Cyber Security Issues and Incident Prevention

Dr. G.N.K. Suresh Babu[1] & Dr. P. Pushpa[2]
[1]Professor – CSE, Prince Dr. K. Vasudevan College of Engineering and Technology, Chennai – 600127. gnksureshbabu@gmail.com
[2]Lecturer, East China University of Technology, Nanchang, P.R. China. ayurpushpa@gmail.com

Abstract–*Now a days, cybersecurity is a buzz term for almost all the organisations. Everywhere people are discussing about the cyber security. Cybersecurity threat is more for common man also. Every one is affecting cyber crimes and other incidents. How do we prevent ourself from cyber security incidents? This article describes about prevention of cyber security threats. A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber attacks include threats like computer viruses, data breaches, and Denial of Service (DoS) attacks.During the last decades, there has been a steep rise in cyber Security incidents in the last few years in various Organizations through infection by malwares, hacking of websites and theft of Information. Security of Cyber Space of all entities in Defense is very critical since we deal with strategic information pertaining to Defense procurements, invent and developmental projects. In the wake of ever-rising threats and vulnerabilities, Security has raised a Cyber Security cluster to address the needs of all organizations of Department of Defense Investigation. In Defense department too, we have established a Sectoral Cyber Security Cell. The group mandated to organize implementation of positive measures to reduce risk of cyber security incidents by means of Policy enforcement, Advisories and Training. The main goal of this explore is to lay down cyber security policy for establishing, implementing, monitoring, review and Executive of information infrastructure in the Defense organization.*

Keywords: –Cyber Security, IT, cloud computing, mobile computing, social media, DDI and ICT.

1. Introduction

The Rapid propagation of information technology and its direct impact on the functioning of an organization, IT and its functional ecosystems no longer viewed in isolation. Propagation of Information Technology has its rear to that of induced vulnerability to danger of cyber crimes. Hence, it has become organizationally imperative to safeguard the official cyber space from immoral cyber crimes keeping the overall threat in perspective On July 2, 2013; the Indian government has released the National Cyber Security Policy 2014 [2]. The Cyber Security strategyaspire at protection of in sequence infrastructure in cyberspace, decrease vulnerabilities, construct capabilities to avoid and act in response to cyber threats and reduceharm from cyber incidents through aamalgamation of institutional structures, public, process, knowledge and teamwork. The intention of this policy in wide terms is to make a secure cyberspace ecosystem and make stronger the regulatory framework at the National level in general and at the Department of Defenseinvention in particular. The growth of the policy was encouraged by a different diversity of factors, including the expansion of India's information technology production, an increasing number of cyber attacks and the country's ambitious plans for rapid social transformation. The nationwiderule sets onward fourteen diverse objectives that range from enhancing the protection of India's dangerous infrastructure, to supplementary the investigation and trial of cyber crime, to developing 600000 skilled cyber security professionals over the next few years.

*Corresponding Author :Dr.G.N.K.Suresh Babu, gnksureshbabu@gmail.com

2. Objectives

To attain these objectives thepolicy details numerous action items for the Indian government including:

a. To design a national agency to coordinate all cyber security matters.
b. Encourage all private and public organizations to designate a Chief Information Security Officer responsible for cyber security [4].
c. To expand the dynamic legal framework to address cyber security challenges in the area of cloud computing, mobile computing and Social media.
d. To Operating a National Critical Information Infrastructure protraction Centre Promoting research and development in cyber security.
e. Fostering education and training programs in cyber security.
f. To establish public and private partnerships to determine the best practices in cyber security rule.

2.1 Objectives of this rule

a. Assure the guarantee availability for networks and information systems.
b. Avoid loss, modification or misuse of information.
c. Plan and implement new Information Technology Project.
d. Stop unauthorized access, damage and interference to information infrastructure.
e. Give directions and support for Information Assurance and Risk Executive (RE) inorganization.
f. Lay down guidelines for incident response within the Organization.
g. Develop information systems and communications assignment.

2.2 Survival Analysis

This rules based on National Cyber Security Policy of Government of India as notified on 02 July 2013, security guidelines and best code of practices as given in International Standard ISO/IEC 27001 and ISO/IEC 17799 and Information Technology Security Guidelines given by Department of IT, Ministry of Communications & IT, and Government of India.The rule evaluated on swapping of threat occurrence of a major confidential incident [5]. Due to frequent evaluation in information Technology and swapping, a threat situation a cyber security group developed under the auspices of DDI will be responsible for establishment and periodically reviewing cyber security in the department of Defense Investigation including this policy after few years.

2.3 The key considerations for securing the cyber space

The security of cyber space is not an elective issue but avery importantrequire in vision of its impact on national security, public safety and economic well being, refer the Figure1.

a. The issue of cyber security needs to move beyond traditional technological measures such as anti-virus and firewalls. It wants to be lively in nature and have essential depth to detect, stop and prevent attacks.
b. The Cyber security intelligence shapes an integral component of security of cyber space in order to be able to anticipate attacks, adopt suitable counter measures and attribute the attacks for possible counter action.
c. Effective correlation of information from multiple sources and real-time monitoring of assets that need protection and at theparallel time ensuring that adequate expertise and process are in place to deal with disaster situations.
d. There is a need to focus on having a suitable security posture and adopt counter measures on the basis of hierarchy of priority and understanding of the inter dependencies, rather than attempting to defend against all intrusions and attacks.
e. Security is all about what people, process and technology should do and as such there is a clear need for focusing on people and processes while attempting to use the most excellent available technological answers, which otherwise could prove unproductive.
f. Use of adequately trained with suitable incentives for effective results in a highly specialized field of cyber security.
g. Protection needs to buildin from the conceptual plan stage itself when it comes to developing and deploying critical information infrastructure as opposite to have security as an afterthought.

2.4 Information and Communication Technologies

The ICT follow open system architectures and standard protocols are public domain knowledge. Consequently, networks and systems are vulnerable to interception, compromise and denial of information unless secured by appropriately planned security measures. The formulation of wide-ranging cyber security rule covering people, processes and technology issues is the opening point in establishing Information Security Executive System in Quality Assurance [5]. The cyber security procedures and guidelines will emerge from this policy and will form the other important documents for implementing cyber security within all entities of Quality Assurance. The present IT environment in Quality Assurance has both networked and stand-alone systems. Though the networks are isolated from the Internet due to air gap maintained, the unsupervised use of removable storage media could plug this vital space and make our networks susceptible to threats that exist on Internet. A major reason for loss or theft of classified information in any organization is due to the misuse of removable storage media. As the protection controls for Executive of removable storage space media is more technical oriented rather than technology, it will be the command responsibility to make sure proper accounting and make use of such devices. Security of information is supreme for any computer network. In adding up to the Confidentiality, Integrity and Availability of information, Authentication and Non Repudiation form other important key security features of such networks. To uphold the confidentiality of information, encryption plays an important role in storage space and transmission of information. The implementation of cyber security based on the directing principles, that the Head of Establishment will be the owner of the information for the establishment. To product information assets, the owner will be the responsible for assigning the security classification of all the information assets and appropriate clearance level for the staff accessing these assets. The strategy is applicable to all end users of information capital as well as personnel tasked to undertake the administration of information systems and resources. All Directorates, Controller and under Quality Assurance, will stick to the guidelines given in this policy.

3 Proposed Approach: Cyber disaster and Incident Prevention

All Functionaries of Information Security Organization will acquaint themselves with "Disaster Executive Plan for Countering Cyber Attacks and Cyber Terrorism issued in, by Ministry of Communication & Information Technology, Government of India" January 2009 so as to facilitate its implementation in Quality Assurance [6]. Implementation of any other directions received from Department of Defense Invention from time to time will be the responsibility of CISO, Quality Assurance.

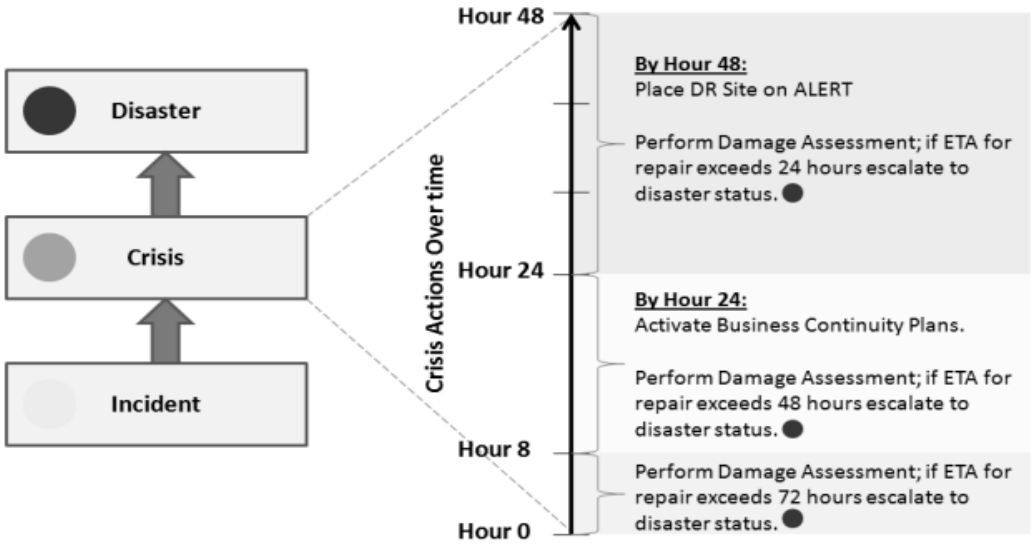

Figure 1: Crisis Level Action 0 to 48 Hrs

3.1.The types of Cyber Crises:

(i) Scanning/Probing of Networks.
(ii) Defacement of Website
(iii) Malicious Code Attacks
(iv) Large Scale SPAM
(v) Identity theft
(vi) Phishing
(vii) Social Engineering
(viii) Denial of Service
(ix) DNS Attacks
(x) Application Level Attacks
(xi) Infrastructure Attacks
(xii) Compound Attacks
(xiii) Router Level Attacks.

3.2 Incident Prevention

(i) Prepare Information Security Policy suited to own needs.
(ii) Implement Information Security Executive System (ISMS) as per ISO 27001.
(iii) Practice Information Security Executive in line with ISO 17799.

(iv) Define business continuity plan to counteract interruptions.
(v) Organize Security Training & Awareness Drive.

3.3Crisis Executive Organization

In the context of Quality Assurance, incident reporting will be to the Control Room established by DDI, which in turn reports to Crises Executive Group. The highest entity in the setup for Crises Executive for countering Cyber Attacks & Cyber Terrorism is the National Crises Executive Committee headed by the Cabinet Secretary, Government of India. Information flow between various entities shown in the following Figure 2:-

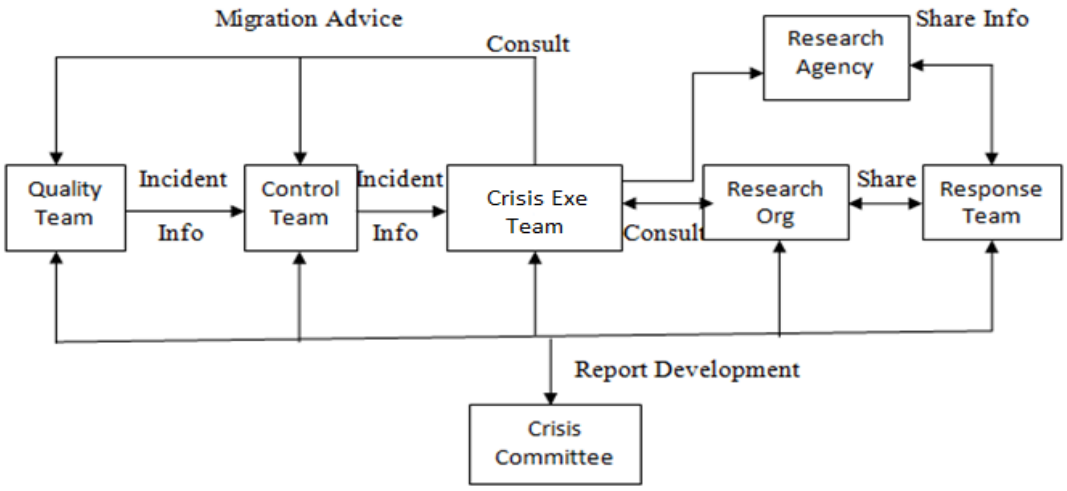

Figure 2: Crisis executive Organization

4 Network Security Executive Controls

Networks will be sufficientlymanaged and controlled, in order to protected from threats and to maintain security for the systems and applications using the network, including information in shipment by integrated appropriate protection solutions at Transport, Network, Physical and Application layers.

4.1 Physical Layer Security

On the Physicallayer,mass media confidentiality devices approved by SAG will used on the entire kind of communication media including Satellite etc.

4.2 IP version 6

IPv6 is a latest version of the Internet Protocol, intended as anheir to the present IP version 4. IPv6 will not only resolve the difficulty for address space lack but also present efficient Executive of address space, enhanced security support and elimination of network address translation. All network devices procured for organizations under Quality Assurance will incorporate IPv6 protocol suite for ease in migration to IPv6 in a phased manner. Adequate bandwidth will be constructing up to provide to the requirements of tone of voice, data and video conferencing. The Networked computers will have only system Printers and

Scanners and will notlinked to personal printers and scanners. Depending on the sensitivity of the data handled, the printer or scanner will be communal among a defined close user collection. Separate printers and scanners are necessary in case of non-networkedsurroundings chosen Network Administrator of the establishment will suitably monitor it. In addition, networked computers will not have writing devices like CD or DVD writers, floppies etc. Every single onecomputer will have their floppy drives, CD or DVD writers removed and USB ports put out of action. If required, only one computer per branch or group and sub group will be enabled with these devices will be under the direct charge of the nominated officer of the establishment. A record of all writing information transferred onto removable media.

5 Cryptographic Controls

5.1 Information Classification

Information in electronic form will classified as per Classification and Handling of Classified Documents (CHCD)-2001.

5.2 Classified System Isolation

Systems handling or processing classified information with safetycategorization of Confidential and above will containdedicated and isolated computing surroundings. Every part of systems will house in a secure area with stringent physical access control machinery in place.

5.3 Secure Transfer of Classified Information

The information proprietors will guarantee that the security classification of the information required to-transfer over a network must commensurate with the security classification of the network or media. For secure exchange of classified information with classification commensurate with or lower than that of the media, following additional cryptographic measures will be incorporated by the owners of such information.

5.4 Network/ Transport Layer Security

The Applications developed will include mechanisms to secure classified information through Network or Transport Layer Virtual Private Network (VPN) implementations such as IPSec/ Secure Socket layer (SSL) or Transport Layer Security (TLS) between the Info Processing Nodes.

6. Performance Evaluation

The performance of proposed approach canevaluated by Comparing with the previous year is using the Cryptographic rule.Our proposed scheme is tested and it shows good performance results shown in the Table 1:-

S.No	*Year*	*Rate in Millions*
1	2013	165.01
2	2014	204.96

3	2015	457.93
4	2016	500.40
5	2017	702.06
6	2018	812.67
7	2019	906.18
8	2020	1100.08

Table 1: Total Cyber Incident Prevention Rate (In Millions)

The results validated by calculating the deviation of the results obtained through the proposed method and the real results obtained from the crisis executive plan for countering cyber disastersystem. The calculation shown in the table 1 and the graphical representation of data rate in the chart Figure 3.

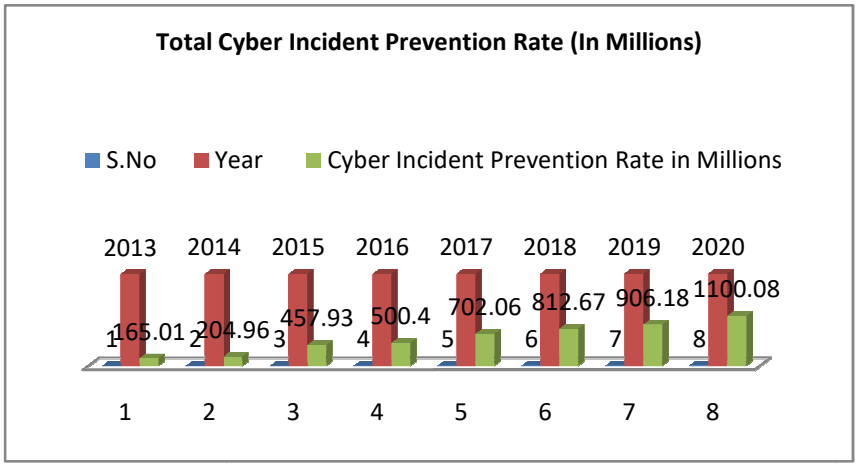

Figure 3: Total Cyber Incident Prevention Rate (In Millions)

7 Conclusion

The Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a trusted system as recognized in classified government classification. Information has been asignificant part of some organization. With ever-rising dependence on Information and Communication Technologies for conduct of warfare and the up-and-coming threats in cyberspace, security of information in storage, processing and communication is the greatest challenge. However, adoption of secure technologies, with proper configuration and use of encryption technologies along with procedural control will build deployment of networks and information systems for conduct of network centric operations a certainty at Department of DefenseInvention (DDI).The results presented in this work establish the correctness and effectiveness of the derived principles and proposed enhancement of Cyber security system. Hence, the charity of this paper over the prior related works is incremental.

REFERENCES

[1] Crystal M. Shipman, K. M. (15 September 2014). Con-Resistant Trust for Improved Reliability in a Smart-Grid Special Protection System, IEEE Transactions on Power Delivery (Volume: 30, Issue: 1), (pp. 455 - 462).

[2]Bert-Jaap Koops, Morag Goodwin, Cyberspace, the Cloud, and Cross-Border Criminal Investigation, The Limits and Possibilities of International Law, Tilburg Institute for Law, Technology, and Society CTLD – Center for Tran boundary Legal Development, December 2014.

[3] Mark Graham, Cloud Collaboration: Peer-Production and the Engineering of the internet, Chapter: Engineering Earth, Page 67-83, and December 2010.

[4]Information security Executive systems Requirements – ISO 27001:2013.

[5] Code of practice for information security Executive – ISO 27002:201 .

[6]Information security Executive system implementation guidance – ISO 27003:2010.

[7] Security risk assessment – ISO 27005:2011.

[8] Business continuity Executive strategy – ISO 22301:2012.

[9] Contingency planning guide for IT systems – NIST SP 800-34.

[10] ICT Disaster recovery services – ISO 24762:2008.

[11]Information Security incident Executive – ISO/IEC 27035:2011.

[12] CIS 20 most important security controls and metrics for effective cyber security and continuous security policy compliance (Prioritizing security baselines).