International Journal of Research in Economics and Social Sciences (IJRESS)
Available online at: http://euroasiapub.org
Vol. 7 Issue 5, May- 2017, pp. 145~155
ISSN(o): 2249-7382 | Impact Factor: 6.939 | Thomson Reuters Researcher ID: L-5236-2015

Information Security Education, Training and Awareness Initiatives by Government of India

Dr. Amishi Arora[1],
Principal
CIBMRD

Amlesh Mendhekar[2]
Research Scholar
CIBMRD

Abstract

India is experiencing a phenomenal growth in the use Information Technology in every industry sector. Even the government is focusing more on cashless economy, e-governance and smart cities projects.

India has a dubious distinction of being one of the fastest growing Internet population in the world but at the same time it has one of the lowest information security aware population. In the past few years the technology adoption has shown exponential growth in India both in urban as well as rural parts of the country. Due to lack of security awareness among people they are easily falling prey to cyber-attacks.

India is one of the topmost victim of cybercrimes in the world. As large number of Internet users in India are youngsters, the Government of India has started various information security education and awareness programs for them. This paper tries to explore the different initiatives undertaken by the government for imparting the information security education, training and awareness.

Keywords

Information Security, Cyber-security, IT Security, Cybercrime, Security Education, Training and Awareness

Introduction

Humans are the weakest link in the information security chain. Most of the cyber-attacks are due to intentional or unintentional activities of the users. For maintaining a proper posture of information security in the country, and public/private organizations there is need for good planning, designing, implementing, testing and maintaining the security infrastructure. All these phases require skilled people in the domain of information security. Information security education and training programs will help in creating skilled manpower. Apart from skilled manpower, the end-users who has access to vital information in the organization should have the knowledge of protecting this information for overall security.

A strong IT security program cannot be put in place without significant attention given to education, training, and awareness. These skills are vital for employees and users as they are required to carry out their assigned duties effectively. Failure to give attention to the area of security education, training and awareness puts the enterprise as well as the nation at great risk because security of resources is as much a human issue as it is a technology issue. [**1**]

What is Information Security?

Information Security is the practice of defending information and information assets from unauthorized access, use, modification, disclosure, disruption, inspection, perusal, inspection, recording or destruction in order to provide confidentiality, integrity and availability.

Information Security is also sometimes shortened to InfoSec. It is a broad term which encompasses the various topics like Cyber-security, Data security, or IT Security [**2**]

Understanding Information Security Education, Training and Awareness

Information security education, training and awareness are the best countermeasure/control in preventing or reducing the cybercrimes. Education, training and awareness are actually three different concepts. For any good security implementation, different information security skills are required. Right from a CEO of the organization to a person who uses a smart phone, computer, etc. needs to take due care of his organization's data or personal data. Unless proper education, training and awareness is provided it is impossible to stop cybercrimes. There are different target audience for education, training and awareness depending on the security requirement.

Security Education

Information security education aims at building in-depth knowledge, as required to plan, design, develop, implement and maintain information security programs for systems and organizations. National Institute of Science and Technology (NIST) defines security education as the process which "integrates all security skills and competencies into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response." [**1**]. Education is something which is beyond training and awareness, such and can be accomplished mostly through a degree program at a university or a college. Education can be considered as a long term course like a college degree or a research work which allows students to make in-depth study of the specific topic.

Security Training

Security training aims to develop and enhance relevant security skills and competencies of the users by providing detailed and hands-on instruction so that they can perform their job in secure manner.

Training as defined by NIST is as follows: "The 'Training' level of the learning continuum strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing)." [**1**].

The training duration is short as compared to education but it is on higher level and more formal as compared to awareness.

Security Awareness

Security awareness aims to make everyone aware of their duties regarding information security. NIST defines security awareness as "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly." [**1**] There are many techniques used to spread awareness such as lectures, posters, mailers, screen savers, puzzles, award program, videos, newsletters, etc.

Importance of Information Security Education, Training, and Awareness

Information security education, training and awareness plays a vital role not only in maintaining the security posture on the organizations but it also helps in reducing the loss to the nation due to cybercrimes. The country is moving towards E-Governance though its Digital India program. As more and more government services are made available online for the citizens, there are increased threats of cyber-attacks both on infrastructure and the people accessing it. As India is now one of the fastest growing economy in the world it has also become target of the cybercriminals. Also due to increased use of mobile/smart phones by people the problem has aggravated as the users lack awareness about safe use of technology.

Some of the major benefits of Information security education, training and awareness includes:

1. It is the first line of defense against security risks
2. It is the best countermeasure against any cyberattack and it also helps to reduce cybercrimes.
3. Information security education and training helps in creating a pool of security skilled manpower which can be readily absorbed by the government agencies and other organizations.
4. It helps in protecting confidential and sensitive information
5. Security awareness helps individuals to understand the importance of information security and also ensures they understand their responsibilities towards maintaining security.
6. It helps to make security safeguards more effective and increases accountability as well
7. Security awareness helps users to effectively deal with social engineering, identity thefts, and other cybercrimes
8. It is necessary for regulatory requirement compliance

Impact of Cyber-crimes on India

Cybercrimes in India is growing at a very fast rate which is also reflected in different studies and surveys. As per EY 2016 Global Forensic Data Analytics Survey “Cybercrime is perceived as the fastest growing fraud risk (40 per cent), followed by bribery and corruption (36 per cent) in India”. [**3**]. The Indian Computer Emergency Response Team (CERT-In) also has reported a surge in the number of incidents till October 2016 with close to 39,730 security incidents. [**4**]. More than 8000 Indian websites hacked the first three months of 2016. [**5**]

The country is witnessing increase in number of cybercrimes since last few years. Internet penetration is growing rapidly and many new users are accessing the internet using their smart phones. Internet subscribers in India crossed the 400 million mark, and are expected to reach 462 million by June 2016. The cybercriminals are taking advantage of low cybersecurity awareness among the users to commit cybercrime. India has also emerged as the third top destination of cyber-attacks [**6**]. As per the data from the National Crime Records Bureau (NCRB) there was around 70% rise in cybercrimes annually between 2013 and 2015. Cybercrime not only triggers financial loss but also induces emotional loss to the victims.

As per the Symantec Corp. report, 48% (i.e. 113 million) of all overall Indian internet population has become a victim of cybercrime and for every cybercrime an average of Rs. 16,000 was paid by every victim [**7**]. The amount consumers lost to cybercrimes in India was Rs. 1882 billion. (or Rs.188200 crore) [**8**].

Demand of Information Security Professionals in India:

In India the information security sector is growing rapidly. There was estimated requirement of 5 lakh Information Security professionals in the year 2015 but in reality the available pool of InfoSec professionals was only 50,000. These professionals were required in the institutions which are more prone to cyber-attack like Government departments, , IT/ ITeS, financial institutions, Call Centers, BPOs, Telecom sector, Universities, Schools, Colleges, Hospitals and other institutions.[**2**] The projected information security skills required will be one million by 2020. There is a huge gap between demand and supply of information security professionals and this is a great opportunity for individuals who are interested in adopting Information Security as a career.

Information Security Education, Training and Awareness Initiatives by Government of India

The Government of India has initiated several programs to address the Information security requirements across the country in order to effectively respond to the challenges posed by Information security threats. Due to rapid rise of cybercrime in India, the Government had set up an Inter Departmental Information Security Task Force (ISTF) with National Security Council (NSA) as the nodal agency. Some of the recommendations deliberated by the Task Force with respect to Information security education, training and awareness includes

1. Supporting R&D activities through premier Academic and Public Sector Institutions in the country,
2. Launching nationwide Information Security education, training and awareness programs.

National Cyber Security Policy -2013:

In order to build a secure and resilient cyberspace for citizens, businesses and Government, the National Cyber Security Policy was created in the year 2013 by the Government of India. Some of the important objective of the policy is to create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.

Some of the Information security education, training and awareness strategies [**9**] as mentioned in the policy are:

1. To enable, educate and facilitate awareness of the regulatory framework.
2. To undertake Research & Development programs for addressing all aspects of development aimed at short term, medium term and long term goals. The Research & Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.
3. To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution oriented research
4. To foster education and training programs both in formal and informal sectors to support the Nation’s cyber security needs and build capacity
5. To establish cyber security training infrastructure across the country by way of public private partnership arrangements.

6. To establish cyber security concept labs for awareness and skill development in key areas.
7. To establish institutional mechanisms for capacity building for Law Enforcement Agencies.
8. To promote and launch a comprehensive national awareness program on security of cyberspace.
9. To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security.
10. To conduct, support and enable cyber security workshops / seminars and certifications.

Ministry of Electronics and Information Technology (MeitY):

MeitY is part of the Union Government of the Republic of India. It was formed by giving the status of ministry to the Department of Electronics and Information Technology (DeitY) is a division of The Indian Ministry of Communications and Information Technology.
Some of the Autonomous Societies of MeitY [**10**] are:

1. Education and Research in Computer Networking (ERNET)
2. Centre for Development of Advanced Computing (C-DAC)
3. Centre for Materials for Electronics Technology (C-MET)
4. National Institute of Electronics and Information Technology (NIELIT) — Formerly DOEACC Society
5. Society for Applied Microwave Electronics Engineering and Research (SAMEER)
6. Software Technology Parks of India (STPI)
7. Electronics and Computer Software Export Promotion Council (ESC)

The Government of India has initiated the implementation of the objectives of National Security Policy-2013 through MeitY. The following are some of the government organizations associated with MeitY and engaged in cybersecurity education and awareness program across the various industry sectors including the educational institutions.

1. **Education and Research in Computer Networking (ERNET**): is an autonomous scientific society dedicated to support the needs of the research and education community within the country. Apart from providing connectivity the focus of ERNET is to provide consultancy, training, project management for the academic and research institutions in India. Apart from this other value added services are also provided such as video conferencing, email service, web-hosting, and domain registrations, etc. More than 1300 institutions are served by ERNET India in various sectors, such as, educational institutions (higher education and schools), agriculture, health, science & technology.

ERNET India regularly organizes information security related programs which includes both short term and long term courses. [**11**]
Short term courses:

1. Computer Security Fundamentals for IT Users
2. Computer and Network Security for Administrators: Advanced level – I
3. Computer and Network Security for Administrators: Advanced level – II
4. IT Law & Forensics

Long term courses:

1. Diploma in Information and Network Security
2. Advance Diploma in Information Communication Technology and its Security

2. **Centre for Development of Advanced Computing (C-DAC):** is a research and development organization under the Ministry of Electronics and Information Technology (MeitY), Government of India. C-DAC is primarily carrying out R&D in IT, Electronics and associated areas and also offers various education and training programs.

C-DAC's provides Education and Training programs in the field of IT and Electronics in order to create skilled manpower in the country. It has its own training centers in Pune, Hyderabad, Bengaluru, Kolkata, Chennai, Mohali, Nida, Mumbai, and Thiruvananthapuram. CDAC also has its Authorized Training Centers (ATC) throughout the country. These training centers offers both short term as well as long term courses. [**12**]

Short term courses in formation security are of one day to one month duration. Some of the topics covered are Database Security, Ethical Hacking, Perimeter Security, Security Engineering, Web Application Security, Wireless Security, Security Administration Linux, Cyber Forensics, Cyber Crime, IT Law, Mobile Security, etc.

CDAC also offers a long term course 'The Post Graduate Diploma in IT Infrastructure, Systems and Security' (PG DITISS) which is a 24 week full time program. This course is intended for students to understand the various concepts of information security.

3. **National Institute of Electronics and Information Technology (NIELIT) — Formerly DOEACC Society:**

NIELIT is an Autonomous Scientific Society under the administrative control of MeitY, Government of India. It was formed to carry out mainly the Human Resource Development activities in the field of Information, Electronics & Communications Technology (IECT). NIELIT is engaged in developing industry oriented quality training and education programs in India. NIELIT is a premier institution in the field of IECT for Examination and Certification and is also one of the National Examination Body, involved in accrediting institutes and organizations for conducting various courses in IT. At present, NIELIT has pan India presence with 35 offices and over 800 accredited institutes across the country.

NIELIT offers both short term and long term courses in cyber security and cyber laws apart from other IT related courses. It accredits institutes to conduct these courses by utilizing the facilities and expertise readily available with various institutions in the non-formal sector.

Some of the courses offered by NIELIT are: [**13**]

1. PG Diploma in Information Security and Cloud Computing
2. PG Diploma in Information System Security
3. Certificate Course in Cyber Forensic
4. Diploma in Cyber Law
5. Certification Scheme in Information Security
    a. Certified System Security Analyst (CSSA)
    b. Certified System Security Professional (CSSP)
    c. Certified Computer Forensic Professional (CCFP)

d. Certified Information Systems Security Auditor (CISSA)
e. Certified System Security Solution Designer (CSSSD)

4. Information Security Education and Awareness (ISEA) Project:

The MeitY, Government of India, started ISEA project Phase-I in the year 2004 to create a qualified and well trained manpower to take up the ever growing challenges of maintaining Information security in the country. These resources will secure and maintain system and critical infrastructure within the country by engaging in Research & Development (R&D), and also developing indigenous solutions / software. Presently the Phase-II of the project is underway.

ISEA project intends create information security manpower by education, training and awareness programs for government employees, working professionals as well as for general public. The project will cover all the information security requirements at various levels viz. from certificate level to doctoral level, training of Industry Professionals and faculty, creating mass awareness on information security in the country.

The major objectives of the ISEA project are:

1. Creating skilled manpower to address the human resource requirement in the area of Information security.
2. The project emphasizes on providing adequate facilities for doing research in the areas which are of national strategic importance and also in designing and developing indigenous products.
3. Introducing Information security curriculum through the academic institutions in their formal courses like M.E./M.Tech./M.S./B.E./B.Tech., PG diploma courses, short term modular knowledge-cum-skill oriented courses, and faculty training.
4. For working professionals introducing formal and virtual short term courses, and certificate programs.
5. Training of Government Personnel
6. Creating mass Information Security Awareness which are targeted towards various sections of society such as:
   a. General Users: Small enterprise/Business users, SME Sector/Non IT industry, NGO's, CSCs, Cyber cafes and general public at large
   b. Academic Users: School level - Children, Parents & Teachers, College level - Students & Faculties

   Government Users: Central/State Government employees (non IT professionals), Legal / Police personnel's etc. [**14**]

Under ISEA Education project around 1,14,038 persons will undergo training under formal & non-formal courses, faculty training, professionals, etc. Apart from this, around 400 paper publications are expected from various research centers. [**15**]

The objective of ISEA Training project is train 13,170 state and central government officials, legal and police department personnel. The mode of delivering training is both direct and virtual mode. [**16**]

The core objective of ISEA Awareness program is to spread information security awareness to at-least 25% of the internet users in India. The mode of spreading awareness will be through conducting awareness workshops (multilingual) for general users and government employees, introducing cyber security curriculum in schools, awareness campaigns through print and electronic media, via newsletters and annual magazines for government and academic institutions, online media campaigns, and setting up toll free technical support center. Around 20887 people from various sections of the society has participated in various awareness workshops. [**17**]

5. **STQC (Standardisation Testing and Quality Control):** SQTC is a part of MEITY involved in providing quality assurance services like Testing, Training, Calibration, IT & e-Governance, and Certification to public and private organizations in the field of Electronics and Information Technology (IT).STQC has network of centers and laboratories across the country.

SQTC conducts public as well as onsite customized training programs in India and abroad. These programs are mostly oriented for working professionals to upgrade their knowledge and skills. Some of the training programs in the area of Information security includes:

1. STQC Certified Network Security Manager (STQC-CNSM)
2. Information Security Management System Lead Auditor as per ISO 27001
3. STQC Certified Information Security Professional (STQC-CISP)- A Program on ISO 27001 implementation
4. STQC Certified Internal Information Security Auditor (STQC-CIISA)- A Program on ISO 27001 based Internal Auditing
5. Information Security Management System - Best Practices (Based on ISO 27001)
6. Secure Software Development Life Cycle Practices (SSDLC)

These courses from STQC are well recognized in the industry both within and outside the country. [**18**]

7. **CERT-In (The Indian Computer Emergency Response Team):**

CERT-In is a National Incident Response Center for major computer security incidents and find solutions to counter the cyber-attacks in India. One of the principal activity of CERT-In is to raise the awareness among the Indian cyber community. It also advices and offer technical assistance to help them in recovering from computer security incident, report on new vulnerabilities and promote effective and best IT security practices all over the country.

CERT-In provides information security awareness and training regularly to Government, Public, and to other critical sector organizations. The target audience for awareness and trainings includes CIOs, CISOs, Decision makers, System/Network/Database administrators, Security administrators, and other Security/IT professionals. Some of the topics covered in the trainings are: Information policy and procedures, secure coding, system and network security, database security, Application security, Wireless network security, cyber-crime and computer forensics, cloud security, security attacks and countermeasures. [**19**]

8. NSDC (National Skills Development Council):

The National Skill Development Corporation, (NSDC) works under the Ministry of Skill Development & Entrepreneurship, Government of India. [**20**] It is a Public Private Partnership which aims to promote various skill development by creating a pool of quality vocational and educational institutions. NSDC conducts many IT security skills related courses in various institutes across the country.

NSDC's IT-ITeS Sector Skills Council in association with National Association of Software and Services Companies (NASSCOM) and Symantec (SSC NASSCOM) has jointly started a program to build Cyber Security Skills which is an initiative to develop skilled and certified information security professionals in the country.

SSC NASSCOM project's special focus is on promote cyber security skills development in women. After successful completion of SSC NASSCOM program they will get certificate and scholarship. The objective of this program is to train at least 1000 women in various cyber security qualification packs. [**21**]

Apart from government organizations some industry trade association and other bodies are also actively collaborating with government agencies implementation of the requirements of National Cybersecurity Policy.

National Association of Software and Services Companies (NASSCOM) and Data Security Council of India (DSCI):

National Association of Software and Services Companies (NASSCOM) is the principal organization that represents and sets the strategic direction, advocating policies, developing best practices and workforce development for the Indian software industry. NASSCOM is a trade association of Indian Information Technology (IT) and Business Process Outsourcing (BPO) industry [**22**]. Data Security Council of India [DSCI] is a leading industry body on data protection in India, setup by NASSCOM, committed to making cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. [**23**]

Department of Information Technology (DIT), Ministry of Communications and Information Technology (MCIT) has assigned NASSCOM – DSCI with the responsibility for developing cyber security R&D plan, providing cyber security solutions, developing a skilled workforce of cyber security experts and implementing the Cyber Security Awareness Project across the country.

DSCI works towards creating a manpower in security, privacy and cyber forensics via training and certification program for professionals and law enforcement agencies. As a part of the awareness campaign, DSCI regularly conducts events in various educational institutions in India. The objective is to build up the security and privacy culture in the India. DSCI also has its own certification in data privacy to cater the growing need of the privacy professionals in the country.

1. DSCI Certified Privacy Professional (DCPP)
2. DSCI Certified Privacy Lead Assessor (DCPLA)

DSCI, in collaboration with IT/ ITeS Sector Skills Council of National Skills Development Corporation (NSDC) has been working towards building a robust Cyber Security skills environment in the country. DSCI in accordance with the NSDC's framework has developed career map for cyber security sector and qualification packs for 10 upcoming job roles which are as under:

List of Cyber Security Qualification Packs: [**24**]

1. Analyst Application Security
2. Analyst Compliance Audit
3. Analyst End Pint Security (EPS)
4. Analyst Identity and Access Management (IdAM)
5. Analyst Security Operations Centre (SOC)
6. Architect Identity and Access Management (IAM)
7. Consultant Network Security
8. Forensics Specialist
9. Penetration Tester
10. Security Infrastructure

Conclusion

There is a huge shortfall of skilled cybersecurity manpower in the country. For the country which is adopting technology at an exponential speed there should be corresponding ready skilled workforce available to counter the cyber-attacks and cybercrimes in the country. Educational institutions can play a vital role in bridging the cybersecurity workforce skill gap in India. Even tough Government has taken commendable steps in this direction there is still a need for more collaboration between the government agencies, public and private educational institutions.

References:

1. NIST Special Publication 800-50 *Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf*
2. Meeting the Information Security Skills Demand in India, Amlesh Mendhekar *Retrieved from*
3. EY Global Forensic Data Analytics Survey 2016 *Retrieved from http://www.ey.com/gl/en/services/assurance/fraud-investigation---dispute-services/ey-shifting-into-high-gear-mitigating-risks-and-demonstrating-returns*
4. India sees large rise in cybercrime: ASSOCHAM-PwC study *Retrieved from http://www.assocham.org/newsdetail.php?id=6149*
5. IT minister Ravi Shankar Prasad revealed Cyber Crime statistics in India *Retrieved from http://computerera.co.in/it-minister-ravi-shankar-prasad-revealed-cyber-crime-statistics-in-india/*
6. 2016 Internet Security Threat Report *Retrieved from https://www.symantec.com/security-center/threat-report*
7. Cybercrime: 113 million Indians lost an average of Rs 16,000 *Retrieved from http://indianexpress.com/article/technology/tech-news-technology/cybercrime-113-million-indians-lost-an-average-of-rs-16000/*
8. Norton Cybersecurity Insights Report *Retrieved from https://us.norton.com/norton-cybersecurity-insights-report-india*
9. National Cyber Security Policy – 2013 *Retrieved from http://meity.gov.in/sites/upload_files/dit/files/National_cyber_security_policy-2013.pdf*
10. Ministry of Electronics and Information Technology *Retrieved from http://meity.gov.in*
11. Education and Research Network *Retrieved from http://www.ernet.in*

12. CDAC Education and Training *Retrieved from https://cdac.in/index.aspx?id=education_training*
13. NIELIT *Retrieved from http://www.nielit.gov.in/content/introduction-3*
14. Information Security Education and Awareness (ISEA) Project *Retrieved from https://www.isea-pmu.in/home/About*
15. Information Security Education and Awareness (ISEA) - Education *Retrieved from http://isea-pmu.in/home/I_Education?p=1*
16. Information Security Education and Awareness (ISEA) – Training *Retrieved from http://isea-pmu.in/home/I_Training?p=1*
17. Information Security Education and Awareness (ISEA) – Awareness *Retrieved from http://isea-pmu.in/home/I_Awareness?p=1*
18. STQC Trainings *Retrieved from in http://www.stqc.gov.in/content/about-stqc-trainings*
19. Indian Computer Emergency Response Team *Retrieved from http://www.cert-in.org.in/*
20. National Skill Development Corporation *Retrieved from http://www.nsdcindia.org/organisation-profile*
21. SSC NASSCOM - Building Cyber Security Skills *Retrieved from http://www.sscnasscom.com/building-cyber-secutrity-skills/*
22. NASSCOM *Retrieved from http://www.nasscom.in/about-nasscom*
23. Data Security Council of India *Retrieved from https://www.dsci.in/*
24. Data Security Council of India - Cyber Security Skills *Retrieved from https://www.dsci.in/taxonomypage/1424*