Incident Response Strategy in Cyber Security Space

[1] K.Priya, [2] S.P.V.N.D Suneetha
[1] Assistant Professor , [2]Assistant Professor
[1] Department of Computer Science
[1]P.B Siddhartha College of Arts and Science ,[2] P.B Siddhartha College of Arts and Science, Vijayawada, India
[1]pppriyamca@gmail.com, [2]suneethasampada@gmail.com

Abstract: The cyber security focuses on the issue regarding security of information shared within the decision-making processes concerning control activities and information protection, which represents a key factor in the cyberspace. One of the main principles, which are considered as the basis for network operations and information sharing under the conditions of environment digitalization for users, lies in security and protection of mutually interconnected networks. Information superiority on the one hand and meeting requirements for secrecy and security on the other hand will result in high demands on personnel and implementation of cyber security and protection measures. The way these virtual crimes cause real-life consequences is the main concern. This cyber security examines some of those threats and discusses the steps that could be taken to minimize the threats.

IndexTerms: Communications, information systems, Cyber security and protection, Information.

I. Introduction

The trusted mechanism that supports the above four principles must include highly reliable measures—cyber security—that can confirm, beyond reasonable doubt, the identity of users for the purpose of *authentication*, and that can attest the validity of the *authorization* parameters presented by a user. In addition to the above measures, the trusted mechanism must be able to provide *accountability* through an electronic audit trail. Such a trail should be able to attribute each and every activity taken place in the information system to an action caused by an identifiable person or by an automated process.[1]

Today, all communication and computation technologies have merged, creating a seamless medium where digitized data, text, sound, images, and video travel at electronic speeds from one end of the world to the other. Such activities implement functions and operations that cannot be realized in any other way. Cyberspace has engulfed all aspects of life, and each and every aspect of life has some direct or indirect dependence on it. Consequently, the uninterrupted, unobstructed, and secure availability of cyberspace constitutes a prerequisite to the efficient performance of practically all sectors of society.

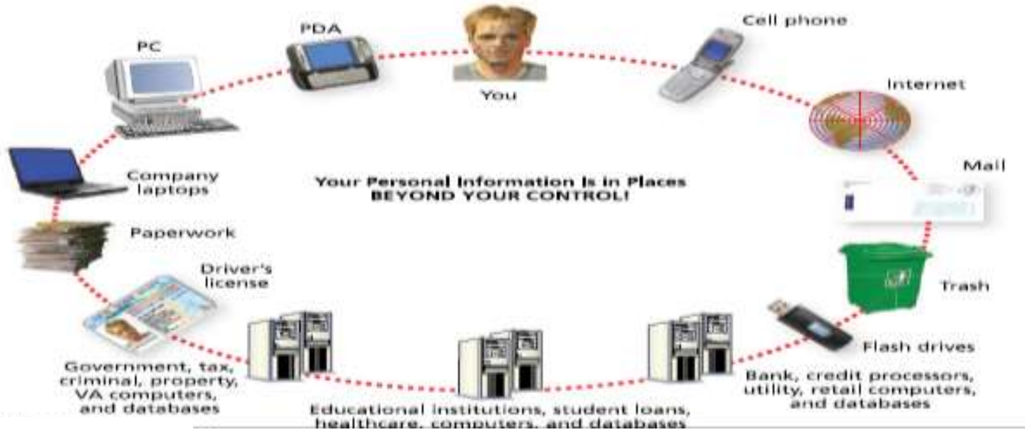
Cyberspace and cybersecurity are two wagons of a fast-moving train, and this book aims to help the reader pick up speed and hop on the train. Once on it and with the acquired background, the reader will be able to follow the technological advances and eventually contribute to making the train safer. Toward that end, the book has been arranged into ten cyber securities[2].

II. RELATED WORK

2.1 Vulnerabilities in Information Systems.

In this cyber security quantifying and measuring vulnerability are discussed, along with ways to avoid it through secure coding. Also, the Security Content Automation Protocol developed by the National Institute for Standards and Technology is reviewed, which is extensively used in measuring vulnerability in software systems.

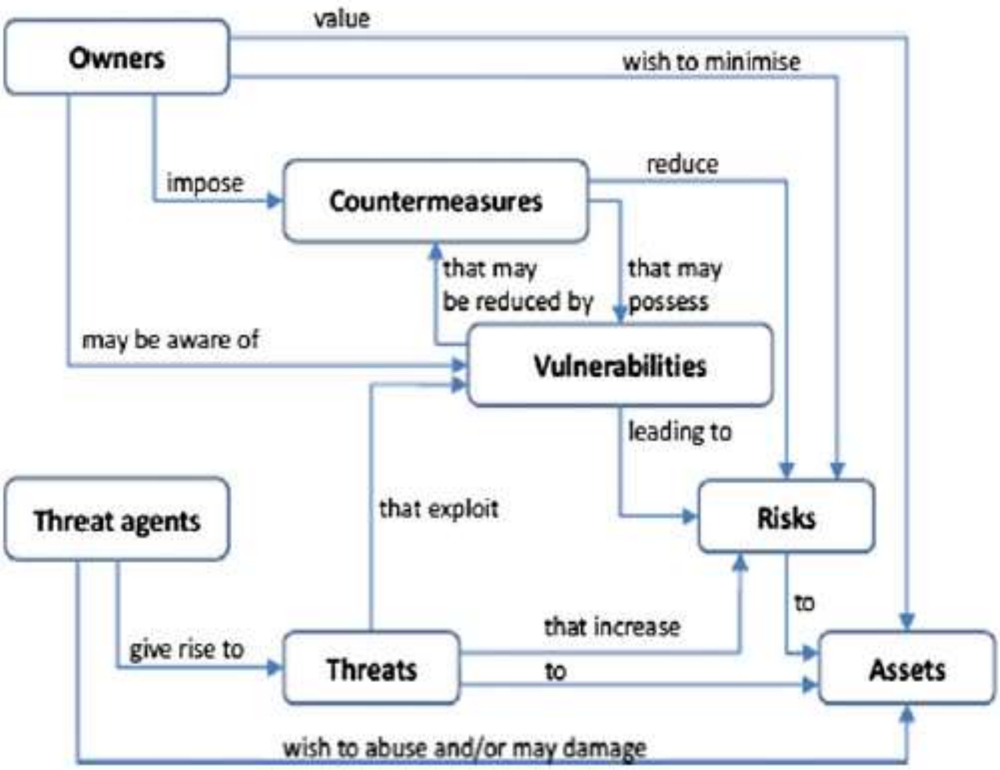
Figure 1: Distribution of Personal Information.


PC
PDA
You
Cell phone
Internet
Mail
Company laptops
Your Personal Information Is in Places BEYOND YOUR CONTROL!
Paperwork
Driver's license
Trash
Flash drives
Government, tax, criminal, property, VA computers, and databases
Educational institutions, student loans, healthcare, computers, and databases
Bank, credit processors, utility, retail computers, and databases

2.2 *Vulnerabilities in the Organization.*

Here, organization-related vulnerabilities are reviewed. They include access authorization and user authentication, as well as human factors in information security and ways to minimize risk [3]. Also covered are the wireless networks—Bluetooth, Wi-Fi, and Wi-MAX—and measures to increase their security. Cloud computing is examined, along with its advantages and disadvantages.

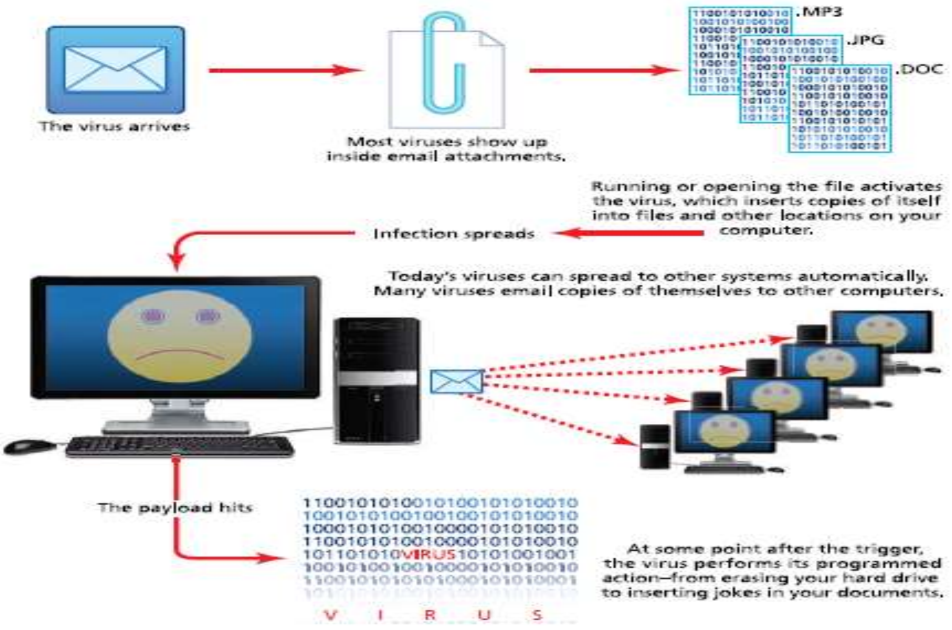
Figure 2: Interaction model for cyber vulnerabilities, cyber risks and cyber threats counter measures.



2.3 Risks in Information Systems Infrastructure.

Risk assessment is examined here are the risks inherent in the various information system components, namely, hardware, software, and people, as well as in cyberspace at large. Also reviewed are available cyberspace insurance programs and the offered coverage.

Figure 3: Likelihood of risk in cyber space.


.MP3
.JPG
.DOC
The virus arrives
Most viruses show up inside email attachments.
Running or opening the file activates the virus, which inserts copies of itself into files and other locations on your computer.
Infection spreads
Today's viruses can spread to other systems automatically. Many viruses email copies of themselves to other computers.
The payload hits
At some point after the trigger, the virus performs its programmed action—from erasing your hard drive to inserting jokes in your documents.
VIRUS
V I R U S

III. PROPOSED WORK

3.1 Measures to be followed to overcome from security threats in cyber space

3.1.1 Secure Information Systems: In this cybersecurity the need for an information security strategy is emphasized, pointing out asset identification as a cornerstone to such strategy. Also discussed are communication issues between assets and between users, focusing on email security[4]. The cybersecurity concludes with coverage of information security management, identifying and discussing the related issues.

3.1.2 Education & Experience: *Cybersecurity* needs to have to successfully address the cybersecurity challenges. Included are the personality characteristics, the needed education and experience, and the responsibilities that come with the position from a strategic planner.

3.1.3 *Building a Secure Organization*. Here, the prime concern is incident take place. Such an incident may not necessarily be a hostile intrusion, but possibly an act of nature. Also reviewed in this cybersecurity is the need for a flexible corporate policy on data security and Internet use, and the compliance requirements that are posed by the cognizant authorities.

3.1.4 *Cyberspace Intrusions*: In cyber security focusing on configurations, capabilities, selection, management, and deployment. Also covered are the application-based software versus the appliance based software, which now constitute the trend.

3.1.5 *Cyberspace Defense*: This cybersecurity focuses on the defense of the personal computer while in cyberspace against attacks and malware. Discussed are defense principles, techniques, and, most importantly, security tools. The tools reviewed include security analyzers, firewalls, antivirus software, file shredding, file encryption, and anti-loggers. Here, the emphasis is that file security is in the hands of the user, and files can be totally safe if proper defense measures are applied. [5]

Figure 4: Different layers in cyber security.

Cognitive Layer
Cyber Attack: Phishing, Online Behavior Tracking, Social Engineering.

Service Layer
Cyber Attack: Spoofing, Denial of Service, Advanced Persistent Attack.

Semantic Layer
Cyber Attack: Destroying Information, Theft of Information, Compromising Secure Information.

Syntactic Layer
Cyber Attack: Search Engine Poisoning, System Admin Assumption, SQL-Injection Attacks.

Physical Layer
Cyber Attack: Physical Theft/Loss/Damage, Lab Attack.

Cyberspace and the Law: Cyber space and law reviewed here are the various laws and legal initiatives aiming at providing a legal infrastructure for what transpires over the Internet may play in establishing an international cyber order that will address intellectual property and cybercrime issues.

Cyber Warfare and Homeland Security: This cyber security has three parts. The first is on cyber warfare, where cyber terrorism and cyber espionage are discussed, along with the hope of a possible cyber weapons treaty, a treaty that will curtail sovereign states from open cyber hostilities. [6] The second part is on the role in the country's cyber preparedness. The third part views the Internet as a cyber ecosystem where its defense has to be in a worldwide distributed for cyber training and its components. Each cybersecurity has carefully on cyber security-related issues.

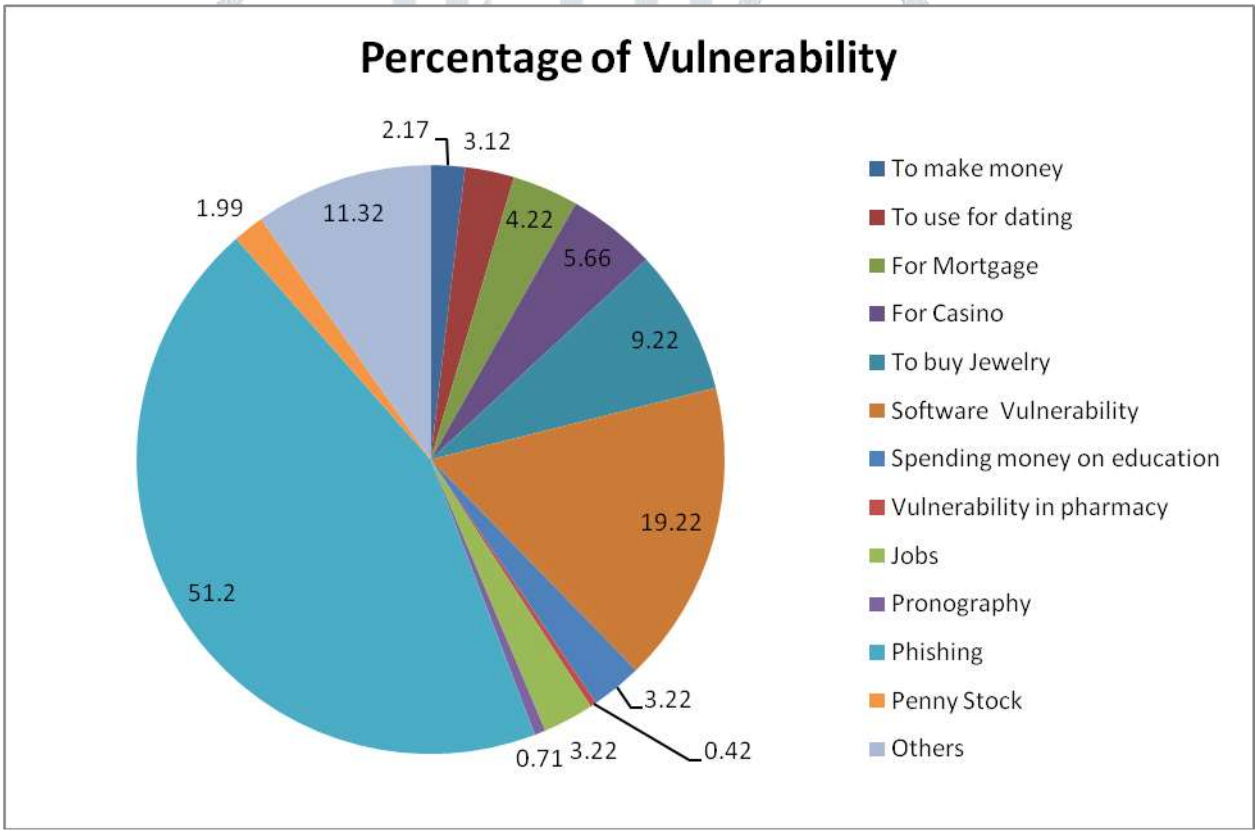
IV. RESULTS & ANALYSIS

After analysis 51.2 percentages of secure zone is achieved. The illustration is described below.

Table 1: Vulnerability in different areas before implementing cyber security measures.

Vulnerability in different areas	Percentage of Vulnerability
To make money	2.17
To use for dating	3.12
For Mortgage	4.22
For Casino	5.66
To buy Jewelry	9.22
Software Vulnerability	19.22
Spending money on education	3.22
Vulnerability in pharmacy	0.42
Jobs	3.22
Pronography	0.71
Phishing	51.2
Penny Stock	1.99
Others	11.32

Figure 5: Percentage of Vulnerability before implementing cyber security measures.

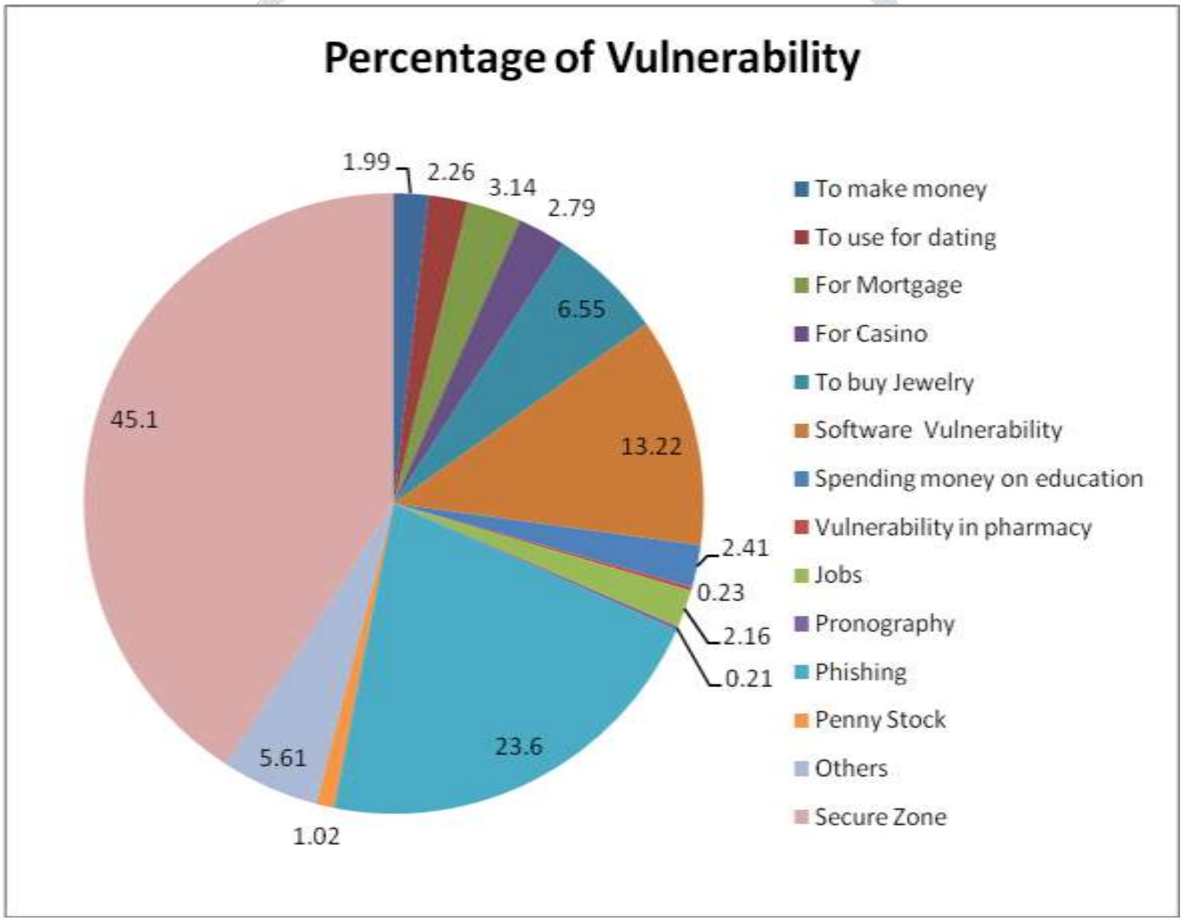


- ✓ Natural disasters (e.g. earthquake, tsunami, volcanic eruption, flood).
- ✓ Environmental disasters (e.g. nuclear fallout, oil spill, toxic chemical discharges).
- ✓ Widespread technical disruptions (especially those in ITC systems).
- ✓ Conventional warfare with kinetic weapon systems.

Table 1: Vulnerability in different areas after implementing cyber security measures.

Vulnerability in different areas	Percentage of Vulnerability
To make money	1.99
To use for dating	2.26
For Mortgage	3.14
For Casino	2.79
To buy Jewelry	6.55
Software Vulnerability	13.22
Spending money on education	2.41
Vulnerability in pharmacy	0.23
Jobs	2.16
Pronography	0.21
Phishing	23.6
Penny Stock	1.02
Others	5.61
Secure Zone	45.1

Figure 5: Percentage of Vulnerability before implementing cyber security measures.



I. Conclusion

This cybersecurity presented a system modeling approach for increasing understanding of those phenomena that may be important, when studying the cyber world for developing security in the society. The complex adaptive system theory was applied for understanding the nature of the cyber world and a social system model was introduced as a method to approach the cyber world. The cybersecurity showed how some of the emergent phenomena of the complex cyber world can be identified by using.

By exploiting weaknesses/vulnerabilities, threats may lead to a loss or takeover of assets. The threats to society's vital functions can be divided into three entities which are: physical threats, economic threats and cyber threats. These are concentrating these issues to reduce like

- ✓ Terrorist strikes with kinetic weapon systems, and
- ✓ Civil unrest (violence, sabotage).
- ✓ Economic threats include:
- ✓ Deep national depression.
- ✓ Deep global depression.

- ✓ Disruption in national or global financing markets, and
- ✓ Sudden global shortage of goods and services.
- ✓ Threats in cyberspace can be classified in many ways. The threat landscape is a list of threats containing information about threat agents and attack vectors. By exploiting weaknesses/vulnerabilities, threats may lead to a loss or takeover of assets.

II. REFERENCES

[1] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay, "DifferentTypes of Attacks on Integrated MANET-Internet Communication", *InternationalJournal of Computer Science and Security (IJCSS)* Volume (4): Issue (3), pp.265 –274,2010.

[2] Almotairi.S, Clark.A, Mohay.G and and J. Zimmermann, "Characterization ofAttackers' Activities in Honeypot Traffic Using Principal Component Analysis",*International Conference on Network and Parallel Computing, IEEE ComputerSociety*, pp.147- 154,2008.

[3] Animesh Patcha and Jung-Min Park, "A Game Theoretic Formulation forIntrusion Detection in Mobile Ad Hoc Networks" *International Journal ofNetwork Security*, Vol.2, No.2, PP.131–137, 2006.

[4] Chee-Wooi Ten, Chen-Ching Liu, and Govindarasu Manimaran, "VulnerabilityAssessment of Cybersecurity for SCADA Systems", *IEEE Transactions on PowerSystems*, Vol. 23, No. 4, pp 1836 – 1846, 2008.

[5] Chee-Wooi Ten, Manimaran.G and Chen-Ching Liu,"Cybersecurity for CriticalInfrastructures Attack Defense Modeling", *IEEE Transactions on systems,Man, and Cybernetics*—part a: Systems and Humans, vol. 40, no. 4, pp 853 – 865,2010.

[6] Cheung.S, "Modeling multistep cyber attacks for scenario recognition," in*Proceedings of the Third DARPA Information Survivability Conference andExposition*, vol. I, pp. 284-292, 2003.