IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 2 (May. - Jun. 2013), PP 67-75
www.iosrjournals.org

Cyber security: challenges for society- literature review

Atul M. Tonge[1], Suraj S. Kasture[2] , Surbhi R. Chaudhari[3]
[1](*CSE, Jawaharlal Darda Institute Of Engineering And Technology, India)*
[2](*CSE, Jawaharlal Darda Institute Of Engineering And Technology, India)*
[3](*CSE, Jawaharlal Darda Institute Of Engineering And Technology, India)*

Abstract :*Cyber security is the activity of protecting information and information systems (networks, computers, data bases, data centres and applications) with appropriate procedural and technological security measures. Firewalls, antivirus software, and other technological solutions for safeguarding personal data and computer networks are essential but not sufficient to ensure security. As our nation rapidly building its Cyber-Infrastructure, it is equally important that we educate our population to work properly with this infrastructure. Cyber-Ethics, Cyber-Safety, and Cyber-Security issues need to be integrated in the educational process beginning at an early age. Security counter measures help ensure the confidentiality, availability, and integrity of information systems by preventing or mitigating asset losses from Cyber security attacks. Recently cyber security has emerged as an established discipline for computer systems andinfrastructures with a focus on protection of valuable information stored on those systems fromadversaries who want to obtain, corrupt, damage, destroy or prohibit access to it. An Intrusion Detection System (IDS) is a program that analyses what happens or has happened during an execution and tries to find indications that the computer has been misused. A wide range of metaphors was considered, including those relating to: military and other types of conflict, biological, health care, markets, three-dimensional space, and physical asset protection. These in turn led to consideration of a variety of possible approaches for improving cyber security in the future. These approaches were labelled "Heterogeneity" ,"Motivating Secure Behaviour" and "Cyber Wellness" .*

Cyber Security plays an important role in the development of information technology as well as Internet services. Our attention is usually drawn on "Cyber Security" when we hear about "Cyber Crimes". Our first thought on "National Cyber Security" therefore starts on how good is our infrastructure for handling "Cyber Crimes". This paper focus on cyber security emerging trends while adopting new technologies such as mobile computing, cloud computing, e-commerce, and social networking. The paper also describes the challenges due to lack of coordination between Security agencies and the Critical IT Infrastructure.

Keywords *– cyber safety,e-commerce ,intrusion detection system (IDS), internet engineering task force (IETF),metaphors*

I. Introduction

"In India we went straight from no telephones to the latest in mobile technology" says Cherian Samuel of the Institute for Defence studies and Analysis,(IDSA)in New Delhi and the same with internet connected computers.They came in on all of a sudden and no one was taught even the basic fact about cyber security". India stands fifth in worldwide ranking of countries affected by cybercrime.Although it should be emphasised that these figures are extrapolations.Much of its vulnerability is explain by widespread computer illiteracy and easily pirated machines.

Internet is one of the fastest-growing areas of technical infrastructure development [1]. In today's business environment, disruptive technologies such as cloud computing, social computing, and next-generation mobile computing are fundamentally changing how organizations utilize information technology for sharing information and conducting commerce online [1]. Today more than 80% of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. The scope of Cyber Security extends not only to the security of IT systems within the enterprise, but also to the broader digital networks upon which they rely including cyber space itself and critical infrastructures. Cyber security plays an important role in the development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being[1]. Society has become dependent on cyber systems across the full range of human activities, includingcommerce, finance, health care, energy, entertainment, communications, and national defense [2]. Recent research findings also show that the level of public concern for privacy and personal information has increased since 2006 ,[3]Internet users are worried that they give away too much personal information and want to be forgotten when there is no legitimate grounds for retaining their personal information.Exploration of the metaphors we use in the cyber security domain may help improve our thinking and discussion in four ways. First, we maygain a clearer understanding of the value and limitations of the concepts we have mappedfrom other domains into the cyber security domain. Second, trying out less common

or newmetaphors may feed the imagination of researchers and policy developers. Third, metaphorsthat work particularly well might be developed into a whole new models or sets of conceptsfor approaching cyber security problems. Fourth, a metaphor serves a heuristic purpose --bringing clearer understanding of abstract concepts from the field of cyber security intodomains with which the non-specialist may be more familiar[4].

Cyber security depends on the care that people take and thedecisions they make when they set up, maintain, and usecomputers and the Internet. Cyber-security covers physicalprotection (both hardware and software) of personalinformation and technology resources from unauthorizedaccess gained viatechnological means.Albert Einstein was quoted as saying "Problems cannot besolved with the same level of awareness that created them."The problem of End-User mistakes cannot be solved byadding more technology; it has to be solved with a joint effortand partnership between the Information Technology community of interest as well as the general business community along with the critical support of top management [5].

II. Headings

1. Current Approaches To I T – Security

Most IT security management approaches consist of checklistswhich decision makers use to develop a coverage strategy; thesegenerally are little more than a triage approach to categorizingthreats. One popular approach for risk visualization has been theconstruction of a risk cube, where each axis or dimension representsone of the three components of risk (threats, assets, and vulnerabilities),and the volume of the cube represents the amount of risk[6].models have been developed which attempt to deal withrisk analysis in a qualitative manner. Mark Egan (the then CTO forSymantec) in his book The Executive Guide To Information Securityintroduced a very simple tabular model which allows users to ratethreat severities into one of three categories/columns (low, medium,and high) and then to average across columns. This simple triageapproach to subjective threat impact analysis, though insightful, is notable to capture system uncertainty. Alberts and Dorofeedevelopeda system called OCTAVE which also utilizes qualitativeinformation to assess risk.Others have tried approaches that quantify IT security riskanalysis. Beauregard applied the Value Focused Thinking (VFT)approach from general risk analysis to assess the level of informationassurance within the Department of Defense units [7].

1.1 India Stress Test

India has a national CERT (CERT-in, since 2004), a crisis management plan and is setting up a Cyber Command and Control Authority. A draft of a national cyber-security policy is under discussion.The premium on internet privacy in India is low and data control therefore tends to be neglected.This is another reason of phishing and other scams". People in India have to understand basic security like pin numbers and passwords" Kamlesh Bajaj of the Data Security Council of India (DSCI), an organization promoting data protection.The govt. is taking a two pronged approach teaching best practices to prevent attacks, and helping capacity building to handle incidents when attack happen.India is actually aware that cybercrime is a bad for its reputation as a country where foreign investors can do business and has been investing heavily in cyber security.The main challenge now for India is to train and equip its law enforcement agencies and judiciary, particularly outside big city like Delhi,Mumbai and Bangalore.Training must expand to cover the whole country says Bajaj,at DSCI,we have developed training and investigation manual for police officer.We have trained more than 9,000 personnel of local education authorities and the judiciary on cyber security.

2. Threats To Cyber Security

Threats to cyber security can be roughly divided into two general categories: actions aimed at andintended to damage or destroy cyber systems ("cyber attacks") and actions that seek to exploit the cyberinfrastructure for unlawful or harmful purposes without damaging or compromising that infrastructure("cyber exploitation") [8]. While some intrusions maynot result in an immediate impact on the operation of a cyber systems, as for example when a "TrojanHorse" infiltrates and establishes itself in a computer, such intrusions are considered cyber attacks when they can thereafter permit actions that destroy or degrade the computer's capacities [9]. Cyber exploitation includes using the Internet and other cyber systems to commit fraud, to steal,to recruit and train terrorists, to violate copyright and other rules limiting distribution of information,to convey controversial messages (including political and "hate" speech), and to sell child pornographyor other banned materials.Following are some new threats to cyberspace[10].

2.1Smart Phones Pose Security Challenges

Development like smart phones and cloud computing mean we are seeing a whole new set of problem link to inter-connectivity that required new regulation and new thinking.Experts talks of internet of things and services and things are smart phones,androids(mobile operating system),tablets and sensors and services including the cloud."The mobile internet is the changing thing," says Canadian expert Rafal Rohozinski". The next 2 billion

users will be connecting from mobile devices and many of those devices are in developing countries.The sheer number are likely to have social impact like flash mobs.A lot more politics is migrating to cyber space ,with parallel calls to regulate cyber space.The governance of internet as whole is reinvesting states with authority to regulate cyber space"[10].

2.2 Cloud Computing

As for cloud computing,outsourcing the filling of data has been around 40 years.What's new is the geographical spread of this storage.The National Institute Of Standards and Technology(NIST) provide the standard definition for cloud computing:a rapid ,on demand network to a shared pool of computing resources. These are not the stratosphere,they are basically hangers full of servers.Outsourcing means considerable cost savings and many companies are now using it for computation and data storage.Amazon,eBay,Google,Facebook and all the big names are outsourcing computation to cloud."Cloud computing means the separating the contents in a way that did not exist before says Rohozinski. The laws we have governing copyright and territorial security get skewed." Among other issues raised by cloud computing is the cost of process power and connectivity and the whole issues of net neutrality.But Luna Warns that these new storage facilities give rise to problem of security and jurisdiction."Who are you going to sue if there's a problem" ?Google for instances keep 1/3th of its cloud in Canada".

3. Current Cyber-Security Measures

The Internet currently is secured primarily through private regulatory activity, defensive strategiesand products, national laws and enforcement, and some limited forms of international cooperation andregulation.

3.1. Private Measures

Non-governmental entities play major roles in the cyber security arena. Technical standards for theInternet (including current and next-generation versions of the Internet Protocol) are developed andproposed by the privately controlled Internet Engineering Task Force ("IETF")[2]; the Web Consortium,housed at the Massachusetts Institute of Technology, defines technical standards for the Web.Other privately controlled entities that play significant operational roles on aspects of cyber securityinclude the major telecommunications carriers, Internet Service Providers ("ISPs"), and many otherorganizations, including:

 The Forum of Incident Response and Security Teams ("FIRST"), which attempts to coordinatethe activities of both government and private Computer Emergency Response Teams ("CERTs") and is also working on cyber security standards;

 The Institute of Electrical and Electronics Engineers ("IEEE"), which develops technical standardsthrough its Standards Association and in conjunction with the U.S. National Institute of Standards andTechnology ("NIST");

 The Internet Corporation for Assigned Names and Numbers ("ICANN"), which operates pursuantto a contract with the U.S. Department of Commerce (September 2009) transferring to ICAAN thetechnical management of the Domain Name System[11].

3.2.National Measures

Many national governments have adopted laws aimed at punishing and thereby deterring specific forms of cyber attacks or exploitation. The U.S., for example, has adopted laws making criminal variousforms of conduct, including improper intrusion into and deliberate damage of computer systems.Theselaws have little or no effect, however, on individuals, groups, or governments over whom the U.S. lacksor is unable to secure regulatory or criminal jurisdiction.US national security experts almost exclusively emphasize the need for national measures forenhancing cyber security[2]. They recommend national laws to protect the sharing of information aboutthreats and attacks; methods for government bodies, such as the NSA, to cooperate with private entitiesin evaluating the source and nature of cyber attacks; and more effective defenses and responses to cyber attacks and exploitation developed through government-sponsored research and coordinationpursuant to cyber security plans.The GAO's July 2010 report details the specific roles being played by many U.S. agencies in effortsto enhance "global cybersecurity", but ultimately concludes that these efforts are not part of a coherentstrategy likely to advance U.S. interests[12].

3.3.International Measures

National governments often cooperate with each other informally by exchanging information,investigating attacks or crimes, preventing or stopping harmful conduct, providing evidence, and evenarranging for the rendition of individuals to a requesting state. States have also made formal, internationalagreements that bear directly or indirectly on cyber security. [13]. The international agreements applyto the criminal activities specified, including situations in which the alleged criminals have used

cybersystems in those activities.International agreements that potentially bear upon cyber-security activities also include treaties(the UN Charter and Geneva Conventions) and universally accepted rules of conduct (customary law).International law also provides rulesrelated to the use of force during armed conflict that presumably apply to cyber attacks, including for example requirements that noncombatants and civilian institutions such as hospitals not be deliberatelyattacked, and that uses of force be restricted to measures that are necessary and proportionate.[2].

4. Necessity Of Cyber Security

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

1) Protecting unauthorized access, disclosure, modificationof 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 sitesagainst hijacking.
4) One key to improved cyber security is a betterunderstanding of the threat and of the vectors used by theattacker to circumvent cyber defences [5].
6) Need of separate unit handling security of theorganization.
7) Different organizations or missions attract differenttypes of adversaries, with different goals, and thus needdifferent levels of preparedness [14].
8) In identifying the nature of the cyber threat anorganization or mission faces, the interplay of an adversary's capabilities, intentions and targetingactivities must be considered [15].With respect to state and country
1) Securing the information containing various essentialsurveys and their reports.
2) Securing the data basis maintaining the details of all therights of the organizations at state level.

5. Recent Survey Issues On Cyber Security Trends

The following list was developed from cyber security research and survey [1] [16] [17] [18].

5.1 Mobile Devices and Apps

The exponential growth of mobile devices drives an exponential growth in security risks. Every new smart phone, tablet or other mobile device, opens another window for a cyber attack as each creates another vulnerable access point to networks. This unfortunate dynamic is no secret to thieves who are ready and waiting with highly targeted malware and attacks employing mobile applications. Similarly, the perennial problem of lost and stolen devices will expand to include these new technologies and old ones that previously flew under the radar of cyber security planning.

5.2 Social Media Networking

Growing use of social media will contribute to personal cyber threats. Social media adoption among businesses is skyrocketing and so is the threat of attack. In 2012, organizations can expect to see an increase in social media profiles used as a channel for social engineering tactics. To combat the risks, companies will need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention, enhanced network monitoring and log file analysis.

5.3 Cloud Computing

More firms will use cloud computing. The significant cost savings and efficiencies of cloud computing are compelling companies to migrate to the cloud. A well designed architecture and operational security planning will enable organizations to effectively manage the risks of cloud computing. Unfortunately, current surveys and reports indicate that companies are underestimating the importance of security due diligence when it comes to vetting these providers. As cloud use rises in 2012, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.

5.4 Protect systems rather Information

The emphasis will be on protecting information, not just systems. As consumers and businesses are like move to store more and more of their important information online, the requirements for security will go beyond simply managing systems to protecting the data these systems house. Rather than focusing on developing processes for protecting the systems that house information, more granular control will be demanded - by users and by companies - to protect the data stored therein.

5.5 New Platforms and Devices

New platforms and new devices will create new opportunities for cybercriminals. Security threats have long been associated with personal computers running Windows. But the proliferation of new platforms and new devices - the iPhone, the I Pad, Android, for example - will likely create new threats. The Android phone saw its first Trojan this summer, and reports continue with malicious apps and spyware, and not just on Android.

6. Metaphors Of Cyber Era

Computer networks in which all the components have the same vulnerabilities are easier forattackers to bring down, but more diverse systems would deprive attackers of sufficient targetknowledge to do as much damage.It can thus be argued that diversity is one of the ways of "baking" security into systems—designing them from the start to be more secure, as opposed to adding on security measures later[4].A second approach, "Motivating Secure Behaviour," took a market perspective on theadoption of cyber security measures. The central concept is that many of the vulnerabilitiesin current systems can be traced to human behaviours shaped by the structure of incentivesfacing both suppliers and users of information technology.The third approach was called "Cyber Wellness," exploring analogies with efforts toimprove individual and public health. Its objective is to keep the population (of users andnetworked systems) as healthy as possible: resistant to attacks, resilient under stresses, waryof dangerous environments, treatable if diseased, and able to limit contagions. Generally speaking, the literatureon cyber security usually refers to three characteristics of information systems that needprotection:

1. Confidentiality -privacy of information and communications. In government thismight mean, for example,assuring access to classified information only byauthorized individuals. In commerce, it might mean the protection of proprietaryinformation.
2. Integrity -assurance that information or computing processes have not beentampered with or destroyed. In the case of critical infrastructures (say, for example,the power grid), loss of data integrity could take the form of destructive instructionsto the system resulting in financial, material, or human losses.
3. Availability- assurance that information or services are there when needed. Denialof service attacks, which overload system servers and shut down websites, areexamples of interfering with availability.

Two important characteristics of the much ofthe discourse on this subject (as well as most discourse on most subjects). that is, first,metaphors are hard to avoid, even if we are not consciously using them. Second, how aproblem is framed frequently implies certain kinds of solutions, while implicitlyreducing the likelihood that others will be considered.The newer or rarer metaphors were then grouped into several categories tofacilitate further elaboration.

6.1 Predominant Metaphors

As mentioned above, a common metaphor in cyber security is that of the fortress[19]. Avalued body of information is held within a walled enclosure, perhaps encircled by a moat,accessed by portals or gates, and guarded by watchmen assigned to keep out theunauthorized. A second common metaphor is that of cops and robbers: criminals (or maybejust vandals) break into the house and steal valuables. Forensic measures are taken to trackthem down, after which they are identified and legally prosecuted. A third common metaphoris that of warfare: enemies, using various weapons and tactics, attack and steal or destroyproperty (or perhaps just commit espionage) in order to achieve some strategic goal.

6.2 Newer metaphors

6.2.1 Biological

Some cyber security metaphors come from the field of biology. A broad approach is tothink of cyber systems as instances of complex, adaptive systems—as our biological systems.One example of such systems is the ecosystem: a complex system of interdependent speciesin populations in a particular kind of environment. A concept drawn from ecosystem studiesis that of biodiversity: the idea that systems with diverse components are likely to be morestable, resilient, and adaptable to change. This metaphor is utilized below in thesection on "Heterogeneity".

6.2.2 Market Systems

In many ways, of course, the Internet is a vast marketplace in which goods and services arebeing bought and sold continuously, even though it lacks the physical accoutrements oftraditional marketplaces. Hardware and software systems themselves are bought and sold.But the direction of this metaphorical exploration was to consider how market and economicprinciples might be applied to cyber security problems. A related business concept is that of risk management, in which organizations (possiblycorporations, possibly government agencies) attempt to assess the risks they face, prioritizethem, and take management measures

appropriate to those risks: avoidance, reduction,acceptance, or transfer[20]. Each of these has a cost, which is weighed against the potentiallosses.

6.2.3 Spatial Metaphors

The term "cyberspace" was invented in 1982 by science fiction writer William Gibson, andit became commonly applied to the Internet and the World Wide Web in the 1990's[4]. It is agood example of how a metaphor—mapping of one domain (three dimensional space ashumans experience it) to another domain (computer networks)—has become so pervasivethat we scarcely even think of it as a metaphor any more. The newly formed Air Force CyberCommand describes its mission in ways that imply that cyberspace is not a metaphoricalconcept, but just one more class of physical spaces that it calls "domains".

7. Some Counter Measures For Cyber Security

7.1 GPRS Security Architecture

In order to meet security objectives, GPRSemploys a setof security mechanisms that constitutesthe GPRS security architecture. Most of thesemechanisms have beenoriginally designed for GSM,but they have been modified to adapt to the packetorientedtraffic nature and theGPRS networkcomponents. The GPRS security architecture, mainly,aims at two goals: a) to protect the networkagainstunauthorized access, and b) to protect the privacyofusers. It includes the following components[21]:

Subscriber Identity Module (SIM)

- Subscriber identity confidentiality
- Subscriber identity authentication
- GPRS backbone security

7.1.1 Subscriber Identity Module – SIM

The subscription of a mobile user to a network ispersonalized through the use of a smart card namedSubscriberIdentity Module (SIM). Each SIM-card isunique andrelated to a user. It has a microcomputerwith a processor, ROM, persistent EPROM memory,volatile RAM and an I/O interface. Its softwareconsists of an operatingsystem, file system, andapplication programs (e.g., SIMApplication Toolkit).The SIM card is responsible for the authentication ofthe user by prompting for a code (Personal IdentityNumber PIN).A serious weakness of the GPRS securityarchitecture isrelated to the compromise of theconfidentiality of subscriber identity. Specifically,whenever the serving network (VLR or SGSN)cannot associate the TMSI withthe IMSI, because ofTMSI corruption or database failure, the SGSNshould request the MS to identify itself bymeans ofMSI on the radio path.

7.1.2. Subscriber Identity Authentication

A mobile user that attempts to access thenetwork mustfirst prove his identity to it. Userauthentication protects against fraudulent use andensures correct billing. GPRS uses the authenticationprocedure already definedin GSM with the samealgorithms for authentication andgeneration ofencryption key, and the same secret key, Ki.However, from the network side, the wholeprocedureis executed by the SGSN (instead of the basestation)and employs a different random number (GPRSRAND),and, thus, it produces a different signedresponse(GPRS-SRES) and encryption keythan theGSM voice counterpart.The authentication mechanism used in GPRSalso exhibits some weak points regarding security.More specifically, the authentication procedure isone-way, and, thus, it does not assure that a mobileuser is connected to anauthentic serving network.This fact enables active attacks using a false basestation identity.

7.1.3 GPRS Backbone Security

The GPRS backbone network includes the fixednetworkelements and their physical connections thatconvey userdata and signalling information. Signallingexchange inGPRS is mainly based on the SignallingSystem 7 (SS7)technology, which does not supportany security measure for the GPRS deployment.Similarly, the GTP protocol that is employed forcommunication between GSNsdoes not supportsecurity. Thus, user data and signalling information inthe GPRS backbone network are conveyedin cleartextexposing them to various security threats.Inaddition, inter-network communications (betweendifferent operators) are based on the public Internet,whichenables IP spoofing to any malicious third partywho getsaccess to it. In the sequel, the securitymeasures appliedto the GPRS backbone network arepresented.Based on the analysis of the GPRS securityarchitectureit can be perceived that the GPRSsecuritydoes not aim at the GPRS backbone and thewire-lineconnections, but merely at the radio accessnetwork andthe wireless path.

7.2 Intrusion Detection System (IDS)

Attacks on the computer infrastructures are becoming an increasingly serious problem[22]. An intrusion is defined as any set of actions that attempt to compromise theintegrity, confidentiality or availability of a resource. Intrusion detection is therefore required as anadditional wall for protecting systems. Intrusion detection is useful not only in detecting successfulintrusions, but also provides important information for timely countermeasures.Intrusion detection is classified into two types: misuse and anomaly detection. Misuse intrusiondetection uses well-defined patterns of the attack that exploit weaknesses in system and applicationsoftware to identify the intrusions. These patterns are encoded in advance and used to match againstthe user behaviour to detect intrusion. Anomaly intrusion detection uses the normal usage behaviour patterns to identify the intrusion. The normal usage patterns are constructed from the statisticalmeasures of the system features. The behaviour of the user is observed and any deviation from theconstructed normal behaviour is detected as intrusion.Dorothy Denning proposed the concept of intrusion detection as a solution to the problem ofproviding a sense of security in computer systems. The basic idea is that intrusion behaviour involvesabnormal usage of the system. Different techniques and approaches have been used in laterdevelopments. Some of the techniques used are statistical approaches, predictive pattern generation,expert systems, keystroke monitoring, state transition analysis, pattern matching, and data miningtechniques [23].

7.3 Distributed Intrusion Detection System (DIDS)

In Distributed IDS (DIDS) conventional intrusion detection system are embedded inside intelligentagents and are deployed over a large network[22]. In a distributed environment, IDS agents communicatewith each other, or with a central server. Distributed monitoring allows early detection of plannedand coordinated attacks and thereby allowing the network administrators to take preventive measures.DIDS also helps to control the spreading of worms, improves network monitoring and incidentanalysis, attack tracing and so on. It also helps to detect new threats from unauthorized users, backdoorattackers and hackers to the network across multiple locations, which are geographicallyseparated. In a DIDS it is important to ensure that the individual IDS are light-weight and accurate. A number of IDS have been proposed for a networked or distributed environment.Cooperating Security Managers (CSM) enable individual distributed intrusion detection packages tocooperate in performing network intrusion detection without relying on centralized control. Eachindividual CSM detects malicious activity on the local host. When suspicious activity is detected,each CSM will report any noteworthy activity to the CSM on the host from which the connectionoriginated. The local CSM will not notify all networked systems, but rather only the systemimmediately before it in the connection chain. DIDS are simply a superset of the conventional IDSimplemented in a distributed environment [22].

8. Some Elements To Create Awareness In Cyber-Security Educational System

In education system, the children must be made aware ofthe possible attacks and types of intruders [5]. They must also be aware of the terms like: Hardware/Desktop Security, Wi-Fi security, wired security, Password Protection/(File/Folder)level security, Social networking attacks security and Malicious software:

- Phishing, Hoaxes
- Scare ware, Malware, Virus, Worm,
- Trojans, Zombie and Botnet, Spyware, Adware,

Students are acquiring information technology skillsmarks question on the educators' abilities to ensure thatpositive habits of on-line behaviour are being formed.Whereas, the teacher giving information about security lacksthe knowledge and up-to date information related to Cyberawareness issues, particularly with respect to security.Teacher technology training must be provided for skillsdevelopment and awareness[23].

8.1. Additional Class Room Improvement Measures

Class XII, Graduate and Post graduate level students aswell as the employees of an organization must be given:Mock test, Case-studies, Virtual environment creation givingthe feel of a problematic situation, must be set in order tocreate more awareness about the current technologies andrelevant threat, General awareness websites creation,Power-point slides, FAQ can be implemented in class room teaching

8.2 Class Room Conducted FAQ'S Showing the Need of the Awareness

There are some expected questions that the educationalsecurity professionals must be aware of:

1) A computer program automatically installed on yourcomputer, spyware tracks personal information youentered and sends it to its creator. Unlike computer viruses, this leaves the computer owners totally unaware of its presence: worm, spyware, Trojan horse.
2) What is Cyber-safety?Cyber-safety are steps that one can take to avoid revealinginformation by "social" means, cyber-safety focuses onacting safely and responsibly.

3) What is the difference between a Virus and a Hacker?
4) What is the difference between a Hacker and a Cracker? A hacker is a person who is proficient with computersand/or programming to an elite level where they know all of the inn's and out's of a system. There is no illegality involvedwith being a hacker. A cracker is a hacker who uses theirdata, changing bank accounts, distributing viruses etc.
5) What is a Hoax?A deceptive alert disseminated via forwarded emailwarning users of a computer virus, internet worm, or hersecurity threat which in reality does not exist.Students with different background are not aware of thisbasic awareness about cyber security. Hence there is a needfor awareness in educational system.

III. Conclusion

This paper has examined the significance of privacy for individuals as a fundamental human right. Violations of human rights arise from the unlawful collection and storage of personal data, the problems associated with inaccurate personal data, or the abuse, or unauthorised disclosure of such data. In this paper we also includes the current threats , issues, challenges and measures of IT sector in our society. With the increasing incidents of cyber attacks, building an effective intrusion detection model withgood accuracy and real-time performance are essential.

The metaphors implicit in the current mainstream of cyber security thought canilluminate the assumptions, logic, and perhaps the limitations of that thought. Experimentingwith alternative metaphors can lead to different perspectives on the problem and may evenstimulate creatively different ways of dealing with it. System security and Data security is a critical issue today. Gridsecurity involves an architecture that includessecurity from the beginning, consists of more thanjust protective devices such as firewall, and engagesprocesses as well as products. GPRS promises tobenefit network users greatly by providing always onhigher bandwidth connections than are widelyavailable today. In order to be successful, dataconnections must be secure and be available all thetime from anywhere. With the increase in the use of wirelessmedia, security problems of confidentiality, integrity,and authentication are also increasing. The weakpoints of the GPRS security architecturemay lead tocompromises of end-users and network security ofthe GPRS system.

Indian citizens must identify the best techniques in order toprotect the information and system, as well as the network inwhich they work. The IT industry has been playing catch-upwith hackers and cybercriminals for decades. Thus there is aneed of cyber –security curriculum in the near future whichwill in-build the cyber-security understanding in the currentyouth and finally the IT sector will get more profound,securely skilled professionals not only in the security sectorbut also in the every sector, thus enhancing thecommunication, the brain compatibility skills of theemployees and the employers.

Acknowledgment

It gives us a great pleasure to submit the paper topic titled"Cyber Security: A Challenge To Society".We wish to take this opportunity to express our heartiest gratitude with pleasure to J.D.I.E.T, Yavatmal, which gave us an opportunity in fulfilling our desire of reaching our goal.We are indebted to our proactive guide Dr. Rajesh Sambhe because without his valuable guidance this work would not have a success. His constructive, useful, timely suggestions and encouragement in every step immensely helped us to carry out our work.

References

Journal Papers:

[1] Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, *International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 IJSER © 2012*
[2] Abraham D. Sofaer, David Clark, Whitfield Diffie ,Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/catalog/12997.htmlCyber Security and International Agreements ,*Internet Corporation for Assigned Names and Numbers pg185-205*
[3] ThillaRajaretnam Associate Lecturer, School of Law, University of Western Sydney, The Society of Digital Information and Wireless Communications (SDIWC),International *Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 232-240 2012 (ISSN: 2305-0012)*
[4] Thomas H. Karas and Lori K. Parrott , Judy H. Moore , *Metaphors for Cyber Security* ,Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0839
[5] BinaKotiyal, R H Goudar, and Senior Member, A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India PritiSaxena, *IACSIT International Journal of Information and Education Technology, Vol. 2, No. 2, April 2012*
[6] Loren Paul Rees, Jason K. Deane , Terry R. Rakes , Wade H. Baker, *Decision support for Cyber security risk planning*, Department of Business Information Technology, Pamplin College of Business, Virginia Tech., Blacksburg, VA 24061, United States b Verizon Business Security Solutions, Ashburn, VA 20147, United States
[7] S. Bistarelli, F. Fioravanti, P. Peretti, *Using CP-nets as a guide for countermeasure selection*, Proceedings of the 2007 ACM Symposium on Applied Computing (Seoul, Korea, 2007), 2007, pp. 300–304.
[8] Admiral Dennis C. Blair, *Annual Threat Assessment*, House Permanent Select Committee on Intelligence, 111th Congress, 1st sess., 2009.
[9] Mike McConnell, "Mike McConnell on *How to Win the Cyber-war We're Losing*," February 28, 2010, (accessed on July 19 2010).

[10] Bibliothequesolvay, parcLeopold , *Security and Defense Agenda*, 137 rue Belliard,B-1040 Brussels,Belgium
[11] Clarke and Knave, 92. The authors anticipate that "*logic bombs"*—software that erases all programming, effectively negating further use of a device—will be used in attacks and may already be in place.
[12] E.g.Fraud , *Related Activity in Connection with Computers*, U.S. Code 18,1030.
[13] See Convention on *Cybercrime CETS No. 185* at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG.
[14] Cisco, Cisco 2009 Annual Security Report: Highlighting *Global Security Threats and Trends*, December 4, 2009.
[15] D. J. Bodeau, R. Graubart, and J. Fabius-Greene, "*Improving cyber security and mission assurance via cyber preparedness (Cyber Prep) Levels*," September 9, 2010.
[16] Audry Watters, *Read Write Cloud*, RWW Solution Series, 2010
[17] AmichaiShulan, Application DefenceCenter (ADC), AmichaRegu-larlyLectures, Security, 2011
[18] Booz Allen and Hamilton, Reports, "*Top Ten Cyber Security Trends for Financial Services*", 2012
[19] "Guarding the Castle Keep: Teaching with the Fortress Metaphor*," IEEE Security & Privacy*, May/June 2004, p. 69, available at http://ieeexplore.ieee.org/iel5/8013/29015/01306975.pdf.
[20] See Steve Burbeck's description at http://evolutionofcomputing.org/Multicellular/ApoptosisInComputing.html
[21] Anju P Rajan Mathew1, A. Ajilaylwin2 & Shaileshwari M, *Cyber Security Solutions For Dlms Meters Using Gsm/Gprs Technology* ,U3 1&2 Department Of Cse, *The Oxford College Of Engineering, Bangalore*3engineering Officer Grade 2, Central Power Research Institute, Bangalore, India
[22] Ajith Abraham1, Crina Grosan2, Yuehui Chen3, *Cyber Security and the Evolution of Intrusion Detection Systems*, School of Computer Science and Engineering, *Chung-Ang University*, Korea 2Department of Computer Science Babes-Bolyai University, Cluj-Napoca, 3400, Romania 3School of Information Science and Engineering Jinan University, Jinan 250022, P.R.China
[23] Denning D., An Intrusion-Detection Model, *IEEE Transactions on Software Engineering, Vol. SE-13, No. 2, pp.222-232, 1987.*