ACTA INFOLOGICA 2019;3(1):34-45
dergipark.org.tr/acin

İSTANBUL UNIVERSITY PRESS

DOI: 10.26650/acin.502589

REVIEW ARTICLE

A Review on Cyber Risk Management*

Siber Risk Yönetimi Üzerine Bir İnceleme

Şükrü Okul[1], **Orhan Muratoğlu**[1], **M. Ali Aydın**[2], **H. Şakir Bilge**[3]

*This work was presented at the 1st International Symposium on Graduate Research in Science and published in the conference abstract book.

[1]TUBİTAK BİLGEM, Kocaeli, Turkey
[2]Istanbul University-Cerrahpasa, Department of Computer Engineering, Istanbul, Turkey
[3]Gazi University, Department of Electric Electronic Engineering, Ankara, Turkey

ORCID: Ş.O. 0000-0001-6645-7933;
O.M. 0000-0003-1831-940X;
M.A.A. 0000-0002-1846-6090;
H.Ş.B. 0000-0002-4945-0884

Corresponding author:
Şükrü Okul,
TUBİTAK BİLGEM, Kocaeli, Turkey
Telephone: +90 539 915 02 91
E-mail address: sukru.okul@tubitak.gov.tr

Submitted: 25.12.2018
Revision Requested: 05.02.2019
Last Revision Received: 26.03.2019
Accepted: 02.04.2019

Citation: Okul, S., Muratoglu, O., Aydin, M. A. ve Bilge, H. S. (2019). A review on cyber risk management. *Acta Infologica, 3*(1), 34-45. https://doi.org/10.26650/acin.502589

ABSTRACT

In this study, important studies on Cyber Risk Management are discussed. The stages of these studies are explained with examples of the steps, methods and steps they take and the details of the studies are presented. Before these details are presented, important and detailed information about risk analysis and cyber risk is provided in the introduction. In addition, cyber threat preparedness levels and cyber threat tools are mentioned in the introduction. The mentioned cyber threat tools are described in detail. As mentioned earlier, 9 studies related to the subject were examined. The literature review of these 9 studies has been examined in detail. In these studies, it is stated which steps are applied and some examples are given. In the light of these studies, it is stated that what kind of studies can be done in this area or what other methods and steps can be added to the current studies as a point that can be included in future studies. It is also mentioned in the studies that the classification of these studies in the literature can be done in more detail.

Keywords: Cyber Security, Cyber Risk, Cyber Risk Management

ÖZ

Bu çalışmada Siber Risk Yönetimi ile ilgili yapılmış önemli çalışmalar aktarılmaktadır. Bu çalışmaların içeriğinde hangi aşamalara, yöntemlere ve adımlara yer verdikleri örneklerle açıklanmakta ve yapılan çalışmalarla ilgili detaylar sunulmaktadır. Bu detaylar sunulmadan önce giriş kısmında risk analizinden ve siber risk ile ilgili önemli ve detaylı bilgiler verilmektedir. Ayrıca yine giriş bölümünde siber tehdit hazırlık seviyelerinden ve siber tehdit araçlarından bahsedilmektedir. Bahsedilen siber tehdit araçları detaylıca anlatılarak örneklenmektedir. Sonrasında daha öncede belirttiğimiz gibi toplamda konu ile alakalı 9 çalışma incelenmiştir. İncelenen bu 9 çalışmanın literatür taraması yapılmıarak ayrıntılarıyla ele alınmaktadır. Bu çalışmalarda hangi adımların hangi yöntemlerin uygulandığı ifade edilmekte ve bazı örnekler verilmektedir. Bu çalışmalar ışığında bu alanda başka ne tür çalışmalar yapılabileceği veya mevcut çalışmalara başka hangi yöntem ve adımlar eklenebileceği de ileriki çalışmalarda yer verilebilecek bir nokta olarak da belirtilmiştir. Ayrıca yapılacak çalışmalarda literatürdeki bu çalışmaların sınıflandırmasının da daha detaylı olarak yapılabileceğinden bahsedilmektedir.

Anahtar kelimeler: Siber Güvenlik, Siber Risk, Siber Risk Yönetimi

1. INTRODUCTION

According to official figures, the annual cost of cybercrime for the UK economy alone is estimated to be 38 billion USD; however, an astonishing ratio of 68% of organizations in Europe did not predict the financial impact of a cyber attack, and only 25% of these organizations had an incident response plan for cyber cases.

Cyber threats can arise from different sides, from hacker groups to activists and former employees, and the risks presented by these threats can affect a company at any time. Today, companies are largely dependent on technology and maintain their operations and business processes. When no action is taken on cyber risk management and transfer; it may cause loss of brand and reputation, data violations, regulation examinations, shareholder dissatisfaction and financial losses.

Moving this digital world of information, which is effectively used by individual as well as corporate users, facilitates accessibility and makes the information more attractive and targeted. Today, it is estimated that there are approximately 4.2 billion Internet users, 20 billion web pages, 3 billion pictures and 50.5 million audio-image files in the world (Internet World Stats, 2018). This cyber world, which is used very effectively by both individuals and institutions, has become an increasingly dangerous place.

Banks, investment companies and insurance companies are the main target of cybercriminals who want to steal money or information, disrupt operations, destroy critical infrastructures or damage data-rich financial services institutions. When financial services institutions are compared with other industries, taking into account both cyber attacks carried out both internally and externally, it ranks first in terms of average cost.

In order to get to the bottom of these problems, interviews were held to help us learn more about the experience and strategies of top-level cyber security experts, technology and risk management experts across the industry. As a result of the interviews, shared cyber war stories reveal challenges and obstacles as well as the progress made and the plans to realize the idea, approach and institutional culture transformation.

Several studies have been conducted with Cyber Risk Management. In this article, the most critical of these studies are discussed and presented. A total of 9 studies were included and many studies on Cyber Risk were included.

A. Risk Analysis

In order to protect an asset, it is necessary to first know its value and determine which risks it is exposed to. In the investigations, it was determined that cyber attacks increased every year. For this reason, it is of vital importance that security risks are analyzed and necessary risk models are created (In Hoh, 2011).

The main benefits of risk analysis are as follows (In Hoh, 2011):

- Improving secure information management,
- Ensuring that the organization's critical assets are monitored and effectively protected,
- To ensure effective information security policies in decision making,
- To provide valuable analysis data estimates for the future.

Known risk factors are affected by assets, threats and existing perspectives. As assets, threats or deficits increase, the risk is also increased.

Assets generally consist of info / data, hardware, software, documents, personal resources and conditions. Threats can be classified as person / non-person factors, network / physical, technical / environmental, internal / external and intentional / accidental threats. Deficits can be classified as administrative documents, personnel, regulations, physical conditions and facilities, technical equipment, software, communication / network related deficits (Wills, 2012).

A closer look at the security vulnerabilities, which are the first priority among risk factors, can be seen to have a life cycle. Each system has an open, and it is possible that this vulnerability is exposed to attack. If you are lucky, it will be discovered by white pirates and you will have a chance to close. When the deficits were first noticed, the date of discovery, the date of disclosure to the date of disclosure, the date of disclosure to the public, the date of exploitation of the exploitation code created for the open date, and the date of publication of the relevant patch for the closure of the deficit are called the patch date. Each patch published can be a new open discovery, ie the beginning of a new cycle (Jumratjaroenvanit, 2008).

Factors that affect the accuracy of an opening can be categorized in 3 areas. These areas are described below (Jumratjaroenvanit, 2008):

- Each application is likely to be the target of the attack during the safety-on-life cycle. Exposure of an application or system to the attack depends on which stage of the safety-on-life cycle is interrupted or how long. As the probability of completion of the cycle increases, it is far from being an attractive target.
- The popularity of openness and market share are the factors increasing the attack target. If the market share and popularity are greater than 60%, it can be assessed in the high-risk group and in the low-risk group if it is less than 30%.
- The age of opening, the date of the date of receiving the patch and the dates of the opening were also influential factors. It is evaluated as young in one year, middle age in 1-3 years and age after 3 years from an open date. The light loses its value over time. If the difference between injury and patch date exceeds 20 days or the patch has not yet been released, the risk is low if the risk is high, less than 1 day, or if the exploit code is not published. Likewise, if the difference between the date of introduction and patch date is greater than 80 days, the risk is high and the risk is low if it is small.

B. Cyber Threat and Preparedness Levels

Cyber defense preparedness process four consecutive can be summarized as a stage. Cyberspace in the first stage the mission's mission must be categorized against threats; for the achievement of the mission in the second stage preparedness level should be determined, prepared at the third stage Strategy plan for cyber security by setting targets the required safety at the fourth stage investments should be planned and decisions should be made (Bodeau, 2010).

The main step of the cyber defense is that of threat levels It is determined. Determination of threat levels is a five-step process. In Table 1 the threat levels, types of attackers at these levels, targets, strategies and methods are listed. The second step of the cyber defense is that It is determined. Determination of preparedness levels is a five-level process (Bodeau, 2010).

Table 1: Cyber Threat Levels (Badeau, 2010)

Level	Attacker Types	Attacker Target/Goal	Methods
Level 1 (Cyber Vandalism)	- Small attacker groups	- To disrupt the organizational structure - It's bad news.	- Accessing sensitive data - Performing experiments - Targeting files on systems with global access - To make network attacks - Present social engineering activities for enterprises
Level 2 (Cyber Fraud)	- Individual or small attack groups	- Political-ideological purposes - Indirectional spying - Purchasing	- Providing physical access with in-house assistance - Access to information used for pepper attack from open source - Monitoring of data traffic - Playing information system devices - Monitoring of external information systems and networks Adjusting angles to access -IIS links
Level 3 (Cyber Surveillance)	- Great attack groups - Sofistic terrorist organizations - Professional organized crime organizations	- Growth of sources - To have general infrastructure knowledge - To obtain the basic data for large-scale attacks	- Inserting spyware pieces to the organizational structure to facilitate data transfer - Add general-purpose information collectors to internal networks - Hatching and scanning of organizational networks - Realization of information systems and operations - Interface software used - Perform targeted attacks on targeted days - Contact data of the public

Level 4 (Cyber Spying)	- Professional intelligence organizations	- Special missions and programs of the countries	- Adding hardware equipment to the supply chain - Seize the session information - Install the viewing contents onto enterprise information systems and networks - Surgical insertion into the organization - Targeting new hosts and critical points Target enterprise information systems with daily attacks - Designing malicious software to enable the target board to be used by the organization - Including wireless detectors into the target structure
Level 5 (Cyber War)	- Therrier groups	- Destroy the information infrastructure of the target	- Targeting critical information system components and functions -To threaten the organization by using production, production and / or distribution components - To organize attacks on the organization by using coordinated, internal, and supply chain attacks - To create false-open organizations by injecting malicious software into the supply chain - To inject data incorrectly but incontestably - Add custom, non-directional, malicious software based on system configurations - Access to wireless communication system - Placing a spy in the privileged positions within the Board

The second step of the cyber defense is that it is determined in Table 2.

Table 2: Preparedness Levels (Badeau, 2010)

Level	Goal	Measures	Solutions
Level 1 (Environmental Defense)	- General preparedness against attacks from outside environment	-Commercial security products and desktop applications	-Creating security wall and detecting attack -To make identity validation - Anti-virus software installation on e-mail servers and client systems - Monitoring openings and environmental systems with the audit log
Level 2 (Critical Information Protection)	- Prevent access to critical or sensitive data	- Authentication - Access control systems - Encryption - Storing critical data in independent systems	-Use of reliable encrypted applications between -D) and internal systems (SSL, VPNs) - Creation of a separated and detached zone in corporate networks - Scanning of portable systems (laptops, flash drives, etc.) before reconnection - Creating a strong physical security check on critical systems to prevent malicious internal access -Periodical on-call and information defense settings - Virtualization of desktops to better control risky user behavior - Improving architecture / architecture with additional security software
Level 3 (Difference)	-Protect information system infrastructure	-Penetration tests	- Transmitting recipients to critical points to detect To analyze network traffic to monitor abnormal conditions and external currents -Following my content -To make analytical and physical access analysis - Monitoring of environmental transmission channels for data transfer
Level 4 (Architectural Flexibility)	-To examine the history of	- Backing up the information system infrastructure - Restriction of components - Create a flexible architecture against the attackers	-Use strong access to critical information systems - divide the system into sub-sections to control the internal structure and make reconfigurations quickly - To minimize the time between supply and supply chain -Performing the physical structure of structures (Penetration Test) - Using trusted devices -Making small changes in soft-software configurations

Level 5 (Agility)	- Ready for attacks targeting target organization structure	- Design of systems as soon as possible - Selecting flexible and adaptable architecture	-Use multiple suppliers for key components -To obtain critical components to the name of the Board through reliable means -Penetration tests - Virtualize services -Recrease critical functions to reduce the aggressive ability periodically -To make a structural analysis and analysis of recent attacks in order to respond to future attacks

C. Cyber Threat and Their Affects

The effects of cyber threats are short and long term. Short-term threats are threats that affect the daily activities of the organization, government, business and end users it targets. Examples include daily activities such as fraudulent activities, customer data breaches, cash withdrawal from ATMs. Long-term threats are threats such as industrial and military espionage, social discontent and discomfort, and a national security breach, which have long-lasting effects, aiming to change the balances of the country and society (Choo, 2011).

Malicious Software, Unsafe Environments, DOS Attacks, Password Handling Attacks, Side Channel Attacks, HTML Injection, SQL Injection and Command Injection threats can be assumed as major threats.

a. Malicious Software

Obtain, change, or discard data using malicious software, such as Trojans, viruses, keyboard listening, spyware, junk e-mail, are used for such purposes. Malicious software is often considered to be the most dangerous cyber-attack tool for governments, businesses and end users, both in terms of ease of use and quick results. Malicious applications can be hardware-rich as well as software. An example of this is the keyboard listening devices that process hardware. Sometimes a small device is inserted into the device and any information (passwords, file names, file contents, etc.) that are entered from the keyboard can be saved (Choo, 2011).

Attacks do not necessarily have to be made through the network. Malicious software can be installed on devices that do not have a network connection, and data override can occur. Spyware installed on ATM and POS devices can allow users to acquire data illegally or cause loss of material (Choo, 2011).

b. Unsafe Environments

Network security depends on the safety of the network-forming network elements. By using the product's security aspects, it is possible to attack the systems and access information. An example of this is the Stuxnet virus. PLC rootkit index of a particular product brand this virus, which has been developed as a benefit, has brought the industrial system to a standstill (Choo, 2011).

c. DOS attacks

These attacks are direct attacks to the system which causes serious damage by stopping or interrupting systems (Yang, 2011). DDOS attacks are attacks aimed at bringing the system to a standstill, targeting more than the number of requests that the operating system, server, or application can answer, targeting the accessibility rule of information (Altundal, 2012).

d. Password Handling Attacks

The main methods used in these attacks, which are considered in the context of privacy breaches, are social engineering attacks, dictionary attacks and password prediction applications. With the help of social engineering attacks and social skills, information about people is obtained and the population is tried to be spread (Yang, 2011).

e. Side Channel Attacks

Side channel attacks are attacks on power analysis, electromagnetic applications, and scheduled tasks of systems. The main purpose of these attacks is to squeeze a spy application into the system to capture the encryption key. Many Intelligent

Systems have unfortunately lost their customer information, usage information and passwords as a result of these attacks (Yang, 2011).

f. HTML Injection

This vulnerability benefits programmer's incorrect coding during coding. The fact that data taken from the database or data from the database is not passed through a control mechanism in the web software. A session and a cookie play are made by using the so-called XSS (Çitil, 2009).

In applications, it is logical to return a response to a request sent to the page. The request sent to the page is evaluated on the server and a reply is returned. But if your page is redirected to a malicious URL or tools like Trojan horse are placed, your response will be different from what you expected. The purpose of this attack type is not to damage the web application, but rather to access users who visit the application (Dwen-ren, 2009).

g. SQL Injection

The SQL injection is an attack targeting the query from the database. This attack is performed using the interrogation language construct. SQL Injection is one of the most serious vulnerabilities in web applications. Especially with the popularization of additional database layers such as frameworks and ORM (Object Relational Mapping), it is a little less common than before, but make sure they're still everywhere!

Web application developers do not fully understand SQL Injection because they make some fatal errors. That is why we do not see many simple SQL Injection methods known today, but you can see the advanced SQL Injection vulnerabilities from large companies to ready systems.

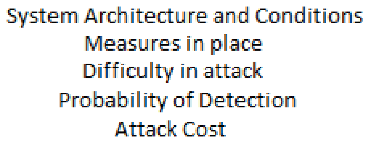
h. Command Injection

Generally, shell injection attacks are a type of attack that directly targets servers, as opposed to SQL injection and XSS attacks. It aims to access the information on the operating system, database management system and server by remote access using the command line of the web application (Dwen-ren, 2009).

2. CYBER RISK ANALYSIS, ASSESSMENT METHODS AND TOOLS

A. Attack Trees

Attack Tree method is of the comman method that is used to evaluate the attack surface of physically cyber vulnerable systems, called cyber physical systems, such as SCADA, Nuclear Power Plant, Energy Grid. In SCADA systems, for example, Byres et al. states that attack trees, MODBUS and MODBUS / TCP communication protocols based on SCADA systems were used to evaluate security vulnerabilities. MODBUS is a protocol developed for the communication and compatibility of devices used in industry. The attack tree provides a structured view of the events that lead to the attack, and ultimately helps to identify appropriate security measures. These measures appear in Figure 1.



System Architecture and Conditions
Measures in place
Difficulty in attack
Probability of Detection
Attack Cost

Figure 1: Attack Tree Events (Byres at al., 2004)

The aim of the evaluation was done by Byres, to calculate the characteristics of the best attack event and to determine the possible ways to achieve the ultimate goal of the attack. To achieve this, an industry team of experts first sets out an attacker's possible goals and designs the tree with the targets shown as tree nodes. Subsequently, a tree assigns a technical difficulty level on each lever's technic Trivial - Moderate - Difficult - Unicely scale. Based on the two functions, the difficulty of each node with one child node is calculated. The degree of difficulty may vary over time. The article has attack tree (Figure 2).

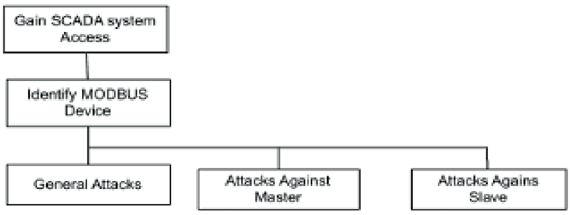


Figure 2: Attack Tree System (Byres at al., 2004)

B. Vulnerability Methodology

A cyber security assessment methodology within the SCADA systems in Permann and Rohde is based on the process of assessing the safety of as part of a program funded by the Ministry of Energy. The methodology defined includes the following stages (Perman and Rohde, 2005):

a) Production of Evaluation Plan: At the beginning, an evaluation should be summarized with the participation of a plan, budget, program, objectives, resources and the necessary experts.
b) Environment Creation: the test environment should be created and configured under the best conditions.
c) Safety Assessment: This phase is usually carried out by penetration testing. A number of open source and commercial vehicles are listed to assess system vulnerabilities.
d) Reporting: The assessment and testing methodology should be documented along with the results.
e) Metrics and scoring: The safety of the SCADA system should be quantitatively measured to compare with other systems.

C. Quantitative Methodology

McQueen proposes a methodology to help reduce cyber risk for a again SCADA system with increased assurance of cyber attacks. For risk reduction estimation, a directed graph of a cyber attack is developed using both initial and advanced systems. Then the difference between time and compromise is measured and analyzed in each system. The methodology consists of ten steps. These steps are shown in Figure 3.

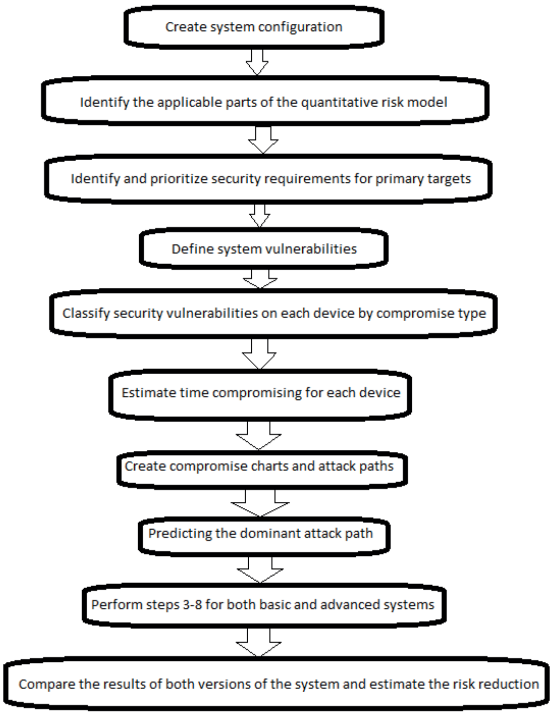
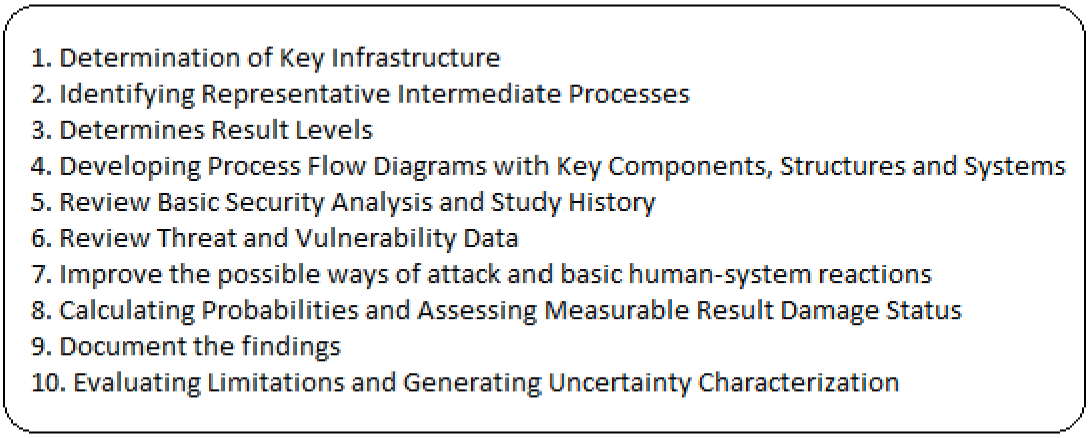

Create system configuration
Identify the applicable parts of the quantitative risk model
Identify and prioritize security requirements for primary targets
Define system vulnerabilities
Classify security vulnerabilities on each device by compromise type
Estimate time compromising for each device
Create compromise charts and attack paths
Predicting the dominant attack path
Perform steps 3-8 for both basic and advanced systems
Compare the results of both versions of the system and estimate the risk reduction

Figure 3: Quantitative Methodology (McQueen et al., 2006).

McQueen has developed a formula to calculate the likelihood of an undesirable event. This expressed probability is defined as follows; the possibility of the system being included in the target list of an attacker, the possibility of being attacked by the system, the possibility of an environmental violation when the system is attacked, the situation where a successful attack is a environmental violation and the possibility of harm to the system is successful. (McQueen et al., 2006).

D. Scenario-based Analysis in Supporting Cyber Security

Gertman National Security Department has introduced a scenario-based approach to cyber risk assessment for the National Cyber Security Division. This process consists of ten cases. These are shown in Figure 4.



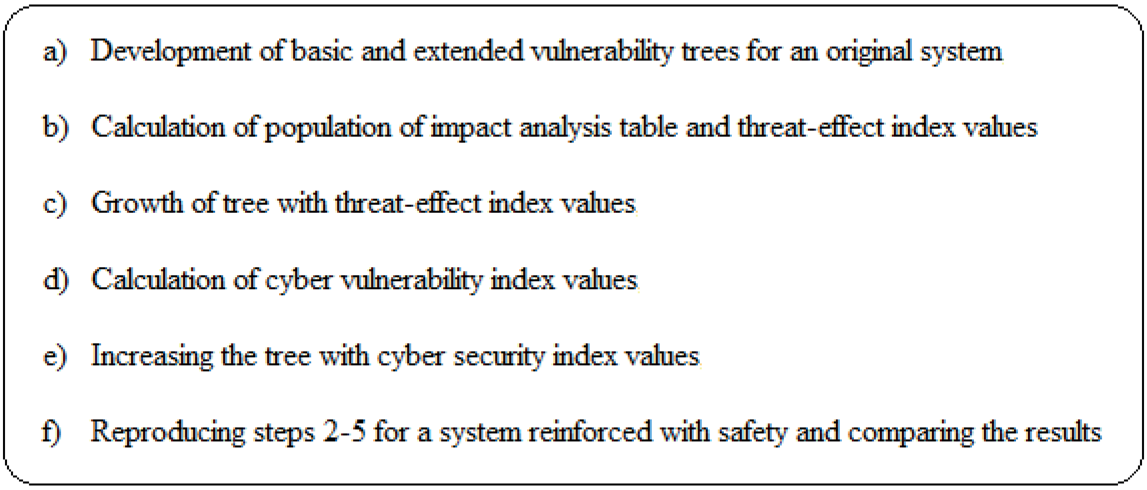
1. Determination of Key Infrastructure
2. Identifying Representative Intermediate Processes
3. Determines Result Levels
4. Developing Process Flow Diagrams with Key Components, Structures and Systems
5. Review Basic Security Analysis and Study History
6. Review Threat and Vulnerability Data
7. Improve the possible ways of attack and basic human-system reactions
8. Calculating Probabilities and Assessing Measurable Result Damage Status
9. Document the findings
10. Evaluating Limitations and Generating Uncertainty Characterization

Figure 4: This Analysis steps (Gertman et al., 2006).

The system is modeled by experts who are familiar with the industrial process and safety requirements. Security vulnerabilities and threats, and the expected human-system response were reviewed through operational experts, while probabilities and possible violations were expressed by cyber experts. Experts' opinions are produced using Delphi technique.

E. Two Index Methods

This method for evaluating the distrust of Patel SCADA systems has been proposed (Patel et al, 2008). The method supports system administrators to make more logical and accurate decisions about the security measures to be implemented. The method consists of a tree of vulnerability that is supported by two arrays, the threat directory. The method requires six steps to be in Figure 5.



a) Development of basic and extended vulnerability trees for an original system

b) Calculation of population of impact analysis table and threat-effect index values

c) Growth of tree with threat-effect index values

d) Calculation of cyber vulnerability index values

e) Increasing the tree with cyber security index values

f) Reproducing steps 2-5 for a system reinforced with safety and comparing the results

Figure 5: The Method of Steps (Patel et al, 2008).

This method of Patel was developed using the analysis of attacks launched in the past. Economic losses due to attacks were estimated by discussing with experts and those affected. The attack probabilities were determined by looking at all past data.

F. Adversary-driven State-based System Security Evaluation

LeMay, Advertising View Safety Assessment method is proposed. Enriches the attack graph with competitors' features. Simulate an attack is aim for this method, determine the most likely attack path, and calculate the likelihood of an attack using a system's executable status-based model for security. This method recommends following three steps to respond to a security question (Lemay et al., 2010):

- Characterizing competitors and the system and specifying safety measures,
- Describing possible attacks,
- Conduct produce an answer.

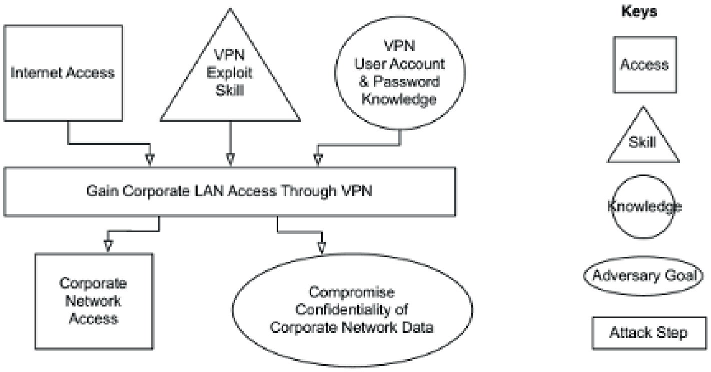
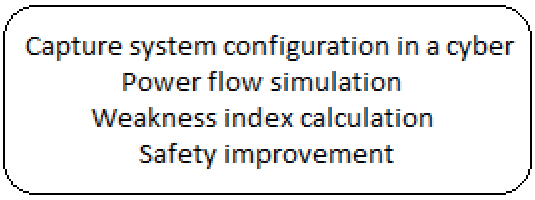

Internet Access
VPN Exploit Skill
VPN User Account & Password Knowledge
Gain Corporate LAN Access Through VPN
Corporate Network Access
Compromise Confidentiality of Corporate Network Data
Keys
Access
Skill
Knowledge
Adversary Goal
Attack Step

Figure 6: The Attack Step (LeMay et al., 2011).

A system's security model includes an attack execution graph, a series of attack stages, and security-related system features that are presented as features of an opponent. An attack step as shown in Figure 6 is characterized by the attack prerequisite, execution time, cost, a series of results, result distribution, detection distribution, payment and status variable updates. One competitor is characterized by two system independent features and characteristic connected to three systems (Lemay et al., 2010).

G. Cyber Security for Defense Modeling

A four-part SCADA security method was introduced by the RAIM Ten. This is then done to collect data for impact analysis. Impact analysis is to examine the effects of the theft and the effect of cyber attack on a SCADA system. This review consists of four steps. These steps are given in Figure 7 (Ten, 2010).



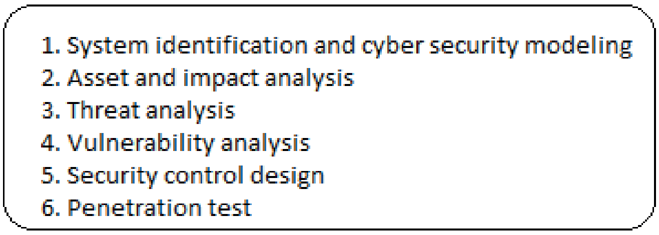
Capture system configuration in a cyber
Power flow simulation
Weakness index calculation
Safety improvement

Figure 7: This Cyber Modeling steps (Ten, 2010).

Impact analysis is based on an attack tree where a cyber insecurity index indicates the probability of endangering branches of an attack tree, the probability of a particular attack scenario or general attack. Information about security measures and password policies. The implementation of the frame is shown in a test subnet of the electrical power control network (Ten, 2010).

H. Cyber Security Risk Assessment in Nuclear Power Plants

Song has introduced a cyber security risk assessment method that can be used in control systems's designs in nuclear power plants. This method outlines the six steps for cyber security. These steps are given in Figure 8 (Song, 2012).



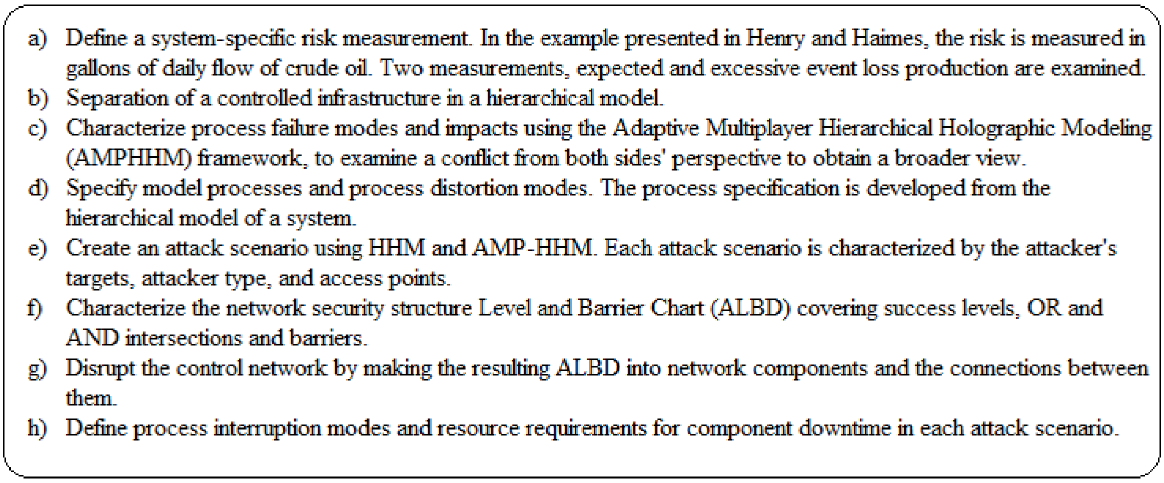
1. System identification and cyber security modeling
2. Asset and impact analysis
3. Threat analysis
4. Vulnerability analysis
5. Security control design
6. Penetration test

Figure 8: This Plants steps (Song, 2012).

The article summarizes the relevant NIST standards and explains the activities that should be carried out at each step. Possible attack scenarios for use in the threat analysis are listed. It is recommended that you use an existing vulnerability list for vulnerability analysis and adapt it to the properties of the analyzed system. Safety checks are acceptable to the relevant NIST standards. Finally, the security check design must be confirmed (Song, 2012).

I. Network Security Risk Model (NSRM)

NSRM was introduced by Henry and Haimes. NSRM is a directed graph representing an attack. In this graph, the nodes define the components of a system and the edges indicate the connections a component can affect the other. The aim of the design is to assist in the selection of risk management controls by setting a risk value and calculating the measurement of a baseline and calculating the improved security versions of a system. This model consists of eight steps. These steps are given in Figure 9 (Henry and Haimes, 2009).



a) Define a system-specific risk measurement. In the example presented in Henry and Haimes, the risk is measured in gallons of daily flow of crude oil. Two measurements, expected and excessive event loss production are examined.
b) Separation of a controlled infrastructure in a hierarchical model.
c) Characterize process failure modes and impacts using the Adaptive Multiplayer Hierarchical Holographic Modeling (AMPHHM) framework, to examine a conflict from both sides' perspective to obtain a broader view.
d) Specify model processes and process distortion modes. The process specification is developed from the hierarchical model of a system.
e) Create an attack scenario using HHM and AMP-HHM. Each attack scenario is characterized by the attacker's targets, attacker type, and access points.
f) Characterize the network security structure Level and Barrier Chart (ALBD) covering success levels, OR and AND intersections and barriers.
g) Disrupt the control network by making the resulting ALBD into network components and the connections between them.
h) Define process interruption modes and resource requirements for component downtime in each attack scenario.

Figure 9: This Risk Model steps (Henry and Haimes, 2009) (Haimes and Horowitz, 2004)(Salinas, 2003).

Depending on the return, most appropriate attack policy for which the attacker can do which components of a system can be determined. The probability of an attack is calculated for a basic system. Then, for security versions in the system, the same parameters that the attacker can use are estimated. The analysis of the comparison between the cost of security solutions for the risk criteria for every improved security version in the system helps to identify most appropriate security strategy and to determine the security budget. Henry and Haimes have designed a methodology to calculate all parameters of the system (Henry and Haimes, 2009).

J. The CORAS Method

CORAS is a method for creating and controlling security risk analysis and controlling all these processes. This method provides a customized language for risk modeling. At the same time, this method includes detailed guidelines that explain how to use the language to access relevant information in various steps for security analysis and to collect them in a framework. In this respect, CORAS is based on the model. Unified Modeling Language (UML) is often used to model the target of analysis. This method provides a computerized tool designed to document and report analysis results using risk modeling (Lund, 2011).

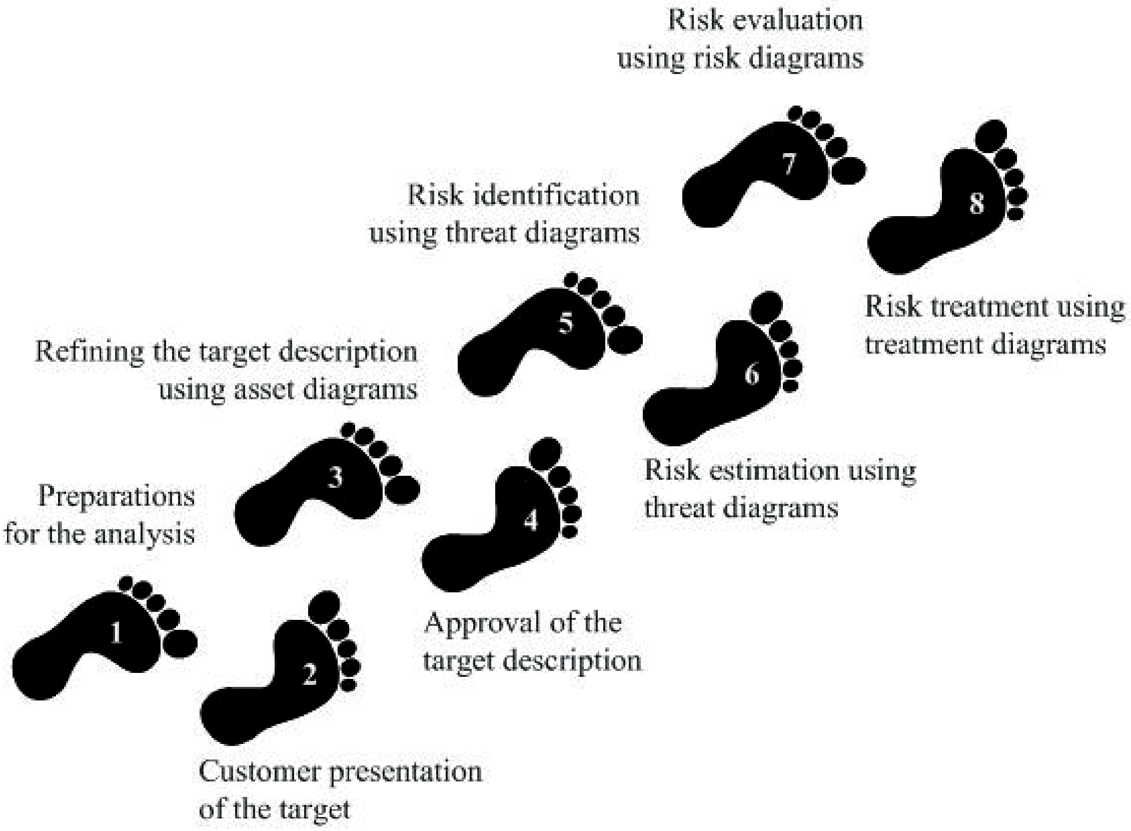


Figure 10: This CORAS Method steps (Lund, 2011).

There are five types of diagrams in the CORAS language:

- Asset diagram,
- Threat diagram,
- Risk diagram,
- Measure diagram,
- Measure specific / diagram.

Some concrete steps in each type of diagram risk analysis processsupports. Three types of diagrams that can also be used for various purposes there is more:

- High-level CORAS diagram,
- Dependent CORAS diagram,
- Legal CORAS diagram.

K. STS Tool

This tool is a type of software that allows drawing and matching the diagrams of the CORAS method. With this software all CORAS diagrams can be created. In addition, these generated diagrams can be interpreted by making sense.

3. CONCLUSION

In this study, 9 studies about Cyber Risk Management are included. The details of these studies are mentioned. In future studies, in the light of these 9 studies, the areas in which Cyber Risk Management can be addressed and how it can be realized can be discussed. Furthermore, the addition of new steps or methods to the methods and steps mentioned in the 9 studies mentioned herein may be added as another contribution.

Nowadays, digitalization is perceived as the formula of achieving business objectives and profitability of institutions with the widespread and effective use of information systems. For this purpose, the combination of different manufacturers' solutions and different technologies brings together a digitalization complex. The use of this intensive technology can turn into a technology addiction if risks are not taken into consideration. Being resistant to cyber risks requires awareness-raising at all levels, from employees to senior management levels. Where cyber hazards can come from. Identifying possible attack scenarios for the values, resources and assets that form the core of the organization, and then determining how these scenarios and threats affect the workflows, making the risk assessments constitute the essence of this service. At the next stage, necessary process improvements and, if necessary, software / hardware solutions are determined to reduce risks / avoid risks. All these solutions can be considered as a result of the studies we have described in this study and other than the ones we have described here. As a result of this Cyber Risk Management process, the current technological developments can be demonstrated.

As a result, the main purpose of all these Cyber Risk Management activities is to anticipate, prevent, and eliminate the things that will cause attacks before they come. As we mentioned before, in the future, which method is better, the same type of attacks can be made with different variations, or a new method can be proposed.

Grant Support: The author received no financial support for this work.

References

Altundal, Ö. F. (2012). *DDoS nedir, ne değildir*? Erişim adresi: http://www.siberguvenlik.org.tr/makaleler/ddos-nedir-ne-degildir

Bodreu Deborah, J., Graubart R., & Fabius-Greene J. (August 2010). *Improving cyber security and mission assurance via cyber preparedness (cyber prep) levels*. 2010 IEEE Second International Conference on Social Computing (SocialCom).

Byres, E., Franz, M., & Miller, D. (2004). *The use of attack trees in assessing vulnerabilities in SCADA systems*. Proceedings of the international infrastructure survivability workshop.

Choo K., & Kwang R. (2011). "The cyber threat landscape: Challenges and future research directions". *Computers and Security*, November, (719–731)

Çitil, F. (2009). *HTML injection tehlikesi*. Erişim adresi: http://www.cybersecurity.org.tr/Madde/220/HTML-Injection-Tehlikesi-

Dwen-Ren, T., Chang, A.Y., Peichi L., & Hsuan-Chang C. (2009). "Optimum Tuning of Defense Settings for Common Attacks on the Web Applications", Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on, January 2009, (pp. 89–94).

Gertman, D., Folkers, R., & Roberts, J. (2006). *Scenario-based approach to risk analysis in support of cyber security*. Proceedings of the 5th International Topical Meeting on Nuclear Plant İnstrumentation Controls, and Human Machine Interface Technology.

Haimes, Y. Y., & Horowitz, B. M. (2004). Adaptive two-player hierarchical holographic modeling game for counterterrorism intelligence analysis. *Journal of Homeland Security and Emergency Management*, *1*(3), 121.

Henry, M., Haimes, Y. A. (2009). Comprehensive network security risk model for process control networks. *Risk Analysis*, *29*(2), 223–248.

Jumratjaroenvanit, A., & Teng-Amnuay, Y. (2008). *Probability of attack based on system vulnerability life cycle*. Electronic Commerce and Security, 2008 International Symposium.

In Hoh Peter, Kim Young-Gab, Lee Taek, Moon Chang-Joo, Jung Yoonjung, Kim Injung, "A Security Risk Analysis Model for Information Systems", http://www.luisolis.com/seminario2011/papers/A Security Risk Analysis Model for Information Systems.pdf, 2011.

Internet World Stats. (2018). www.internetworldstats.com/stats.htm

LeMay, E., Unkenholz, W., Parks, D., Muehrcke, C., Keefe, K., & Sanders, W. H. (2010). *Adversary-driven state-based system security evaluation*. Proceedings of the 6th International Workshop on Security Measurements and Metrics.

Le May, E, Ford, M., Keefe, K., Sanders, W., & Muehrcke, C. (2011). *Model-based security metrics using adversary view security evaluation (advise)*. 2011 Eighth İnternational Conference on Quantitative Evaluation of Systems (QEST). IEEE, 191– 200.

Lund, M. S., Bjørnar, S., & Stølen, K. (2011). *Model-driven risk analysis: The CORAS approach*. Berlin, Germany: Springer.

McQueen, M., Boyer, W., Flynn, M., & Beitel, G. A. (2006). *Quantitative cyber risk reduction estimation methodology for a Small SCADA control system*. Proceedings of the 39th annual Hawaii International Conference on System Sciences.

Patel, S., Graham, J., & Ralston, P. (2008). Quantitatively assessing the vulnerability of critical information systems: a new method for evaluating security enhancements. *International Journal of Information Management*, *28*(6), 483–491.

Permann, M. R., & Rohde, K. (2005). *Cyber assessment methods for SCADA security*. 15th annual joint ISA POWID/EPRI controls and instrumentation conference, Nashville, TN.

Salinas, M. H. (2003). *Combining multiple perspectives in the specification of a security assessment methodology* (Ph.D. thesis, University of Virginia)

Song, J., Lee, J., Lee, C., Kwon, K., & Lee, D. (2012). A cyber security risk assessment for the design of I&C Systems in nuclear power plants. *Nuclear Engineering and Technology*, *44*(8), 919–928.

Ten, C-W., & Manimaran, G., & Liu, C-C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Trans Syst Man Cybern A Syst Hum*, *40*(4), 853–865.

Barnard-Willsi D., & Ashenden, D. (2012). Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture*, *15*(2), 110–123.