Some say that people are the biggest risk of cyber security.

Select five terms from ISO/IEC Standard 27000 Section 3 Terms and Definitions and write a 300-word blog post on how people can be managed to overcome cyber security attacks from the inside.

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

Cyber attacks from inside the organisation are as common as external attacks. Types of internal attacks could range from employees being malicious, making mistakes, and accidentally causing harm or plain theft. The organisation's assets need to be protected. My five terms from ISO/IEC Standard 27000 Section 3 Terms and Definitions on how people can be managed to overcome cyber security attacks from the inside.

The first is Risk Identification – performing a risk analysis helps to identify threats and allows an organisation to introduce mitigation actions to reduce the likelihood of the event occurring.

The organisation must implement cyber security policies, including password, email, and remote working.

The organisation should implement an Access Control using the principle of least privileged access. If any task requires privileged access, like root or admin, then the manager has to approve the release of the password.

A dedicated team who can continue monitoring should be present to ensure that threats are not breached and react accordingly

Finally, continual improvement is required, and a review of the process and policies should be performed periodically to ensure that risk, threats, and countermeasures are still appropriate.

ISO/IEC 27000:2018(en)

Information technology — Security techniques — Information security management systems — Overview and vocabulary Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en (Accessed: 15 December 2022).