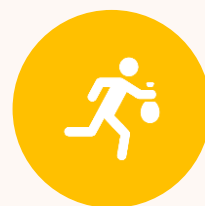# Cyber Security – Career Opportunities

R.Chandrasekhar
Partner- TrustUs LLP

HACKING  RANSOMWARE  CYBER CRIME

# Coverage

INTRO TO CYBER SECURITY/INFORMATION SECURITY

VARIOUS DOMAINS UNDER CYBER SECURITY

QUALIFICATIONS/ CERTIFICATIONS RELEVANT TO CYBER SECURITY

PROBABLE CAREER OPPORTUNITIES/ ROLES

# Introduction

**Cyber Security/Information Security** primarily deals with securing information technology assets- i.e Computing Hardware, Software, Databases, Networks etc.

Goal is to identify **vulnerabilities – weaknesses- and also threats**-factors which can cause loss or damage- like malware/hackers etc.

Implement **necessary controls-** to mitigate the vulnerabilities/threats

# Domains under Cyber Security

| | | | |
|---|---|---|---|
| Application/Software Security | Network Security | Data Protection/Privacy | Data Centre Security |
| Legal/Regulatory Compliances | Business Continuity/Disaster Recovery | Cloud Security | Digital Forensics |

# Software Security

Securing the software we use- say net banking, mobile banking, payment apps etc.

Involves testing the software for bugs, vulnerabilities etc.- both manually and by use of automated software testing tools

Aspects like authentication, encryption, validations are tested

Some specific courses : American Software Testing Qualification Board- International Software Testing Qualification Board

ASTQB®
AMERICAN SOFTWARE TESTING QUALIFICATIONS BOARD
ISTQB Certification in the U.S.

# Network Security

Securing/testing network links- local area networks, wide area networks, wireless networks

Securing/testing network devices- routers, switches

Managing/testing network security components- Firewalls, Intrusion detection systems/Intrusion prevention systems

Being part of Security Operations Controls(SOC) /Network Operations Controls (NOC)

Some specific qualifiactions- CISCO Certifications, PenTest+

## Data Protection

Data is probably the most valuable asset today- competitive advantage

Protecting data involves several aspects- including confidentiality, privacy etc.

Ensure data- in transit, at rest- are secured from unauthorized access, use etc.

Regulatory driven in several countries- GDPR in Europe, PDP in India etc.

Certifications of International Association of Privacy Professionals , Data Security Council of India

# Data Centre Security

Data Centres are today the hub of all IT activities- most critical installation for any Corporate

All the Core Hardware- like Servers, Core Network Devices like L3 Switches, Databases etc. are housed here

Physically securing these facilities, logically securing this facilities and securing them from natural hazards like fires, floods etc. is 24/7/365 job

Certifications like CDCP are relevant in this regard

## Regulatory/Legal Compliances

Several industries are regulated for information and cyber security by the governing bodies

- RBI Regulations for Banks, NBFCs

- SEBI guidelines for MFs, Stockbrokers

- IRDAI regulations for Insurance Companies

- Information Technology Act Compliance for Corporates

- Payment Card Industry Standards (PCI) for card operators, intermediaries like aggregators
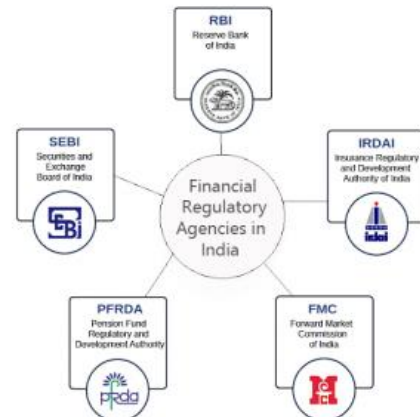
## Business Continuity/Disaster Recovery

Too much reliance on Information Technology- a system failure leads to large scale disruptions

Organisations need to plan and implement stratagies for preventing/recovering from such failures- called BCP/DR
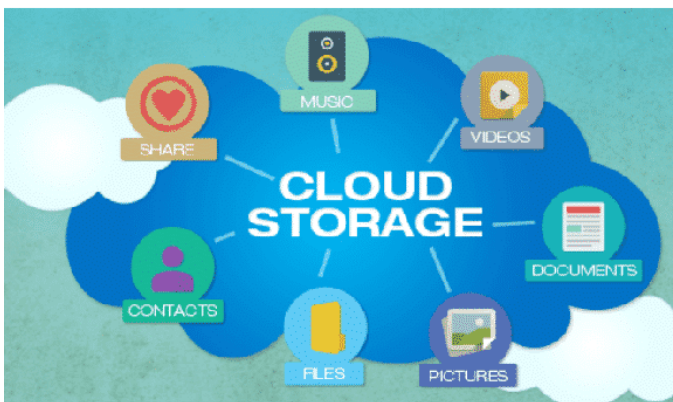
Significant investments made for implementing and managing BCP/DR

Certifications- Offered by DRII, BCI

# Cloud Security



Most businesses moving IT to the Cloud- which is like a pay-per-use/shared service model

Security concerns heightened due to such deployments- as its not owned by any single user- rather a common platform

Securing cloud deployments an emerging area of work

CompTIA Cloud+, Certified Cloud Security Professional (CCSP)

# Digital Forensics

Digital Forensics- involves recovering, analysis and preserving of evidences from digital media like HDD, Mobiles, Emails etc.

Integral part of Cyber Crime Investigation including proceedings in Court of Law

Advanced Forensic Labs emerging

Digital Forensic Essentials- SANS, CDFE- NICCS USA

# Few Global Certifications

- CISA/CRISC/CISM etc. from ISACA

- CISSP/CSSP from ISC2

- Offensive Security Certification (OSCP)

# Full time /Part Time Programs / Courses

- MSc in Cyber Forensics- University of Madras,

- MTech Information Security and Computer Forensics- SRM University

- PG Diploma in Cyber Law- NALSAR

- C-DAC- Cyber Security Programs

# Thank You

**R Chandrasekhar, CISA, CISSP, CDCP**

Partner – Trustus InfoSec Services LLP
Head IS Audit – Yoganandh & Ram LLP

+91 98415 82933

sekhar@trustusinfosec.in

sekhar@yandr.in

# Answers to the queries raised during Q and A session

1. Sir how can v say that our data is safe in cloud and The person who owns it doesn't use our data Wrongly?

   Cloud is nothing but a collection of computer systems which we use connected through internet on pay-per-use model. In any system, be it stand alone, in Data Centre or on the cloud data security is dependent on controls implemented to protect the data. In case of cloud computing, there are specific agreements that the cloud service provider will not misuse or access our data.

2. Is online shopping/online payment safe ?

   Yes- so long as you do it through trusted websites, using $2^{nd}$ factor of authentication like OTP etc. its safe. Never share card details with untrusted sites.

3. Whatsapp says our all chat are END TO END crypted so no one even whatsapp cannot read it,but i noted that when i say HI to someone, for whom i sent this message on their device it ask (can i send reply as) how are you?How is this possible sir?

   Good question. First and foremost we need to understand that most of the times when these Companies say "No one can read" they generally refer to human beings cannot read- however they may have automated tools/softwares which can read the content. In case of WhatsApp , end to end encryption means from the time it leaves your device till it reaches the other device- the moment it reaches the other device, it has to be in readable form only as a human being as to be able to read it- that's when these messages pop up.

4. Which colleges in India offer courses on cyber security and data protection sir? in Tamilnadu which are the top colleges sir?

   There are several institutions offering such programs- you may look up University of Madras, SRM University, C-DAC etc.  For data protection, there are several certifications like from IAPP, DSCI etc.

5. What exams should we take up for cyber crime for example doctor me neet. Like that is there any exam for cyber crime ?

   Except C-DAC I don't think any institution has any entrance exam- its direct entry.

6. Sir in data protection it is possible to delete any of us personal datas ?

If you are referring to our data with online portals like Google, FB etc., yes- the proposed Personal Data Protection Law has a right to delete- generally this is called "Right to be forgotten". As an individual you can write to these Organisations asking them to delete your data with them.

7. When we do transactions through apps accidentally when our mobile switch offs or our data pack gets ended what will happen to the transaction sir?

   Current day mobile apps are built in such a way that if transaction is not successful in entirety, it will fail and if account is debited, it will auto reverse in few hours or days time.

8. Can you give some examples of data centres where students can visit sir?

   Like we discussed during the presentation, data centres are not open for anyone to visit- unless with specific permission.

9. Do IT companies offer these trainings after placement sir?

   Yes- most corporates do offer such training if you choose that line of work. But preferable to go with a certification/qualification in that field from a global organisation or university- as it will be more wholistic.

10. What courses or certifications you undertook to become a cyber security expert/Officer

    Please refer to the PPT shared. Have referred several programs/courses. Kindly note that there is nothing will make us an "Expert" unless we qualify in the relevant field and work for several years specialising in it !!!

11. Legal aspects, will an attorney at law specialize in or anyone can take up the course and become a cyber security attorney sir?

    Yes- please look up courses for NALSAR or other universities- there are several programs.

12. When i use my Desktop sometimes it says your location is being used, when i click that i am not able to see which app used my location so i disabled location on my Desktop but it will be my location still visible to apps in desktop sir?

    Most apps seek your permission to track location/IP Address etc- which we permit . Generally if you block location or any other service, some of the Apps may not function- like maps etc.

13. Sir.Which is better? cyber security degree course or certified courses with any other degrees.

    Both are good. A college program in cyber security + certifications will help.

14. The scope of cyber security is more in which country sir?

    In every country !!! As we are fully dependent on systems everywhere. US, UK, Australia, Middle East and most importantly India have great demand for such qualifications.

15. Sir now a days when we didn't send the account then how they hacked ??

    Hacking is a generic term- account compromise can happen due to variety of reasons- it may be even a compromise at the Bank End, Card service provider end, ATM,POS etc.- not necessarily at customer end.

16. Sir, Are the students can join directly to these courses and need any basic degree

    I would recommend a basic degree- preferably in the same field if that's of interest + global certifications – best combination.

17. How does Firewall and network security apps protects from hackers or some harmful forums??

    In simplest non-technical terms, these are filters- they understand the network traffic and filter few of them based on rules configured.  Just like security guards who check ID etc. before permitting someone to enter, these components check things logically (like source IP address, protocols used , country of origin, whether from black-listed IPs etc.)- hundreds of rules .

18. Is data science a good subject to take for bachelor's for getting into cyber security field??

    Data science is a separate stream altogether- not directly related to cyber security- though cyber security does involve a lot of data analytics- most of which is automated.

19. sir , do we need to coding for cyber security ?

    Not necessarily- but it will help. Cyber Security is much wider in scope beyond coding.

20. Some messages from fraudulent people are same as the genuine websites ,how can we differentiate between fake and genuine ones sir ?

Search engines, spam filters, anti-virus softwares etc. do a lot of analysis based on several factors before they give you an alert that website or mail looks suspicious. Best way to identify is to install a licensed anti-virus software with web filtering capabilities.

21. sir i have a doubt (in future) if i select ethical hacking course is it have value or not sir

Ethical Hacking is a good program- but you will need a lot of work experience in that field – hands on working- to be proficient. Just qualification will not suffice.

22. Namaste Sir, the upcoming crypto currency is getting popular among many corporate companies. Is this safe and is it going to be the future? Is there any assurance that this block chain system won't get hacked

Crypto is in very early stages of commercial usage- we need to wait and watch. RBI is likely to come up with regulations. Yes- things can go wrong here too .

23. What is the difference between data science and Artificial intellegence?

Data Science leads with methods to extract useful information from both structured and unstructured data. AI  in simplest terms are machines thinking like human beings. AI may take inputs from data science- but they are two different fields altogether.

24. What is the main objective of Cyber Security

Primary objective of Information/Cyber Security is to ensure that computing devices are protected from threats like hackers, systems failures etc- through a set of controls. This will ensure that such systems on which we rely on for several things- like banking, online sales, mail system etc.- are well protected and continue to be available to legitimate users with minimum or no downtime.

25. sir while installing a app why do they ask for storage and media access sir and is it safe to give the permissions to the apps sir?

Not all apps are safe and not all permissions granted are assured of proper usage- chances of tracking and misuse is very high. Hence limit usage of Apps to only those absolutely required and are from trusted sources.

26. How can i become a ethical hacker sir. after seeing movies I want to be in forensic either in medical or cyber sir. how can I go to it ?

Good that movies inspire your career !! Ethical hacker qualification is offered by EC-Council. You can take that exam and become a certified Ethical Hacker. However as mentioned in one of the earlier queries qualification alone will not suffice- you need several years of actual work experience to become a proficient ethical hacker.

27. Will AI not replace cyber security roles in future?

   To some extent they will and are actually put to use even now. But it will not completely replace human skills.

28. Sir what exam we have to became  digital forensics ?

   Programs in digital forensics are offered by several institutes- few of them are SANS, CDFE exam by CISA USA etc.

29. sir What can be the impact of a computer network attack?

   Network attacks – especially attacks on WAN like internet - will have same impact of our telephone lines going down- complete communication will come to a stand still. Significant impact- as everything we do today online is network dependent.