Individuals and Security

An often overlooked aspect of cyber security is the behaviour of individuals. Dedicating hours of work to ensure that a system or network is as secure as possible can often become pointless if the people interacting with this on a regular basis are either unable to or unwilling to show the same level of care for the security of systems and networks as is built into those aforementioned products.

ISO / IEC 27000 (2018) is an internationally recognised standard within cyber security which provides a framework for how organisations should treat cyber security. Within Section Three of this, there are a number of terms and definitions provided that can help with the human management aspect of cyber security and potentially help to prevent inside attacks on systems. Some of these are as follows:

3.1: Access Control. Controlling who can access what information is essential to ensure that any attacks that involve obtaining information that isn't authorised are more difficult, or potentially made impossible. Without this, an organisation could be at risk of breaching things such as GDPR.

3.24: Governing Body. Strong governance is important when thinking about the human aspects of cyber security, as this provides an overall level of accountability for the operations of frontline staff, as well as providing a body that monitors conformity to things such as standards and legislative requirements.

3.46: Monitoring. Being able to monitor activity is essential if any organisation wants to catch potential breaches or employees acting in bad faith at an early stage. By doing this, it avoids potential escalation and worsening outcomes.

3.33: ISMS Professional. Having an ISMS Professional within an organisation ensures that effective risk management takes place, and ensures that any changes or potential breaches are analysed, reflected on, with any lessons from this taken and implemented.

3.53: Policy. Effective policies, written with legislative compliance in mind, ensures that security is at the core of any organisation, and ensures that there is a framework that can be used to challenge breaches or any employee who may contradict these.

References

ISO/IEC 27000 (2018). Information Technology — Security Techniques — Information Security Management Systems — Overview and vocabulary. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed 29 August 2024].