International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

CYBER SECURITY IN DIGITAL ECONOMY

Shivani Grover [1]

Abstract

Nation Crime Record Bureau (NCRB) report shows the rapid increase in Cyber Crime in India by 50% from 2012 to 2013. As we move in 2016, cyber-attacks will continue to become more innovative and sophisticated. There have been several incidences of cybercrimes on corporate and individual level in the past few years. Putting the data of 1.2 billion people on the cloud could be risky and could threaten the security. Hence the Digital India project demands very strong network security at all levels of operation. It is undoubtedly one of the largest and most exciting initiatives that we have embarked upon in the last decade.

Keywords

Cyber, security, Digital India, Cybercrimes, cyber-attacks, e-governance

1. Assistant Professor (Computer Science) Swift Technical Campus, Ghaggar Sarai, Rajpura

Introduction

India is a very late starter as far as cyber security is concerned. The speed of cyber security initiative of India is still very slow. Further, there is no dedicated cyber security law of India that can be used in cases of cyber-crimes, cyber-attacks and cyber contraventions. The information technology act, 2000 is ill suited to take care of the cyber security related issues in India.

"I dream of a Digital India where cyber security becomes an integral part of our national security... The world is so worried about cyber security. One click can change a lot of things," said Prime Minister Narendra Modi at the launch of Digital India Week on July 1, 2015.

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

These words could not have come at a more appropriate time, for national security, enterprise security and individual privacy were never at risk as they are now with the world going more digital every passing day. This is precisely why security needs to be at the heart of the Digital India vision.

Digital India

'Digital India' aims to transform India into a 'digitally empowered society and knowledge economy' India is trying to implement the Digital India project to the best of its capabilities. The success of Digital India project would depend upon maximum connectivity with minimum cyber security risks. The Digital India initiative seeks to transform the country into a connected economy and it can be successful only when the security of the connected devices is assured. The Digital India concept involves so many different technologies communicating with each other in so many ways. The only way to predict and eliminate all possible security issues is by embedding security from the planning to the actual implementation of digital technologies along with strict compliance with the cybersecurity policy. This includes privacy protection, data protection and adherence to cyber laws. With the Digital India initiative, a lot of data will be collected by different bodies and this needs to be protected.

With growing digitization, the landscape for potential cyber security threats will also grow. Therefore, if security is not addressed early on, it could make the program difficult to achieve the real goal. When building the foundation of a Digital India, it is extremely important to not only think about the comfort, energy and cost efficiencies that the new technologies will bring, but also about the cybersecurity issues that might arise.It is not only the number of intrusions getting higher day by day, but also the nature and characteristics of these attacks.

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

Cyber security

Cyber security is an international issues and it requires international cooperation to be effective. This is also a problem for India as India has a poor track record of cyber security. Cyber security and wellness is an area where strong Public Private Partnerships can benefit the country. Intel has always been a strong believer of the PPP model and is working very closely with the government in the proliferation of digital literacy in the country and most recently we've also begun working on creating awareness on cyber security and wellness. With the evolution and implementation of varied disruptive technologies and the revolutionizing shift over enterprise architecture, eventually moving towards social, mobile, analytics and cloud in conjunction with technologies goes for a toss, if not aided with a comprehensive security system. Constructing the security frameworks and responses to such dynamic environment needs to be much more efficient. Cyber criminals use a seemingly endless array of techniques to compromise and infiltrate nearly every aspect of electronic environment. The global economy has become increasingly dependent on Web-based systems. Cyber-attacks have grown so complex and varied that traditional IT system defenses such as antivirus software and intrusion prevention systems are not enough on their own. Cybercrime thus has become big business with cyber-criminal counter intelligence available to the hackers accelerating the volume, variety and velocity of threats we are dealing with.

Degree of Threat

Stealthy attacks are being used to target organizations, to steal consumer's secrets and criminal customer information. It is very much clear that traditional techniques won't be able to prevent all threats. Additional layered security and specialized visibility into these attacks

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

is needed. There are several challenges which the organizations are facing in terms of security. The vast majority of businesses does not have the resources or the capabilities to properly detect and defend against emerging cyber threats. It's because most businesses are not aware of a breach until it is too late. Cyber intelligence data often lacks the necessary enrichment to make it actionable and relevant. There is an urgent need to move to a more proactive, "over the horizon" threat awareness posture.

Why cyber security has become the backbone of the industries and enterprises now?

Thirty years back, no one had even heard of cyber security, but then, no one had heard of hackers and hacks either. This is because of the Internet. It did not come into being with a Big Bang like the Universe, but it sure is expanding like Universe in all directions and now has become all-pervasive. Internet has changed everything. Quick adoption of the technology by businesses and enterprises has made mobile-banking, on-line shopping, on-line trading and social networking possible. Its many benefits help the business growth by creating new opportunities.

However, Internet is not altogether a safe place because its anonymity also harbor's cybercriminals. They have found ways and means to launch cyber-attacks on banks, large financial and manufacturing organizations, industries, even other nations. Their motives are financial gain, or ill-conceived patriotism or notoriety or just sheer destructive fun.

Defending against cyber attacks

Cyberspace touches nearly every part of our daily lives through broadband networks, wireless signals, local networks, and the massive grids that power our nation. Defending against and defeating cyber-attacks will require the combined efforts of both the public and private sectors, working to develop new technologies and new approaches, for maintaining real-time

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

protection of their individual networks. With most of the business using open source due to cost implications, the cyber threat not just becomes a reality but lethal for the business.

Cyber-attacks have increased tremendously world over and India is also required to protect its cyber frontiers through techno legal measures. Cyber-attacks are global in nature as they are designed like that only. Initially, cyber-attacks were conducted more on the side of fun but now they have become weapons of Tran's border crimes. Cyber security attacks have become very sophisticated in nature. At the same time efforts must be made by India to formulate effective cybercrimes prevention strategy

Some specific areas against which India needs to strengthen its cyber security are warfare, cyber, cyber espionage, critical infrastructure protection (PDF), international cyber security cooperation (PDF), etc.

India needs to strengthen its cyber security capabilities that must include both offensive and defensive cyber security capabilities. As a result, organizations need to have rapid detection and response capabilities that allow for the synthesis of external and internal threat intelligence in a timely manner. This situational awareness is a required component of an organizations overall security posture and critical for maintaining the confidentiality, integrity and availability of its information assets.

E-Governance

With e-governance coming into power, the private sector sees a lot of opportunity in this space. This will magnify the efficiency of the government and induce more transparency into the system. Digital payment companies stand to benefit with this move as it will increase the number of people accessing Internet in India. The future of a country is generally determined

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

by the growth of its economy and the Digital India campaign is one such way that will not only strengthen the economy of India but will also play a major role in pulling India in the league of developed nations. The transformation of the country into a knowledge economy will ensure the industry gets rock solid support and a fertile ground to flourish in the time to come. Furthering the benefits of Digital India, the roadmap ahead looks promising. With these developments India is expected to become the world leader in IT interface with e-governance and e-services getting maximum exposure. The disruptive technology and trends including social, cloud computing, mobile, and analytics can play a major role in providing governance and services on demand to the citizens. The paradigm is now shifting from e-governance to mobile- governance by enabling one web approach. But all these activities need a high cyber security.

As the part of "Digital India" initiative, the Indian government has already planned to launch 'Botnet cleaning centers'. This proposal is part of the national cyber security policy to cleanup botnet infections in Internet-enabled devices. Botnet is a network of malicious software that can remotely gain control of devices, steal information and carry out cyber-attacks like Distributed Denial-of-Service (DDoS), which can prevent access to websites. This facility will be under the guidance of national cyber security watchdog Indian Computer Emergency Response Team (CERT). The Indian government has also been stepping up its efforts to address these challenges by increasing awareness about the cyber threats and we think it is just a matter of time that we will have the appropriate regulations and compliance in place.

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(2),2015

Conclusion

The implementation of a secure Digital India will need to adopt an end to end approach like never before. Information security is an important part of the overall national and corporate governance model wherein nations and organizations should strive to make a coherence system of integrated security components which exits to ensure that the organizations operations are not hampered with the evolving security threats thus creating a nation of survivability. As a nation, we shouldn't let security concerns undermine the growth potential of India, instead, security has to help create a new and bold Digital India. Partnerships with international researchers and organizations coupled with public and private partnerships will be the best way to address the ever increasing threats and potential risks for Digital India. This would thus assist the "Digital India" initiative with an umbrella program to prepare India for a knowledge based transformation. Therefor it can be concluded that "Digital India" is all set to transform the interface of the countries socio-economic dynamics.

References

1. TRAI Performance Indicator Report – June 2014
2. Digital India Employment Opportunity, August 2014. See: http://post.jagran.com/pm-modis-digital-india-project-to-give-employment-to-17crore-youth1409050390
3. Digital India, Government of India Press Release, August 2014. See: http://pib.nic.in/newsite/PrintRelease.aspx?relid=108926