Individual Essay – The human factor in Queens Medical Centre – Michael Geiger

Introduction:

- Special obligations of the Community Clinic in relation to GDPR (Article 5f) due to sensitive patient data (GDPR, 2022). Protective measures relate to a technical as well as an organizational level.
- Cyber Security Breaches Survey 2019: "fraudulent emails ob being directed to fraudulent websites" is the most common cause of a breach.

Human factors:

- 2020 Data Breach Investigations Report (Langlois, 2020): Human factor threats for breaches:
  1. Social
     Threats such as phishing and pretexting, which aim to obtain unauthorised information, can be listed under the social factor.

Social threats affect employees at all levels as well as patients.

Phishing represents one of the biggest threats for companies to release sensitive information to unauthorised persons and can be used as a first step for further cyber attacks.

Particular danger of spear phishing.

Both employees and patients must be made aware of the danger.

Information campaigns, spam recognition training, behavioural training and clear company guidelines and policies can help to reduce this risk.

  2. Misuse
     The misuse factor relates to administrative abuse, use of non-approved assets and policy violations. Data mishandling, privilege abuse, email misuse and knowledge abuse are threats that fall under this factor.

Misuse can be accidental or intentional.

While accidental misuse can be reduced through staff training, intentional misuse poses an inherent risk.

There are behaviours that can indicate malicious insiders, these are: Immaturity, Low self-esteem, Amoral and unethical, Superficial, restlessness and impulsiveness, lack conscientiousness, manipulative, emotionally unstable and mood swings.

Accidental misuse can result from a lack of knowledge/skills, human performance limitations and human error.

Since competence and human performance limitations are central aspects of the threat of misuse, these must be given special consideration.

3. Human Error
   Actions are summarised under human error, which were carried out or omitted incorrectly or inadvertently. This includes threats such as misconfiguration, disposal error, loss, and misdelivery.

Human error is closely related to accidental misuse, but different influencing factors can be identified in relation to the human factor.

The same influencing factors as in the case of accidental misuse are a lack of knowledge and human performance limitations.

In addition, there are other influencing factors that can lead to human error, including: short and long-term memory, external sources of interference (noise and other distractions), cognitive limitations and stress.