Security Review: How people can be managed to overcome cyber security attacks from the inside.

Security threats do not just originate from external hackers. There can be many threats to security which occur from inside the organisation. These can be mitigated using the following strategies:

1. **Access Control**
   The principal of least privilege limits users to the minimum level of access rights to perform their job function. T

2. **Monitoring**
   In particular, event monitoring is crucial when resolving any security attack from the inside. Effective monitoring ensures that any attack is not deniable as there is a log of events.

3. **Authentication**
   Systems should always use secure authentication, over insecure authentication. This could include, for example, the use of multi-factor authentication and the use of secure, hashed passwords.

4. **Documented Information**
   Secure systems must be accompanied by documentation. For example, UML diagrams may document the system functions and use. They may also include mis-use diagrams for threat modelling. These should be updated as new threats emerge and software updates occur.

5. **Governance of Information Security**
   Systems and processes in themselves are not sufficient to maintain security and vigilance. An effective organisation will take steps to lead security management and review effectiveness through effective governance. This will take into consideration both the organisation's aims and objectives and the legal requirements such as GDPR as outlined but the Information Commissioner in the UK.

References

ISO (2018), Information technology — Security techniques — Information security management systems — Overview and vocabulary. Available from: ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary [Accessed 09 September 2024].