GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 10, Issue 9, Sep. (2022)

# CYBER THREATS, VULNERABILITIES AND RISKS IN ECONOMIC SECTORS

Ibragimov Nodirjon Nusriddinovich
iffn (PHD), TUIT Karshi Branch IT-Service
Department Associate Professor

Askarova Nargiza Ilhomkhojayevna
TUIT Karshi Branch IT Department Assistant

Amirov Akbarshakh Dilshad son
TUIT Karshi Branch IS-11-20 Group Student

Abdurakhmanov Vahid Abdumuqim son
TUIT Karshi Branch IS-12-20 Group Student

## ABSTRACT

Terms such as cyberthreats, vulnerabilities, and risks are often used interchangeably and confused. This article aims to define each term, highlight how they differ, and show how they relate to each other.

**Keywords:** DDoS, Phishing, SQL Injections, Cross-site scripts, hacktivists.

## INTRODUCTION

Cyberthreats, or simply threats, refer to cyber security situations or incidents that can cause harm due to their consequences. A few examples of common threats are: a social engineering or phishing attack that causes an attacker to install a Trojan and steal personal information from your applications, a DDoS hijacking of your website by political activists, an administrator's production leaving random data unprotected on the system.

Cyber security threats are carried out by threat actors. Threat actors typically refer to individuals or organizations that may initiate a threat. Although natural disasters, as well as other environmental and political events, constitute a threat, they are not usually considered as threat entities. Examples of common threat subjects include financially motivated criminals (cybercriminals), politically motivated activists (hacktivists),include competitors, disaffected employees, disgruntled employees, and nation-state attackers.

Cyber threats can become more dangerous if attackers use one or more vulnerabilities to gain access to a system, including the operating system.

Vulnerabilities simply refer to weaknesses in a system. They make the outcome of the threat possible and even more dangerous. A system can be exploited through a single vulnerability, such as a single SQL Injection attack, which can give an attacker complete control over sensitive data. An attacker can also combine multiple exploits using multiple vulnerabilities to gain more control.

Examples of common vulnerabilities are: SQL Injections, Cross-site scripting, server misconfiguration, sensitive information transmitted in plain text, etc.

Risks are often confused with threats. However, there is a subtle difference between the two. Cybersecurity risk refers to the combination of the likelihood of a threat and the impact of loss. Basically, this means:

Thus, the risk is the scenario that should be avoided along with the losses that may occur as a result of this scenario. Here's a hypothetical example of how you might create risks:

1. SQL Injection is a vulnerability.
2. The theft of sensitive data is one of the biggest threats that SQL Injection enables.
3. Financially motivated attackers are one of the threats.
4. Theft of confidential information brings significant financial costs (financial and reputational loss) to businesses.
5. Given that SQL Injection is an easily accessible, widely used vulnerability, and that the site is viewed from the outside, the likelihood of such an attack is high.

Therefore, in this scenario, the SQL Injection vulnerability should be considered a high-risk vulnerability.

The difference between a vulnerability and a cyber threat and the difference between a vulnerability and a risk are usually easy to understand. However, the difference between threat and risk can be more subtle. Understanding this difference in terminology allows for clearer communication between security teams and other parties and a better understanding of how threats affect risk. This, in turn, helps prevent and mitigate security breaches. Effective risk assessment and risk management, developing effective security solutions based on threat intelligence, and creating an effective security policy and cybersecurity strategy require a good understanding.

## SUMMARY

Professionals who develop safety standards should pay more attention to the harmonization of rules used in different fields. For example, using the approaches shown in the principles of complementarity. Also, don't forget to eliminate human error and organizational weaknesses. The implementation of risk management in enterprises helps to increase the level of security.

## LIST OF REFERENCES

1. Шубинский И.Б. Структурная надёжность информационных систем. Методы анализа /Ульяновск: Печатный двор, 2012.
2. BS 31100:2008. Risk management — Code of practice.
3. BS OHSAS 18001:2007. Occupational health and safety management systems. Requirements.
4. CWA 15793:2008. Laboratory biorisk management standard.
5. ISO/IEC 51:1999. Safety aspects — Guidelines for their inclusion in standards.
6. ISO/IEC Guide 73:2009. Risk management — Vocabulary — Guidelines for use in standards.
7. ISO 31000:2009. Risk management — Principles and guidelines.
8. IEC/ISO 31010:2009. Risk management — Risk assessment techniques.
9. ISO 15190:2003. Medical laboratories — Requirements for safety.
10. Reason J. Human error. — New York: Cambridge University Press, 1990. —316 p.