Advances and Applications in Mathematical Sciences
Volume 20, Issue 10, August 2021, Pages 2061-2070

CYBER SECURITY: A NECESSITY, NOT AN OPTION

PRIYANKA RATTAN, SHALU TANDON and NIKHIL GARG

Jagannath International Management School
New Delhi, India
E-mail: priyanka.rattan@jagannath.org
shalu.tandon@jagannath.org

Abstract

Information Security is needed to safeguard an organisation's essential resources, such as sensitive data, hardware and software. By applying suitable safeguards an organisation's important work, research, data, resources and other tangible and intangible assets etc, can be made secure against theft and misuse. Many People see security as a waste of time and money. They perceive security measures as hindrances and find it bothersome for users, managers, and systems. Well-chosen security protocols and procedures are adopted just to safeguard valuable assets not clearly understanding their need and importance.

Building an information security program that adheres to the principle of security as a business enabler is an initiative in an enterprise's effort to create an efficient security program. Organizations must continuously (1) discover and evaluate information security risks to business operations; (2) regulate what policies, standards, and controls are worth applying to cut back these risks; (3) endorse awareness among the staff; and (4) evaluate compliance and control effectiveness. As with other varieties of internal controls, this is often a cycle of activity, not an exercise with an outlined beginning and end.

What is Cyber Security?

Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. [1]

Researchers in cybercrimes have established that cyber attacks hit businesses in every day. The number of cybercrimes is rapidly increasing

2010 Mathematics Subject Classification: 97P70, 03B70, 92C42, 68U01.
Keywords: Social Media, Traffic, Events, Twitter, Hashtag, Tweets, Prediction, Regression, Analysis.
Received October 7, 2020; Accepted January 15, 2021

every year as people try to benefit from vulnerable business systems. Often attackers are looking for ransom. It has been found that the number has been increasing manifold every year. Some of the companies don't get to know that they have been hacked for quite some time.

Some cyber criminals have specific objectives in their mind while planning an attack. They know who they want to harm, and its potential benefits. They will go to any extent to achieve their goals. In this section we will describe significant threats faced by organisations and individuals during 2019-2020.

It is a type of attack in which user is unknowingly redirected to malicious sites. Instead of the user going to the intended site, he or she is led to a malicious site. Once you arrive at the malicious site, the attacker is now in a position to install malware, collect your credentials/confidential data, and even impersonate and act on your behalf.

2. Remote Access Trojans (RATs)

RATs include the ability to steal and temper saved usernames and passwords. Once they have usernames and passwords in their hands the attacker can log in to the shared server. Imagine you are working on a sensitive project and someone makes in roads in your system and he has access to all your confidential and sensitive information which he can use in a manner he desires.

3. Phishing

Phishing is a type of cyber crime in which target is contacted by e-mail, sms by a fraudster posing as a legitimate entity to lure an individual to provide sensitive details, usernames and passwords.

4. Social Engineering

It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information through a broad range of malicious activities.

There was a time when the locks on doors were counted as safety and security, but in today's world security breach in the cyber world can result in

grave consequences to an individual, an organisation or a country. We are connected through the web to every person. Any unauthorized access to someone's personal, professional or organisations information is a security breach and hence strong measures are needed to prevent it and therefore comes the need for a secure and robust system to protect sensitive and vital information so that an organisation or company is not vulnerable against any cyber-attack or theft. [2] The overall security objectives comprise the following:

- Confidentiality
- Integrity, which may include authenticity and nonrepudiation
- Availability

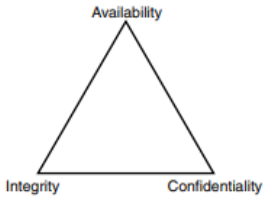


Figure 1. CIA Triad.

This is true for the majority of cyber security-related threats a user and/or organisation could be exposed to. However, this paper contends that cybersecurity threats don't form a part of the formally defined scope of data security. This section will briefly present a couple of scenarios as examples:

1. Ransomware Attack on a financial institution: For instance, some 35000 computers at the energy company Saudi Aramco were infected by the Samoon Virus which made business operations non operational for 10 days and destroyed 85% of the company's hardware.

2. Cloud Security Breaches: No organization is completely safe from data breaches. With retail corporations like Target and insurance companies like Anthem previously experiencing breaches to customer data, the distress and probability of being the target of a cybersecurity breach is at an all-time high. Many businesses tend to believe securing sensitive data within the cloud would prevent hackers from gaining access to the data.

3. Cyber Terrorism: Cyber terrorists or competitor or enemy nation's spies might target a nation's critical and confidential information through cyberspace. This could either be indirect, for example, by influencing and manipulating the available information services using denial-of-service attacks or, more directly, defacement of government websites like the Supreme Court of India website. In the case of attacks against such critical infrastructure, the loss entails not only to the integrity or availability of information resources but also that of access to such vital services. Because In such cases, it is not an individual, but the welfare of society as a whole is at risk. An excellent example of such attacks is the attacks on Estonia in April/May of 2007.

These discussed scenarios deal with various aspects of cybersecurity where the interests of an individual, society, or nation, including their non-information-based assets, need to be shielded from risks stemming from interaction with cyberspace.

5. Risk Management

Risk analysis is a tool used to identify, determine, and evaluate risks and susceptibilities through a cyber-attack or threat. To define risk analysis more elaborately, it is a systematic process to examine the threats facing the information technology assets and the vulnerabilities of these assets and show the likelihood that these threats will be realised.

Thus, risk analysis is an aid by which risks to IT assets can be identified and quantified, also it can determine the probability of the risk occurring and the consequence if the adverse event actually happens. Risk analysis is, therefore required and is essential for securing IT assets. Once risk analysis is done, and vulnerabilities are identified, the identified risks have to be suitably managed, reduced and eliminated as far as possible through risk management by applying proper security measures.

Today is the information era, where information has become a vital resource and is extremely valuable to an organisation just like any other valuable asset information that needs to be adequately protected to ensure business viability and progress. Today we need to protect not only the technical information but also both business and personal information

wherever it resides. The emphasis has thus shifted more towards the protection of information rather than just the infrastructure [3].

Although asset valuation is a vital portion of risk analysis, quantifying information could prove to be a rather frightening task. The quantification of risks to physical or tangible assets already showed to be an extremely tough task.

What is the need for Risk Management?

Recent focus and concern on information security breaches have led to a better understanding of information security issues. Increased instances of security breaches have led to the formulation of legislation addressing these risks.

Awareness and legislation to regulate and manage security risks have forced corporations in many sectors to employ various means to measure and find solutions to corporate assets' information security risks.

These affected agencies and firms have now got the motivation to at least implement the minimum-security practices. After years of unders pending in other industries in information technology improvements, the healthcare industry more recently began outspending these industries to make up for time-lapsed and to comply with the Health Insurance Portability and Accountability Act (HIPAA). Although the recent spurt of attention in this area appears to be new, regulations that require information security practices have been introduced and revised since the 1980s.

Management of Risk

Risk management "refers to planning, monitoring and controlling activities which are based on information produced by risk analysis activity". In contrast, the management of risk is described as the "overall process by which risks are analysed and managed" as illustrated in Figure 2.

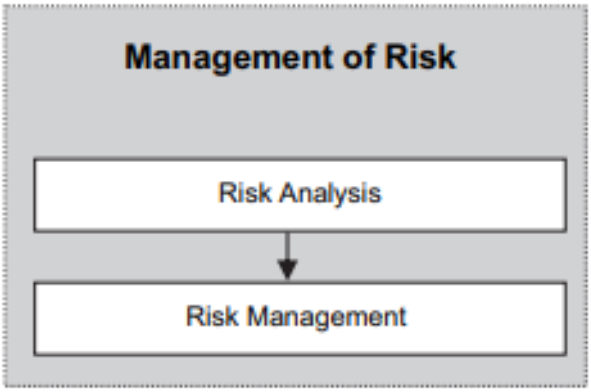


Figure 2. The Process within the overall management of risk.

According to the previous explanation, it may be concluded that risk analysis comes before risk management. Together, the method of risk analysis, followed by the method of risk management can be considered a part of the management of risk. Both these processes, risk analysis and risk management will independently be discussed in more detail.

Risk analysis

Risk analysis is the sum of risk identification, estimation, and evaluation. The basic phase of risk analysis, as illustrated in Figure 3, is risk identification.

The primary purpose of risk identification is to identify risks involved, weigh its probability and magnitude in different scenarios. Cybersecurity specialists follow a set method when evaluating risks. The first step is to determine what can go wrong, second is to assess its probability and lastly, to determine how severe impact would be if it actually did go wrong.

According to Kirkwood [4], the evaluation of risk as:

Risk=probability x severity of harm

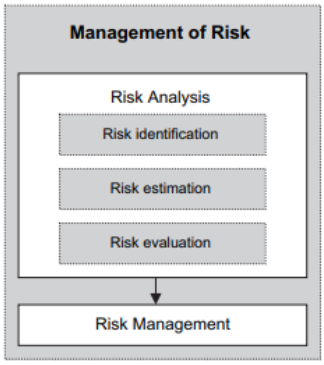


Figure 3. The sub-processes of risk analysis.

The evaluation of risk in this way places an undesirable connotation on risk and depicts that risk is wicked. Although bizarre at first, the risk is, however, still a neutral concept, as it used to be regarded during the late seventeenth and eighteenth century. It is equally accurate to see risk as something going right, like something going wrong.

6. Risk Assessment

A significant side benefit of risk assessment is – an in-depth knowledge about a system and organisation. In order to make a system more secure, risk analysts try to figure out the interrelation between the systems and functions. The risk assessment process consists of four steps:

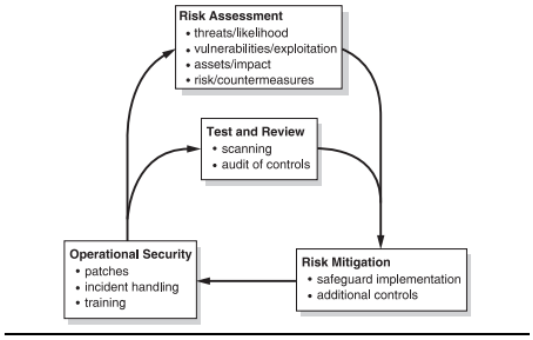
• Preparing for the assessment. This stage establishes a context for the risk assessment by applying the outcomes from the risk framing step of the risk management process. Risk framing classifies organizational information regarding policies and requirements for conducting risk assessments, specific assessment methodologies to be employed, procedures for selecting risk factors to be considered, the scope of the assessments, thoroughness of analyses, degree of formality, and requirements that facilitate steady and repeatable risk determinations across the organization. Organizations should use the risk management strategy to the extent feasible to obtain the desired information for the risk assessment and to prepare for the assessment.

• Conducting the assessment. This step produces a list of information security risks that can be arranged by risk level and used to inform risk

response conclusions. Organizations analyse threats and vulnerabilities, impacts and likelihood of harm, and the doubt connected with the risk assessment process. They also gather essential information as a part of each task to assure that this step is conducted in accordance with the assessment context established in the previous step. The objective is to adequately cover the entire threat environment in accordance with the specific definitions, guidance, and direction established during the first step. To accomplish adequate coverage within available resources, organizations may have to simplify threat sources, threat events, and vulnerabilities and assess specific, thorough sources, events, and vulnerabilities necessary to achieve risk assessment objectives.

- Communicating assessment results. This step communicates the assessment results and helps the sharing of risk-related information. Once the decision maker come across the results, the organisation are made aware of the results and they now have the appropriate risk related information. It guides them in their risk decisions.

- Maintaining the assessment. In carrying out this phase, organizations should maintain the currency of their specific knowledge of the risk situation. The outcomes of risk assessments inform risk management decisions and guide risk responses. To support the ongoing review of risk management decisions, organizations should maintain their risk assessments by incorporating any changes noticed through risk monitoring. Risk monitoring delivers organizations with a continuing ability to determine the effectiveness of risk responses, to identify risk-impacting changes to organizational information systems and their operating environments, and to verify compliance. [6]



7. Risk Mitigation

Risk Mitigation is basically managing risks involved. It entails strategies devised to eliminate, reduce or control the impact of identified risks inherent with a specified undertaking before a severe injury or damage is done. The purpose of risk mitigation is to for see and deal with the risks involved.

8. Conclusion

With the rapid development of information technology, personal computers, telecommunications, and the internet, people can access the information at any place, at any time. Though most people acquire the information legally, hackers to bypass the security loophole and attack the computer systems for personal benefits or intention to cause losses and harm to different organisations, government and individuals. The attacker may be an insider or may be hired by a competitor ot it may even a guy with destructive intention. The attack can either be Denial of Service (DoS) or be significant damage to the whole framework. The concept of information security has become a burning issue for the entire world. To safeguard the computer systems and data, Risk analysis is done.

Risk analysis was conventionally used to analyse risks posing a threat to mostly IT assets. However, with the onset of the information age, a rising need for protecting information from risks currently faced by many organizations globally came about. As the protection of information is deemed crucial for the continued existence of most organisations an alternative, more comprehensive approach to risk analysis is suggested in this document. This is complex and difficult, if not impossible.

References

[1] School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth 6031, South Africa, 2013, From information security to cyber security.

[2] Thomas R. Petlier, Justin Petlier and John Blackley, Information Security Fundamentals.

[3] Douglas J. Landoll, The Security Risk Assessment Handbook, A Complete Guide for Performing Security Risk Assessments.

[4] Mariana Gerber and Rossouw Von Solms, Management of risk in the information age, 2005.

[5] M. Eric Johnson, Managing Information Risk and the Economics of Security

[6] NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments

[7] Kwo-Jean Farn, Shu-Kuo Lin and Andrew Ren-Wei Fung, A study on information security management system evaluation—assets, threat and vulnerability 2003,

[8] Yikai Xu, Yi Yang, Tianran Li, Jiaqi Ju and Qi Wang, Review on Cyber Vulnerabilities of Communication Protocols in industrial Control Systems.

[9] Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment, https://strategicstudyindia.blogspot.com/2019/10/cyber-risk-scenarios-financial-system.html.

[10] NIST SP 800-12, October 1995, An Introduction to Computer Security: the NIST Handbook.