SURVEY ON NEED OF CYBER SECURITY AND CYBER AWARENESS IN E-GOVERNANCE PLAN IN INDIA

Seema B Joshi
Assistant Professor
School of Engineering and Technology
Gujarat Technological University
Ahmedabad, India
ap_seema@gtu.edu.in

ABSTRACT

Electronic Governance is a precious way for Indian government to deliver public services efficiently. This paper focuses on the need for Cyber Security and Cyber Awareness in e-Governance. Various initiatives are taken by Government for cyber security, thoughcyber security incidents are increased in India over the last few years. These incidents are phishing attacks, website defacements, web-based intrusions, denial of service attacks, malware attacks, mobile botnets, etc. The strong system and legally approved framework are required for cyber security and data protection. The e-Governance should be secured for Indian citizens' private information, business and government operations and policies. Nowadays the security breaches are most challenging issues on all over the world. Cyber security and cyber awareness are the very important part for the e-Governance because it relates with government operations and Indian citizens. It is necessary to have knowledge about security and awareness at every aspect. This paper stretches the concept of e-Governance, Cyber threats and vulnerabilities as well as need of cyber security and awareness for the secured e-Governance in India. Moreover, cyber threat matrix is designed and analyzed based on the concept of e-Governance pillars and its various components. That shows the importance of cyber security in e-Governance.

Keywords: e-Governance, Cyber security, Cyber threats and vulnerabilities, Cyber security awareness.

1. INTRODUCTION

Electronic Governance has already changed many manual and monotonous processes with the different e-Governance plans. The main purpose of e-Governance is to empower the people through giving easy access to information with assurance of confidentiality, integrity and availability. The former president of India Late Dr. APJ Abdul Kalam had been defined the concept of e-Governance as, "A transparent smart e-Governance with seamless access, secure and authentic flow of information crossing the inter-departmental barrier and providing a fair and unbiased service to all the citizens" [1].

The aim of transformation is to increase gross national production and productivity of the land and people through maximizing the performance of each sector namely, cultivation, engineering and services, synergized by the system of inter and intra-sectoral electronic and knowledge connectivity to serve a billion people[1].

Good e-Governance means TRUST of Indian citizens; that can be explained as,T= Transparency, R= Reliability, U= Utility, S=Security, T= Triumph. Good e-Governance ingrained with these properties of transparency and openessthat brings government more closely to their citizens. Hence, e-Governance ensures a more wide and representative democracy. Today the global scenario of the government record keeping and dealing with the citizens is totally implemented computerized as well as use of these technologies is very vast in all the sectors. As digitization of the world affected with the positive approach, behind security questions arise. Henceforth, various procedures, processes and practices that involve

protecting networks, computers, online devices and data from attack, damage or unauthorized access, that is cyber security becomes very essential.

Moreover, cyber awareness is also very essential because everyone is dealing with the various e-Governance applications and processes. Many individual users are being targeted to attack the Government, bankingand other infrastructure in India. The application or system is easily compromised because lack of knowledge and awareness of individual users. It is required to create awareness among various stake holders including Indian citizens, public and private sectors, student communities, etc., as their interests has to be secured.

The rest of the paper is organized as follows: Section II discusses pillars of e-Governance and cyber threats. Section III discusses need of cyber security in e-Governance. Section IV is about need of cyber awareness in India. Section V contains the conclusion part of the study.

2. PILLARS OF E-GOVERNANCE AND CYBER THREATS

The e-Governance providesgreatest possible use of Internet technology to communicate and provide information to common peoples and businessman. Anyone can pay different types of bills such as electricity, water, phone, etc. over the internet in the era of digitization. It is essential to understand the four pillars upon which e-Governance is dependent. The success of electronic governance widely depends upon political strength, citizens' support and cooperation of various departments amongst each other. There are four pillars of e-Governance as shown in Figure 1 [2].

Figure 1 Pillars of e-Governance

2.1 Connectivity: -

The main objective of e-Governance is to connect the people to the Governance services. The strong connectivity should be required for an effective e-governance.

2.2 Content: -

There should be data content to share with citizens. This database should be available in all regional language so that everyone can connect and use e-Governance services. It is helpful to create transparency in services between different e-Governance components such as G2C (Government to Customer), G2E (Government to Employee), G2B (Government to Business), G2G (Government to Government).

2.3 Capacity: -

Capacity is the ability to plan and implement government work in synergy with people, identifying and solving their problems so that actual benefits of e-Governance can be reaped.

2.4 Capital: -

Capital is referred as money used by Governance to provide their services or to that sector of the economy based on its operation. It fulfills the motive of speedy and efficient at subsidized rate with public and private partnership [3].

In e-Governance, government has to invest a lot for the data security solutions because hackers may pose the integrity of the critical national infrastructure and it becomes crucial disastrous of nation. e-Governance system is also major part of the nation and there are more security threats that harm the government confidentiality as well as citizen's data availability. Threat matrix for e-Governance is shown in Table 1, it is shown that cyber threats affect the pillars of e-Governance which is marks with '√' sign and candamage the confidentiality, integrity and/or availability of system.

Table 1: Cyber Threat Matrix for e-Governance

Pillars of e-Gov affected / Cyber Threat	Connectivity	Content	Capacity	Capital	e-Governance Components
Malware attacks	√	√	√	√	**G2C**
Denial of Services	√	√	√	√	**G2E**
Web Defacement	√	√			
Damage to critical databases & applications		√		√	**G2B**
Mobile Botnets	√		√		**G2G**

There are various cyber security incidents has gradually increased in India over the last few years. As per the information collected by Computer Emergency Response Team India (CERT-in), 44,679, 49,455 and 50,362 cyber security incidents took place in India during the years 2014, 2015 and 2016, respectively [4]. These incidents include phishing, website defacements, Denial of service attacks, etc.

3. NEED OF CYBER SECURITY IN E-GOVERNANCE

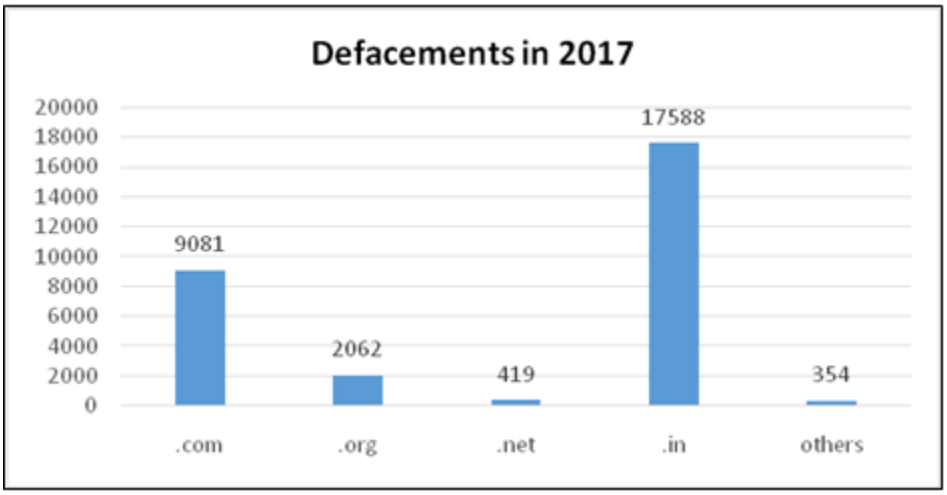
The main security measures such as firewall system, intrusion detection and intrusion prevention system (IDS/IPS), encryption and secure networks must be defined, designed and implemented for government agencies to provide the appropriate levels of security.The people and processes are dependent on the information systems that must be taken as consideration. The government employees as well as users must be trained on cyber security who are daily accessing e-Governance systems.

Electronic governance is implemented with highly complex processes that requires provisioning of hardware and software, networking and process re-engineering and change management. National e-Governance Plan (NeGP) contains the following elements as the methodology and implementation strategy in which cyber security role is required a most.

- Common Support Infrastructure
  - State Wide Area Networks (SWANs)
  - State Data Centres (SDCs)
  - Common Services Centres (CSCs)

  - Electronic Service Delivery Gateways.
- Governance
  - Roles of NIC, STQC, CDAC, NISG for strengthen DEITY.
- Centralized Initiative with Decentralized Implementation
- Public-Private Partnerships
- Integrative Elements
- National and State Levels Programs
- Facilitator role of MEITY
- Ownership of Ministries

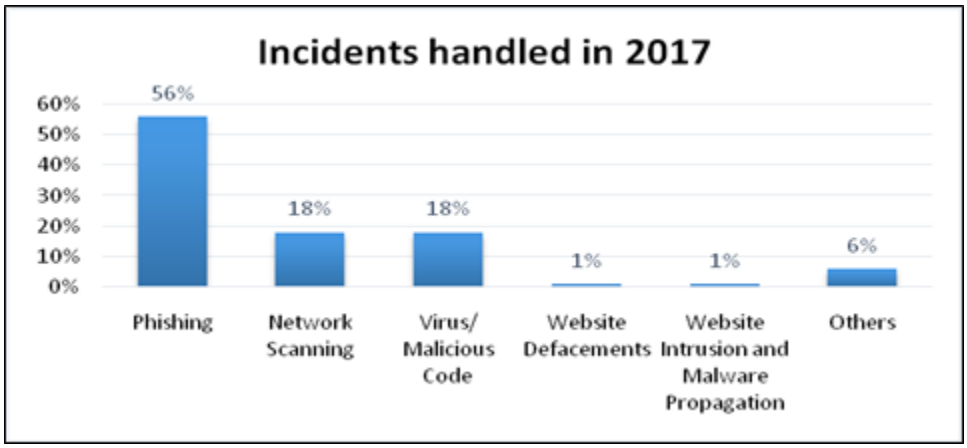
Graph 1: Indian website defacements tracked by CERT-in during 2017



Source: Annual Report 2017, CERT-in

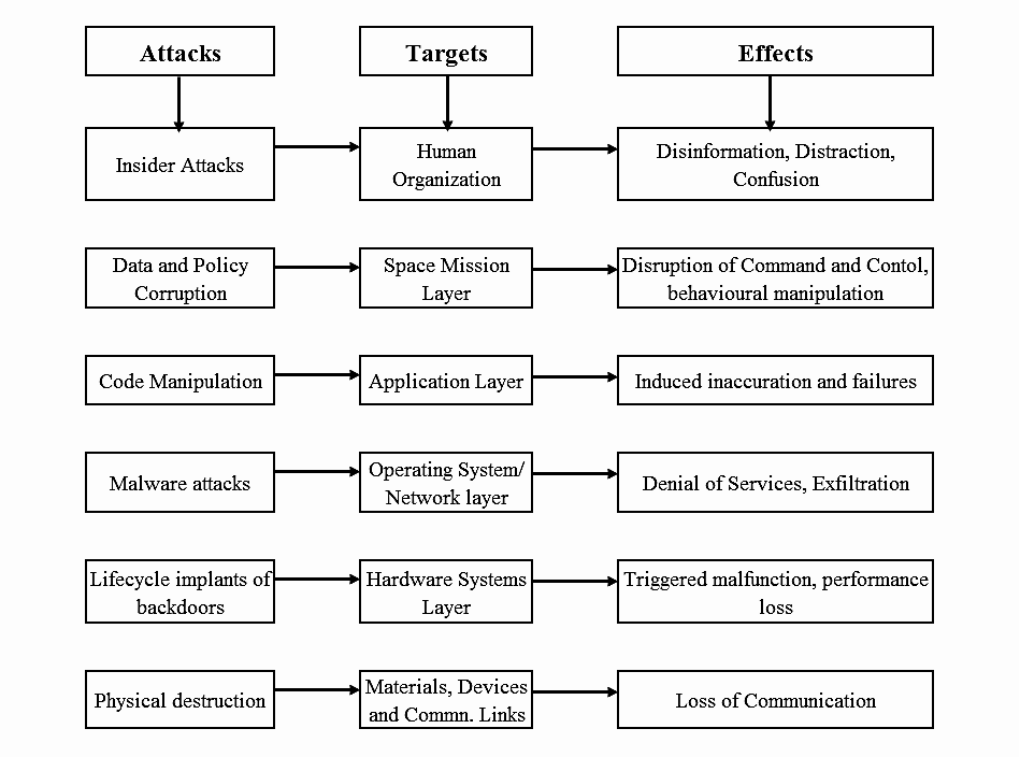
As shown in Graph 1, CERT-in tracked 17588 Indian website defacements incidents during 2017. CERT-in handled 53081 incidents during the year 2017. Various types of incidents such as website defacements, malware attacks, phishing attacks, Distributed Denial of Service attacks (DDoS), data theft, etc. were happened (Graph 2). In addition, 53692 spam incidents were also reported to CERT-in [3].

Graph 2: Summary of incidents handled by CERT-in during 2017



Source: Annual Report 2017, CERT-in

Figure 2: Challenges increasing in cyber space domain

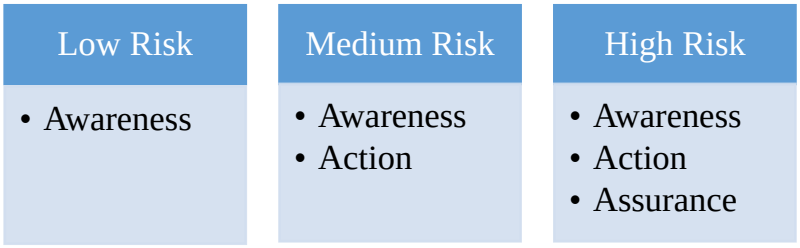


The challenges are increasing in cyber space domain as shown in Figure2. There are many initiatives taken by Indian government, but it is required to change mindset of citizens to support the implementation and the change will happen through e-Governance. Another challenge is business process reengineering, lack of need analysis across Mission Mode Project (MMP), managing with technology trends like Cloud Computing, Mobile and digital signatures and Policy issues. It is basic responsibility to take care of resources as well as to be aware about cyber security.

4. NEED OF CYBER AWARENESS IN INDIA

Cyber security is required for secured e-Governance and for assurance of citizens. Security assurance emphasis depends on the kind of environment in e-Governance.

Figure 3 Risk and mitigations strategies in e-Governance



Cyber Security awareness concerns with the best practices at low risk in all the area of e-Governance as shown in Figure 3. As proactive measures people and government should know the security threats and the security policies to take proactive decisions for e-Governance Systems. Security failures could

be disastrous and may lead to unaffordable consequences, assurance that the security controls work when needed at high risk.

India is the fastest growing country and there would be more than 730 million Internet usersby 2020. The rank of India is 3rd after USA and China in terms of the highest number of internet users in the world. According to a 22 October report by security firm "Symantec Corp", India was ranked in the top five countries to be affected by cybercrime [5].

Cert-in conducts trainings and workshops for government officials and public sector industry to create security awareness within the public and private organizations. CERT-in has conducted 22 trainings on various specialized topics of cyber security in the year of 2017 [3].

Security challenges have increased in the past few years in terms of technical complexities, scale and its spread. Information Security domain has been continuously evolving to meet the increasing threats and challenges. Cyber security awareness is the best way to safely take part online as the Internet dependency is increasing. Indian government initiates Information Security Education and Awareness (ISEA) project for general users, academicians, children, government employee, etc. The guidelines are provided on the web portal about a complete understanding of cyber world with latest tips to safeguard every citizen of India. Indian citizens should be aware about cyber security and also share knowledge with others to be safe in digital world.

5. CONCLUSION

E-Governance has already started to conquer role in the global and economy. There are many initiatives taken for securing information systems at different levels in the e-Governance. Many government agencies, public-private partnership, network service providers, large businesses, common users are required to play their role to secure the cyber space within the country. There are so many challenges in cyber security; it is necessary to develop smart security solutions to secure e-Governance systems and infrastructure. Moreover, cyber security awareness is also very important for every Indian citizen to use this technology wisely.

6. REFERENCES

[1] Dr. APJ Abdul Kalam. (2005). 92nd Indian Science Congress, Ahmedabad, India. Presentation. Retrieved from www.abdulkalam.nic.in/presentation/1speechpresentation462.pps
[2] Sheel, S. V., Sheel, N. (2017). E-Governance: Challenges in the way ahead. International Journal of Science Technology and Management, 6 (02), 703–709.
[3] CIRT, India. Annual Report (2018). MIETY. Government of India. Retrieved from https://www.cert-in.org.in
[4] IANS. (2017, February 21). Article title Government of India launches 'Cyber Swachhta Kendra'; a new mobile and desktop security solution.Retrieved from http://tech.firstpost.com/news-analysis/government-of-india-launches-cyber-swachhta-kendra-a-new-mobile-and-desktop-security-solution-363415.html
[5] Dr. V K Sarswat. (2018). Cyber Security. NitiAyog. Presentation. Retrieved from http://niti.gov.in/writereaddata/files/document_publication/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf
[6] Kumar D. Panchanatham, N. (2015). A case study on Cyber Security in E-Governance, 272–275.
[7] Pandya, D. C.,Patel, N. J. (2017). Study and analysis of E-Governance Information Security (InfoSec) in Indian Context, 19(1), 4–7.