THE BUSINESS OF INFORMATION SECURITY IN INDIA

-Testbytes Software

Table of Contents

1. Introduction

Stealing information happens frequently in the digital world nowadays. Statistics states that 95% of the breaches affect government, retail and technology-based industries.

The most alarming fact about such breaches is that, once it happens, the devastating effect of it on any organization can be irreversible and grave.

Reputation, the most valuable aspect to any business is at stake at any point in time. So protecting it at any cost is cardinal at this juncture of time.

In order to protect, companies are willing to invest a great deal of money.

In this white paper, we are trying to examine the booming business of information security in India and why a bright future is assured for the candidates who are working and going to work in this industry.

Research for this white paper has been done by Softbreaks, an IT recruitment service which offers a complete solution for recruiters, employers, and employees.

Sponsors for the research are,

Redbytes (App Development Company)https://www.redbytes.in/ and Trackschoolbus (software and hardware providers for complete tracking solution)
https://www.trackschoolbus.com

1.1 What's information security testing?

Information security testing is mainly performed on platforms, services, applications, systems, devices and processes that handle valuable information in a business.

The process is mainly performed with automated tools which can scan and point out vulnerabilities in a system. It can also mimic attacks to fish out the loopholes.

1.2 Rise of information security business in India

Recent reports revealed that 93% of Indian companies are planning to increase their IT security spending which is much higher than that of global average. But why?

Within the time span of 2017-2018 more than 22,000 websites were hacked and

among them 114 were government websites. Among the hacked websites 493 websites were used to spread malwares.

Two of the infamous attacks were,

In 2018, hackers gained access to Andheri Bank accounts by getting hold of the credentials of an employee, they managed to siphon out Rs. 97 lakh within no time.

Pune's Cosmos bank had to face cyber attack and the hackers managed to steal Rs. 94 crore by cloning Visa and RuPay cards.

Statistics states that 95% of the breaches affect government , retail and technology-based industries.

2. The Scarcity, a gold mine for employees

2.1 Global demand

- Cybersecurity business report released on last summer has clearly stated that the shortage of professional in the field of cyber security is immense. In 2016 alone there was 1 million job opening in the sector and it is expected to rise. 5 million (1.5 million) by 2019

- PARC (Palo Alto Research centre) renowned research and Development Company said that by the end of 2019 there will be huge rise in demand of cyber security professionals. (approximately 6 million globally)

- This imbalance in demand and supply of information/cyber security employees will increase the monetary benefits of people who are working in this industry

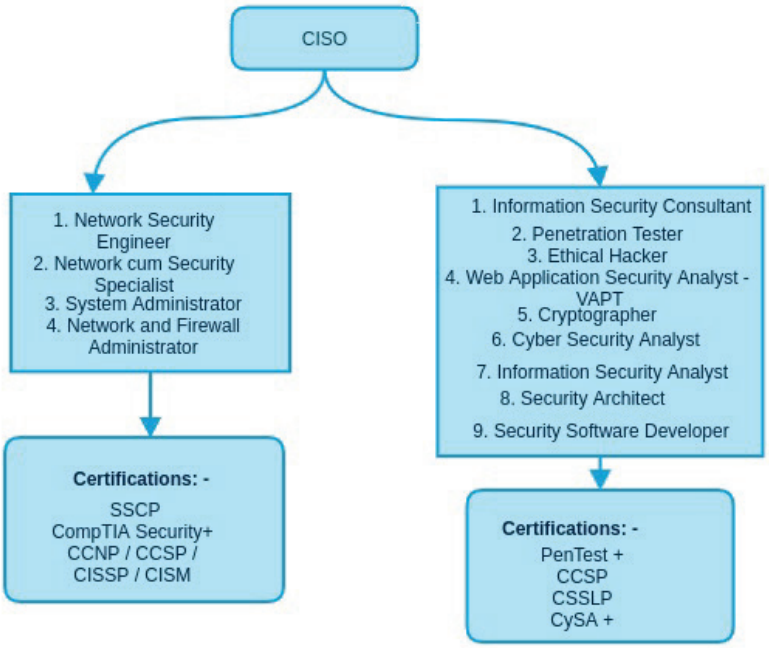
- The profession is going to be so crucial that chief security officers (CSO) and chief information security officers (CISOs) will have to report directly to the CEO not the CIO

93% of Indian companies are planning to increase their IT security spending which is much higher than that of global average.

2.2 Demand in India

- Economic Times on Mar 19, 2018 NEW DELHI has reported that India India is heading towards scarcity of cyber security professionals, specifically at the leadership level. At Present companies have spiked the salaries by 25%-35% over the past year.
- Thehindubusinessline.com has stated that there is a 150 percent jump in cyber security roles in the time period of January 2017 and March 2018.
- According to data collected by softbreaks 89% hiring request is by firms who are building this competency.
- On April 16 2018 QuartzIndia has reported that there are 30,000 vacancies in cyber/information security industry.
- **Factor Daily has reported that there is going to be the requirement of 1 million skilled people by the end of 2020**

2.3 Hierarchical division of roles in an information security company



Abbreviations

SSCP: Systems Security Certified Practitioner

CCSP: Certified Cloud Security Professional

CSSLP: Certified Secure Software Lifecycle Professional

CySA+: CompTIA Cyber Security Analyst

ECES : EC-Council Certified Encryption Specialist

CISSP : Certified Information Systems Security Professional

CCSP : Certified Cloud Security Professional

CISM : Certified Information Security Manager

Security Analyst: He/she should be able to analyse and assess vulnerabilities in software, hardware and network system. Using appropriate tools a security analyst should be able to rectify all the vulnerabilities. Implementation of best practices and recommending solutions is also one of the duties. Complying with security policies and procedures is a must in information security business. Security analysts should make sure company procedures and complying with it.

Security Engineer: Carries out security monitoring, forensic analysis, should trace out security incidents, log analysis, investigate and utilize new technologies and should be well-versed with processes and tech to increase security capabilities etc.

Security Architect: Must be in the forefront of a team when it comes to security system design. He/ she should also be experienced in designing it.

Security Administrator: Installation of huge security systems across an organisation is the duty of a security administrator.

Security software developer: Software development, traffic analysis, breach detection, virus/malware/spyware etc. detection etc. are the main duties of a security software developer

Cryptographer/cryptologist: Encryption of malicious files and understanding it is the main duty of a cryptographer

Chief Information security officer: A high level position, with main duty to control and lead the entire information security division

Consultant/specialist: Broad responsibilities which includes protecting networks, software, data, systems that work against malicious programs, computers etc.

2.4 Major Job requirements in information security industry

Senior consultant – IT consulting – Information Security

Requirement

4 years of experience in information security and related functions such as IT audits and IT risk management

Certifications required ITIL, PMP , CISA, CISSP, CEH, COBIT, ISO 27001

Job description – knowledge in industries such as capital markets, telecom, IT/TES etc.

.Impeccable knowledge in security testing methodologies and methodologies web server security/ firewalls/ networks/PKI/ TCP/ UNIX/ IP etc.

Network / security specialist

Requirement

4 years of experience

Certifications required: CCNP / CCSP / CISSP / CISM

.Job description: should be able to install, configure and administration of network and security equipment, switches, vulnerability assessment, IS audit, security policy design, BCP design and implementation, configuration of firewall etc.

Penetration testing engineer

Requires 4+ years of experience

Job description: should be able to identify and validate high quality MSSps. Apart from that short listing them using effective evaluation methods are also a must

Should also be able to review proposals, visit M S S P websites and recognize tools etc.

Senior application security analyst

Requires 3 years of experience

Certifications required, SANS, OSCP,GPAN ,OSCE, CREST

.Job description: must be able to review DAST and SAST, experience in dynamic application security testing tools like IBM, Appscan, HP webinspect, Acunetix, Burp Professional etc. Ability to maintain standard such as, SANS Top 25, OSSTMM, PTES, OWASP Top 10 is also recommended. Should have the skill to Consult and coordinate with project teams for security assessment

Web Application security analyst – VAPT

Experience required: 3 years

Job description: should be able to handle manual and automated application tests. Should well-versed in application technologies and its components. Hands-on experience of security code review

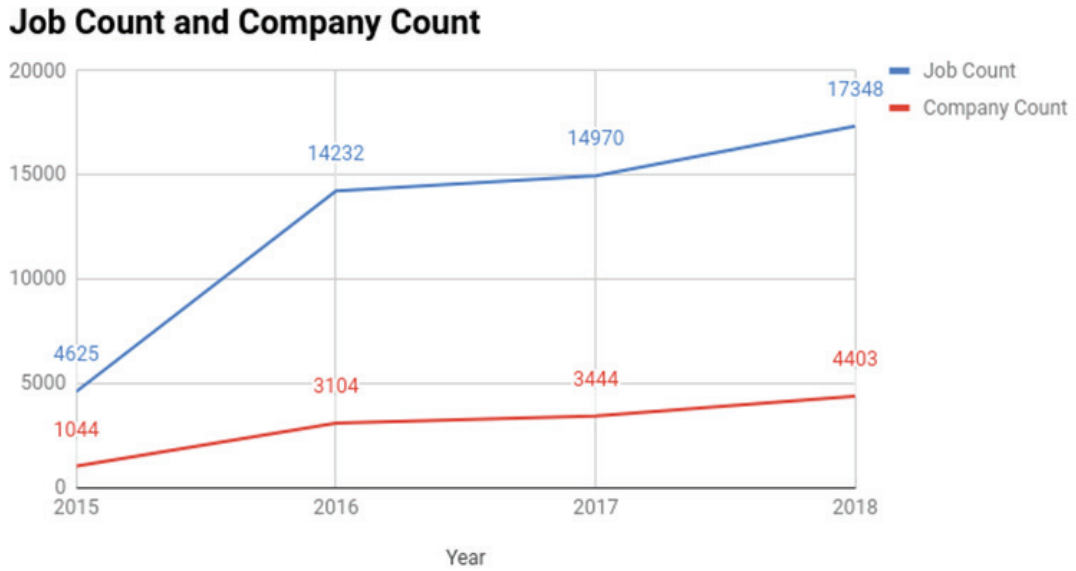
IT security administrator

Experience required: 1 year

Job description: Should have good knowledge and experience in RSA Archer, PKI, Nessus and hardware security modules. Experienced with Security frameworks such as SO27001, ITIL, NIST etc. Ability to develop and implement vulnerability testing methodologies. Should be able to configure and conduct automated scanning and limited manual testing. Candidate should be able to perform application code review and training activities.

2.5 A detailed view into the current demand trends

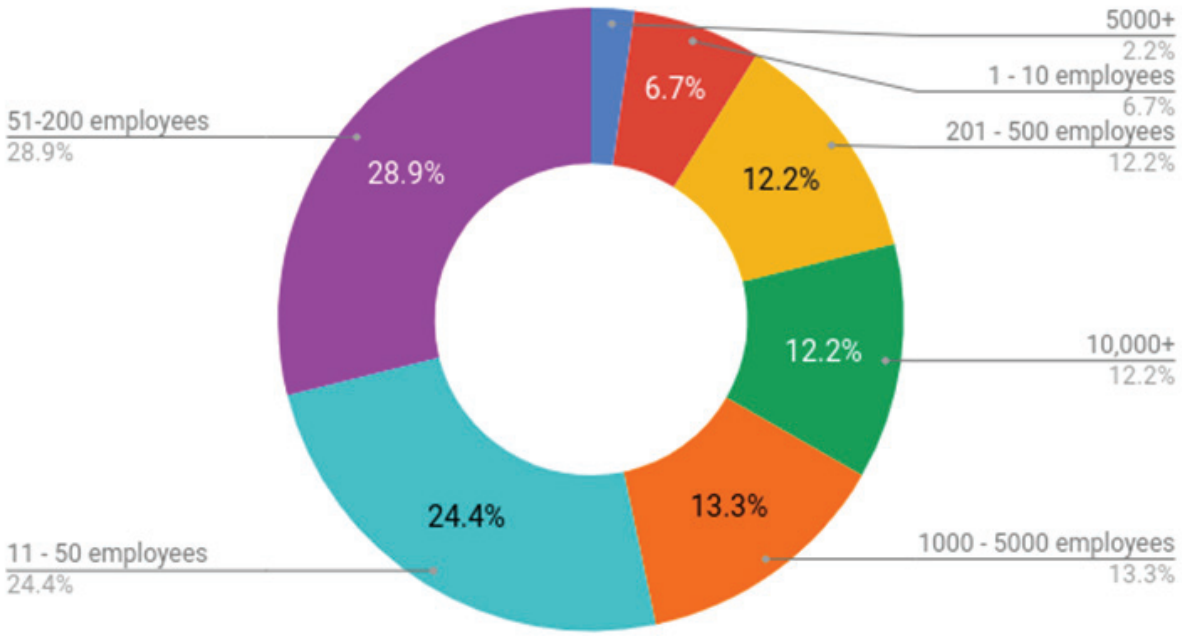
Below graph is a comparison to the rise of information security companies and jobs they posted in the period (2015-2018)



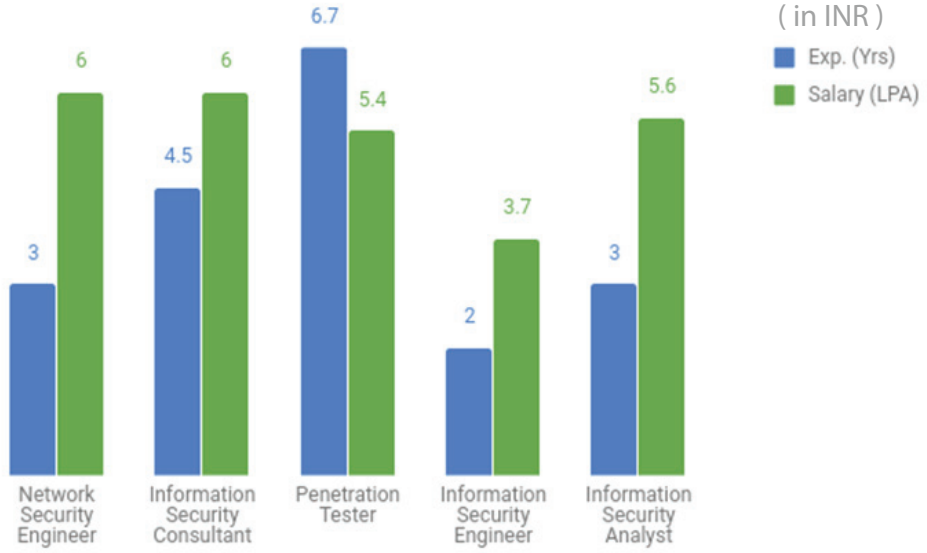
City wise breaks up of companies and consultancies hiring in Information security domain.

Company size VS jobs posted

The below graph shows a detail view of the company size. For instance, 28.9% of jobs are posted by the companies with the 51- 200 employees.



Current salary analysis for employees working in information/cyber security



- 73% of Information Security Companies do not use job portal for Information Security jobs as they tried a year back.

2.6 Certification ISO 27001:

- ISO/IEC 27001 is basically an information security standard devised as a part of ISO/IEC 27000. The last version of ISO/IEC 27001 was published in the year 2013 however, minor updates were added to it till date. ISO/IEC 27001 is published by the International Organization for Standardization(ISO) and the International Electro technical Commission(IEC) under the joint ISO and IEC subcommittee, ISO/IEC JTC 1/SC 27

- The sole purpose of ISO/IEC 27001 is to bring information security under management control and to have certain requirements so that standards can be maintained. Organisations that meet these requirements will be certified by a body after a successful audit.

- Soon companies will be forced to acquire this certification as a proof of their standard and for marketing purposes. This will, in turn, create further job opportunities which people can leverage of

3. Supply for the immense demand

3.1 IT company and recruitment services

- In India, overall 189 Primary hiring Companies and 192 Secondary hiring companies are present to meet the requirement.
- There are 26 recruitment consultant who are primarily focussed on information Security and 980 others who serve their clients not as primary focus.
- However, to meet the requirements new talents have to sprout. To make that possible universities and online learning websites are offering courses on information/cyber security and lots of people are enrolling in it.
- From our observation, Jobs for Information Security are majorly available in metropolitan cities of India i.e Bengaluru, Chennai, Pune, Delhi, Hyderabad, Mumbai, Kolkata, Ahmedabad etc.

3.2 Universities

- Seeing the immense potential of the job and the business, technology institutes like, Galgotias University, Graphic Era University- Dehradun, Chandigarh University, UPES- Dehradun, BITS- Hyderabad have specialised stream for Information Security and provide a B.Tech degree for the same and are the manpower suppliers for InfoSec in India.

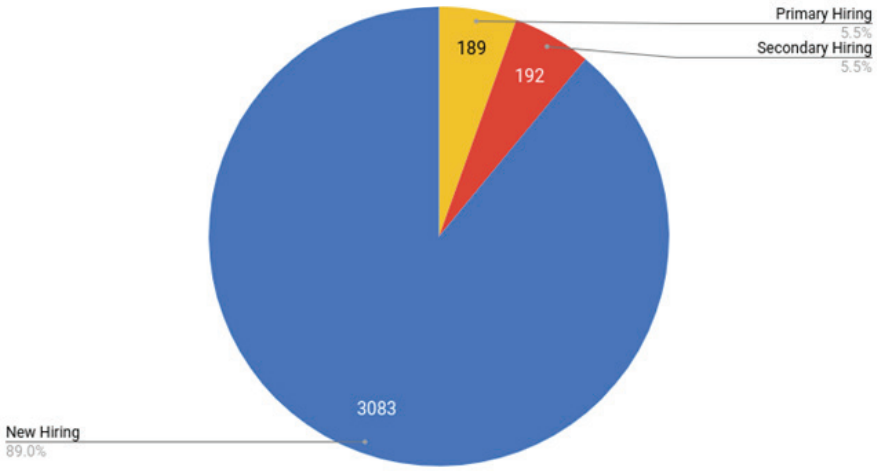
There are

30,000+ vacancies

in cyber security industry

at present

3.3 Distribution of total number of companies :



3.4 Services by information/cyber security companies

There are lot of companies that exists at present, most commonly services they offer are

01. Strategic IT security services
02. Vulnerability Assessment
03. Web Application Penetration Testing
04. Penetration Testing Service
05. Application Security Audits
06. Training & Awareness Program
07. Governance, Risk & Compliance
08. CyberSecurity Operations
09. Data Protection Services
10. Identity & Access Engineering
11. Managed Security Services
12. Cyber Defence
13. Managed Vulnerability Scanning
14. Digital Investigation Services
15. Incident Response Services & SOCs
16. Security Assessment, etc.

3.5 Online courses

- Udemy one of biggest online learning website offers a course with the name Web Security: Common Vulnerabilities and Their Mitigation. (A guide to dealing with XSS, session hijacking, XSRF, credential management, SQLi and a whole lot more). The course will enable a person to understand how web security attacks works, implement secure coding practices and will know how to write codes which mitigates security risks.

- Cybrary one of the big shots when it comes to offering online courses. Their online course on Penetration Testing and Ethical Hacking is very useful for those who are eager to step their foot into information security. This 19 module course offers extensive study materials for you to be a good ethical hacker.

- Coursera offers a course with the name Cybersecurity Specialization. It's a 5 module course which covers major aspects of cyber security

- edX offers a course on network security including intrusion detection, evidence collection, network auditing, and contingency planning against attacks.

According to data collected by softbreaks 89% hiring request is by firms who are building this competency.

4. Inference

Our research of 4 years has coincided to certain evaluations, here they are

- Billions of dollars are flowing to information/cyber security industry. Organisations are now well aware of the importance of security.

- Owing to the same reason Information/Cyber security is going to be one of the most prominent industry in the future,

- But the demand is not yet met owing to the scarcity in information security related employees at the moment

- Because of this scarcity, information security is one of the best career to choose from at this point of time

- Salary packages, especially for the experienced employees are ascending

- Courses offered by colleges and online learning plenty anyone who has the basic knowledge of programming, internet and networking can be a certified information security employee.

- VAPT (Vulnerability Assessment and Penetration Testing) is mostly done using tools any manual tester who does not want to move toward automation testing can look at this as a career option.

- Network administrators, server administrators with their background can pick up VAPT as up skill action.

- People who are professional performance tester, can also fill up VAPT position since performance testing is also simulation and reporting

- Customers are asking for certificate which can serve as a proof for customers that the solution which is provided for the services is tested and does not have any risk of security or vulnerability,

- Professional Association / Professional Organisation can be formed in India for providing professional (Information Security) Certifications:

A professional association (professional body, professional organization, or professional society) is meant for safeguarding interests of individuals engaged in that profession and of course, the public interest.

Other duties of the body involve monitoring of professional educational programs, and the updating of skills, and thus perform professional certification to indicate that a person possesses qualifications in the subject area.

5. References

https://timesofindia.indiatimes.com/business/india-business/over-22000-indian-websites-hacked-between-apr-2017-jan-2018/articleshow/63203998.cms

https://indianexpress.com/article/india/hackers-siphon-rs-70-lakh-from-ludhiana-businessmans-account-4759208/

http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

https://www.businesstoday.in/technology/news/93pc-indian-companies-plan-to-inrease-it-security-spending/story/280717.html

https://cybersecurityventures.com/jobs/

https://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

https://www.csoonline.com/article/3237675/data-protection/the-cio-should-report-to-the-ciso.html

https://economictimes.indiatimes.com/jobs/cybersecurity-jobs-now-at-a-premium-as-india-goes-digital/articleshow/61347784.cms

https://www.cisco.com/c/dam/m/en_au/cybersecurity-reports/pdfs/at-a-glance.pdf

https://www.udemy.com/comptia-network-cert-n10-007-the-total-course/

https://www.udemy.com/web-security-common-vulnerabilities-and-their-mitigation/?couponCode=LIVE_AND_LEARN

https://www.udemy.com/learn-ethical-hacking-from-scratch/

https://www.simplilearn.com/cyber-security/cissp-certification-training

https://www.isc2.org/Certifications/CISSP

http://www.galgotiasuniversity.edu.in/

https://www.geu.ac.in/content/geu/en.html

http://www.bits-pilani.ac.in/hyderabad/

https://www.upes.ac.in/

Contact Us

65, Brodway Suite, Newyork NY, 10006
PH: +1 (212) 744-1256

Kalas road, Vishrantwadi, Pune,
Maharashtra-411015
PH: +918113865000