UNIT-1 INITIAL POST

There is an increased danger of large-scale or high-consequence incidents that could cause harm or interrupt services that our economy and the daily lives of millions of people depend on as information technology (IT) becomes more integrated with physical infrastructure operations. Because of the danger and potential effects of cyber events, it has become a vital security mission to increase the security and resilience of cyberspace. [CISA]

Health care and financial services are the two industries most frequently affected by data breaches. Breaches are common in the healthcare industry. A variety of things can lead to this, such as credential-stealing malware, an insider mistakenly or purposefully disclosing patient data, or misplaced devices.

Cyber criminals more likely target medical databases as PHI (Personal Health Information) earns them more money value than credit card numbers or regular Personally Identifiable Information (PII) because, unlike credit card numbers or Social Security numbers, it cannot be changed.

More than 40 million people's health records were compromised in significant data breaches in 2021, according to the US Department of Health and Human Services' website. Health data breaches reported to the HHS website in 2021 were overwhelmingly due to hacking/IT incidents. [USDHHS]

Data breaches can have a wide range of negative effects on a company, including revenue reduction, long-term damage to a company's brand reputation, and a reduction in the company's ability to compete in the market through Intellectual-Property loss. Legal expenditures, investigation fees, and regulatory fines are only a few examples of the hidden costs.

So it's must for businesses to invest in cybersecurity measures. Physical security, awareness trainings, zero-trust framework, data encryption, email and online security and firewalls are just some of the techniques to defend from cyber-attacks, but there are many more.

Quoting the following which appears perfect to me with today's cybercrime situation -

"To create a cyber-secure world, we must be as fast and globally integrated as the cyber-criminals." [David Lipton ,2020]

REFERENCES:

1. CISA [N.D]
   https://www.cisa.gov/cybersecurity#:~:text=CISA's%20Role%20in%20Cybersecurity&text=Cyberspace%20is%20particularly%20difficult%20to,consequences%20in%20complex%20cyber%20networks.
2. CIS [N.D]: Data Breaches: In the Healthcare Sector
   https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector
3. USDHHS [N.D]: U.S. Department of Health and Human Services
   https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
4. David Lipton (2020): Cybersecurity Threats Call for a Global Response
   https://blogs.imf.org/2020/01/13/cybersecurity-threats-call-for-a-global-response/