Cyber Security Fundamentals

Assignment-2

N Ravinder Reddy

Roll No:

Q.1. Prepare a Case Study on the shortage of cybersecurity professionals in India, its impact on organizations, and the measures needed to address this challenge(Discuss the specific implications for the Indian context)

Ans: A big fight is underway for cybersecurity professionals, with a nearly 30% demand-supply gap for cybersecurity jobs.

There are between 20,000 and 25,000 unfilled positions in cyber security profiles in India currently, and this number is expected to expand as telcos push 5G roll out, and companies continue their digital transformation journeys, staffing experts said.

“(Between) 70-75% of tech companies in India, including IT companies, are looking to hire more cyber security professionals as their existing teams are understaffed or do not have adequate skills to handle the evolving dynamics of internet privacy,” said Sanjay Shetty, director, professional search & selection, and strategic accounts at Randstad India.

Staffing experts add that apart from tech firms, even enterprises are investing in building a cybersecurity workforce as they adopt digitalisation of their processes.

This is in addition to security professionals needed by telcos to ensure secure network operations in both, their enterprise and mobility arm. For telcos, the demand for security experts spans multiple niche profiles given the diversity of security functions that rise due to 5G roll out and its enterprise use cases.

“Profiles like security analyst, incident report analyst, cloud and IoT security experts are going to see an increase in demand as telcos roll out 5G as they push enterprise use cases,” said Kartik Narayan, chief executive-staffing, TeamLease Services.

Indian mobile phone operators are expected to at least double their investments on network security with the 5G roll out expected to spark a surge in network vulnerabilities, which assume critical importance especially for enterprises.

Even if we do not talk about 5G (specifically), the security talent in general in the country is very sparse at the moment. We need to get more (security) professionals in the system," Brijesh Datta, executive vice president & CISO at Reliance Jio, said recentl

The Data Security Council of India has forecast that the cybersecurity ecosystem will expand up to a point where nearly one million professionals will be required by 2025. Additionally, the demand for cloud security skills is estimated to grow by 115% between 2020 and 2025, representing almost 20,000 job openings, Narayan added.

An extensive exercise in reskilling and/or upskilling the existing workforce, believe staffing experts, is one of the ways that telcos can future proof their workforce in this regard.

"Bridging this gap will take diligent upskilling and reskilling endeavours from employers as well as government bodies. To prepare for the 5G technology, several telecom companies have initiated in-house training programmes to upskill their workers," added Sachin Alug,chief executive, NLB Services, a staffing firms.

Bharti Airtel, for example, has been preparing for 5G roll out by upskilling its professionals and offering them certification courses such as CCNA (Cisco Certified Network Associate) and CCNP (Cisco Certified Network Professional). The courses are offered based on skill and eligibility level free of cost.

Even as cyber threats continue to rise in India – the second-largest global active internet user base – the country is currently facing a big skill gap in the cybersecurity domain and represents just six per cent of global cybersecurity jobs, finds a report.
As of May 2023, the industry had about 40,000 open opportunities, indicating the growing demand for skilled cybersecurity professionals. However, the demand-supply gap stood at 30 per cent, projecting a major skill challenge in the industry, finds the study by tech staffing firm TeamLease.

The report further says Indian organizations experienced over 2,000 weekly attacks in Q1 2023, marking an 18 per cent increase compared to the previous year. The healthcare industry was a prime target, with 7.7 per cent of attacks directed towards it. The global weekly cyber-attacks have increased by 7 per cent to surpass 1,200 attacks per week.
According to the report, India's cybersecurity workforce stood at around 0.3 million in 2023, up from 0.21 million in 2022, and 0.1 million in 2021. This compares to the global workforce of some 4.7 million cybersecurity professionals. There is a similar discrepancy when it comes to cybersecurity revenues, with India forming estimated revenue of $2.50 billion out of global revenue of $222 billion.
The staffing firm has projected India's cybersecurity market share to reach $3.5 billion by 2027, with an expected compound annual growth rate (CAGR) of 8.05 per cent.

Sunil Chemmankotil, Chief Executive Officer, TeamLease Digital, said there was “an urgent need for upskilling the workforce and hiring qualified professionals.”

“As India Inc. embraces digital infrastructures, the heightened vulnerability to cyber threats necessitates proactive measures. The prevalence of malware attacks, social engineering tactics, and other sophisticated cyber threats demand a comprehensive approach to safeguarding our digital frontiers,” Chemmankotil said.

Specializations in areas such as data privacy, cloud security, AI security, and network security are in high demand. Soft skills such as problem-solving, communication, teamwork, and collaboration are also essential in this field, as per the staffing firm.

The top job roles identified in the research study include IT auditor, information security analyst, network/IT security engineer/specialist, security testing/penetration tester, and computer forensics analyst, with a base pay ranging from 3 to 6 lakhs for 0-3 years of experience. Moreover, senior and mid-level professionals with over 12 years of experience have the potential to earn an annual salary within the range of 50-80 Lakhs.

Why Is Digital Transformation Difficult?

Digital transformation is not only adopting new software, technologies, and processes that are more efficient and automated than traditional business practices and processes; it’s an entirely new, innovative way of doing something that is core to your business.

That means organizations must consider everything when taking on a digital transformation initiative – from how people will react to the change, how it will impact customer relations, the cost, how it will align with business goals, etc. Digital transformations empower organizations to take their business into the future, position companies to withstand competition, and grow into new areas.

Digital transformation is difficult for several reasons, including:

- **Complexity**: Digital transformation involves legacy application modernization and the integration of various technologies, processes, and strategies, which can be intricate and challenging to implement and manage.
- **Organizational resistance**: Change can be uncomfortable, and organizations may face resistance from employees who are accustomed to traditional ways of working, making it difficult to embrace new technologies and processes.
- **Skills gap**: There is often a shortage of skilled professionals with the expertise required to drive digital transformation efforts, creating a significant talent gap that organizations must address.
- **Legacy systems**: Outdated infrastructure and systems can hinder the adoption of modern technologies, leading to technical debt and difficulties in transitioning to new digital solutions.

- **Strategy and vision**: Developing a clear digital transformation strategy that aligns with an organization's overall business goals is challenging, and inadequate vision or leadership can impede progress.
- **Security and privacy concerns**: Ensuring data protection and compliance with privacy regulations is a critical aspect of digital transformation, but it can be difficult to manage and maintain.
- **Resource constraints**: Digital transformation often requires significant investment in technology, skills, and resources, which may be limited for some organizations, particularly small and medium-sized businesses.
- **Evolving landscape**: The digital landscape is continuously changing, making it difficult for organizations to keep pace with new technologies, trends, and customer expectations.
- **Measuring success:** Quantifying the return on investment (ROI) of digital transformation efforts can be challenging, as benefits may not be immediately apparent or easily quantifiable.

Q.2. Analyze a significant cyber attack(s) that has affected an Indian organization or institution. Evaluate the specific challenges faced, the response to the incident, and the lessons learned.

Ans:

For example, in December 2020, **a global cyberattack on SolarWinds, a US-based software company that provides network management tools**, affected several Indian organisations, including the National Informatics Centre (NIC), the Ministry of Electronics and Information Technology (MeitY), and Bharat Heavy Electricals.

The Union government on Thursday, December 16 2023, informed the Rajya Sabha that five servers of the All India Institute of Medical Sciences (AIIMS) were affected by the recent cyberattack and an estimated 1.3 terabytes of data was encrypted.

The government was responding to a question by Communist Party of India (Marxist) MP John Brittas. He had asked the government if AIIMS servers had been hacked by ransomware, the quantum of data that was compromised, and the steps taken to prevent such incidents.

In response to his question, the minister of electronics and information technology, Rajeev Chandrasekhar, said in a written reply in the Upper House that there was a "cyber security incident" at AIIMS, which manages its own information and computer systems.

He added that the Indian Computer Emergency Response Team (CERT-In) evaluated the incident. "As per preliminary analysis, servers were compromised in the information technology network of AIIMS by unknown

threat actors due to improper network segmentation, which caused operational disruption due to non-functionality of critical applications," he said.

He added that "CERT-In and other stakeholder entities have advised necessary remedial measures."

On the quantum of data that was impacted, the minister said "five servers of AIIMS were affected and approximately 1.3 terabytes of data was encrypted."

In the Lok Sabha, responding to questions from several MPs, the minister of state for health and family welfare Bharati Pravin Pawar said that no specific amount of ransom was demanded by the hackers "though a message was discovered on the server suggesting that it was a cyberattack".

"All the data for e- Hospital has been retrieved from a backup server which was unaffected and restored on new servers. Most of the functions of e-Hospital application like patient registration, appointment, admission, discharge etc. have been restored after two weeks of the cyber-attack," she said.

'CERT-In has counter plan for attacks'

Chandrasekhar told the Rajya Sabha that a Cyber Crisis Management Plan for countering cyberattacks and cyberterrorism had been formulated by CERT-In for implementation by all ministries and departments of the Union and state governments and their organisations and critical sectors.

He added that CERT-In has been mandated to track and monitor cyber security incidents and a "special advisory on security practices to enhance resilience of health sector entities has been communicated by CERT-In to the Ministry of Health and Family Welfare, for sensitising health sector entities regarding latest cybersecurity threats."

He said the ministry has been requested to disseminate the advisory among all authorised medical care entities/service providers in the country. "It has also been suggested that they may carry out special audit through CERT-In-empanelled auditors on a priority basis, comply with the findings of such audit and ensure implementation of security best practices," he added.

In his written reply, the minister said CERT-In has been issuing alerts and advisories regarding the latest cyber threats/vulnerabilities and countermeasures to protect computers and networks, on an ongoing basis. It said the team also published "India Ransomware Report H1 – 2022" in August 2022, covering the latest tactics and techniques of ransomware attackers and ransomware-specific incident response and mitigation measures.

Earlier, investigations into the cyberattack, which had crippled the functioning of the premier health institution in New Delhi, had revealed that

"the IP addresses of two emails, which were identified from the headers of files that were encrypted by the hackers, originated from Hong Kong and China's Henan province".

A recent news report stated that the cyberattack is feared to have compromised the records of nearly 3-4 crore patients, including high-profile political personalities. The investigations by CERT-In, it said, revealed that the hackers had two Protonmail addresses – "dog2398" and "mouse63209". The encrypted files were sent to these two Protonmail IDs through CERT-In and Interpol.

The report said these two addresses, 'dog2398' and 'mouse63209', were generated in the first week of November in Hong Kong. Another encrypted file was sent from Henan in China.

Investigations also revealed that the targeted servers were infected with three ransomware: Wammacry, Mimikatz and Trojan. "CERT-In and DRDO (CIRA) found five servers of NIC infected with ransomware and seven servers of the computer facility in AIIMS infected with these three ransomware," the *IE* report quoted sources as saying

Q. 3. Investigate the top cybersecurity problems faced by universities and colleges, with a focus on the specific types of cyberattacks targeting higher education institutions.

Ans: Biggest Threats to the Education Sector This includes **phishing attacks and ransomware attacks**. Cybercriminals benefit from access credentials to gain access to a school or university network. The most common way for them to get such credentials is via a successful phishing attempt.

Educational institutions are among the top targets for hackers and cybercriminals. Education is among the sectors that experience the most cyber attacks, including healthcare, finance, and retail.

According to Check Point's Mid-Year Report for 2022, the education sector had 44% more cyber attacks than the year earlier. An average of about 2300 attacks against educational organizations were reported weekly.

These figures are alarming — though conservative by some estimates —- because the education sector is a prime target for cyber attacks due to a combination of valuable data, lack of cyber risk awareness, and significant, widespread vulnerabilities.

Why Do Cybercriminals Target the Education Industry?

Educational institutions are targeted for a number of reasons, primarily for the amount of personal student data that they handle, along with student loan information, confidential research data, and a lack of adequate cybersecurity.

Personal Data

From local kindergartens to internationally renowned higher education institutions, all educational organizations keep data on the learners enrolled with them. This data may include personally identifiable information, such as:

- Full names
- Street addresses
- Email addresses
- Phone numbers
- Grades and aptitude information
- Credit card details
- Social security numbers
- Student loan information

The bigger the organization, the more records it is likely to store. Unfortunately, from a cybersecurity standpoint, a larger organization is likely to have organizational and security challenges and large amounts of student data.

This means that threat actors know where they might find large amounts of personal data and where that data is likely to be easy to access.

Valuable Research Data

Universities often perform cutting-edge research and such intellectual property (IP) can be worth millions of dollars. While university researchers might think of the prestige of developing techniques and making discoveries, failing to think about cybersecurity to protect this research can make it vulnerable to data leaks and data breaches.

Cybercriminals able to access a network can steal IPs to sell on the dark web. Alternatively, they may encrypt the data as part of a ransomware attack, threatening to upload or destroy it if the institution does not pay.

Lack of Cybersecurity

The education sector is one of the slowest adopters of modern cybersecurity solutions typically due to a lack of funding which can lead to the use of outdated technology, limited resources to invest in cyber solutions, and ever-growing institution sizes. Public schools receive funding from the government,

which in turn can result in many budget constraints, and in turn, cybersecurity is often deprioritized in favor of staff salaries, school resources, and infrastructure upgrades.

However, this has proven to be particularly damaging to educational institutions because cybercriminals often target the schools with the least funding since they typically have poor cyber defenses.

One recent example of this is Lincoln College, which shut down in 2022 due to a ransomware attack that crippled the entire school. Because the school was already facing budgetary issues due to COVID-19, the school would ultimately fail to recover from the cyber attack.

Biggest Threats to the Education Sector

Social Engineering

Social engineering is the most significant threat to the education sector. This includes phishing attacks and ransomware attacks.

Cybercriminals benefit from access credentials to gain access to a school or university network. The most common way for them to get such credentials is via a successful phishing attempt.

With the personal data acquired during a phishing attempt, cybercriminals can target more high-profile individuals with spear phishing and whaling attacks. Phishing is also a vector for malware, including ransomware.

Ransomware gangs are known to attack specific school districts as they will have researched their cybersecurity capabilities and how much ransom they can afford to pay. This research tells cybercriminals which school systems are prime targets for attacks.

Distributed Denial of Service (DDoS) Attacks

The education sector also has a significant risk of DDoS attacks, which could impact students trying to access learning resources or submit time-sensitive assignments online. DDoS attacks are meant to deny access to various websites or domains and force a server overload, which can significantly impact day-to-day operations.

This attack is a risk for all education facilities since the motivation is not normally financial gain but to cause disruption. A DDoS attack can impact the university's ability to function and can lead to reputational damage.

Another reason DDoS attacks are a significant threat to the education industry is that it's relatively straightforward to carry out such an attack compared to other cyber attacks. A disgruntled teacher or student could

spearhead this attack successfully, especially if the educational institution were typically ill-prepared for cyber attacks.

Cyber Espionage

Spyware, insider threat, and other forms of cyber espionage are also a threat to the education industry, particularly higher education institutions that perform valuable research.

University research is frequently scientific, medical, or engineering-related. The theft of this work can give a professional organization an unfair competitive advantage, giving them the knowledge without investing time and money into research. For this reason, cyber espionage is often funded by corporate entities.

Alternatively, a cybercriminal may be focused on data theft because they intend to sell the research on the dark web.

Reasons that the Education Sector is Vulnerable to Hackers

Several factors common to educational institutions make them more susceptible to cyber attacks and hackers than organizations in other sectors. These are as follows:

New Learning Technologies

During the COVID-19 pandemic, many schools and universities turned to remote working and remote learning to minimize the impact on their students. This increased attack surfaces by adding many new endpoints to education networks. These endpoints were frequently unvetted personal devices using unvetted connections.

Q. 4. Select and analyze three real-world malware attacks, covering different malware types such as viruses, worms, and ransomware. For each case, describe the attack vector, the target, the impact.

Ans:

A malware attack is a common cyberattack where malware (normally malicious software) executes unauthorized actions on the victim's system. The malicious software (a.k.a. virus) encompasses many specific types of attacks such as ransomware, spyware, command and control, and more.

Criminal organizations, state actors, and even well-known businesses have been accused of (and, in some cases, caught) deploying malware. Like other types of cyber attacks, some malware attacks end up with mainstream news coverage due to their severe impact.

An example of a famous malware attack is the WannaCry ransomeware attack.

Malware Attacks Examined

Malware discussion typically encompasses three main aspects:

- Objective: What the malware is designed to achieve
- Delivery: How the malware is delivered to the target
- Concealment: How the malware avoids detection (this item is beyond the scope of this discussion)

Here's a breakdown of some of the objectives and delivery mechanisms observed in malware.

Objectives

Malware is created with an objective in mind. While it could be said that the objective is "limited only to the imagination of its creator," this will focus on some of the most common objectives observed in malware.

Exfiltrate Information

Stealing data, credentials, payment information, etc. is a recurring theme in the realm of cybercrime. Malware focused on this type of theft can be extremely costly to a person, company, or government target that falls victim.

Disrupt Operations

Actively working to "cause problems" for a target's operation is another objective seen in malware. From a virus on a single computer corrupting critical OS files (making that one system unusable) to an orchestrated, physical self-destruction of many systems in an installation, the level of "disruption" can vary. And there's also the scenario where infected systems are directed to carry out large-scale distributed denial of service (DDOS) attacks.

Demand Payment

Some malware is focused on directly extorting money from the target. Scareware uses empty threats (ones which are unsubstantiated and/or couldn't actually be carried out) to "scare" the target into paying some money. Ransomware is a type of malware that attempts to prevent a target from accessing their data (usually by encrypting files on the target) until the target

"pays up." While there is debate over whether victims of ransomware should or should not pay, it has become enough of a threat that some companies have preemptively purchased Bitcoin just in case they get hit with ransomware and decide to pay the ransom.

Types of Malware Attack Vectors

There are three main types of malware attack vectors:

- **Trojan Horse:** This is a program which appears to be one thing (e.g. a game, a useful application, etc.) but is really a delivery mechanism for malware. A trojan horse relies on the user to download it (usually from the internet or via email attachment) and run it on the target.
- **Virus:** A virus is a type of self-propagating malware which infects other programs/files (or even parts of the operating system and/or hard drive) of a target via code injection. This behavior of malware propagation through injecting itself into existing software/data is a differentiator between a virus and a trojan horse (which has purposely built malware into one specific application and does not make attempts to infect others).
- **Worm:** Malware designed to propagate itself into other systems is a worm. While virus and trojan horse malware are localized to one infected target system, a worm actively works to infect other targets (sometimes without any interaction on the user's behalf).

Over the years, malware has been observed to use a variety of different delivery mechanisms, or attack vectors. While a few are admittedly academic, many attack vectors are effective at compromising their targets. These attack vectors generally occur over electronic communications such as email, text, vulnerable network service, or compromised website, malware delivery can also be achieved via physical media (e.g. USB thumb drive, CD/DVD, etc.).

Best Practices Against Malware Attacks

The following best practices can help prevent a malware attack from succeeding and/or mitigate the damage done by a malware attack.

Continuous User Education

Training users on best practices for avoiding malware (i.e. don't download and run unknown software, don't blindly insert "found media" into your computer), as well as how to identify potential malware (i.e. phishing emails, unexpected applications/processes running on a system) can go a long way in protecting an organization. Periodic, unannounced exercises, such as intentional phishing campaigns, can help keep users aware and observant. Learn more about security awareness training.

Use Reputable A/V Software

When installed, a suitable A/V solution will detect (and remove) any existing malware on a system, as well as monitor for and mitigate potential malware installation or activity while the system is running. It'll be important to keep it up-to-date with the vendor's latest definitions/signatures.

Ensure Your Network is Secure

Controlling access to systems on your organization's network is a great idea for many reasons. Use of proven technology and methodologies—such as using a firewall, IPS, IDS, and remote access only through VPN—will help minimize the attack "surface" your organization exposes. Physical system isolation is usually considered an extreme measure for most organizations, and is still vulnerable to some attack vectors.

Perform Regular Website Security Audits

Scanning your organization's websites regularly for vulnerabilities (i.e. software with known bugs, server/service/application misconfiguration) and to detect if known malware has been installed can keep your organization secure, protect your users, and protect customers and visitors for public-facing sites.

Create Regular, Verified Backups

Having a regular (i.e. current and automated) offline backup can be the difference between smoothly recovering from a destructive virus or ransomware attack and stressful, frantic scrambling with costly downtime/data-loss. The key here is to actually have regular backups that are verified to be happening on the expected regular basis and are usable for restore operations. Old, outdated backups are less valuable than recent ones, and backups that don't restore properly are of no value.

Malware Summary

Malware takes on many different forms and attacks in different ways. But with some thoughtful preparation and process improvements, as well as ongoing user education, your organization can gain-and-maintain a solid security stance against malware attacks.

An attack vector, or threat vector, is **a way for attackers to enter a network or system**. Common attack vectors include social engineering attacks, credential theft, vulnerability exploits, and insufficient protection against insider threats.

Weak or compromised access credentials. Compromised access credentials give hackers a linear path into a computer system or organizational network. ...
Phishing.
Malware.

Unpatched software.
Third-party vendors & service providers.
Insider threats.
Lack of encryption.
Misconfigurations

Attack vectors take many different forms, ranging from **malware and ransomware, to man-in-the-middle attacks, compromised credentials, and phishing**. Some attack vectors target weaknesses in your security and overall infrastructure, others target weaknesses in the humans that have access to your network.

Q. 5. Provide Comparative Analysis on DES, AES, RSA.

Ans: Cryptography is playing a fantastic role in shielding our records from steal by way of hackers. These days everywhere anybody is using internet for sending information,information,cryptography play a excellent function in protective those facts from frauders,hackers.Cryptography has distinctive algorithm for encrypting the information earlier than sending it to receiver. The Cryptography set of rules will continually remodel the plaintext into ciphertext which cannot recognize by way of unknown individual. So, sending a message to the receiver calls for encrypting that message with the sender's public key. The textual content encrypted with a private key can handiest be decrypted with the equal public key. This paper represents the evaluation of DES,AES,RSA set of rules. these algorithms are one-of-a-kind from every other based totally on time taken to encrypt or decrypt the given information

	Parameters	**AES**	**DES**	**RSA**
i.	Computation Time	Faster	Moderate	Slower
ii.	Memory Utilization	Requires moderate memory space	Requires least memory space	Requires more memory space
iii.	Security Level	Excellent Security	Adequate	Least Secure

As we know securing the data is becoming a big issue now a day. Today is the era of technology, so there is big need to keep our data very secure. As numbers of users are increasing day by day the need to secure the data is become a big challenge now. First of all, we need to classify that data before securing it. Though classification we divided the data. In this paper we divided the data into two parts sensitive and non-sensitive. By the usage of KNN classifier classification is performed initially. Than by apply different security mechanisms and performed the comparison among these security algorithms. We apply RSA, AES and DES one by one to our datasets. We calculate at end encryption time. Securing the data is challenging task. If we want security than there is need to keep the data very secure. Through security we provide confidentiality to the users. The results obtained at end shown AES is strongest as compared to DES, RSA

For secure and save our data encryption is a good method. Cloud security refers to broad set of policies, technologies and controls deployed to protect data, associated applications and the infrastructure of cloud computing. Cloud Computing and storage provides users with capabilities to store and process their data in third-party data centers. Organizations use the cloud in a variety of different service models and deployment models. Security concerns associated with cloud computing fall into two categories: Security issues faced by cloud providers and security issues faced by their customers. Somani and Mundra (2010) proposed RSA algorithm issued to ensure the confidentiality aspect of security where as digital signatures were used to enhance more security by authenticating it through digital signatures. The approach used carryout encryption in 5 steps. In first step key is generated in second step digital signing is performed and in step 3 and step 4 encryption and decryption were carried out in last step signature verification is performed.

Dubey and Shrivastava (2012) they provide at two-way security protocol which helps both the cloud and the normal user. They applied RSA and MD5 algorithm. When the cloud user uploads the data in the cloud environment, the data is uploaded in encrypted from using RSA algorithm and the cloud admin can decrypt using their own private key for updating the data in the cloud environment admin request the user for a secure key. Cloud users ends a secure key with message digest tag for updating data if any outsiders perform a change in the key, the tag bit is also changed indicating key is not secure and correct.