RESEARCH ARTICLE OPEN ACCESS

Taxonomy of Security Risk threats in information systems Risk Management

Morteza Pakizeh*
*(Department of Computer and Software Engineering, Science and Research Branch, Islamic Azad university, Tabriz, Iran)

--************************--------------------------------

Abstract:

Information is an important asset a business has always been in all organizations and institutions. Therefore, it must be protected against attacks. One of the objectives is to protect the security of information. One of the best ways to deal with security threats in the corporate world, using the company's security problems through a risk-based approach is achieved. We believe that the classification and assessment of new threats to enterprises will help to give an accurate assessment and true risks with respect to the new concepts of the reputation And to learn appropriate ways to deal with a variety of attacks and threats have the ability to recognize and deal with As well as our new classified assessment that helps organizations not only be able to understand better the risk assessment with regard to the comparison of new concepts and select the appropriate tasks but the way to do a risk assessment to be done correctly. In addition, this classification will help to better ways for future research in the growing field of security risks assessment done.

Keywords **—Information security, management, threats, classification of information, risk classification**

--************************--------------------------------

INTRODUCTION

A business asset information is important and like any other valuable asset should be cal optima privacy (A. Shameli-Sendi,2016). Information asset value will vary from organization to organization (ISO 27002,2013). Depending on the type and size of business and provide certain services differently (Iijima T, Curtis,2004) . Especially because of the relatively important role they stay in today's competitive market (Brook et al., 2013). There are many factors in sustainable development has an organization and existing businesses in the it and drop to unsafe, but without a doubt, increase the vulnerability of an organization can lead to disaster. A significant number of scholars of various aspects of the vulnerability of such scientific information systems, supply chain, information systems have been reviewed but few of them are business and computer networks. The concept of vulnerability to the sensitivity of the issue provides several different means. In information science, vulnerability reflects the well-known weaknesses in the system that can be exploited by malicious software or hackers. The Organization of a sling, consider that part of it is damaged chains and thus the Organization at risk and makes the ability to reduce the organization. The vulnerability may be new risks, including risks from new technologies, economic, political, and risks. Come create, that if an unintended event like the vulnerability the same reliability as well as event happen equally to the risk of falls. Financial loss, misuse Amnytydrgzarshat many companies have created security concerns that have prevented the adoption of cloud computing services(Rusheed,2014;Sun,srivastava & Mock,2006). Based on the report of the Institute of ponmon (Ponemon Institute LLC, 2012), the cost of failure and defect data, on average in the UK 68از% in 2007 to 79% in 2011. These threats and dangers are created by hackers. This sharp rise means that the value of information in organizations is growing markedly increased. Malicious software, disgruntled employees, competitors and other sources called the called the risk factors and can be internal or external in the form of an organization with a variety of different interests and motives of these resources are (Harris,2010;Landoll,2006). Given these facts, researchers, professionals, journalists, legislators, government and even ordinary citizens to information security and their actions have attracted(Jourdanet et al ,2010). A number of approaches to information security risk assessment, such as the central computing and telecommunications, risk analysis, risk assessment Microsoft(The Security Risk Management Guide,2006)؛ The risk assessment process easy Frap)FRAP (Peltier,2001)(Presented by a variety of methods, some business situations that are not remedial none of them) Jones,2007.(The problem, many of these methods is that they are mainly on the General principles and browse recipes have been working and have not run for details (Shameli et al,2010).

I. SECURITY

Strategies to deal with security threats that if we do not know how you stand against these threats and how to do it do not know the security solution will be of no use Safe and secure communication channels between users and trends unless they make between them. The security of a computer system associated with the reliability of it. By definition, reliable system is so reliable that it can offer your service (Lapry, 1995). Systems should be reliable, accessible, reliable, secure and maintainable.To make sure a computer system, we must also consider features such as confidentiality and integrity. The most important assets a computer system hardware, software, and its data. A vulnerability is a flaw or weakness in methods, design or implement security system. The vulnerability can be from different perspectives such as Pro Tools channels, etc. The questionnaire found that there are three stages in the risk assessment The objective of the first stage is to identify the assets of the system and in the second stage the aim of creating a list of asset vulnerability and risks that affect the value of the secured asset, vulnerability, and impact of the threats in the final step can be calculated and that the stage will be the impact of risk calculation. Another attitude to information security on a computer system that is trying to serve and its data are protected against security threats. Security threats can be divided into four types of banditry, forgery, manipulation and disruptive split (Fletcher,2003) .

III. The evaluation of information risks

Information security risk assessment ISRA, is a major part of an ISMS Information Security Management System An organization will be able to identify vulnerabilities and threats and then decidesthat due to potential threats to select countermeasures (Landol,2006; shamli_sendi et al 2012a,2013b). Organizations that assess risk properly and regularly doing intense, such as the consequences may be, loss of reputation, legal issues, or even direct financial impact to have (shedden et al, 2011). . A number of approaches to ISRA include: central computing and Telecomm unications Agency risk analysis risk assessment type, Microsoft (The security risk management Guide, 2006) easy ri sk assessment process, frap (peltler, 2001), Cobra COBRA risk method (Coras den Brab er et al

, 2007), and operational threats and vulnerability of the octave (Octave, 2005) have been introduced that in spite of the variety of methods some business conditions exist that non e of them are instrument choice (Jones, 2007). The problem, many of these methods is that they are mainly on the General principles and the browse command and have not worked out the details (Shameli,2010).

IV. Identify vulnerabilities

A vulnerability is a weakness or defect in the design or implementation methods, the security of the system is that it can be used by an attacker to be about hand or triple security goals affected. Identify vulnerabilities can be used with a variety of means, such as software inventory form in the network, and so won that three-step risk assessment model that exists are as follows: firstly that the objective of identifying assets and potential threats applicable to the system. The second stage, the goal is to have a list of asset vulnerability and risks, we aim toshow the final step calculates the effects of risk. Based on an old classification of information security risk assessment methods are now based on the three criteria-based approaches ISRA classification. The qualitative and quantitative mix (half a bit) in Figure 1-1 is displayed. Figure 1-1) classification and risk assessment , Information Security Risk Assessment (ISRA).

A. Quantitative

Little evaluation that relies on numbers long, time consuming calculations and to determine the level of risk exposure will be realized for an organisation or a network goes to work (Hulitt and Vaughn, 2010; Lichtenstin,1996). The purpose of the evaluation the survey analyzes security risks regardless of current needs. Little risk assessment is based on the measuring of the aim and the results that can be managed in a certain language (for example, monetary value, percent, and probability, input and output of the assessment of monetary and non-monetary risk a little bit that can be found in two categories: In the assessment of monetary assets in any money has been assigned the vulnerability; the threat and keep it running. In front of the non-monetary valuation; and non-monetary returns that risk factor in evaluating a value between 1 to 25, which is the model used to affix a mint; and split the other operators to calculate risk. This simple model may lead to the effective participation of managers and staff in the risk assessment process. And for the risk assessment of proposed the following formula is used.

*The likelihood of * extremely * sensitivity = risk exposure (Risk) threat x 2 (strictly) = exposure rating*

system common vulnerability (CVSS), which uses a formula is very complicated and requires a tool to fruition. To be used and it is clear that a lot of factors to measure risk and there are many of these equations; an example for this are the agents that some of these solutions. The following are the most common calculations for them:

*Annual loss expectancy = average rate of occurrence * only hope to lose*

However, most of these items are not used in the industry. The main problem in the evaluation of a bit time consuming, being a long-lasting process that depends on accurate information we have. Information such as the value of the assets; log and data, used for removing it and set the expectation that arises from the limitation of time, money and human resources by organization or network is that its implementation will not be easy (Farahmand et al 2003; Hulitt and Vaughn,2010).

B. Qualitative

One of the most common assessment in the evaluation of qualitative risk assessment, information security is that the organizations to find out their requirements it is sufficient. (Landoll,2006) . Information security risk assessment, based on the probability of the occurrence of the damage and the potential impact is (Guan et al, 2003) that the risk factors with respect to the ISO 17799 standard category. A qualitative asse ssment of the impact and the possibility to show a specific scenario and the relative values of the class are used. Information security risks with the use of the methods and principles for the evaluation of non-numeric levels (qualitative) are measured (NIST, 2012). The input and output of quality risk assessment based on two categories: variable scope and the language variable. The range variable for the input, and the output variable as a rank. For dealing with a very important condition is still not well defined some of the qualitative assessments to rank and prioritize the dangers that face an organization normally is designed. Due to insufficient evaluation data and computing histor y beingwidely used that the impact and probability of occurrence of risk scenarios to calculate and also because they are easy to understand and implement is used (Wheeler, 2011). As well as with the calculation of this assessment, the evaluation of assets, threats and vulnerabilities can be easier to NIST, 2012). However, the lack of sufficient detailto support the measurement of cost management decision ther e (Vaughn and Hulitt, 2010). Furthermore; they are based on the analysis of knowledge and those who are in the process (and shareholders) that cause this assessment are more subjective and prone to error and inaccuracy of their little counterparts (Wheeler, 2011). Another problem of this kind of assessment is that the level of vulnerability and the likelihood of the threat is small though that prioritize information sec urity risks and compare Ann results with risk assessment (NIST, 2012).

C. Hybrid (semi-quantitative)

Because of the weaknesses and strengths, both quantitative and qualitative assessment of the information security risk is that the combination of the two and is a combination of evaluation is used. Qualitative assessment that utilizes the speed and simplicity of use while a whole well with little assessment of the assets is more important than it used to. (Deng et al,2011). The probability of system failure and the consequences of such a failure (the intensity of the loss). These elements are described by experts to determine the overall riskto the system. The purpose of this model is offered; facilitate the risk assessment by the overall security risk analysis and information with tiny details and the details associated with each of them separately, and evaluate the impact of specific threats and control the following components of the overall risk can be considered. With this theory the two types can be added to the cost. A cost to implement countermeasures, on the other hand, holding the value of the potential loss of assets (value) that is due to the occurrence of the risk and threat. Due to the lack of information and adequate understanding of the failure mechanism of the risk analysis can be challenging.

V. Risk assessment

The first step in the risk management of information technology systems for risk assessment (nist, 2002) that turn risk assessment includes not following step: Identify the system, identifying the threats, vulnerability identification, control and analysis, to determine the probability of the impact, ISS, analysis, control and results recommended documentation. This section to specify the risks based on the ratio of the probability of occurrence of legal, regulatory, financial and in the form of the impact of the decision in order to create a reputation for solving them (Jones, 2007; Strecker et al,2011) Here step determine risk by fuzzy logic and decision theory used to be that the chance of the occurrence of the incident and judge it gives support and security to thecalculation using the mathematical equations. So this approach in dealing with the security of information technology systems that enables managers to better understand the shape with a surface of fulfilling these threats specific procurement scenario. The necessity of information security in your organization or network as a structural change in the type of a network goes to) sharmala et al, 2013 (resulting in several risk management framework and the methods it information security have been developed in the literature (chen Londal, 2012) according to the (Silva, Gusmao, and Costa Poleto, 2014) to fuzzy sets in information security the next five. Access to information and systems, communications, infrastru cture, security management, security and the development of information systems. (Power, 2001) of the Security Institute of electricity during the report that more than 49% of its employeesare subversive organizations events, but despite this the majority of internal and external factors are ignored (shultz, 2002). Four ways to deal with the first one there is a danger that the Organization of the risk and the

consequences it
will understand and consciously decides to accept it. II avoid activities that are at risk or are more risks in an organization are not available. III the transfer of all or part of its responsibility and obligations associated with a specific activity and risk factors related to one side last grdennd and passed that reduced risk and its consequences in the range of some of the roads and reduce the risk of a lower level than the level of acceptance for this. ISO/IEC 7352-2 security classification information in the following five categories and classification. Authentication, access control, data confidentiality, data integrity, and non-being denial of data according to article (Alireza shameli_sendi et al, 1997), the vulnerability can be the following procedures as to how important information relating to the assets and resources available in the organization can identify and assess return,
Automated vulnerability scanning tools, security testing and assessment, penetration testing and code review (ISO/IEC 2010; Formen, 27005, 2011; Mell et al,2006; Wheeler, 2011), these methods may have
some false actions to show your interview location, inventory, physical inspection, review documents (ISO/IEC 27005, 2011). Copyright brmjamoah data in 1998, DARPA focus based on a targeted network connections is based on the resources that this data set are attacked are the services and use of a network on some hosts, the cost of the damage and respond based on surface type of detector, access remote computer user to root level, and on the contrary specific statistical basis (Lee et al , 2012) is a form of cost-sensitive based on the three factors were suggested: 1. with regard to operational costs, that is) the cost of processing the flow of hodthby intrusion detection systems, 2) the cost of the damage, which is the amount of damage to the source of the attack means that refers to arise and when it is intrusion detection system cannot be effective, accountability, cost 3) that the cost of employing a response at the time of the attack unfold. Kay hacelom, a real time intrusion prevention of templates based on close relationship between security and network and sensitive to the cost of the proposal have predicted its execution units. The main advantage of this approach is that for a unit based on fuzzy dynamic risk assessment and that of applying the method of fuzzy hererelated to the process of estimating the risk register will be automatically that your skill and judgment of such experts analysis. The main disadvantages of this type is that it can be the root user to the level of attacks, Remote access to the remote computer to Local (R2L) and type
of detector (Probe) to identify, but attack (Denial Of Service (DOS)), could not be identified (Haslum et al, 2007).

Denial of service (DOS)-1: the
attacker tries that the required resources are not available to users or bandwidth resources or disk space consumption.

2- User to Root (U2R): The user tries to explicitly illegal with the exploitation of the vulnerability of the system access privileges to the root.

3- Remote to Local(R2L): The attacker tried to proceed to obtain unauthorized access to a remote computer from a machine with the exploitation of the vulnerability of the system.

4- Probe: The attacker's network to collect information and identify the possible vulnerabilityscans are examples that use automated tools are used include portsweep, ipsweep-nmap and etc.

VI. Threat model

The purpose of the definition of a model is that the risk of a threat for us is understanding and risk based on the values of the following two factors can be estimated. The likelihood of an attack, and the consequences of this attack, the enemy threat model should give a description of the capabilities and identify threats and security requirements have been considered against the attacks

Classification of security threats

The classification of the threat is important, because they chiefly identify and understand threats to let features and resources to protect the assets of the system up; Moreover, they express the security risks and help in understanding the features and choose the security solutions you can prdazannd these threats. The classification is based on two main types of attacks:

1- External attacks

External threats could working people or organizations which work outside of a company and they allow access to the computer systems or networks, most foreign threats in compu ter systems and data on natural disasters include flood, fire, aztofan and earthquake

2- **Internal attacks**

Internal threats occur when that person to the network and to an account on a server is authorized to have access, as well as physical access to the network. An internal threat could be the result of the organized process or operation process in the organization.

Threat agents

The factors that threaten the system as a threat to impose three classes specific for this classification:

1- Human

These threats arising from the activities of members, employees or unhappy hackersthat are causing the damage and the risk in the system.

2- Environmental threats

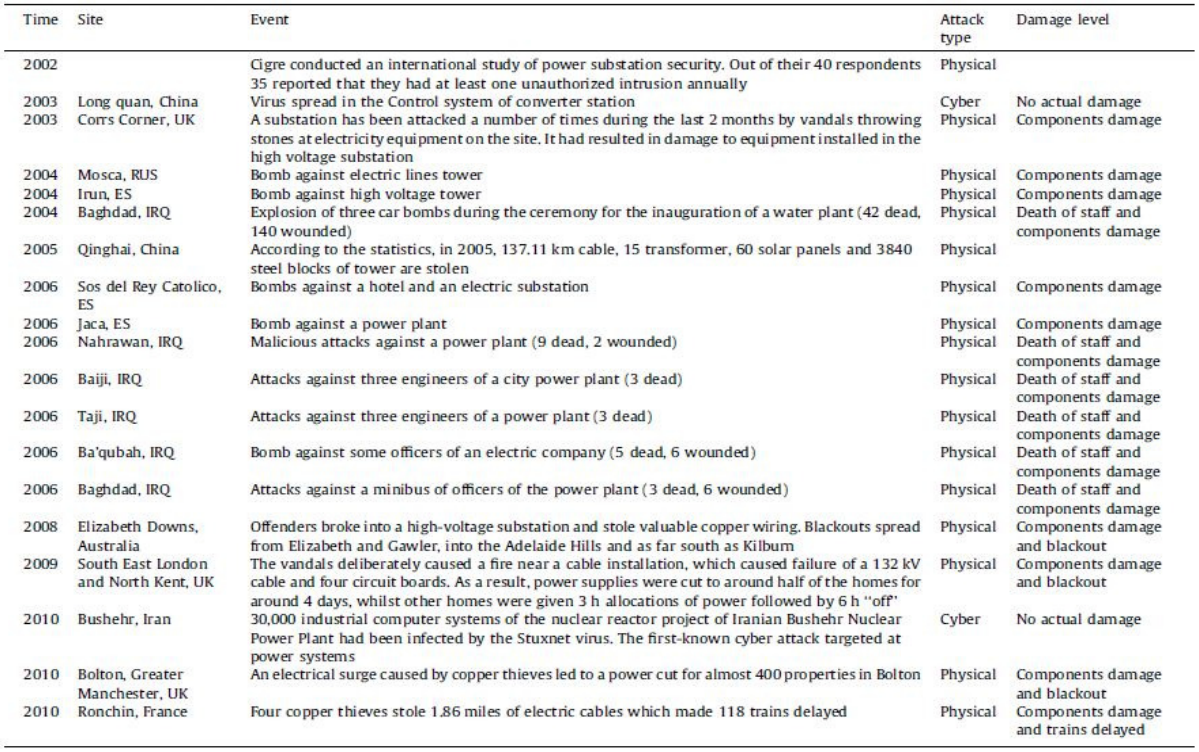
The result of the non-human factors are such as: natural disasters, threats, earthquake, flood, fire, lightning, wind, water, tsunami and other threats such as war, riots, terrorist attacks and the rebellion can shunned.

3- Technology

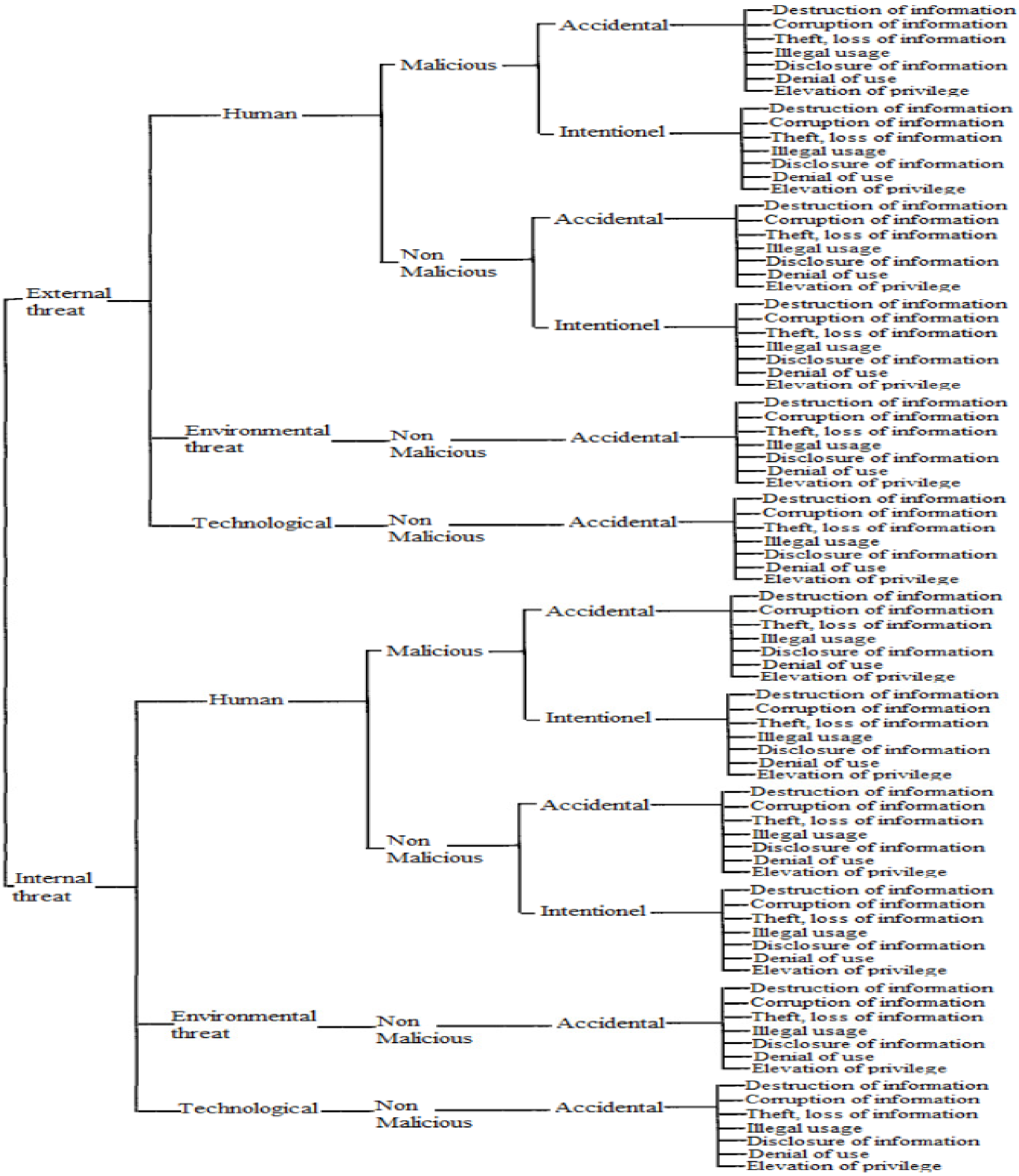
By physical and chemical processes are created on the material. Physical processes include the use of physical means to gain entry to restricted areas of a building, Office or company, or damage to hardware or software, and also includes the chemical processes of technology hardware and software, and Motivated by the threat of The invaders, which are typical of a specific target or incentive to attack a system to have these targets can be non-fatal outcomes or ruining. That includes non-destructive and malicious threats. Malicious threats consist of the internal or external attacks that cause employees or non-employees to an organization or network harm, such as viruses, Trojan horses and worms. Non-destructive attacks due to poor security policies and controls that allow by vulnerabilities and errors occur and this is dissatisfied by the staff and ignorant with the objective of damaging the system. The intention of the threat Represents the goal of man is the result of threats and intentional threats into two parts and random unwanted threats and Division tha t the intentional threats as an example someone who deliberately damage the property or information, such as computer crimes, espionage, identity theft, and credit card crime as well as unwanted threats represent threats that are e ssentially without the knowledge of unauthorized modification of software are included. Like operator error or programming errors; Moreov er each attack can be in one of two final attack and attack middle class. The final attacks are the ones that are the ultimate goal of the attacker it's doing and is one of the high levels of security requirements to medium attacks and end angers other attacks and facilitator stepping stone to climb to attack the other and increase its functionality. The following table some of the attacks that overwhelm in some countries in recent years have occurred is displayed.

And in the chart figure 2-2) the classification of attacks and displays the effects of the threat.

Malicious attacks happened in other countries.



Time	Site	Event	Attack type	Damage level
2002		Cigre conducted an international study of power substation security. Out of their 40 respondents 35 reported that they had at least one unauthorized intrusion annually	Physical	
2003	Long quan, China	Virus spread in the Control system of converter station	Cyber	No actual damage
2003	Corrs Corner, UK	A substation has been attacked a number of times during the last 2 months by vandals throwing stones at electricity equipment on the site. It had resulted in damage to equipment installed in the high voltage substation	Physical	Components damage
2004	Mosca, RUS	Bomb against electric lines tower	Physical	Components damage
2004	Irun, ES	Bomb against high voltage tower	Physical	Components damage
2004	Baghdad, IRQ	Explosion of three car bombs during the ceremony for the inauguration of a water plant (42 dead, 140 wounded)	Physical	Death of staff and components damage
2005	Qinghai, China	According to the statistics, in 2005, 137.11 km cable, 15 transformer, 60 solar panels and 3840 steel blocks of tower are stolen	Physical	
2006	Sos del Rey Catolico, ES	Bombs against a hotel and an electric substation	Physical	Components damage
2006	Jaca, ES	Bomb against a power plant	Physical	Components damage
2006	Nahrawan, IRQ	Malicious attacks against a power plant (9 dead, 2 wounded)	Physical	Death of staff and components damage
2006	Baiji, IRQ	Attacks against three engineers of a city power plant (3 dead)	Physical	Death of staff and components damage
2006	Taji, IRQ	Attacks against three engineers of a power plant (3 dead)	Physical	Death of staff and components damage
2006	Ba'qubah, IRQ	Bomb against some officers of an electric company (5 dead, 6 wounded)	Physical	Death of staff and components damage
2006	Baghdad, IRQ	Attacks against a minibus of officers of the power plant (3 dead, 6 wounded)	Physical	Death of staff and components damage
2008	Elizabeth Downs, Australia	Offenders broke into a high-voltage substation and stole valuable copper wiring. Blackouts spread from Elizabeth and Gawler, into the Adelaide Hills and as far south as Kilbum	Physical	Components damage and blackout
2009	South East London and North Kent, UK	The vandals deliberately caused a fire near a cable installation, which caused failure of a 132 kV cable and four circuit boards. As a result, power supplies were cut to around half of the homes for around 4 days, whilst other homes were given 3 h allocations of power followed by 6 h "off"	Physical	Components damage and blackout
2010	Bushehr, Iran	30,000 industrial computer systems of the nuclear reactor project of Iranian Bushehr Nuclear Power Plant had been infected by the Stuxnet virus. The first-known cyber attack targeted at power systems	Cyber	No actual damage
2010	Bolton, Greater Manchester, UK	An electrical surge caused by copper thieves led to a power cut for almost 400 properties in Bolton	Physical	Components damage and blackout
2010	Ronchin, France	Four copper thieves stole 1.86 miles of electric cables which made 118 trains delayed	Physical	Components damage and trains delayed


External threat
Human
Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Intentionel
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Intentionel
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Environmental threat
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Technological
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Internal threat
Human
Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Intentionel
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Intentionel
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Environmental threat
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Technological
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege

Refrence:

A. Aleksić, M. Stefanović, D. Tadić, S. Arsovski, A fuzzy model for assessment of organization vulnerability, Measurement (2014), doi: http://dx.doi.org/10.1016/j.measurement.2014.02.003

Chithra Selvaraj, Sheila Anand. A survey on Security Issues of Reputation Management Systems for Peer-to-Peer Networks. www.elsevier.com/locate/cosrev. 6 (2012) 145–160

Alireza Shameli-Sendi, Rouzbeh Aghababaei-Barzegar, Mohamed Cheriet. Taxonomy of information security risk assessment (ISRA). www.elsevier.com/locate/cose. 57 (2016) 14–30

Alireza Shameli Sendi, Masoume Jabbarifar, Mehdi Shajari and Michel Dagenais. Fuzzy Expert Model for Risk Assessment. The Fifth International Conference on Internet Monitoring and Protection.

Alireza Shameli-Sendi, Naser Ezzati-jivan, Masoume Jabbarifar, and Michel Dagenais. Intrusion Response Systems: Survey and Taxonomy. IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.1, January 2012.

Mouna Jouini, Latifa Ben Arfa Rabai, Anis Ben Aissa. Classification of security threats in information systems. Procedia Computer Science 32 (2014) 489 – 496.

Bassem Mokhtar , Mohamed Azab. Survey on Security Issues in Vehicular Ad Hoc Networks. Alexandria Engineering Journal (2015) 54, 1115–1126.

ZHANG Li, WANG Qing, TIAN Bin. Security threats and measures for the cyber-physical systems. www.sciencedirect.com/science/journal/10058885. August 2013, 20(Suppl. 1): 25–29.

Ettore Bompard , Tao Huang , Yingjun Wu, Mihai Cremenescu. Classification and trend analysis of threats origins to the security of power systems. www.elsevier.com/locate/ijepes. 50 (2013) 50–64.

Alvaro A. Cardenas, Tanya Roosta, Shankar Sastry. Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems. www.elsevier.com/locate/adhoc. Ad Hoc Networks 7 (2009) 1434–1447.

Ana Paula Henriques de Gusmão, Lúcio Camara e Silva, Maisa Mendonc¸ a Silva,Thiago Poleto, Ana Paula Cabral Seixas Costa. Information security risk analysis model using fuzzy decision theory. www.elsevier.com/locate/ijinfomgt. International Journal of Information Management 36 (2016) 25–34.

Sultan Alneyadi, Elankayer Sithirasenan, Vallipuram Muthukkumarasamy. A Survey on Data Leakage Prevention Systems. http://dx.doi.org/10.1016/j.jnca.2016.01.008.

Harris S. CISSP all-in-one exam guide. 5th ed. NewYork: McGraw- Hill; 2010.
Jones A. A framework for the management of information security risks. BT Technol J 2007;25(1):30–6.

Landoll DJ. The security risk assessment handbook: a complete guide for performing security risk assessments. 2nd ed. Boca Raton: Auerbach Publications; 2006.

Misra SC, Kumar V, Kumar U. A strategic modeling technique for information security risk assessment. Inf Manag Comput Secur 2007;15(1):64–77.

Ponemon Institute LLC. Cost of data breach study: United Kingdom [Online]. http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach -uk.en-us.pdf>; 2012 [accessed 08.15].

NVD. National vulnerabilities database [Online].<http://nvd.nist.gov/cpe.cfm>; 2013 [accessed 08.15].

NIST. NIST SP-800-53 rev3 [Online]. <http://www.nist.gov/customcf/get_pdf.cfm?pub_id=903280>; 2009 [accessed 08.15].

NIST. NIST SP-800-30rev1 [Online]. <http://www.nist.gov/customcf/get_pdf.cfm?pub_id=912091>; 2012 [accessed 08.15].

OCTAVE. Managing information security risk. USA: Carnegie Mellon; 2005.

Shamala P, Ahmad R, Yusoff M. A conceptual framework of info structure for information security risk assessment (ISRA). J Inf Secur Appl 2013;18(1):45–52.

Shameli-Sendi A, Dagenais M. ARITO: cyber-attack response system using accurate risk impact tolerance. Int J Inf Secur 2014;13(4):367–90.

Shameli-Sendi A, Jabbarifar M, Shajari M, Dagenais M. FEMRA:fuzzy expert model for risk assessment. In: The fifth international conference on internet monitoring and protection (ICIMP). 2010. p. 48–53.

Shameli-Sendi A, Ezzati-Jivan N, Jabbarifar M, Dagenais M.Intrusion response systems: survey and taxonomy. Int J Comput Sci Netw Secur 2012a;12(1):1–14.

Shameli-Sendi A, Jabbarifar M, Dagenais M, Shajari M. System health monitoring using a novel method: security unified process. J Comput Netw Commun 2012b;2012:151205.

Shameli-Sendi A, Cheriet M, Hamou-Lhadj A. Taxonomy of intrusion risk assessment and response system. Comput Secur 2014;45:1–16.

A. Shameli-Sendi and M. Dagenais, "Real Time Intrusion Prediction based on improving the priority of alerts with Hidden Markov Model," Journal of Networks, 2012.

Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of infostructure for information security risk assessment (ISRA). Journal ofInformation Security and Applications, 18, 45–52.
Shedden P, Scheepers R, Smith W, Atif A. Incorporating a knowledge perspective into security risk assessments: very informal newsletter on library automation. VINE 2011;41(2):152–66.

Stango A, Prasad NR, Kyriazanos D. A threat analysis methodology for security evaluation and enhancement planning. In: Third international conference on emerging security information, systems and technologies ECURWARE.2009.

L. Zadeh. Fuzzy sets. Info. & Ctl., 8:338–353, 1965.

Farahmand F, Navathe SB, Sharp GP, Enslow PH. A management perspective on risk of security threats to information systems. Inf Technol Manag 2005;6(2–3):203–25.

International Organization for Standardization, ISO/IEC. 27005.2011 information security risk management. Geneva: ISO;2011.

International Organization for Standardization, ISO/IEC. 27000.2012 information technology security techniques Information security management systems overview and vocabulary.Geneva: ISO; 2012.

International Organization for Standardization, ISO/IEC. 27001.2013 information technology security techniques Information security management systems requirements. Geneva: ISO;2013a.

International Organization for Standardization, ISO/IEC. 27002.2013 information technology security techniques code of practice for information security management. Geneva: ISO;2013b.

Iijima T, Curtis J. Need to justify IT security? Measure your risk! J Corp Account Finance 2004;15(5):47–51.

International Standard Organization, ISO/IEC 27005,Information Security Risk Management, 2008.

http://www.iso.org/iso/catalogue_detail?csnumber=44651.

http://www.iso.org/iso/catalogue_detail?csnumber=44379

Tang j, Wang D, Li x. A scalable Architecture for classify network security threats. science and technology on information system security laboratory,2012.

C.Strasburg, N.Sstakhanova,S.Basu and J.S.Wong. The methodology for evaluationg response cost for intrusion response systems. technical report 08-12,IOWA state university.

Alter, S., & Sherer, S. (2004). A general, but readily adaptable model of information system risk. Communications of the AIS, 14(1), 1–28.

Feng, N., & Li, V. (2011). An information systems security risk assessment modelunder uncertain environment. Applied Software in Computers, 11(7),4332–4340.

Power, R., 2001. '2001CSI/FBI Computer Crime and Security Survey', VolumeVII—No. 1, Computer.

Rasheed, H. (2014). Data infrastructure security auditing in cloud computingenvironments. International Journal of Information Management, 34, 364–368.

Microsoft. The security risk management guide. Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence; 2006.

Verizon. 2012 data breach investigations report [Online].<http://www.verizonenterprise.com /resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf>; 2012 [accessed 08.15].