REVIEW OF RESEARCH
IMPACT FACTOR : 5.7631(UIF) UGC APPROVED JOURNAL NO. 48514 ISSN: 2249-894X
VOLUME - 8 | ISSUE - 7 | APRIL - 2019

A SYSTEMATIC REVIEW ON CYBER SECURITY THREAT AND MANAGEMENT

Amit Kumar Yadav[1] and Priyanka Rajbhar[2]
[1]Asst. Prof. St. Aloysius' College (Auto.) Jabalpur.
[2]Student, M.Sc. (Computer Science) IV Semester
St. Aloysius' College (Auto) Jabalpur.

ABSTRACT :

The development of information technology or cyber infrastructure had growth which is very fast in production a wide range of computer products cause some medium sized organization are confused and ambiguous as to what should be done or the IT infrastructure. He cyber security play important role ensure that the IT components or infrastructures execute well along the organizations business successful. The paper will present a study of cyber security threat and management model to guideline the security maintenance on existing cyber infrastructures. In order to perform security model for the currently existing cyber infrastructures the implemented cyber security maintenance within security management model in a prototype and evaluation it for practical and theoretical scenarios.

KEYWORDS : *Cyber, Cyber Security, Cyber Threats Security–Dependability, Systems-Crime Protection Cyber Safety-e-commerce.*

CYBER SECURITY INTRODUCTION

- Cyber space is such a term which is not yet completely defined and also has no geographical limitation.
- It is a term associates with application of the internet world wide.
- It is a term called as a virtual space as a physical existence of cyber space is not detectable at all.
- Cyber space is "the total interconnectedness of human beings through computers and telecommunication without regard to physical geography.
- A set of activities and other measures intended to protect from attack , related hardware and devices software and the information they contain and communication, including software and data , as well as other elements of cyber space.
- The state or quality of being protected from such threats.
- The broad field of endeavor aimed at implementing and improving those activities and quality.

Cyber Security – Threats

- The cyber security threats emanate from a wide variety of sources.
- Their effects carry signification risk for public safely, security of nation and stability of the globally linked economy as a whole.
- Cyber security threats pose are of the most serious economic and national security challenges.

There are Mainly Two Types of Cyber Threat

Cyber Crime

- It can be against individuals, corporate, and institutes.

Cyber Warfare

- It can be against state.

Types of Security Threats

- Hacking
- Phishing
- Child pornography
- Cyber stalking

Malware

- Malware, short for malicious S/W, defined as a software designed to perform as unwanted illegal act via the computer network.
- It could be also defined as S/W with malicious intent.
- Malware can be classified based on how they get executed, how they spread And /or what they do.
- Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive S/W including computer viruses, worms, Trojan horses, ransomware, spywares adware and other malicious program.

Malware Types

- Virus
- Worms
- Trojans
- Spy ware
- Ransomware

Virus

- A virus is a program that can infect other program by modifying them to include a possible evolved copy of itself.
- A virus can spread throughout a computer or network using the authorized of every user using it to infect their program.

Worms

- Worms are also disseminated through computer network , unlike viruses, computer worms are malicious programs that copy themselves from system to system, rather them infiltrating legitimate files.

Trojans

- Trojans is another form of malware, Trojans do things other than what is expected by the user.
- Trojan or Trojan horse is a program that general impairs the security a systems.
- Trojan are used to create backdoors (a program that allows outside access into a secure network) on computer belonging to a security network so that a hacker network.
- Unlike computer viruses and worms, Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.

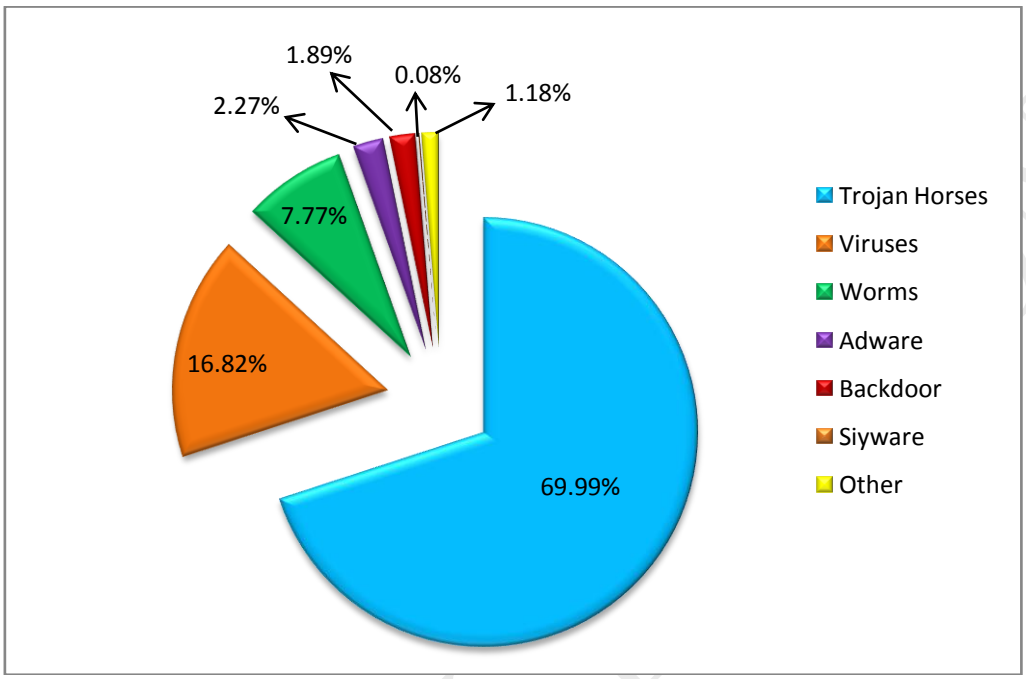
Spyware

- Spyware invades a computer and as its name implies, monitors a user's activities without consent.

- Spyware are usually forwarded through unsuspecting e-mails with confide e-mail ids.

Ransomware

- A type of malicious S/W designed to block access to a computer system until a sun of money is paid.



MALWARE BY CATEGORIES

How can a malware disrupt the computer or network

- It can attack on banking transaction, can acquire the debit/ credit card info. Can do economic frauds and destabilize the whole economy.
- It can after a data or destruct the data by spreading pornography fake identity, virtual impersonation.
- It can misuse the social media for fanning intolerance, communal tensions, outrange modesty of women, can humiliate girls and harm their reputation.
- Hence, cyber crime/attack can harms all the spheres of human life and dignity.
- It can be called as a major threat to humanity.

Current Scenario - India

- In case of India it is major challenge for governments as it involves various ministries and departments.
- Now a days India is going to acquire its digital aspirations through Jam trainty and also spreding digitally in various levels and fields such as digital lockers, digital certificate, digital payments from banks to railway tickets.
- Hence, India speading digitally within.
- In banking sector thoughts like phishing denial or cards, credit card frauds causes thousands and lakhs of money every day which causes huge financial risk and effects India economy.
- RBI aim of cash less transactions will be delayed and this goal can't be reached it such attacks keep repeating.
- Recent decision for demonetisation is a major step towards less cash to cash less.
- Through less cash we are heading towards digital payments where data is going to be feed for far.
- This should have a major shield as threat is going to be major.

- Latest deasion of gst tax system also required a network and digital system though which going to work.
- All industries, institution, companies have to develop an invoice which will contain all its transactions.
- Thus there is a major need to protect the data of such a big market entities who contributes majorly to GDP.

Concerns

- Frequent data brunches.
- Institutional economic and social neglect.
- Appointment of national cyber security staffed.
- Private sector failure.

Government Efforts

- India has already launched-e-sorveillance projects like national intelligence grid (NATGRID), Internet monitoring system (CMS), Internet spy system network and traffic analysis system (NETRA) of India, etc.
- Pradhan Mantri Gramin Digital Saksharta Abhiyan.
- National Crisis Management plan for Countering cyber attacks and cyber terrorism has been prepared and is being update annually.
- Information technology (Amendment) Act. 2008 has been enacted to cater to the need of national cyber security.
- Indian computer emergency response team (CERT-in) has been operational as a national agency for cyber security incident response.
- Growth and application of digital signature certificates in a member of areas.
- Security auditors have been empanelled for conducting security audits.
- R&D activities have been supported through premier academic and R&D institutions.
- Nation – wide information security education and awareness programme have been in progress to create necessary cyber security awareness.
- Government has set up three cyber – f over & ic laboratories in Banglore, Pune and Kolkata.

National Cyber Security Policy, 2013

- To build secure and resilient cyber space.
- Creating a secure cyber ecosystem generate trust in IT transaction.
- 24x7 National Critical information infrastructure protection center (NCI IPC).
- Indigenous technological solutions.
- Testing of ICT products and certifying then.

National Cyber Crime Policy

- It is under the ministry of communication and information technology department of electronics and information technology.
- Aim is to secure and resilient cyber space for citizens, business and governments.

Mission of the policy

1. Protect information and information infrastructure in cyber space.
2. Build capabilities to prevent and respond to cyber threat.
3. Reduce vulnerabilities.
4. Minimize the Damage from cyber incidents.

The cyber regulations appellate tribunal

- The cyber regulations appellate tribunal has power to entertain the case of any person aggrieved by order made by the controller of certifying authority or the adjudicating officer.
- It has been established by the central government in accordance with the provisions controlled under section 48(1) of the information technology act. 2000.
- The body is quasi judicial in nature.

From Recent Editorials

- छुनिया भर में पिछले कुछ सालों के दौरान साइबर हमले में वृद्धि हुई है। इसकी एक बड़ी वजह आभासी मुद्रा बिटकवाइन को माना जा रहा है।
- इसका इस्तेमाल कालाधन, हवाला और आतंकी गतिविधियों में ज्यादा हो रहा है।
- भारत समेत ज्यादातर दे"ाों में इसे कानूनी तौर पर वैधता नही दी है।
- संभवट : यही एक बड़ी वजह है कि रैनसनवेयर जैसे साइबर अटैक की चपेट में भारत जैसे दे"ा कम आ रहे है और जहॉ इसे वैधता मिली हुई है। वहॉ ज्यादा हमले हो रहे है।
- वर्ष 2016 में पूरी दुनिया में रोजाना Ramsoware के 4000 से भी अधिक अटैक हुए है।
- वही 2015 में Ramsoware के करीब 1000 मामले समाने आये है।
- Cyber Crime से Last year कारोबारी जगह को 30 खरब डॉलर का नुकसान झेलना पड़ा।
- सरकार ने पिछले साइबर हमले के बाद एक उच्चस्तरीय समिति गठित की थी।
- समिति को बिटकवाइन को प्रतिबंधित, नियंत्रित या स्वनियमित करने पर राय देने को कहा था।
- कंपनी मामलों का मंत्रालय उन कंपनियों पर कड़ी नजर रखे हुए है जो लेन देन में बिटकवाइन जैसी आभासी मुद्रा का इस्तेमाल करती है।
- वि"ोषज्ञों का कहना है कि Ramsoware जैसा कोई Cyber attacks भारत में हुआ तो बचाव करना बेहद मु"किल होगा।
- इसकी वजह यह है कि यहॉ ज्यातर सर्वर सुरक्षित नहीं है।
- संतोष की बात यह है कि ब्रिटेन, अमेरिका और यूरोपीय दे"ाो की तरह भारत में अभी पूरी व्यवस्था कम्प्यूटरीकृत नहीं है।

Solution

- Integration of agencies involved in the area of cyber security.
- Creating centres of excellence for research in area of advanced security.
- Establishing security information sharing and analysis centres (ISACS).
- Establishing sartorial CERTs.
- Strengthening National cyber alert system for rapid identification and response to security incidents and information exchange.
- Setting up cyber security Help Desks at regional levels for general users.
- Establishing cyber security training labs/facilities across the country.
- Setting up of think tanks in public – private mode to identify graps in the existing policy and framework and take action to address them.
- Lunching formal security education, skill building and awareness programmes.

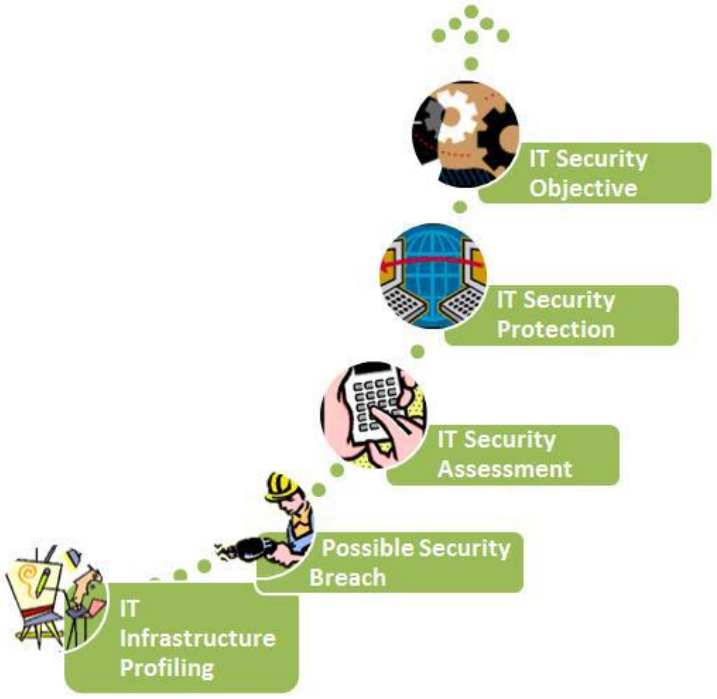
NECESSITY OF CYBER SECURITY

Information is the most valuable asset with respect to an individual, cooperate sector, state and country. With respect to an individual the concerned areas are:

1) Protecting unauthorized access, disclosure, modification of the resources of the system.
2) Security during on-line transactions regarding shopping, banking, railway reservations and share markets.
3) Security of accounts while using social-networking sites against hijacking.
4) One key to improved cyber security is a better understanding of the threat and of the vectors used by the attacker to circumvent cyber defences.
5) Need of separate unit handling security of the organization.

6) Different organizations or missions attract different types of adversaries, with different goals, and thus need different levels of preparedness.
7) In identifying the nature of the cyber threat an organization or mission faces, the interplay of an adversary's capabilities, intentions and targeting activities must be considered With respect to state and country.
8) Securing the information containing various essential surveys and their reports.
9) Securing the data basis maintaining the details of all the rights of the organizations at state level.

Proposed cyber security maintenance model



Security training and awareness

Security Training and Awareness The human factor is the weakest link in any information security program. Communicating the importance of information security and promoting safe computing are key in securing a company against cyber crime. Below are a few best practices:

1. Use a —passphrase‖ that is easy to remember — E@tUrVegg1e$ (Eat your veggies) and make sure to use a combination of upper and lower case letters, numbers, and symbols to make it less susceptible to brute force attacks. Try not to use simple dictionary words as they are subject to dictionary attacks – a type of brute force attack.
2. Do not share or write down any —passphrases.‖
3. Communicate/educate your employees and executives on the latest cyber security threats and what they can do to help protect critical information assets.
4. Do not click on links or attachments in e-mail from untrusted sources.
5. Do not send sensitive business files to personal email addresses.
6. Have suspicious/malicious activity reported to security personnel immediately. Secure all mobile devices when traveling, and report lost or stolen items to the technical support for remote kill/deactivation.
7. Educate employees about phishing attacks and how to report fraudulent activity.

CONCLUSION

Actually, a novel conceptual model of the security maintenance has proposed to make any IT infrastructures and services that follow those guidelines will accessible properly and secure by any authorized people:

Now days, security should be concern in any IT services and infrastructures including in any proposed maintenance model and guidelines.

Security maintenance is more important in cyber space for any organization especially for IT services and infrastructure usage in safe and secure manner.

STRICT CYBER LAWS

Should be deployed : Maximum people out there think we cannot should not categorize cyber crimes in to regular crimes. But as the events are happening and the world has started facing heaving losses be cause of cyber crimes it is becoming more and more clew that introducing strict cyber laws is the only way to handle these activities.

REFERENCES

1. Journal of Education and Social Sciences, Vol. 8, Issue 1, (October 2017) ISSN 2289-1552.
CYBER SECURITY MAINTENANCE BASED ON HUMAN-TECHNOLOGY ASPECTS IN DIGITAL TRANSFORMATION ERA.
2. Proceedings of the 51st Hawaii International Conference on System Sciences, 2018.
INTRODUCTION TO THE MINITRACK ON CYBER-OF-THINGS: CYBER CRIMES, CYBER SECURITY AND CYBER FORENSICS.
3. international conference on new horizons in science, Engineering and management and humanities IIMT college of Engineering, greater Noida (India) (NHSEMH-18) 16th February 2018, www.conferenceworld.in ISBN: 978-93-87793-00-2
ISSUES BASED ON CYBER CRIME AND SECURITY G.Balaji1,V.S.Hari Prassath2, V.Sriram3
4. See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/307594049
A Study on the Cyber - Crime and Cyber Criminals: A Global Problem, Article June 2014.
5. Overview of Cyber Laws In India.