183/2024 **(Pages : 2)**

SHORTHAND DICTATION

Maximum : 100 marks

Time for Dictation : 5 minutes

Time for Transcription : 1 hour

Instructions :

(1) The following matter should be dictated to the candidates loudly and distinctly and only once, at a speed of 120 words per minute.

(2) Speed should be regulated at every quarter of the minute.

(3) Before commencement of the dictation, the candidates should be asked to take down the matter in short-hand and transcribe into longhand in ink.

As enterprises, the government and public rely increasingly on digitalisation, cybersecurity has become pivotal to their basic functioning nowadays. Cyberattacks have been on the rise over the past 12-18 months, / affecting businesses of all nature and sizes, where the reliability of the data network is a prerequisite to their operations. As a result, cybersecurity has come to occupy a prime // position in a company's list of governance priorities. As more companies shifted to work from home, there were database breaches and hackings, leading to loss of ///revenue opportunity across industries ///. Even systems believed to be highly secure could be breached in cyberattacks. Reports say almost 26,000 Indian websites were hacked in the 10-month period ended October. The hackers had been [1] operating from different parts of the world with hidden identities.

While weak passwords are the common cause for such attacks, systems with unprotected or unchanged passwords are highly vulnerable. Second, / different types of malware take advantage of expired antivirus software. Third, working in unsecured environments such as a common Wi-Fi network to access private emails and USB drives may prove // risky. The onus is on the organization to take steps to prevent and counter potential threats. They should educate their employees to create strong passwords, being insisted upon in organisations. /// Internal threats could be a result of employee negligence follow proper protocols in keeping passwords secure and ensure firewalls are equipped to resist any malware attacks by installing regular software [2] updates. This is also why virtual private networks are or ignorance, while external threats could be from former employees, competitors, and hackers who steal / corporate data and money through / spoofing and phishing. These would obviously need to reputational damage, financial loss, litigation, regulatory probes, and above all, loss of clients and thereby revenue.

[P.T.O.]

Ransom ware attacks continues to evolve // in the market, with the past 8-10 months witnessing the highest number of threats of sensitive data exposure. A leading social network platform suffered a data breach, wherein millions of /// profiles containing email addresses, names, dates of birth, and phone numbers were sold on the dark Web. In another incident, a large foreign bank was hacked, causing financial loss. Ransom [3] attackers can expose employees' HR files or clients' vulnerable data. Insurers also add crime policies to cover collusion by staff. There are cyber insurance solutions available in the market to / protect against losses caused by cyberattacks, including first-party and third-party losses, and cyber extortion.

First-party insurance covers loss caused due to electronic theft, loss of electronic communication, e-vandalism, business // interruption and the like. Third-party loss covers disclosure liability, content liability. reputational liability, and conduit liability. An expenses cover includes privacy notification expenses; crisis expenses and reward expenses. A few /// insurers even provide cover for proactive forensic services in a possible threat situation. Companies should first understand the need for cyber insurance solutions rather than just getting a cyber insurance [4] cover. Cyber insurance helps cover legal expenses stemming from damages due to a cyberattack. It should be part of the company's overall business continuity strategy, as it helps quickly recover / post an incident.

The ability to identify an attack and quickly shield against it are a few underwriting principles of the insurers. Insurers conduct meticulous due diligence via proposal forms, // interaction, network diagrams and reviews of cyber strategies of a firm before providing cyber insurance covers insurers check the process of Multi –Factor Authentication, tested backups, network monitoring, and whether /// the users are employees or vendors. Buying a cyber insurance policy alone will not suffice; the company should ensure that protocols are followed strictly and train employees in digital hygiene. [5]