International Research Journal of Human Resources and Social Sciences
ISSN(O): (2349-4085) ISSN(P): (2394-4218)
Impact Factor- 5.414, Volume 4, Issue 8, August 2017
Website- www.aarf.asia, **Email** : editor@aarf.asia , editoraarf@gmail.com

CYBER SECURITY AND SUSTAINABILITY: CT CHALLENGES AND STRATEGIES

Ms.Monika Bhatia

Assistant Professor

School of Management Studies, Ansal University Gurgaon.

Information and Communications Technologies (ICTs) help business to attain sustainability in many aspects. Internet is the key transmission channel of ICT. It is the backbone of the global information society and its importance is increasing with the aspect of global, social, political and economic life for two decades or more. The different types of different and development have brought many benefits like information sharing, Internet work, and ease of access, access control, data authentication, confidentiality and integrity. Along with these advantages some of the threats like data leak, unauthorized data access, etc. also prevails. Some of the serious cyber-attacks demonstrated over the past few years through acts of cyber espionage and cyber crime within the virtual networked ecosystem that we live provoke us to protect the sensitive data from hackers or attackers. The paper covers the various ITC Challenges and the respective strategies to protect and secure the sensitive information from different hackers or attackers across the world of different business companies or institutes. The paper also concentrates on the security of the data in-transit. Different transit attacks and its prevention strategies are also discussed.

Keywords: ICT, Cyber Security, Cyber Crime, Cyber Attacks

INTRODUCTION

The primary concern of Information and communication Technology (ICT) has been the security of data and with the developments in the field of cyber crime the intensity of the security concern has magnified. Protecting the intellectual property is the most important concern for corporate sectors. However, it was only in the recent past that the Government began to understand the significance of ICT security for societies and others sectors that are begin transformed by technology and that have become most popular or computer networks. The security of ICT is thus becoming a policy priority of many governments to handle these situations.

Cyber security strategies are setting goals measures and institutional responsibilities in a proper manner to achieve the goals of cyber security issues. Generally, the primary concern is to ensure the confidentiality, integrity and a availability of computer data and system and to protect against or prevent intentional and non-intentional incidents and attacks, which are possible in the current scenario. Some of these strategies contain also measures against cyber crime provide a criminal justice response to (C-I-A) attacks against computers and thus complement technical and procedural cyber security responses.

CYBER SPACE

Cyberspace is defined as the virtual space of all IT systems which is linked at data level on a global scale for retrieving the private data which are secretly shared among different IT sectors. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network, which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space aren't part of cyberspace but it is part of cyber crime.

Cyber Security - Traditional and Current

Cyber security strategies are set to focus on technical, procedural and institutional measures, such as risk and vulnerability analyses of data, early warning and response, incident management and information sharing. To handle these types of situations setting up of Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) is necessary and it is as increased international cooperation and other measures to ensure protection, mitigation and recovery of the data in different IT sectors. The Internet allows users to gather, store, process, and transfer vast amounts of data, including proprietary and sensitive business, transactional, and personal data. At the same time that businesses and consumers rely more and more on such

capabilities, cyber security threats continue to plague the Internet economy. Cyber security threats evolve as rapidly as the Internet expands, and the associated risks are becoming increasingly global and not secure anymore. Staying protected against cyber security threats requires all users, even the most sophisticated ones, to be aware of the threats and improve their security practices on an on-going basis to secure their sensitive data. Creating incentives to motivate all parties in the Internet economy to make appropriate security investments requires technical and public policy measures that are carefully balanced to heighten cyber security without creating barriers to innovation, economic growth, and the free flow of information over the different networks without affecting it.

With the help of its Task Force, the Department of Commerce will recommend public policies and to promote private sector norms which are directly aimed at markedly improving the overall cyber security posture of private sector as well as public infrastructure operators, software and service providers, and users outside the critical infrastructure and key resources realm and of their customers.

Cyber security is the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum. As a great example "cyber security in Germany is the desired objective of the IT security situation, in which the risks of the German cyberspace have been reduced to unacceptable minimum. Cyber security in Germany is the sum of suitable and appropriate measures. Civilian cyber security focuses on all IT systems for civilian use in German cyberspace. Military cyber security focuses on all IT systems for military use in German cyberspace" as described above the same security is implemented nowadays in India also but not fully, as it is on count of partial fulfilment.

Cyber Crime

Cyber crime is defined as the criminal activity, which is done using computers, and the Internet by which the sensitive data is sent over different networks. Cyber crime also includes the offences, which are normally committed for creating and distributing viruses on other computers or posting confidential business information on the Internet. Perhaps the most prominent fact of cyber crime is to identify theft, in which criminals use the Internet to steal personal information from other users. This can be done in two most common ways that is through phishing and pharming.

Cyber crime may be defined in a narrow sense as any cyber act, which is targeting computer data and systems or in a very broad sense as any activity involving a computer system. The first one risks being too restrictive as it would exclude phenomena that do exist in the physical world but

have gained a different quality and impact through the use of computers, such as fraud or intellectual property right violations, etc. The latter would be too broad as most crimes nowadays involve a computer in one way or the other.

It is therefore expedient to apply a definition that covers new types of crime as well as old types of crime using computers without being too broad and therefore meaningless so that the definition should be sufficiently robust to cover all relevant types of conduct even if technology evolves and phenomena of cyber crime appear to change almost every day. Finally, it is possible to operationalize it for criminal law purposes in order to meet the rule of law principle that there cannot be a crime without a law. Only conduct established as a criminal offence or any activity can be considered as a crime.

The Challenges of Cyber Security

There are different types of cyber attacks, which are performed; by different hackers or attackers at different places, which is, known as cyberspace and these acts become as cyber crime and also the challenges for the security of information or data in the corporate sector.

There are different types of challenges, which are given in some specific areas:

1. ***Passive Attacks:*** These types of attacks are those in which the hackers or attackers are just trying to monitor the sensitive information or data for their entertainment. The passive attacks can occur only to just monitor the information, which is transmitted from sender's side to the receiver's side. There are some categories of passive attacks, which are performed by hackers for only monitoring the information that is transmitted through any transmission channel. They are as follows:
   (a) Eavesdropping
   (b) Traffic analysis
   (c) Monitoring of unprotected communications
   (d) Capturing authentication information such as passwords
2. ***Active attacks:*** In these types of attacks, the attackers try to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to break the protective features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or

dissemination of data files, or modification of data. There are some types of it by which the modification of the message is done. A few of these types of attacks are as follows:

(a) Masquerade

(b) Release of content

(c) Denial-of-service (d) Modification of message

3. ***Routing Attacks***: These types of attacks are done in the shortest area means in between the routers. Routing attacks is often seen in routers, which implemented the original RIP Routing Information Protocol (RIP) is used to distribute routing information within networks, such as shortest-paths, and advertising routes out from the local network. The original version of RIP has no built in authentication, and the information provided in a RIP packet is often used without verifying it. An attacker could forge a RIP packet, claiming his host "xyz" has the fastest path out of the network. All packets sent out from that network would then be routed through xyz, where they could be modified or examined. An attacker could also use RIP to effectively impersonate any host, by causing all traffic sent to that host instead of the name of the real attacker.

   Example: "The version 2 of RIP was enhanced with a simple password authentication algorithm, which makes RIP attack harder to happen. IPsec VPN provides a way to V keep routing information encrypted among the routers implemented the IPsec VPN".[3]

4. ***Countering Insiders:*** An insider attack involves someone disgruntled employee. The network Insider attacks can be from the inside, such as a or not malicious. Malicious insiders intentionally eavesdrop information in a fraudulent ma net, or den, steal, or damage information, use y access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task.[3]

STRATEGIES ANDSUSTAINABLILITY TO FACE THE CHALLENGES

In the current scenario, there are possibilities to face the challenges of cyber security to a greater extent but with the present Cyber Security Strategy the Federal Government adapts measures to the current threats or the current cyber activities on the basis of the structures established by the CIP (Critical Infrastructure Protection) implementation plan and the implementation plan for the federal administration.

Sustainable Implementation

With the implementation of the strategic measures the Government contributes to ensuring cyber security and thus to freedom and prosperity in India. In this context, a lot will depend on the success at international level in taking effective measures to protect cyberspace or cyber crime. The information technologies used are subjected to change short innovation cycles. This means that the technical and social aspects of cyberspace will continue to change and bear not only new opportunities, but also new risks. For this reason, the Government will regularly review whether the aims of the Cyber Security Strategy have been achieved under the overall control of the National Cyber Security Council (NCSC) and will adapt the strategies and measures to handle the given requirements and other conditions.

The Government will specifically focus on ten strategic areas:

1. ***Protection of critical information infrastructures (CII):*** Today, the primary concern of cyber security is the protection of critical information infrastructures becomes an important or the main priority of cyber security. These are the central components nearly for all critical infrastructures and they become increasingly important in the current scenario. The public and the private sector must create an enhanced strategic and organizational basis for closer coordination based on mixed information sharing to handle these basic situations. To this end, cooperation established by the CIP implementation plan is systematically extended, and legal commitments to enhance the binding nature of the CIP implementation plan are examined and implemented. With the participation of the National Cyber Security Council (NCSC), the integration of additional sectors is examined and the introduction of new relevant technologies is considered as greater extent, which is clearly clarified for these types of situations. Whether and where protective measures have to be made mandatory and the additional powers are required in case of specific threats have to be clarified, too. Furthermore, we will examine the necessity of harmonizing rules to maintain critical infrastructures during IT crises.
2. ***Secure IT systems:*** For the protection of Infrastructure, the requirement of more security with regard to IT systems used by citizens or by small and medium-scale businesses is necessary. Users will need appropriate and consistent information with the different risks related to the use of IT systems and on security measures they can take to use cyberspace in a protective and secure manner. We will organize joint initiatives with the groups from different society or other areas to pool information and advice consistently. Furthermore,

we will examine whether providers may have to assume greater responsibility and make sure that a basic collection of appropriate security products and providers make services available to users. To achieve the secure IT-system we want to provide specific incentives and funds for basic security functions. To support small and medium-sized businesses in the secure use of IT systems, the participation of the industry is necessary.

3 ***IT Security in Public Administration:*** The public administration with further enhance the protection of its IT systems. State authority plays an important role in data security. We will create a common, uniform and secure network infrastructure in the World as a basis for electronic audio and data communication. We will continue to press ahead with the implementation plan for the country. IT security situation is getting worse and this plan may be aligned accordingly with the different situations that will occur. Effective IT security requires powerful structures in all authorities. For this reason, resources must be deployed appropriately at central and local level. To facilitate implementation, through uniform action by authorities, joint investments into the Government's IT security will be made regularly in line with budgetary possibilities. Operational cooperation particularly with regard to CERTs (Computer Emergency Response Teams) will be further intensified by the IT planning council.

4 ***National Cyber Response Centre:*** To deal with the different crimes or attacks that can occur in business companies we can improve the coordination of protection and response measures for IT incidents we will set up a National Cyber Response Centre. It will report to the crime Office for Information Security and cooperate directly with the Office for the Protection of the Constitution and the Office of Civil Protection and Disaster Assistance. Cooperation in the National Cyber Response Centre will strictly observe the statutory tasks and powers of all authorities involved on the basis of cooperation agreements, which are set by the government. The Criminal Police Office, the Customs Criminological Office, the Intelligence Service, etc., supervising critical infrastructure operators all participate in this centre within the framework of their statutory tasks and powers. Quick and close information sharing on weaknesses of IT products, vulnerabilities, etc., and forms of attacks and profiles of crime office operators enables the National Cyber Response Centre to analyse IT incidents and give consolidated recommendations for action. The interests of the private sector to protect itself against crime and espionage in cyberspace should also be adequately taken into account. At the same time, respective responsibilities must be

observed. Every stakeholder takes the necessary measures in its remit on the basis of the jointly developed national cyber security assessment and coordinates them with the competent authorities as well as partners from industry and academy.

Example: "Since security preparedness is best achieved by early warning and prevention, the Cyber Response Centre will submit recommendations CO the National Cyber Security Council either on regular basis or on specific incidents. If the cyber security situation reaches the level of an imminent or already occurred crisis, the National Cyber Response Centre will directly inform the crisis management staff headed by the responsible State Secretary at the Ministry of the Interior."[1]

5. ***National Cyber Security Council:*** An important preventive tool for cyber security is to identify and removal of structural causes for crises are considered in the best manner. For this reason we want to establish and maintain cooperation within the Governments the public and the private sector as a responsibility for Information Technology more visible and set up a National Cyber Security Council. The Chancellery and a State Secretary from each Foreign Office, the Ministry of the Interior, the Ministry of Defence, the Ministry for Economics and Technology, the Ministry of Justice, the Ministry of Finance, the Ministry of Education and Research will participate. On specific occasions additional ministries will be included. Business representatives will be invited as associated members. Representatives from academy will be involved, if required. The National Cyber Security Council is intended to coordinate preventive tools and the interdisciplinary cyber security approaches of the public and the private sector. The National Cyber Security Council will complement and interlink IT management at federal level and the work of the IT Planning Council in the area of cyber security at a political and strategic level.[1]

6. **Effective crime control in cyberspace:** The capabilities of law enforcement agencies, the crime Office for Information Security and the private sector in combating cyber crime, also with regard to protection against attacks and sabotage, must be strengthened. To improve the exchange of know how in this area we intend to set up joint institutions with industry the participation of the competent law enforcement agencies, which will act in an advisory capacity. Projects to support partner countries with structural weaknesses will also serve the aim of combating cyber crime. To face up to the growing challenges of global cyber crime activities we will make a major effort to achieve global harmonization in criminal

law based on the Council of Cyber Crime Convention. Furthermore, we will examine whether additional conventions in this area may be necessary at world level.

7. **Effective coordinated action to ensure cyber security at world level:** The cyberspace security at world level can be achieved only through coordinated tools at national and international level. At minimum level we support appropriate measures based on the action plan for the protection of critical information infrastructures, in view of the changed threat situation in ICT and the pooling of IT competences institutions. The Internal Security Strategy and the Digital Agenda provide guidance for further activities.

   We will shape our external cyber policy in such a way that interests and ideas concerning cyber security are coordinated and pursued in international organizations, such as the United Nations, the Council of Europe, etc. An increasingly multilateral approach must be brought in line with the necessity of sovereign evaluation and decision-making powers. In this context, a code for state conduct in cyberspace should be established, which is signed by as many countries as possible and includes confidence building security measures. In the G8 framework, we are currently working on intensifying anti-botnet activities. We are in favour of the alliance's commitment to establishing uniform security standards, which Member States may also use for civilian critical infrastructures on a voluntary basis.

8. ***Use of reliable and trustworthy Information Technology:*** The availability of reliable IT systems and components must be ensured on a permanent or regular basis. The development of innovative protection plans for improved security, which takes into account social and economic aspects, is strongly supported. To this end, we will continue and intensify research on IT security and on critical infrastructure protection. Furthermore, we will strengthen the technological sovereignty and economic capacity in the entire range of IT competencies, include them in our political strategies and develop them further. Wherever it makes sense, we will pool our resources with those of our partners and allies, particularly in Europe. We are in favour of diversity in technology. Our aim is to use components in critical security areas, which are certified against an international recognized certification standard.

9. ***Personnel development in authorities:*** The importance of cyber security must be examined as a priority whether additional staff is necessary in authorities in the interest of cyber security. Furthermore, intensified personnel exchange between authorities and appropriate further training measures will enhance inter-ministerial cooperation.[1]

10. ***Tools to respond to cyber attacks:*** If the state wants to be fully prepared for attacks or cyber crimes, a coordinated and comprehensive set of tools to respond to attacks must be created in cooperation with the competent state authorities. We will continue to assess the threat situation regularly and take appropriate protection measures. If necessary, we have to examine whether additional statutory powers must be created at world level. The different strategies that clearly defined above the aims, mechanisms and institutions mentioned must be internalised through a permanent exercise process with the relevant departments and authorities as well as businesses.

CONCLUSION

Cyber security is defined as the security of the information or the sensitive data at a business level that the data is to be travelled from sender side to receiver side without getting affected. It means that the data is reached safely and securely to the appropriate user of that information. Cyber attacks by hackers at cyberspace are becoming challenges for the authorities, corporates or institutions. There are some strategies, which are defined to handle these types of situations in the IT system. These are used to design some laws or authorities or councils to face the above-mentioned challenges. The corporate sector should take part in the above-mentioned councils or authorities' meetings for increasing the efficiency or effectiveness of data to be passed in a secure manner.

References

1. www.cio.bund.de/SharedDocs/.../css_engl_downloacl.pdf
2. www.google.co.in/SharedDocs
3. computernetworkingnotes.com/network-security-access-lists-standards-and-extended
4. William Stallings, Network Security Essentials, Third Edition, TMC