# **Cyber Security**

**Dhirodatta Subba** is an Assistant Professor and Head, Department of Computer Science and Application, Salesian College, Siliguri Campus. He obtained his M. Sc (Mathematics) and M. Tech (Computer Science and Data Processing) from IIT Kharagpur. He worked with Tata Consultancy Services for many years before joining the College. He is associated with editing of the Salesian Journal of Humanities & Social Sciences.

#### Abstract

The growth of Internet Technology has brought huge benefits to mankind. However, new and more complex issues have arrived: cyber crime, cyber terrorism, cyber espionage, cyber war. The subject that deals with the preventive aspect of handling these issues is Cyber Security. It requires an army of trained professionals to make the country safe from these threats. Due to its importance, University Grants Commission (UGC) has mandated that the subject be taught in the institutes of higher education. It is a vast subject, and in this article effort has been made to introduce it in brief with some basic information regarding sources of threat, forms of cyber attack and elements of cyber security.

Keywords: Cyber security, Cyber space, Cyber espionage, Cyber war, CERT-In.

## Introduction

In the recent past we have witnessed some events which are worth mentioning. The first one is about Iran's nuclear program. Many countries in the world had been watching the development with concern as Tehran was determined on producing weapons-grade uranium. The stated intention about the program was for medical research. In his retirement speech to the Israeli Knesset Foreign Affairs and Defense Committee on January 7, 2011, Mossad Chief Meir Dagan stated that Iran would not be able to produce a viable nuclear weapon before 2015. He elaborated that Iran is still far from being capable of producing nuclear weapons and that a series of malfunctions and failures had set the Iranian nuclear weapons program back by several years.<sup>1</sup> Meanwhile, from around June 2010, rumor about Stuxnet, a computer worm, believed to have originated in Israel, was doing the rounds in international media. It made its way into the computers of Iran's nuclear facilities via the laptops used by engineers. The worm first reached the laptops through internet.

It knew exactly what to do. It did not make the control systems go haywire or stop the machines abruptly, which might have caused suspicion. It just tweaked the controls so as to make the centrifuge yield very little without going defunct. It is said to have increased the speed in order to damage the spindle in the machines over a period of time. The centrifuge

machines, during the productive period, worked so inefficiently that they hardly enriched any uranium quantity before going out of order.<sup>2</sup>

Another one that hit the news headlines in April 2010:

Unidentified hackers based in China systematically penetrated computers in sensitive Indian government offices, including the National Security Council Secretariat, electronically stealing documents on Maoists, missiles, and personal and financial information on Indian officials.<sup>3</sup>

Further back, in 2008 South Ossetia war, Russia's initial attack on Georgian soil was preceded by a synchronized cyber attack that crippled Georgian government websites.<sup>4</sup>

These examples give us a sense of how the present and the future looks when we are dealing with the age old issues of conflicts or power game. Cyber world is known as the 'fifth front' by people involved in defense - others being land, air, sea and space. The use of cyberspace depends on physical facilities like undersea cables, microwave and optical fibre networks, telecom exchanges, routers, data servers, and so on.

#### Sources of Threat

Some of the known sources are as follows:

## • Insider Threat

The disgruntled insider is a potential perpetrator of computer crimes. Insiders do have unrestricted access to the system/s; so, they could damage it or steal data for personal gain.

## • Criminal Groups

Criminal groups are increasingly using cyber intrusions, attacking systems for purposes of monetary gain. They are responsible for extortion, credit card frauds, tricking employees into giving up their log-in and password information (identity theft) which they use to break into target systems and vandalize them. They are making use of social media sites to gather intelligence about companies to achieve this objective. They are also using innovative techniques through 'spam', 'phishing' and 'vishing' to steal sensitive user information.

<sup>2</sup> URL: http://www.telegraphindia.com/1120216/jsp/opinion/ story\_15137785.jsp#.UWV\_96I9GxA (accessed on 14/Apr/2013)

<sup>3</sup> URL: http://www.telegraphindia.com/1100407/jsp/frontpage/ story\_12311784.jsp (accessed on 14/ Apr/2013)

<sup>4</sup> URL: http://www.crn.com/news/security/210003057/russian-cyberattacks- shut-down-georgian-websites. htm (accessed on 14/Apr/2013)

## • Malware Developers

Malware (Virus, Worm, Trojan) developers can do more damage to networks than hackers do. Malware attacks are also being launched from social media sites such as Facebook or LinkedIn.

## • Foreign Intelligence Services

Cyber espionage is the practice of using information technology to obtain secret information without permission from its owners or holders. Foreign intelligence services are actively using cyber tools as part of their information gathering and espionage tradecraft; target being sensitive government and private sector information for the purpose of gaining strategic, economic, political, or military advantage. The theft of innovations which are the fruits of costly investments in research and development is an immense strategic and economic loss to the targets.

## • Foreign Military

Although cyber war is not so lethal in the sense of human loss or property destruction, the consequences could be equally severe, especially, if the level of automation is high in the country as the system of governance as well as business and industry could be brought down to a state of total collapse, even if temporarily.

## Terrorists

Terrorists are known to use information technology and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely. There are reasons to expect terrorists to use cyber attacks to disrupt critical systems in order to harm targeted government or civilian populations. The knowledge of making bombs, lethal weapons, and even weapons of mass destruction (WMD) are freely available in the internet.

## • "Hacktivists"

Politically motivated attacks on publicly accessible web pages or email servers. Groups and individuals seek to overload email servers and to hack into web sites in order to send a political message. While these attacks generally have not altered operating systems or networks, they still damage services, and by denying the public access to websites containing valuable information, they infringe on others' right to communicate.

## • "Recreational" Hackers

Virtually every day there is another report about "recreational hackers" or "crackers" who penetrate networks for the thrill of it or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill and

computer knowledge, the recreational hacker can now download attack scripts and protocols from the World Wide Web and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. These types of hacks are numerous and may appear on their face to be benign, but they can have serious consequences.

## Forms of Cyber Attack

Following are the commonly found techniques:

## • Hacking

It is a generic term used for any kind of unauthorized access to a computer or a network of computers. Some technologies like packet sniffing, tempest attack, password cracking and buffer outflow facilitates hacking.

# • Web Defacements and Semantic Attacks

Website defacements are the most common form of politically motivated cyber attack. The most serious consequences of web defacements result from "semantic attacks," which change the content of a web page subtly, so that the alteration is not immediately apparent. As a result, false information is disseminated.

## • Domain Name Server (DNS) Attacks

Computers connected to the Internet communicate with one another using Internet Protocol (IP) addresses. Computers consult domain name servers (DNS) to map the name of a website (e.g. xyz.com) to its numerical IP address (64.12.50.153). If the DNS provides an incorrect numerical address for the desired website, then the user will be connected to the incorrect server, often without the user's knowledge. A DNS attack can thus be used to disseminate false information or to block access to the original website.

# • Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service attacks subject web and email servers to overwhelming numbers of communications from other computers. The high volume of communications can slow or crash the target system. Hackers often multiply the force of their DDoS attacks by using malicious code to take control of other users' machines and using these "zombie" machines to send additional communications to targeted servers. The hijacked computers are also called 'botnets'.

# • Syntactic Attacks using Malicious Code

Worms, Viruses, and Trojan horses are types of malicious code. The computer infrastructure is damaged by modifying the logic of the system in order to introduce

delay or make the system unpredictable. It is a cost-effective way to significantly disrupt the information infrastructure. Malware is getting smarter and has evolved from simple code that can be identified by its signature to one that can change its signature, making it very difficult to detect. Major commercial anti?virus programs are not always able to identify them.

## • Exploitation of Routing Vulnerabilities

Routers are the "air traffic controllers" of the Internet, ensuring that information, in the form of packets, gets from source to destination. Routing disruptions from malicious activity have been rare; but the lack of diversity in router operating systems leaves open the possibility of a massive routing attack. The malicious reprogramming of even one router could lead to errors throughout the Internet.

## • SQL Injection Attack

SQL (Structured Query Language) is the language of computer database. Whenever one fills out a form to purchase a product through a website, the entries are translated into SQL and entered into a database. If a particular web form has been poorly designed, an attacker can enter information to trick the database into revealing information it was not intended to, for example, vast customer lists including email addresses and credit card information.

## • Defamation

E-mails could be used for spreading disinformation, threats and defamatory elements. Similarly, social networking sites could be used.

## • Use of Cryptology

Financial institutions and governments have been using encryption for secure data transmission. But the availability of high frequency encrypted voice/data links has made the task of tracking communications by bad elements and terrorists difficult. It is a herculean task to decrypt the information being exchanged.

## • Compound Attacks

By combining methods, hackers could launch an even more destructive attack. Politically-motivated hackers will seek to attack high-value targets, including networks, servers, or routers whose disruption would have symbolic, financial, political or tactical consequences.

## What is Cyber Security?

"Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access."<sup>5</sup>

"Cyber security involves protecting information and systems from major cyber threats, such as cyber terrorism, cyber warfare, and cyber espionage. In their most disruptive form, cyber threats take aim at secret, political, military, or infrastructural assets of a nation, or its people."<sup>6</sup>

## **Elements of Cyber Security**

The following are the general characteristics of cyber security framework:

# **Application Security**

It is the use of software, hardware, and procedural methods to protect applications from external threats. Following are some examples:

- Application firewall that limits the execution of files or the handling of data by specific installed programs
- Anti-virus software
- Spyware detection/removal programs
- Configuration and patch management
- Following security protocols for Web applications during development
- Performing hostile security test

This involves breaking into own system through the web application - simulated attack.

Penetration tests

These are regular scans for vulnerabilities which can uncover problems and make one aware of software that needs to be patched. Thorough scans can be performed by third party consultants like Qualys, or with use of software like.

## Information security

- User access authorization
- Encryption/decryption programs
- Database logs

5 URL: http://whatis.techtarget.com/definition/cybersecurity (accessed on 11/Apr/2013).

6 URL: http://www.paloaltonetworks.com/community/learning-center/ what-is-cyber-security.html (accessed on 11/Apr/2013).

- Auditing process
- Web Application Firewall (WAF) This new breed of firewall watches for attack signatures and stops them before they reach the application. It comes either as an appliance, made by companies like Imperva or Barracuda Networks, or as a cloud-based service, like CloudFlare.

#### Network security

- A router that can prevent the IP address of an individual computer from being directly visible on the Internet
- Conventional firewalls
- Network security monitoring for detection and prevention of intrusions
- Auditing process

## Disaster recovery / business continuity planning

• One possibility is that of moving some of the infrastructure to the cloud for its ability for network resources to scale elastically in order to mitigate the attacks. Google's AppEngine, Amazon's EC2, RackSpace's Cloud, CloudFlare - they have the infrastructure in place to continue to run even under what would be a withering attack to a traditionally hosted site. This approach allows sites to use only the resources they need under normal conditions, but still not be overwhelmed when an attack occurs.

## **End-user education**

- Insuring all employees/users, not just the IT staff, are aware of safe computing practices by way of training, newsletters, posters and simulations.
- Introducing the subject in regular courses of academic and engineering institutes so students get the knowledge early on.

## **Issues Involved**

Following are some of the key issues:

• Complications associated with cross-border law enforcement

A typical cyber investigation can involve target sites in multiple states or countries, and can require tracing an evidentiary trail that crosses numerous state and international boundaries. Moreover, attribution and identification is extremely difficult as identities of the perpetrator can be easily masked, making it easy for the possibility of denials.

• Slow realization Malware is getting smarter and has become very difficult to detect, even for major

commercial protection software. Often, cyber attacks are silent and go unnoticed for long periods.

- Lack of International Standard/convention With regard to Cyber attack, Cyber war, and appropriate countermeasures, till date there is no common convention agreed upon by all nations. Globally, the issues are still under debate.
- Constantly evolving nature of security risks

To deal with such environment, advisory organizations are promoting a more proactive and adaptive approach. In USA, for example, the National Institute of Standards and Technology (NIST, a unit of the Commerce Department, formerly known as the National Bureau of Standards), issued updated guidelines in its risk assessment framework that recommended a shift toward continuous monitoring and real-time assessments. International Organization for Standardization (ISO) has its own guideline. These guidelines are expatiated on in the NIST 8007 and ISO 270028 publications.

#### How are we doing?

On 9th June, 2000, our parliament passed the "IT Act 2000".<sup>9</sup> It addressed issues primarily related to electronic commerce. In 2008, Parliament passed amendments to the IT Act, with added emphasis on Cyber Terrorism and Cyber Crime, with a number of amendments to existing sections and the addition of new sections, taking into account cyber threats. Further actions include the passing of rules such as the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 under the umbrella of the IT Act.

Indian Computer Emergency Response Team (CERT-In): CERT-In is the most important constituent of India's cyber community. It is modeled along similar agencies in the Western countries. Its mandate states, '*ensure security of cyber space in the country by enhancing the security communications and information infrastructure, through proactive action and effective collaboration aimed at security incident prevention and response and security assurance*'.

Under the IT Amendment Act 2008, only CERT-In is mandated to serve as the national agency in charge of cyber security. The Act also provided for a national nodal agency for protection of CII (Critical Information Infrastructure).

<sup>7</sup> URL: http://www.itl.nist.gov/lab/specpubs/sp800.htm (accessed on 14/Apr/2013).

<sup>8</sup> URL: http://www.iso27001security.com/html/27032.html (accessed on 14/Apr/2013).

<sup>9</sup> URL: http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf (accessed on 15/Apr/2013).

As for National Policy on cyber security, the Department of Information Technology issued a discussion draft on National Cyber Security Policy<sup>10</sup> on 26th March 2011, and invited comments on it. Among the publicly available feedbacks are following:

- Observations from Takshashila Institution were provided back in May 2011.<sup>11</sup> It contained many suggestions for improvement.
- Institute for Defense Studies and Analysis (IDSA) has done a thorough job of assessing the cyber security challenges facing the country in the study report. It includes some feedback by way of references to the original document.<sup>12</sup> It recommends setting up of a central command for handling cyber war, as it is considered to be the fifth front.
- Data Security Council of India (DISC), setup as an independent Self-Regulatory Organization (SRO) by NASSCOM®, to promote data protection, develop security and privacy best practices & standards and encourage the Indian industries to implement the same, has presented its viewpoint from the Industry perspective: "While CERT-In is doing an excellent job in the government sector, same needs to be replicated for the private sector through establishment of appropriate agencies within each of the identified private sectors, that co-ordinate with CERT-In and / or National Nodal Center that may be created. DSCI feels that in this policy, there should be a recommendation for establishment of National Nodal Center, which will co-ordinate the efforts of both the public and private sectors and will also assign roles and responsibilities."<sup>13</sup>
- Dr. Marri Channa Reddy Human Resource Development Institute of Andhra Pradesh also provided some input. Table A in the next page is a summary of procedural recommendations at four levels: Country, Network, Corporation and User.

Chart-1 (page 69) in the following section is a representation of government organizations that would work in collaboration with one another, as proposed in the draft security document.

Department of Electronics and Information Technology initiated the Legal framework.<sup>14</sup>Many other entities are involved in the work.<sup>15</sup>

13 DSCI Comments on National Security Policy\_Final.pdf, URL: http://www.dsci.in/taxonomy/term/591 (accessed on 15/Apr/2013).

14 URL: http://deity.gov.in/content/cyber-laws (accessed on 15/Apr/2013).

15 URL: http://www.cyberlawsindia.net/; http://www.caaa.in/Image/cyber%20laws%200verview.pdf (accessed on 15/ Apr/2013).

<sup>10</sup> URL: http://www.mit.gov.in/sites/upload\_files/dit/files/ncsp\_060411.pdf(accessed on 15/Apr/2013).

<sup>11</sup> URL: http://www.takshashila.org.in/wp-content/uploads/2010/03/TPACyberSecurity-RJSKN-1.pdf (accessed on 15/Apr/2013).

<sup>12</sup> IDSA, IDSA Task Force Report, 2012. URL: http://idsa.in/system/files/book\_indiacybersecurity.pdf (accessed on 15/Apr/2013).

<ul> <li>Policy directives on data security bast</li> <li>Policy directives con data security bast</li> <li>Privacy protection - Compliance, Bablinkow, B</li></ul>		Country	Network		Corporate		User
privacy protection - Compliance, Ibilities and distribution         protection (compliance, information)         protection (compliance)         processes (cold)         processes (cold)         processes         production (cold)         recensity of matrices           1. Information Technology Act 2000)         Standards and guidelines for compliance (ex EOS 2001, Sc ERI)         BOS 20001, Sc ERI (SS 2000), Sc ERI (	•	Policy directives on data security and	Compliance to security best	•	Compliance to security best	•	Maintain a
Ibilities and conformation         conformation (second)         Exactive dealing with malicious activities, protection, activities, protecting, average and updares f5LAS)         (BO 2000) and service level activities, protecting, average activities, protecting, average and updares f5LAS)         (Bo conting and activities, protecting, average and updare strengular malicious activities, ensuring activities, protecting, average and activities, protecting, average and activities, protecting, average and activities, protecting, average and activities, protecting, and activities, protecting, average and activities, average and users. by way of activities, protecting, average and users, by way of activities, average and users, by way of activity activities, and average and users, by way of activity activities, average and users, by way of activity activities, and average and users, by way of activity activities, and activities, and activi		privacy protection - Compliance,	practices (ex.		practices (ex. ISO27001.		level of awareness
Information         Technology Art 2000         (ISO 2000) and service level         activities, protecting average         protection.           • Brandards and updateness for compliance (ex: ISO 27001, ISO 20001, ISO 2000		liabilities and enforcement (e.g.	ISO27001), service quality	•	Pro-active dealing with malicious		necessary for self-
<ul> <li>Standards and guidelines for compliance (or: SO 2000; &amp; CERT)</li> <li>Pro-active actions to deal with mained activities, ensuing and infrastructure (enabling and endorsement infrastructure (enabling and endorsement)</li> <li>Conformity assessment infrastructure (enabling and endorsement)</li> <li>Conformity assessment infrastructure (enabling and endorsement)</li> <li>Conformity assessment infrastructure (enabling and endorsement)</li> <li>Security manpower - CISA, CISSP, ISNS-1A, monitoring, controls and value activities, accounting motioning, protecting and infrastructure (enabling and endorsement activities, accounting motioning, protecting</li> <li>Security manpower - CISA, CISSP, ISNS-1A, monitoring, routing and and value endorsement activities, intervals.</li> <li>Security manpower - CISA, CISSP, ISNS-1A, monitoring, routing and and value endorsement activities, intervals.</li> <li>Security manpower - CISA, CISSP, ISNS-1A, monitoring, routing and and value endorsement activities, intervals.</li> <li>Security manpower - CISA, CISSP, ISNS-1A, monitoring, routing and and value endorsement activities, intervals.</li> <li>Security incluent - early warning and and value endorsement activities, intervals.</li> <li>Information sharing and cooperation and and crisis management)</li> <li>Information sharing and cooperation with neutricons and and crisis management)</li> <li>Information sharing and cooperation on the net by woy of net traffic montoring.</li> <li>Rescurity resonand activities and security formes.</li> <li>Information sharing and cooperation with malicious activities, including prompt actions on the net by woy of net traffic montoring.</li> <li>Rescurity resonand activities and security formes.</li> <li>Rescurity resonand activities and security formes.</li> <li>Rescurity resonand activities and security formes.</li> <li>Security resonand activities and excurtises.</li> <li>Security research and development a</li></ul>		Information Technology Act 2000)	(ISO 20001) and service level		activities, protecting average		protection.
compliance (ex: ISO 27001, ISO 20001 & CIRT-1Pre-active actions to deal with his guidelinemonitoring, routing and quality observices and protectingPre-active actions to deal with gateway controlsand update at regular intervals.conformity assessment infristucture (enabling and endorsement actions concerning security product - ISO 15:40% security product - ISOPro-active actions to deal with protectingPro-active actions to deal with protectingPro-active actions gateway controlsPro-active actions gateway controlsPro-active actions protectingPro-active actions pro-activePro-active actions pro-activePro-active actions pro-actionPro-active actions pro-activePro-active actions pro-activePro-active actions pro-activePro-active actions pro-activePro-active actions pro-active15.40% security process - 150 Z7001 and security incident - activy management)Pro-active actions pro-actionsPro-active actions pro-actionsPro-active actions pro-actionsPro-active active active pristalis15.40% security process - 150 Z7001 and security incident - active with actionsPro-active active active pro-activePro-active active active pro-activePro-active active active pristalisPro-active active pristalis15.40% security procesFradi	•	Standards and guidelines for	agreements (SLAs).		end users by way of net traffic	•	Use legal software
In guidelines)         malicious activities, ensuring intrastructure (enabling and endorsement actions concerning security product - ISO         malicious activities, ensuring quality of services and protecting         malicious activities, ensuring protecting         intervals, keeping up-to-date with security         heaves of security prifialis           1540s, security product - ISO         1540s, security product - ISO         aveage end users by way of advoit on the net traffic         recently improved and vulnerability management)         beware of security withis on the advoit on the net traffic         beware of security aveage end users by way of advoit on the net traffic         beware of security advoit on the advoit on the advoit on the net traffic         beware of security advoit on the advoit on t		compliance (ex: ISO 27001, ISO 20001 & CERT-	Pro-active actions to deal with		monitoring, routing and		and update at regular
<ul> <li>Conformity assessment</li> <li>Conformity assessment</li> <li>infrastructure (enabling and endorsement actions concenting security product -ISO</li> <li>Disk security process -ISO-Z001 and actions concenting security product -ISO</li> <li>Disk security process -ISO-Z001 and security mappower - CISA-CISSP ISMS-LA.</li> <li>Disk security process -ISO-Z001 and security mappower - CISA-CISSP ISMS-LA.</li> <li>Disk sect,</li> <li>Disk security incident - early warning and security incident - early warning and activities,</li> <li>Security incident - early warning and activities,</li> <li>Information sharing and cooperation with and crisis management)</li> <li>Information sharing and cooperation and crisis management)</li> <li>Information sharing and cooperation with an activities,</li> <li>Pro-active dealing with malicious activities,</li> <li>Pro-active dealing with malicious activities,</li> <li>Information sharing and cooperation with law routing and gateway controls</li> <li>Information a security forums).</li> <li>Centoring and gateway controls</li> <li>Information a security forums).</li> <li>Nation - wide security avareness</li> <li>Centry tack interprises and sile of personnel engaged in activities.</li> <li>Nation - wide security awareness</li> <li>Security research and securits</li> <li>Nation - wide security awareness</li> <li>Security and securits</li> <li>Security and securits</li> <li>Security and securits</li> <li>Security awarenes</li> <li>Centor and securits</li> <li>Security research and secures</li></ul>		In guidelines)	malicious activities, ensuring		gateway controls		intervals.
infrastructure (enabling and endorsement actions concerning security product - ISO 1560, security product - ISO     protecting actions concerning security product - ISO     protecting actions concerning security product - ISO     pitfalls       1560, security process - ISO 27001 and security manpower - CISA, CISSP, ISMS-LA     monting and moting and vulnerability advisories     processes     (configuration, patch and vulnerability advisories       0155, Acto     Security incident - early warning and security incident - early warning and response (National cyber alert system and crisis management)     - Conformation to legal     technologies and advisories issued by CIRT-In.     to security advisories       016, 016, with veducts and owelds and or the net by way of net traffic and interceptions and activities, including prompt actions on and visior sissued by CIRT-In.     - Maintain reasonable advisories issued by CIRT-In.     and advisories issued by CIRT-In.     and advisories       00, 016, with veducts and or the net by way of net traffic monitoring, routing and gerway controls     - Conformation to legal     - Conformation of advisories issued by error resonce.     - Conformation of advisories issued by error resonce.     - Conformation of advisories     - Maintain resonces       010, 016, with veducts and services     - Conformation to legal     - Use of secure product advisories issued by error resonces     - Conformation to legal     - Conformation to legal       1     Pro-active dealing with malicious activities, including prompt actions on on the net by way of net traffic monitoring.     - Conformation to legal     - Conformation to le	•	Conformity assessment	quality of services and	•	Keeping up-to-date with security	•	Beware of security
actons concerning security product - ISOaverage end usersby way ofprocesses(configuration, patchwhile on the15408, security manyower - CISA, CISSP, 15MS-LA,monitoring andend valuereability management)net radificand valuereability management)net and adhereDISA etc.)Security manyower - CISA, CISSP, 15MS-LA,monitoring andobligations and cooperation withto security advisoriesDISA etc.)Suctivy manyower - CISA, CISSP, 15MS-LA,monitoring andobligations and cooperation withto security advisoriesDISA etc.)Suctivy management)- Conformation h logal- Conformation h logalto security advisoriesInformation sharing and corisis management)- Keeping up-to-date withlaw refreement activities,met and adhereand crisis management)- Information sharing and cooperation- Wille on themet and adhereand crisis management)- Information sharing and cooperation- Wille on themet and adhere(MoUs with vendors andoverseasConfiguration,- Wille on the advisories issued by CERT-In Mantain reasonable(MoUs with vendors andoverseas- Conformation to legal- Use of secure product and- Control opervent(MoUs with vendors andoverseas- Conformation, to legal- Conformation and- Conformation, advisories(MoUs with vendors and services and skilled manpower Conformation and- Conformation and- Conformation, advisories(MoUs with vendors and service and skilled manpower Conformation sharing aroutodic- Conforma		infrastructure (enabling and endorsement	protecting		technologies and		pitfalls
15408. security process - ISO 27001 and becurity manpower - CISA, CISSP, ISMS-I,A.     net traffic     and vulnerability management)     net and adhere       DISA etc.)     monitoring, routing and becurity incident - early warning and response (National Cyber alert system and crisis management)     - Conformation to logal     to security advisories and vulnerability advisories security technologies and and crisis management)     - Conformation to logal     to security advisories advisories issued by CERT-In.     net and adhere to security advisories       • MoUS with vendors and and crisis management)     - Reeping up-to-date with processes (onfiguation patch and vulnerability mad crisis management)     - Conformation to logal     - Maintain reasonable advisories issued by CERT-In.     net and adhere advisories issued by CERT-In.       • Thornation sharing and cooperation and crisis management)     - Use of secure product and advisories issued by CERT-In.     - Maintain reasonable advisories issued by CERT-In.     - Maintain reasonable advisories issued by CERT-In.       • Pro-active dealing with malicious activities, including prompt actions and the net by way of net traffic monitoring, routing and upgradation enforcement.     - Conformation to logal     - Crisis management advision advisories issued by roution the net by way of net traffic monitoring, roution and Law     - Conformation with law       • Nation- wide security awareness     - Nation- wide security awareness     - Use of secure product advisories issued by routices and services.     - Use of secure product advisories issued by routices and services.     - Use of secure product and visories issued by routice <th></th> <td>actions concerning security product - ISO</td> <td>average end users by way of</td> <th></th> <td>processes (configuration, patch</td> <td></td> <td>while on the</td>		actions concerning security product - ISO	average end users by way of		processes (configuration, patch		while on the
security marpower - CISA, CISSP, ISMS-LA,       monitoring, routing and <ul> <li>DISA etc.)</li> <li>DISA etc.)</li> <li>Security incident - early warning and</li> <li>DISA etc.)</li> <li>Security incident - early warning and</li> <li>Information sharing and cooperation</li> <li>Information starting and cooperation</li> <li>Pro-active dealing with malicious activities</li> <li>Pro-active dealing with malicious actions on</li> <li>Pro-active dealing with malicious actions on</li> <li>Pro-active dealing with malicious actions on</li> <li>Pro-active dealing with malicious and</li> <li>Pro-active dealing with malicious actions on</li> <li>Pro-active dealing with malicious activ</li></ul>		15408, security process - ISO 27001 and	net traffic		and vulnerability management)		net and adhere
DISA etc.)     Bistorial controls     obligations and cooperation with response (National cyber alert system and crisis management)     as a cooperation with response (National cyber alert system and crisis management)     as configuration, response (National cyber alert system and crisis management)     and crisis management)     and crisis management)     menforcement activities, necessary.       and crisis management)     patch and vulnerability technologies and and crisis management)     by enforcement activities, necessary.     mecessary.       and crisis management)     patch and vulnerability prompt actions on advisoris issued by CERT-In.     Maintain reasonable advisoris issued by CERT-In.     and       and crisis management)     patch and vulnerability including prompt actions on advisoris sucue by CERT-In.     Maintain reasonable advisoris issued by Care product and advisoris advisoris issued by Care product and advisoris issued by crisis management and advisoris issued by crisis management and advisoris advisoris issued by Care product and advisoris advisoris issued by crisis management and advisoris issued by crisis for personnel engaged in controls including prompt actions on the net by way of net traffic monitoring.     Nation- wide security is advisorial adviso		security manpower - CISA, CISSP, ISMS-LA,	monitoring, routing and	•	Conformation to legal		to security advisories
<ul> <li>Security incident - early warning and response (National cyber alert system and crisis management) response (National cyber alert system and crisis management)</li> <li>Information sharing and cooperation and vulnerability advisories issued by CERT-In.</li> <li>Information sharing and cooperation with and vulnerability</li> <li>CERTs and security forums).</li> <li>Control to legal overseas</li> <li>Pro-active dealing with malicious activities</li> <li>Provactive dealing with malicious activity acrees and skilled</li> <li>Provactive dealing with malici</li></ul>		DISA etc.)	gateway controls		obligations and cooperation with		as
response (National cyber alert systemsecurity technologies and and crisis management)including prompt actions on advisories issued by CERT-In.• Maintain reasonable and and• Information sharing and cooperation (MoUs with vendors and overseas (MoUs with vendors and overseas)patch and vulnerability advisories issued by CERT-In.• Maintain reasonable and advisories issued by CERT-In.• Maintain reasonable and• Information sharing and cooperation (MoUs with vendors and overseas)• Orio of secure product and advisories issued by restrices and skilled manpower.• Maintain reasonable advisories issued by crisis management and on the net by way of net traffic monitoring, routing and gateway controls• Conformation to legal on the net by way of net traffic monitoring, routing and gateway controls• Conformation to legal on the net by way of net traffic monitoring, routing and gateway controls• Conformation with law of skills for personnel engaged in advisories issued by of skills for personnel engaged in advisories issued by• Periodic training and upgradation of skills for personnel engaged in advisories issued by• Pro-active dealing advisories issued by of skills for personnel engaged in advisories issued by• Pro-active dealing advisories issued by activities• Pro-active dealing advisories issued by activities• Maintain reasonable advisories issued by activities• Maintain reasonable advisories issued by activities• Maintain reasonable advisories issued by activities• Maintain reasonable advisories issued by activities• Pro-active dealing advisories issued by activities• Maintain reasonable advisories issued by <br< th=""><th>•</th><td>Security incident - early warning and</td><td><ul> <li>Keeping up-to-date with</li> </ul></td><th></th><td>law enforcement activities,</td><td></td><td>necessary.</td></br<>	•	Security incident - early warning and	<ul> <li>Keeping up-to-date with</li> </ul>		law enforcement activities,		necessary.
and crisis management)       processes (configuration, link management)       advisories issued by CERT-In.       and         • Information sharing and cooperation       patch and vulnerability       • Use of secure product and trust-worthy access       management)         (MoUs with vendors and overseas       overseas       • Conformation to legal       • Use of secure product and trust-worthy access       trust-worthy access         (MoUs with vendors and overseas       • Conformation to legal       • Use of secure product and trust-worthy access       trust-worthy access         • Pro-active dealing with malicious activities       • Conformation to legal       • Crisis management and abuse of emergency response.       abuse of emergency response.         • Itawful interceptions and Law       obligations and ecurity awareness       • Providit training and upgradation       enforcement activities, of skills for personnel engaged in including prompt actions on ethorities, of skills for personnel engaged in including prompt actions on enforcement.       • Nation-wide security awareness       • Use of secure product       • Pronotion of acceptable users' computer resources         • Nation-wide security awareness       • Use of secure product       • Pronotion of acceptable users' point the interest of advisories issued by outside       • Pronotion of acceptable users' point device and skilled       • Pronotion of acceptable users' products and services.         • Security research and development       • Use of secure product       • Pronotion of acceptabl		response (National cyber alert system	security technologies and		including prompt actions on	•	Maintain reasonable
• Information sharing and cooperation       patch and vulnerability       • Use of secure product and       trust-worthy access         (MoUs with vendors and overseas       management)       estrvices and skilled manpower.       control to prevent         (MoUs with vendors and overseas       management)       • Conformation to legal       • Use of secure product and       trust-worthy access         • Pro-active dealing with malicious activities       • Conformation to legal       • Crisis management and       control to prevent         • Pro-active dealing with malicious activities       • Obligations and       • Periodic training and upgradation       computer resources         • Inviting and gateway controls       cooperation with law       • Periodic training and upgradation       emergency response.       computer resources         I awful interceptions and Law       enforcement activities,       • Periodic training and upgradation       of skills for personnel engaged in         I awful interceptions and Law       including prompt actions on       escurity related       advisories issued by       of skills for personnel engaged in         I awful interceptions and Law       including prompt actions on       security related       ecurity related         I awful interceptions and kendoment       of skills for personnel engaged in       security related       ecurity related         I awful interceptions and evelopment		and crisis management)	processes (configuration,		advisories issued by CERT-In.		and
(MoUs with vendors and overseas       management)       services and skilled manpower.       control to prevent         CERTs and security forums).       • Conformation to legal       • Crisis management and       abuse of         • Pro-active dealing with malicious activities       • Onformation to legal       • Crisis management and       abuse of         • Pro-active dealing with malicious activities       • Onformation to legal       • Crisis management and       abuse of         • Pro-active dealing with malicious activities       • Onformation to legal       • Crisis management and       abuse of         • on the net by way of net traffic monitoring,       cooperation with law       • Periodic training and upgradation       abuse of         • Invitul interceptions and Law       enforcement activities,       • Periodic training and upgradation       enforcement activities,         I awful interceptions and Law       advisories issued by       • Periodic training and upgradation       escurity related         • Nation- wide security       awareness       CERT-In.       • Promotion of acceptable users'       computer resources         • Security research and development       advisories issued by       activities       contoin of acceptable users'       contoin of acceptable users'         • Security research and development       and services and skilled       affe compution of acceptable users'       pelavior in	•	Information sharing and cooperation	patch and vulnerability	•	Use of secure product and		trust-worthy access
CERTs and security forums).•Conformation to legal•Crisis management andabuse of•Pro-active dealing with malicious activitiesobligations andemergency response.computer resourceson the net by way of net traffic monitoring,cooperation with lawePeriodic training and upgradationabuse ofrouting and gateway controlscooperation with lawePeriodic training and upgradationcomputer resourcesrouting and gateway controlsenforcement activities,ePeriodic training and upgradationcomputer resourcesI awful interceptions and Lawenforcement activities,of skills for personnel engaged insecurity relatedadvisories issued byI awful interceptions and Lawadvisories issued byactivitiesectivitiescomputer resourcesenforcement.Nation-wide security awarenessCERT-In.Promotion of acceptable users'behavior in the interest ofsecurity research and developmentand services and skilledsafe computing both within andproducts and services.enforcement andproducts and services.emergency response.outsideoutsideoutside		(MoUs with vendors and overseas	management)		services and skilled manpower.		control to prevent
•Pro-active dealing with malicious activitiesobligations andemergency response.computer resourceson the net by way of net traffic monitoring,cooperation with law•Periodic training and upgradationrouting and gateway controlsenforcement activities,of skills for personnel engaged incomputer resourcesLawful interceptions and Lawincluding prompt actions onescurity relatedcomputer resourcesI and interceptions and Lawadvisories issued byactivitiesof skills for personnel engaged inI and interceptions and Lawadvisories issued byactivitiesincluding prompt actions onI and interceptions and Lawadvisories issued byactivitiesincluding prompt actions onI and interceptions and Lawadvisories issued byactivitiesincluding prompt actions onI and interceptions and Lawbehavior in the interest ofbehavior in the interest ofI security research and developmentand services and skilledsafe computing both within andfocusing on tools, technology,products and services.outsideproducts and services.outsideoutsideproducts and servi		CERTs and security forums).	<ul> <li>Conformation to legal</li> </ul>	•	Crisis management and		abuse of
on the net by way of net traffic monitoring, routing and gateway controlscooperation with law• Periodic training and upgradationrouting and gateway controlsenforcement activities, including prompt actions on• Periodic training and upgradationLawful interceptions and Lawenforcement activities, including prompt actions on• Periodic training and upgradationI awful interceptions and Lawenforcement activities, advisories issued by activities• Promotion of skills for personnel engaged in security related• Nation-wide security awarenessCERT-In.• Promotion of acceptable users' behavior in the interest of safe computing both within and outside• Cusing on tools, technology, products and services.• Use of secure product and services.• Crisis management and outside• Crisis management and emergency response.• Outside• Outside	•	Pro-active dealing with malicious activities	obligations and		emergency response.		computer resources
routing and gateway controlsenforcement activities, including prompt actions on advisories issued byof skills for personnel engaged in security relatedLawful interceptions and Lawincluding prompt actions on advisories issued byof skills for personnel engaged in security relatedNation-wide securityadvisories issued by activitiesercivitiesNation-wide securityawarenessCERT-In.Nation-wide securityawarenessPromotion of acceptable users' behavior in the interest of safe computing both within and outsideProducts and services.end services and skilledbehavior in the interest of safe computing both within and outsideproducts and services.energency response.outside		on the net by way of net traffic monitoring,	cooperation with law	•	Periodic training and upgradation		
Lawful interceptions and Lawincluding prompt actions on advisories issued bysecurity relatedenforcement.advisories issued byactivities• Nation-wide security awarenessCERT-In.• Promotion of acceptable users'• Use of secure productbehavior in the interest of safe computing both within and outside• Crisis management and outside• Cusing on tools, technology, products and services.• Crisis management and emergency response.• Crisis management and		routing and gateway controls	enforcement activities,		of skills for personnel engaged in		
enforcement.advisories issued by activitiesactivities• Nation-wide security awareness campaign.• Promotion of acceptable users' behavior in the interest of safe computing both within and outside• Use of secure product behavior in the interest of safe computing both within and outside• Security research and development focusing on tools, technology, products and services.• Use of secure product and services and skilled outside• Promotion of acceptable users' behavior in the interest of safe computing both within and outside		Lawful interceptions and Law	including prompt actions on		security related		
<ul> <li>Nation-wide security awareness CERT-In.</li> <li>Nation-wide security awareness CERT-In.</li> <li>Use of secure product behavior in the interest of behavior in the interest of and services and skilled safe computing both within and focusing on tools, technology, manpower.</li> <li>Crisis management and encion of acceptable users'</li> </ul>		enforcement.	advisories issued by		activities		
campaign.• Use of secure productbehavior in the interest of• Security research and developmentand services and skilledsafe computing both within andfocusing on tools, technology,manpower.outsideproducts and services.• Crisis management andemergency response.	•	Nation- wide security awareness	CERT-In.	•	Promotion of acceptable users'		
• Security research and development         and services and skilled         safe computing both within and           focusing on tools, technology,         manpower.         outside           products and services.         • Crisis management and         emergency response.		campaign.	Use of secure product		behavior in the interest of		
focusing on tools, technology,     manpower.     outside       products and services.     • Crisis management and emergency response.	•	Security research and development	and services and skilled		safe computing both within and		
products and services.		focusing on tools, technology,	manpower.		outside		
emergency response.		products and services.	Crisis management and				
			emergency response.				

Salesian Journal of Humanities & Social Sciences, Vol. IV, No. 1 (May 2013) ISSN: 0976-1861 | DOI: 10.51818/SJHSS.04.2013.60-71 | Page No: 60-71 | Section: Article

Cyber Security | 69

Table : Actions At Different Levels



Chart 1: Stakeholders : Government Organisations

Thus the legal aspect is also getting refined with collaboration of different groups.

As of writing this article, final policy document has not been released; but the government, the industry, the academia and legal experts are converging, and it is expected to be available soon.

## Conclusion

More and more nations are realizing that their national security, as well as economic prosperity, will depend on their ability to protect themselves in cyber space (which includes the internet, wider telecommunications networks and computer systems). The complex nature of cyber space requires a multi-faceted approach involving a close partnership between Government, industry and academia for ensuring the security of information systems and assets of the country. While the government, the industry, the academia and the law schools are working on the multi-dimensional aspect of capacity building, national and international cooperation, research and development, education and awareness, issues relating to privacy and freedom of expression - we come to the humble realization that cyber security is everyone's responsibility, every contribution is important, though it may seem like a drop in the ocean.<sup>16</sup>

16 Recommended reading
1. URL: http://en.wikipedia.org/wiki/Cyber\_security\_standards
2. URL: http://www.denyall.com/company/
whitepaperrs\_en.html?gclid=CMCElrGF3bYCFU8a6wodNm4A\_Q
3. URL: https://www.prometric.com/en-us/clients/cybersecurity/Assets/
default.html?cshp
4. URL: http://www.cybersecurityindex.org/

5. URL: https://www.eff.org/cybersecurity