corrupt files or software.

Hacker:-
hackers are wise individuals who might not have a passion for their talent initially but they do it for the money involve. The main motive of hackers is to make information available for everyone and they think it is right to use programs produced by someone else in achieving their objective. Before we proceed it is imperative to understand what hacker is (loader &thomas, 2013).

In the first instance, a hacker cannot be regarded as a criminal because he does not break the law nor does he release virus to the system. Similarly, a hacker cannot be regarded as a kid who just sits down and eats and watches his environment (sanglakhi, 2013).

some one that hacks is usually not a computer guru because he cannot enter security codes of all websites nor software applications. Similarly, he is not someone who just sits around to do carpentering work like assembling and coupling of wood to make a chair or furniture (sanglakhi, 2013). Similar to the findings of sanglakhi (2013) sees an hacker as some features and his characterized as someone with interesting features, he uses his brain to think out of the box and usually tries to do what other people do not believe in or even thought of doing.sabahi (2011) posits that someone that explores and creates new things, new episodes and also does things in ways which no one as imagined or thought of as a hacker

In 2013 all these definitions are have turned to significantly more negative meanings. According to the merriam-webster dictionary (2013) described “hacker” as “a person who illegally gains access to and sometimes tampers with

information in a computer system." This definition has led many people to fear computer hackers but not all hackers are bad people. Hackers can be put into different categories which are discussed below.

types of hacker motivation:-

According to online safety expert for intel security,robert (march 16, 2011), xu, hu, and zhang (2013), and bratus (2007), reported that computer hackers are typically grouped into various types, white hats, black hats, grey hats, script kiddie,hacktivist, cyber terrorists, spy hackers,phreaker, and the final hacker is motivated by government popularly known as state sponsored hackers.

White hats attempt to help prevent weak systems from being hacked and attempt to make the web a safer place for individuals. Black hats do the opposite; they cause problems and can sometimes harm individuals and companies by stealing identities, money and other things as well. A grey hat hacker is someone who is between white hat hacker and black hat hacker. Grey hat normally do the hacking without the permissions from the administrators of the network he is hacking. But he will expose the network vulnerabilities to the network admins and offer a fix for the vulnerability for money.script kiddies is a derogatory term for black hat hackers who use borrowed programs to attack networks and deface websites in an attempt to make names for themselves. A hacktivist is a hacker with political intentions. The hacktivist has the same skills as that of a hacker and uses the same tools as the hacker.

The main reason of hacking is to create attention. Cyber hackers usually have a motive which is either politically or religiously in tuned towards their belief and they try to create chaos and tension by destabilizing critical facilities. Hackers usually plan to rob secrets and have access to top security files. Hackers can act within the jurisdiction of the organization where they act like spy or they may act from outside. The main reason for hacking is to get the job for which they are paid done. Someone who hacks a prepaid card without paying is also a hacker. Hackers can be used by a nation or by the government to gain secrets of it enemies. They user the world wide web to gather information about a particular governmentall nine of these groups use various different hacking strategies that they use in order complete their tasks. Many hackers, both black hats and white hats are involved in organizations.

Chapter three: research methodology:-

researchmethod:-

The primary research method for this study is based on literature review and the methodology selected for this proposed study will be detailed here: the planned research design, methods of selection, data collection and analysis of results will be explained. It is hoped that the chosen methodology will provide useful information through the collection and analysis of data on the information security threat and the hackers.

recommendation and conclusion:-

The whole problem with cyber-security presently is that since the cyber-criminal is constantly upgrading his knowledge and methods, most intrusion prevention software applications only deal with the methods previously used.the home user may benefit by subscribing to any one of a variety of newsletters that stay abreast of the hacker world.one such free newsletter can be offered by hackingalert.com.

Therefore, allusers must take a large role in understanding the issues regarding cyber security and implementing their solutions. There are few recommendation that being suggested by scholars such as :

Education and training; teaching a student to hack is still an issue we face today. Some feels that hacking should be put into curriculum in university and that they will teach students how to improve intrusion. It is same like giving a tools for the students on how to hack is simply like giving a crowbar for a burglar to to break into a house. Certain policies need to be applied at university as we never know whether the acquired skills will be used for the good or bad. Policies need to address issue for students who conduct malicious acts by applying security checks on individuals which universities do certain courses such as ethical hacking. For example, a criminal background check, the requirement of some sort of professional certification, and student interviews are a few measures that could potentially weed out several, if not all, all students with potential malevolent intentions.

Trusting the potential enemy; some of skilled professionals use their abilities to harm the society by finding vulnerabilities in the system and attacking them. This is when we need the ethical hacker that may do the job. Two totally different individual would need to be hired to run tests for companies so that no on individual can have total freedom with any one system.

Risk management; ethical hackers can minimize the risk of impact by exploring vulnerabilities beforehand to minimize the risk. Allow the company to undertake penetration test to find if they are vulnerable to attack. There should be some leeway and the hackers should be allowed to use certain tools to help them with their job without any question to identify security vulnerabilities in the company's system.

Penetration testing; penetration testing defined as a legal and authorized attempt to locate and successfully exploit computer systems for the purpose of making those systems more secure. Includes probing for vulnerabilities as well as providing proof of concept attacks to demonstrate the vulnerabilities are real. Proper penetration testing always ends with specific recommendations for addressing and fixing the issues that were discovered during the test. This process will help to secure computers and networks against future attacks by finding security issues.

References:-

1. Abdulkadir, s. S., &dzarma, d. E. (2015).security threats analysis of ibrahimbabangida library, modibboadama university of technology, yola.*international journal of innovation and scientific research*, 13(2), 591-597.
2. Action fraud. (2011). Accessed 31 october2016 http://actionfraud.org.uk/what-is-fraud
3. Afyouni, h. (2006). *Database security and auditing: protecting data integrity and accessibility*, thomson course, canada.
4. Alhabeeb, m., almuhaideb, a., le, p., &srinivasan, b. (2010, april). Information security threats classification pyramid. In *advanced information networking and applications workshops (waina), 2010 ieee 24th international conference on* (pp. 208-213). Ieee.
5. Ateeq, a. (2012). 'type of security threats and it's prevention', *international journal of computer technology and applications*, vol.3, no.2, pp.750-752.
6. Ayuso, p.n., gasca, r.m., lefevre, lft-fw.(2012). A cluster-basedfaulttolerant architecture for statefulfirewalls.*computers& security*; 31(4):524e39.
7. Baker, w., goudie, m., hutton a., hylender, c., niemantsverdriet j, &novak, c, (2010).*verizon 2010 data breach investigations report.*
8. Bompard, e., huang, t., wu, y., &cremenescu, m. (2013).classification and trend analysis of threats origins to the security of power systems. *International journal of electrical power & energy systems*, *50*, 50-64.
9. Bratus, s. (2007). What hackers learn that the rest of us don't. *Ieee security and privacy*.
10. Brown, b. (2009). *Help prevent computer theft*, palmerston north, new zealand.
11. Choo,. (2011). The cyber threat landscape: challenges and future research directions. *Computers & security*; 30(8):719e31.
12. Cyber-media (2006). Increase in cyber-attack against home users retrieved from http://www.ciol.com/ciol-techportal/content/security/news/2006/2061010859.asp
13. Damico, t. M. (2009). "cyber attack prevention for the home user: how to prevent a cyber attack."inquiries journal/student pulse, 1(11). Retrieved from http://www.inquiriesjournal.com/a?id=47
14. Dashora, k. (2011). Cyber crime in the society: problems and preventions. *Journal of alternative perspectives in the social sciences*, 3(1), 240-259.
15. Desai, m., patel, s., somaiya, p., &vishwanathan, v. (2016). Prevention of distributed denial of service attack using web referrals: a review.
16. Dezfouli, f. N., dehghantanha, a., mahmod, r., sani, n. F. B. M., shamsuddin, s. B., &daryabar, f. (2013). A survey on malware analysis and detection techniques.*international journal of advancements in computing technology*, 5(14), 42.
17. Easttom, c. (2006). *Computer security fundamental*, pearson prentice hall, united states of america.
18. Engebretson, p. (2013). *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Elsevier.
19. Farahmand, f., navathe ,s.b., sharp, g.p., &enslow, ph. (2005). A management perspective on risk of security threats to information systems, information technology and management archive; 202-225.
20. Ferrari, e., &thuraisingham, b. (2006). Guest editorial: special issue on privacy preserving data management. *The vldb journal*, *15*(4), 291-292.
21. Greitzer, f. L., strozer, j. R., cohen, s., moore, a. P., mundie, d., &cowley, j. (2014, may). Analysis of unintentional insider threats deriving from social engineering exploits. In *security and privacy workshops (spw), 2014 ieee* (pp. 236-250). Ieee.
22. Hacker.merriam-webster.com. Merriam-webster.(2013). Web. 9th december 2013.

23. Hackingalert (2008).hacker tricks and prevention techniques.retrieved, from http://www.hackingalert.com/hacking-articles/hacker-tricks.php.
24. Hansen, j.v., lowry, p.b., meservy, r., &mcdonald, d. (2007).genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection.*decision support systems*; 43(4):1362e74.
25. Hayes, r. (2014). *Retail security and loss prevention*.butterworth-heinemann.
26. Jamil, d., & khan, m. N. A. (2011). Is ethical hacking ethical?. *International journal of engineering science and technology (ijest), issn*, 0975-5462.
27. Jansen, w. A. (2011, january). Cloud hooks: security and privacy issues in cloud computing. In system sciences (hicss), 2011 44th hawaii international conference on (pp. 1-10).ieee.
28. Jee, j. E., lee, s. J., lee, s. R., bae, b. C., & shin, y. T. (2012). A logical network partition scheme for cyber hacking and terror attacks. *Journal of kiise: information networking*, 39(1), 95-101.
29. Jouini, m., rabai, l. B. A., &aissa, a. B. (2014).classification of security threats in information systems. *Procedia computer science*, *32*, 489-496.
30. Loader, b. D., &thomas, d. (eds.). (2013). *Cybercrime: security and surveillance in the information age*. Routledge.
31. Marchewka, j. T. (2014). *Information technology project management*.johnwiley& sons.
32. Padmanabhan, s. (2012).hacking for lulz: employing expert hackers to combat cyber terrorism. *Vand. J. Ent. & tech. L.*, 15, 191.
33. Ponemon institute. (2014).*cost of data breach*.ibm. Available:http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/ accessed 1st, november, 2016.
34. Posey, c., bennettr.j, &roberts, t.l. (2011).understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes.*computers&security*.30(6e7):486e97.
35. Richardson, r. (2010/2011).csi computer crime and security survey, http://www.gocsi.com; 2011.
36. Robert, siciliano. (mar 6, 2011). Https://securingtomorrow.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/
37. Sabahi, f. (2011, may). Cloud computing security threats and responses. In *communication software and networks (iccsn), 2011 ieee 3rd international conference on* (pp. 245-249). Ieee.
38. Sanglakhi, a. (2013). Hackers and the internet.
39. Shaluf, i. (2007). 'an overview on disaster', disaster prevention and management, vol.16, no.5, pp.687-717.
40. Shedden, p., smith, w., &ahmad, a. (2010).*information security risk assessment:* towards a business practice perspective.
41. Shim, j., qureshi, a. A., &siegel, j. G. (2013). *The international handbook of computer security*.routledge.
42. Shiu, s., baldwin, a., beres, y., mont, m.c., &duggan, g. (2011).economic methods and decision making by security professionals.the tenth workshop on the economics of information security (weis).
43. Silowash, g. J., cappelli, d. M., moore, a. P., trzeciak, r. F., shimeall, t., &flynn, l. (2012).common sense guide to mitigating insider threats.
44. Solomon, m., &chapple, m. (2005).*information security illuminated*, jones and bartlett, united states of america.
45. Stanton, j.m, stam, k.r, mastrangelo, p, &jolton, j. (2005).analysis of end user security behaviors.*computers& security*. 24(2):124e33.
46. Swiderski, f., &snyder, w. (2004).threat modelling microsoft press.
47. Top layer security (2008). Securing tomorrow's networks today. Retrieved, 2008, from http://www.toplayernetworks.com/content/resource/faq.jsp.
48. Vacca, j. (2009). *Computer and information security handbook*, burlington, ma: morgankaufmann.
49. Von solms, r., & van niekerk, j. (2013).from information security to cyber security.*computers& security*, 38, 97-102.
50. Walters, r. (2014). Cyber-attacks on us companies in 2014. *Heritage foundation issue brief*, (4289).
51. Warkentin, m., &willison, r. (2009).*behavioral and policy issues in information systems security:* the insider threat. European journal of information systems. 18(2):101e5.
52. Whitman, m. E., &mattord, h. J. (2008).*management of information security*, course technology.
53. Xu, z., hu, q., &zhang, c. (2013). Why computer talents become computer hackers. *Communications of the acm*, *56*(4), 64-74.
54. Zafar, h., &clark, j.g. (2009).current state of information security research in is.*communications of the association for information systems*; 24(34):557e96.
55. Zhi-jun, w., hai-tao z., ming-hua w., &bao-song, p. (2012). Msabms-based approach of detecting ldosattack.*computers& security* 31(4):402e17.