Indicative Model Question Paper
Professional Programme
Syllabus 2022
Artificial Intelligence, Data Analytics and Cyber Security –Laws & Practice

Time allowed: 3 hours ***Maximum marks: 100***

NOTE: Answer ALL Questions

Question 1. Read the following case study and answer the questions that follow:

M/s Tech Info consulting firm sent a small team to South America to complete a client project. During their stay, an employee used a business debit card at a local ATM. A month after returning to the US, the firm received overdraft notices from their bank. They identified fraudulent withdrawals of $10,000, all originating from South America. There was an additional $1,000 overdraft fee.

The criminals installed an ATM skimmer device to record card account credentials. Many false debit cards were manufactured and used at ATMs in different cities across South America.

Realizing they had been defrauded, the firm contacted their bank and closed the impacted account immediately. Their attempts to pursue reimbursement from the bank were unsuccessful. The commercial account used at the ATM for local currency had different protections from consumer accounts and the bank was not required to reimburse them for their losses. The bank went on to deduct the $1,000 overdraft fee from the firm owner's personal account. The firm severed ties with that bank. The new bank offered comprehensive fraud protection guarantees. The firm created two business accounts: one for receiving funds and making small transfers and another one for small expense payments. The firm updated travel protocols, banning the use of company-provided debit cards. Employees now prepay expenses electronically, pay cash, or use a major credit card, as necessary.

The entire cash reserve for the small business was wiped out, netting losses of almost $15,000.

In view of the above, answer the following:

(i) Knowing how the firm responded, what would you have done differently?
(ii) What are some steps you think the firm could have taken to prevent this incident?
(iii) Is your business susceptible?
(iv) How are you going to reduce your risk?
(v) Explain efforts made by India to ensure cybersecurity.

(5 Marks each)

Question 2.

(a) A small family-owned construction company made extensive use of online banking and Automated Clearing House (ACH) transfers. Employees logged in with both company and user-specific ID and password. Two challenge questions had to be answered for transactions over Rs.10,000. The owner was notified that an ACH transfer of Rs. 1,00,000 was initiated by an unknown source. They contacted the bank and identified that in just one-week cybercriminals had made six transfers from the company bank accounts, totaling Rs. 5,50,000. Cybercriminals were able to install malware onto the company's computers, using a keylogger to capture the banking credentials.

One of their employees had opened an email from what they thought was a materials supplier but was instead a malicious email laced with malware from an imposter account. How this malware impacted the banking transactions of the company?

(5 Marks)

(b) One group of cyber attackers transferred Rs. 10,00,000 from one of the Indian banks to another foreign bank situated in London. The criminals have hacked into the bank's computer system network through the use of some information they acquired from the keylogger programs.

What do you understand by keylogger? What type of keylogger used in the above scenario.

(5 Marks)

(c) A new start-up SME (Small-Medium Enterprise) based in Singapore with an E-government model has recently noticed anomalies in its accounting and product records. It has undertaken an initial check of system log files, and there are several suspicious entries and IP addresses with a large amount of data being sent outside the company firewall. They have also recently received several customer complaints saying that there is often a strange message displayed during order processing, and they are often re-directed to a payment page that does not look legitimate.

What do you understand by cybersecurity forensics and how would you like to have cybersecurity forensics for the given scenario?

(5 Marks)

(d) The accused in the case were working in a BPO, that was handling the business of a multinational bank. The accused, during the course of their work had obtained Personal Identification Numbers (PIN) and other confidential information about the bank's customers. Using these the accused and their accomplices, through different cyber cafes, transferred huge amount of money from the accounts of different customers to fake accounts.

How are you going to reduce your risk of online banking specific in the above scenario?

(5 Marks)

(e) Analytics is the discovery and communication of meaningful patterns in data. Especially, valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistics, computer programming, and operation research to qualify performance. Analytics often favors data visualization to communicate insight. In a nutshell, analytics is the scientific process of transforming data into insight for making better decisions. Data Analytics aims to get actionable insights resulting in smarter decisions and better business outcomes. It is critical to design and built a data warehouse or Business Intelligence (BI) architecture that provides a flexible, multi-faceted analytical ecosystem, optimized for efficient ingestion and analysis of large and diverse data sets.

What is Data Analytics and Business Intelligence?

(5 Marks)

Question 3.

(a) Mr. Akash is running one small business with his family. Their employees do the online transactions by logged in with both company and user-specific IDs and password. The net banking facility of their bank won't allow any transaction without giving answers to two challenge questions for transactions over Rs.1,000. They receive few messages of debit form their company accounts which were initiated by an unknown source. They contacted the bank and identified that in just one-week cybercriminals had made ten transfers from the company bank accounts for Rs. 4,50,000. Cybercriminals had installed the malware onto the company's computers, using a keylogger to capture the banking credentials.

One of their employees received an email from an unknown sender about winning a lottery price of $1,00,000 and he opened that email on his office laptop which he used for net banking transactions. That email was malicious email laced with malware from an imposter account. What precautions one should have while reading email received from an unknown sender?

(5 Marks)

(b) ACH (Automated Clearing House) is run by an organisation called Nacha (previously NACHA - National Automated Clearing House Association) and may also be referred to as the ACH network or ACH scheme. Payment processing via the ACH network has existed since the 1970s. ACH moved financial transactions worth more than Rs.72.6 trillion in 2021, an increase of over 17 percent from the previous year.

What do you understand by Automated Clearing House (ACH) transfers?

(5 Marks)

(c) A staff member in advisory practice opened a file attached to an email received one morning. It turned out the attachment contained a 'worm' that infected not only the staff member's computer, but it also spread to all other computers in the practice network. This malware caused all computers in the office to shut down. The adviser needed to use the platform software that day to ensure his clients participated in a Corporate Action that was closing the following day. With the help from their Business Development Manager, the office worked through the issue, so they were able to log into the platform software to complete this critical work from a home laptop that hadn't been infected with the virus.

Define malware and how you would like to save your system through malware in the above scenario?

(5 Marks)

(d) Technological advances have great societal benefits and make it easier for people to access information, and to collaborate with their communities. They also expose users to risks such as cybercrime, identity theft or misuse of personal data. Software companies share a responsibility to design and operate products and services in a manner that both helps protect customers from these harms and promotes respect for fundamental rights. And software companies share, with many other stakeholders, a collective responsibility to help make the Internet more reliable and trustworthy.
How are you going to improve the security aspects in the above scenario?

(5 Marks)

(e) The banking systems need reporting systems and improve the data warehouse architecture to achieve a smooth and consistent workflow. The challenge was to develop and integrate a data warehouse, to implement a liquidity risk management system in cooperation with the European Bank for Reconstruction and Development. The final goal was to get a "golden source" and develop the main analytical and reporting dashboards.
Define data warehouse architecture for the above scenario?

(5 Marks)

Question 4.

(a) Imagine a scenario where you are visiting some websites and one of them seems to be a little slow. You might blame their servers to improve their scalability as they might be experiencing a lot of user traffic on their site. Most of the sites already take this issue into account beforehand. Chances are, they might be a victim of what is known as a DDoS attack, Distributed Denial of Service Attack.

Discuss the types of DDoS (Distributed Denial of Service) used in the above scenario.

(5 Marks)

(b) The online threat landscape continues to evolve at an accelerating pace with hackers launching more distributed denial of service attacks than ever before, taking aim at new targets, and creating new botnets. The demand for solutions for a wide range of business needs and the rollout of 5G technologies has accelerated the proliferation of Internet of Things (IoT) around the world, creating a huge pool of unsuspecting and under protected new recruits for botnet armies used to launch attacks on massive scales. DDoS attacks are expected to continue to increase in number and complexity as botnets and inexpensive DDoS-as-a-service platforms proliferate.
Based on the above scenario differentiate the DoS and DDoS attack.

(5 Marks)

(c) Mr. B want to start a new business of trading of readymade garments. He wants to set up his office in his home. He approached you to get knowledge of hardware and software required to set up his small office at home. Assume you are computer hardware and software specialist and advise him as per his requirements.

(5 Marks)

(d) ABC Hospital is top ranked hospital out of 10 pediatric specialty hospitals, with about 25,000 inpatient admissions each year and 5,28,000 patients' visits scheduled annually through 200 plus specialized clinical programs. One fine day their computer systems were stopped working and the entire network go down. Later on, it came to their knowledge that the hackers entered in to their server and the entire data of patients was stolen.

Now hospital want to know that what remedies for such cyber-attack on their server are available for an organization and under which law?

(5 Marks)

(e) Company X is in retail business that wants to improve its sales. They have collected data on their sales over the past year, including information on the products that were sold, the location of the stores, and the demographics of the customers. The data analytics team at Company X is asked to analyze this data to identify trends and patterns that can inform the company's sales strategy.

Discuss the different approach of Data Analytics?

(5 Marks)