Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore
Shri Vaishnav Institute of Information Technology

B.Tech. in Computer Science & Engineering (with Specialization in Information and Cyber Security)

About the Program

The ever-evolving digital age affects in Information and Cyber Security more than most people realize. The rate of cybercrimes has grown exponentially and is consistent with the growth of technology. As technology expands and develops, so do the cybercrimes that are committed. Fortunately, as technology has advanced, so has the ability to seek out cybercrimes before they happen and protect people when they occur.

We are introducing the specialization of Information and Cyber Security in CSE branch to enable our students to expertise in Information and Cyber Security to protect internet and network based digital equipments and information from unauthorized access and alteration.

The rapid expansion of technologies is also creating and making the cyber security more challenging as we do not present permanent solutions for concerned problem. Although, we are actively fighting and presenting various frameworks or technologies to protect our network and information but all of these providing protection for short term only. So, efficient security understanding experts are required in huge number. However the future prospects of Information and Cyber Security are more interesting:

1. As long as we have computers, Smartphone’s, ubiquitous gadgets and Internet there will be a rising demand for Information security, not only in India but also across the globe.

2. In future, as we are moving towards digitalization, the security of data and information will become a biggest challenge.

3. There will be more numbers of smart cities as vehicles, phones; home appliances will be run by AI where data and information security will be very much critical issue.

4. As we are moving towards cloud platform, the security of cloud will be highly required.

5. Robots called BOTNETS will be protecting our digital data from unauthorized access in coming future.

The Emerging streams of Information and cyber security are:

1. Data Forensic
2. Cyber Forensic
3. Information Security and Cyber Laws
4. Network Security

5. Ethical Hacking

Need of the Program

As with any technological advance throughout history, whenever new opportunities are created, there will always be those that exploit them for their own gain. In these days we frequently come across things like Data leak, Data theft, hacking, different forms of cybercrimes and many more incidences related to data and information, Information and Cyber Security is all about protecting from this kind of problems. The current problems related to information and cyber security are:

1. 93% of cases hackers took just a minute to Breach. While companies took weeks or months to discover.

2. The majority of these corporate security breaches occur when hackers exploit employees through social engineering and scams. With advancements in technology, hackers are becoming more skilled at finding holes and cracks in corporate security systems and can gain access to protected files and data, posing a significant cyber security threat.

3. Spear Phishing: Unlike regular phishing emails that target random people, culprits who normally lead spear phishing scams are seeking information for monetary gain; business secrets or private information. Spear phishing occurs when hackers target employees through emails that appear to be from colleagues within their own organizations, allowing cyber criminals to steal personal information.

4. Social Media Security Breaches: Not only do social media sites give hackers access to personal information, some sites can also share your exact whereabouts at any point in time. And if someone knows where you are – they also know where you are not.

5. Currently, 45 percent of cell phone owners have Smartphone’s, which hold more data than the older alternative models. Every new phone, tablet and mobile device serves as an additional opportunity for a cyber attacker to gain access to someone’s personal data. As many mobile devices can be plugged into computers to be charged, sharing charging ports with others can create malware issues for many different devises.

6. Data has Gone Digital: Hard copy information is increasingly less common- Practically everything is digital these days. Though often protected by a password, most information is stored on a shared network.

7. As more businesses shift to cloud computing and save documents and information to cloud networks poses an additional cyber security risk.

8. Hacktivism: In 2012 there have been a few instances of hacktivism – the act of hacking for a political or social reason. Hackers are taking the practice to the next level and attempting to reach websites with a large number of visitors accessing information in order to affect as many people as possible. Large websites and companies are at a higher online security risk for these types of acts.

9. Botnets: a number of computers set up to forward information (like spam and viruses) to other computers. With the emergence and advancements in technology, botnets are collecting more data from computers such as name, address, age, financial information, online activity and more. They will then gather your information and sell the data to others. Personal data can be bought and sold by a number of companies and businesses, which is how spammers can obtain so many email addresses.

10. The advanced botnets pose a considerable security risk making personal information extremely vulnerable.

11. With the expanding smartphone market, people are becoming more technologically savvy and need to be educated as technology develops. Proper training should be employed so that the company's workforce understands the cyber security threats, and how to avoid them.

12. According to the present survey report on cyber security about 1, 00,000 virus/ worms are reported to be active each day and out of which 10,000 are indentified as new and unique.

13. Over 2.7 billion people are using internet worldwide while 4.4 billion still needs to be connected. Now a day, our lives look incomplete without internet, mobiles and computers. Records are maintained digitally and transferred on communication lines. Banks and other financial institutions also use internet and connected network to carry out financial transactions. So it becomes necessary to secure our network from treats and hacking.

14. ISTR vulnerability assessment system found that about 82 percent websites have vulnerabilities that invite the terrorists for coordinated attack.

15. At present there is huge requirement of Information and Cyber Security Expert in every field .There is lack of skilled Information Security Expert in almost 75 Percent of organization.

16. A 2015 study by Frost & Sullivan, conducted on behalf of (ISC) estimates that by 2020 there will be a shortfall of 1.5 million trained Information Security professionals.

17. Today Industry wants specialized person for specialized work. At present there is huge amount of B.Tech/BE (CSE and IT) students passing out every year but still there is big

shortage of Information Security Expert, this is just because of lack of expertise in the domain

Job Opportunities

There are a number of roles for Information and Cyber Security Specialists, these include:

1. Network Security Expert(Manage the security issues related to networks in an organization)
2. Cyber Forensic Expert (will help in solving cyber crime cases)
3. Data Security Expert (capable of managing huge amount of organizational data from intruders).
4. Ethical Hacker(responsible for finding out the security breaches)
5. Security Analyst (help to safeguard organization's computer networks and systems)
6. Research scientists (responsible for designing, undertaking and analyzing information)
7. Software Engineer (specialize in a few areas of development, such as networks, operating systems, databases or applications).
8. Security Consultant/Specialist: Broad titles that encompass any one or all of the other roles/titles, tasked with protecting computers, networks, software, data, and/or information systems against viruses, worms, spyware, malware, intrusion detection, unauthorized access, denial-of-service attacks, and an ever increasing list of attacks by hackers acting as individuals or as part of organized crime or foreign governments.
9. Security Architect: Designs a security system or major components of a security system, and may head a security design team building a new security system.
10. Cryptographer/Cryptologist: Uses encryption to secure information or to build security software. Also works as researcher to develop stronger encryption algorithms.
11. Cryptanalyst: Analyzes encrypted information to break the code/cipher or to determine the purpose of malicious software.
12. Chief Information Security Officer: a high-level management position responsible for the entire information security division/staff. The position may include hands-on technical work.
13. Software development manager (playing a key role in the design, installation, testing and maintenance of software systems.)
14. Java Developer (specialized type of programmer who may collaborate with web developers and software engineers to integrate Java into business applications, software and websites.)
15. Software Analyst (studies the software application domain, prepares software requirements, and specification documents.)