International Journal of Engineering Research & Management Technology

May- 2015 Volume 2, Issue-3
ISSN: 2348-4039

Email: editor@ijermt.org www.ijermt.org

"Sharpening Skills..... Serving Nation"

Special Issue: 2nd International Conference on Advanced Developments in Engineering and Technology
Held at Lord Krishna College of Engineering Ghaziabad, India

Cyber Security Issues in India

Mr. K K Dewan
Sr. Scientific Officer
Northern India Textile Research Association, Ghaziabad (India)

Mr. Partha Basu
PRO & Faculty of Management
Northern India Textile Research Association, Ghaziabad (India)

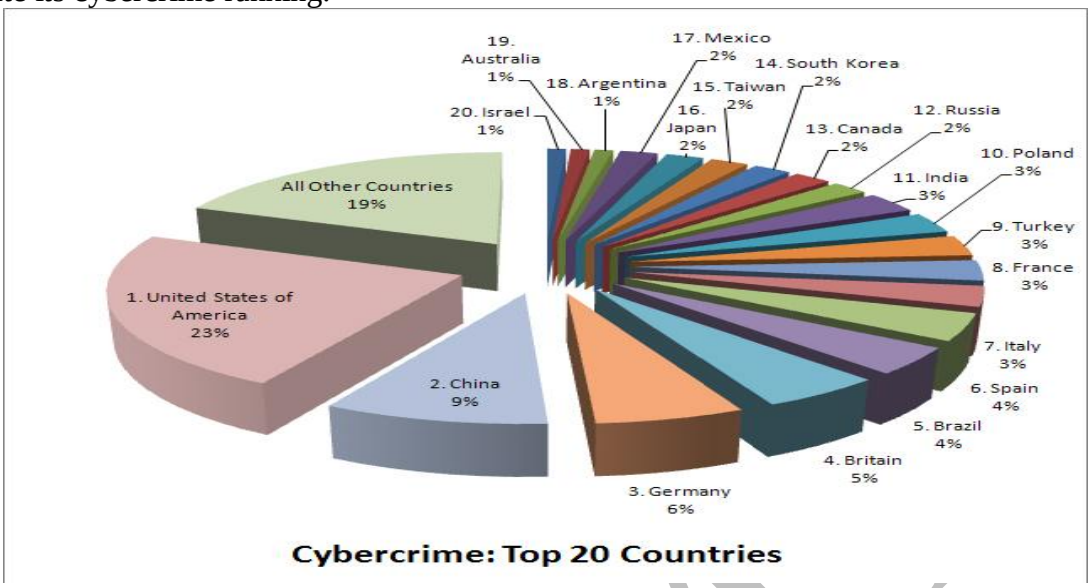
Dr. B. K. Sharma
Principal Scientific Officer & Head
Northern India Textile Research Association, Ghaziabad (India)

ABSTRACT
Cyber crime can be carried out by a host of people ranging between disgruntled employees, individual hacker, organized cybercrime syndicates to enemy government or an activist.Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.India is also not safe from these cyber-attacks as cyber security attacks ate global in nature. Experts believe that the Indian cyberspace must be protected on a priority basis. A massive cyber-espionage attack on both government and commercial computer systems in India, Britain, Germany, Australia, New Zealand, and the USA. Much of this cyber-crime feeds on cyber-carelessness. Companies underestimate the risk. People may not be fully aware - or just careless - about protecting their private data. Against these threats the Government will need to take aggressive, intelligent and persistent action. This action will need to be international, since this is a criminal market that recognizes no frontiers. It will need to be forward looking and imaginative, and extraordinarily flexible in the face of rapid change.

Keywords: Cyber Attacks, Cyber Security, Cyber Space, Cyber Crimes, Cyber Security Policy.

INTRODUCTION
The first cybercrime was noted in 1820 by Joseph-Marie Jacquard, a textile manufacturer in France which produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology.Cyber-attacks can be carried out by a host of people ranging between disgruntled employees, individual hacker, organized cybercrime syndicates to enemy government or an activist.Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber-attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. Strategic decisions taken at the highest level of State in recent years have made cyber security a priority for Indian government action. India reviewed its defense and national security policy in great depth at the time of the 2002, and new priorities were identified and approved by the Parliament. Preventing and responding to cyber-attack was identified as one of the key priorities in the organization of national security.
The reality is that there are no easy or perfect answers to this challenge. Cyber security as an issue is too broad, there are too many devices being connected to the internet that have variable security, too many

vulnerabilities in hardware and software, the rate of change in technology is too great, and actors with ill intent only need to be successful once while defenders of cyber security have to be successful all of the time. In 2014, cyber-attacks and data breaches don't look like they're going to slow down. We've seen high-end data breaches of large companies, with data, personal records and financial information stolen and sold on the black market in a matter of days. Each country lists 6 contributing factors, share of malicious computer activity, malicious code rank, spam zombies rank, phishing web site hosts rank, bot rank and attack origin, to substantiate its cybercrime ranking.



(Source by: Business Week/Symantec)

The Indian Cyberspace

Government's cyber security arm Computer Emergency Response Team-India (CERT-In) reported 62,189 cyber security incidents in the first five months of the current calendar year. Similarly, the government body reported that 9,174 Indian websites were hacked by groups spread across the world. "During the years 2011, 2012, 2013 and 2014 (till May), a total number of 21,699, 27,605, 28,481 and 9,174 Indian websites were hacked by various hacker groups spread across worldwide. In addition, during these years, a total number of 13,301, 22,060,71,780 and 62,189 security incidents, respectively, were reported to the CERT-In,"

These incidents include phishing, scanning, spam, malicious code and website intrusions; there have been attempts from time to time to launch cyber-attacks on Indian cyber space. "These attacks have been observed to be originating from the cyber space of a number of countries including the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE," It has been observed that the attackers compromise computer systems located in different parts of the world and user masquerading techniques and hidden servers to hide the identity of the actual system from which the attacks are being launched. "Cyber space is virtual, borderless and anonymous due to which it becomes difficult to actually trace the origin of a cyber-attack. With the increase in the proliferation of IT and related services there is a rise in the number of cybercrime and cyber security incidents. The trend in increase in cybercrime incidents is similar to that worldwide. "As per the cybercrime data maintained by National Cyber Records. Bureau, a total of 1,791, 2,876 and 4,356 cybercrime cases were registered under Information Technology Act during the year 2011, 2012 and 1013, respectively, thereby showing an increasing trend," he added. A total of 422, 601 and 1,337 cases were registered under cybercrimerelated sections of the Indian Penal Code (IPC) during the year 2011, 2012 and 2013, respectively.

National Security Policy

The cyber security challenges which have significantly contributed to the creation of a platform that IS now capable of supporting and sustaining the efforts in securing the cyber space. Due to the dynamic nature of cyberspace, there is now a need for these actions to be unified under a National Cyber Security Policy,

with an integrated vision and a set of sustained& coordinated strategies for Implementation.

Ministry of Communications and Information Technology Govt. of India define following objectives of the sated policy:

1. To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
2. To create an assurance framework for design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
3. To improve visibility of integrity of ICT products and services by establishing infrastructure for testing and validation of security of such product.
4. To provide fiscal benefit to businesses for adoption of standard security practices and processes.
5. To enable Protection of information while in process, handling, storage and transit so as to safeguard privacy of citizen's data and reducing economic losses due to cybercrime or data theft.
6. To enable effective prevention, investigation and prosecution of cybercrime andenhancement of low enforcement capabilities through appropriate legislative intervention.

Existing Counter Cyber Security Initiatives

National Informatics Centre (NIC)

National Informatics Centre (NIC) was established in 1976, and has since emerged as a "prime builder" of e-Government / E-Govemance applications up to the grassroots level as well as a promoter of digital opportunities for sustainable development. NIC, through its ICT Network, "NICNET",has institutional linkages with all the Ministries /Departments of the Central Government, 35 State Governments/ Union Territories, and about 625 District administrations of India.

NIC has set up state-of-the-art ICT infrastructure consisting of National and state Data Centers to manage the information systems and websites of Central Ministries/Departments, Disaster Recovery Centers, Network Operations facility to manage heterogeneous networks spread across Bhawans, States and Districts, Certifying Authority, Video-Conferencing and capacity building across the country. National Knowledge Network (NKN) has been set up to connect institutions/organizations carrying out research and development, Higher Education and Governance with speed of the order of multi Gigabits per second. Further, State Government secretariats are connected to the Central Government by very high speed links on Optical Fiber Cable (OFC). Districts are connected to respective State capitals through leased lines.

Indian Computer Emergency Response Team (Cert-ln).

Is the Government organization under Ministry of Communications and Information Technology? It is a nodal agency that deals with cyber security threats like hacking and phishing.

It strengthens security-related defense of the Indian Internet domain. In March 2014, CERT reported a critical flaw in Android Jelly bean's VPN implementation.

In December 2013, CERT reported there was a rise in the cyber-attacks on Government organizations like banking and finance, oil and gas and emergency services. It issued a list of security guidelines to all critical departments.

National Information Security Assurance Programme (NISAP). This is for Government and critical infrastructures, Highlights are:-

- Government and critical infrastructures should have a security policy and create a point of contact.
- Mandatory for organizations to implement security control and report any security incident to Cert-ln.
- Cert-ln to create a panel of auditor for IT security.
- All organizations to be subject to a third party audit from this panel once a year.
- Cert-ln to be reported about security compliance on periodic basis by the organizations.

Challenges and Concerns

Lack of awareness

Lack of awareness of information security threats at board level, causing organizations to fail to provide reassurance that they are meeting their information security responsibilities and cost effectively managing information and cyber threats.

More Prominence on Data Destruction

Cybercriminals are in search of finding loopholes in enterprise data online. As pointed out by Websense, this trend shall continue, where hackers compromise on data, they breach it and ask for money in return. So, all the enterprises be warned! A silly-looking malware could cost you millions.

Smartphone's -a Paradise for hackers

Whether your smartphone is white, black or gold, it is now almost 30 times more valuable per ounce than a block of solid silver -and almost as easy to convert discreetly into cash. The revolution that Android made has opened doors for hackers now. We use our smartphones not just for mails and chat but online purchases, internet banking and connecting to your workgroup have become some of the primary uses.

The Cloud Computing

Greatest cloud computing security risk is account or service traffic hijacking. Cloud computing adds a new threat to this landscape. If an attacker gains access to your credentials, he or she can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. "Your account or services instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks,"

Up gradation of OS

Certain statistics say that more than 75% of the Chinese computers rely on these old operating systems. Over the past years we have seen a lot of cyber threats on Windows XP. The best solution is either to upgrade or migrate to a new operating system, say windows 8. Most of the local banking solutions still rely on this OS which won't prove to be a good idea soon.

RECOMMENDATIONS

Be aware of your risks and put foundations into place: Identify key risks, vulnerabilities and critical information assets; implement basic controls and proactively manage information risks

Embrace Technology: Ensure that the security technology infrastructure includes comprehensive threat intelligence, risk and behavioral analytics, and robust, resilient and automatic threat protection Establish a public- private architecture for responding to national- level cyber incidents. Network below the radar. Public profiles on social networking sites put you at risk by exposing information, such as your full birth date, hometown, employment history, etc., that a criminal could use to pose as you. Use privacy settings to ensure your personal information isn't public knowledge.

More investment in this field in the term of Research & Development National awareness programs such as National Information Security Assurance Program (NISAP) needs to be promoted. Amendment in the Cyber policy time to time to make the Law more strengthen.

CONCLUSION

Cyber security in India is in a poor condition. Cyber security of financial transaction in India is also required to be strengthened. In the absence of appropriate skills development and modernization of law enforcement agencies of India, police force are finding it really difficult to solve technology related crimes. Further, cyber security of sensitive databases like National Identity Cards would also require strong privacy protection and cyber security compliances.

India is also not safe from these cyber-attacks as cyber security attacks ate global in nature. Experts believe that the Indian cyberspace must be protected on a priority basis. This would not be an easy task as the new

government has received a paralyzed cyber security infrastructure in India in heritage. Further, cyber security skills development is also missing in India and we do not have the appropriate cyber professionals to deal with sophisticated cyber-attacks. The cyberspace is becoming important area for large number of terrorists to attack on crucial information infrastructure. The existing laws are inefficient to restrain the cybercrimes and, thus urging a need to modify the existing laws through which these activities can be put on a check. There is a need of international cooperation of nations to crack down the efficiency on cybercrime, thereby ensuring a development of the internet cybercrime is not limited to states of boundaries, thus it requires a universal collaboration of nations to work together to reduce the ever growing threats and risk to a manageable level.

REFERENCE

1. Insider Attack and Cyber Security: Beyond the Hacker (Advances in Information Security) , by Salvatore Stolfo (Editor), Steven M. Bellovin (Editor), Angelos D. Keromytis (Editor), Sara Sinclair (Editor),
2. Cyber War: The Next Threat to National Security and What to Do About It by Richard A. Clarke (Author), Robert Knake (Author)
3. 10 Internet Security Predictions For 2015: Symantec
4. National Security Issues in Science, Law, and TechnologyThomas A. Johnson
5. Google.com
6. Wikipedia.com
7. Business week Symantec