Cyber Security Management

1Ayyanar.K  
Librarian, Research Scholar, Vinayaka Mission’s Kirupananda Variyar Engineering College, Salem, Tamilnadu, India  
Email: ayyanar46@gmail.com

2V.K.Krishnan  
Research Scholar, Associate Professor, Vinayaka Mission’s Kirupananda Variyar Engineering College, Salem, Tamilnadu, India  
Email: vvkrishnan_me@yahoo.com

3Subramanian.M  
Assistant Librarian Vinayaka Mission’s Kirupananda Variyar Engineering College, Salem, Tamilnadu, India  
Email: sankaimani@gmail.com

4Gomadhi.G,.M  
Student, Studying in Biomedical Engineering in Vinayaka Mission’s Kirupananda Variyar Engineering College, Salem, Tamilnadu, India  
Email: gomadhi5-4-2001@gmail.com

5Bharathi.S.S  
Student, Studying in Biotechnology Engineering, Vinayaka Mission’s Kirupananda Variyar Engineering College, Salem, Tamilnadu, India  
Email: bharathis0202200@gmail.com

Abstract: Cyber security is the most critical aspect nowadays of our technologically based lives. Information Technologies in their day to day operations everything that uses technologically are based on Communication and Information Systems. It means that it depends on cybersecurity. The public and private sector every year spend huge amount for technogies, security software and hardware devices that will increase the cyber security inside their companies, but they are still exposed. The main problem of this situation is that cyber security is still usually treated as a technical aspect technologically which can be easily implemented.

The main Objectives of this article is to provide theoretical aspects of the cyber security management to ensure security of infrastructure in an Organizations or all Government Departments, and Private sector.

Keyword: Cyber Security, Cyber Management Cyber Laws Security

I. INTRODUCTION

We are interconnected in our world, cyber security management has become the most important thing that influence every part of our life. Every country has several cyber security and want to secure that their Systems like Voting Systems Banking System Educational Systems, Military Systems and Industrial and Private Systems to Operates and Function Carefully Manage and protect their Critical Resources. The main efforts should provide security to solve when problems arise. Researchers have attempted to give for an effective Cyber Security. Cyber treats are particularly difficult to predict, think likely take timely preventive measures, so the risk that cyber attacks will be successfully implemented. It is increasing, Cyber attacks was executed through nasty software pirating fraud, money laundering, cracking pornography a rapid growth of internet has come, adoption of the internet computer crimes.

II. NEED FOR STUDY

Information Security includes Computer Security, plus all the other things. We use to do Business, Procedures, Data, Network, our Staff and Computers

III. OBJECTIVES OF THE STUDY

Demonstrate that organizations have business need for information security explain why a successful information security program is the responsibility of both organizations general management and it management. Identity the treats posed to information security and the more common attacks associated with those treats, and differtiate threats to the information within systems Describes the issue facing software develops as well as the most common errors made by developers and explain how software development program can created software that is more secure and reliable. Models which are can be used to ensure security of critical infrastructure in an Organization or Company. New Threats
Cyber-attacks on critical sectors usually have a big influence to the Government and Private sector. Government institutions, Banking sectors, Public and Private services, Nuclear Power Plants, Power Grid Operators, Water Suppliers or Waste Water Treatment Companies use Information Technologies in their day-to-day operations. Everything that uses technologies are based on communication and information systems and that means that it depends on cyber security, software and hardware devices that will increase the cyber security inside their companies, but they are still vulnerable.

The main problem of this situation is that cyber security is still usually treated as a technical aspect or technology which can be easily implemented inside the organization and this implementation will guarantee cyber security. This article presents the classification of the critical infrastructure attacks, analyzes attack vectors and attack methods used to damage critical infrastructure as well as the most common cyber security mistakes which organizations make in the cyber security field when trying to make themselves safer from vulnerabilities. Identify Four domains of cyber vulnerabilities (each domain has its own attack vectors that are used by cyber criminals to achieve their goals):

- IT Domain.
- ICS Domain.
- Communications Domain.

IV. CATEGORY OF TREATS

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Category Threats</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Compromises to Intellectual Property</td>
<td>Piracy, Copyright Infringement</td>
</tr>
<tr>
<td>2</td>
<td>Software Attacks</td>
<td>Viruses, Worms, Denial of Service</td>
</tr>
<tr>
<td>3</td>
<td>Deviation in Quality of Service</td>
<td>Isp, Power, WAN Service issues from service providers</td>
</tr>
<tr>
<td>4</td>
<td>Espionage or Trespass</td>
<td>Unauthorized access, or Data Collection</td>
</tr>
<tr>
<td>5</td>
<td>Forces of Nature</td>
<td>Fire, Floods, earthquake, lighting</td>
</tr>
<tr>
<td>6</td>
<td>Human Error or failure</td>
<td>Accidents, Employee Mistake</td>
</tr>
<tr>
<td>8</td>
<td>Missing inadequate or Incomplete</td>
<td>Loss of access of information due to Disk drive Failure without proper backup and Recovery plan</td>
</tr>
<tr>
<td>9</td>
<td>Missing inadequate or incomplete</td>
<td>Network Compromised because no firewall security controls</td>
</tr>
<tr>
<td>10</td>
<td>Vandalism or Sabotage</td>
<td>Destruction of Systems or Information</td>
</tr>
<tr>
<td>11</td>
<td>Theft</td>
<td>Illegal Confiscation of Equipment or Information</td>
</tr>
<tr>
<td>12</td>
<td>Technical hardware failure</td>
<td>Equipment of Failure</td>
</tr>
<tr>
<td>13</td>
<td>Technical software failure</td>
<td>Bugs, Code Problems Unknown Ill loopholes</td>
</tr>
<tr>
<td>14</td>
<td>Technological Obsolescence</td>
<td>Out Dated Technologies</td>
</tr>
</tbody>
</table>

Modification. Denial-of-service (DoS) when access to the system is denied for authorized users. Disclosure of information when critical information is disclosed to unauthorized persons or systems. Theft of resources – when system resources are used by unauthorized entities. Physical destruction when physical harm or destruction is achieved through the use of ICS.

V. CYBER SECURITY LAW

We need of the legislative and regulations that affected the Defines cyber security as a set of legal, information dissemination, organizational and technical measures which are needed to be taken to prevent, detect, analyze and respond to cyber incidents, which are described as the event or activity that causes or may cause or allow: unauthorized access to communication and information systems (CIS), electronic communications networks or industrial process control systems; can disrupt or change information systems, including the management takeover; electronic communications networks or industrial process control operations to destroy, damage, delete or modify electronic information, withdraw or restrict access to electronic information, as well as enable to absorb or otherwise use non-public information in electronic format by unauthorized persons. Laws are formally adopted rules for acceptable behavior in modern society. Ethics are socially acceptable behavior. The Key difference between law and ethics is that laws carry the authority of the governing body and ethic do not. The organization formalizes desired behavior in documents called Policies. Policies must be read and agreed to before binding. Civil Law companies a wide variety of law that are used to govern a nation or state. Criminal law addresses violates that large society and enforced by agent of the state or nation. Private law focuses on individual relation ship, and public law governs regulatory agencies.
VI. CONCLUSION

- Information Security has been described as both an art and a science, and also comprises many aspects of social science.
- Each organization has a culture in which communities of interest united by similar values and share communities values the three communities in information in information security.
- There are a number of types of security, Physical security, personal security, national security, and network security.
- Information securities are protection of information assets that the store, transmit information from through the applications of Policy, Education and Technology.
- Information are made up of six components Hardware, Software, Date, People, Procedures and Networks.

REFERENCES