The Human Factor.

Humans are a significant factor contributing to data breaches. While cybersecurity is usually treated as a technology problem, 88% of data breaches are the result of human error (CYDEF,2019)

Experienced attackers with a plan of action in place will always locate and maliciously target the greatest source of weakness – people. But by properly engaging the people in your organisation in the battle against attackers, you can turn your biggest weakness into your greatest asset, argues Mark Hall.

Companies can take a number of steps to prevent cyber-attacks from the inside, whether they are committed by malicious actors or inadvertently by employees.

Authentication is the process of determining whether someone or something is who or what they claim to be is known as authentication. Authentication technology checks if a user's credentials match those in a database of authorised users or in a data authentication server to offer access control for systems. Authentication ensures secure systems, processes, and organisational information security in this way.

Access control is a data security procedure that allows businesses to govern who has access to corporate data and resources. Access control is a data security procedure that allows businesses to govern who has access to corporate data and resources. Secure access control uses policies to ensure that users are who they claim to be and that they have appropriate control access levels.

Monitoring is the process of continuously observing an IT system to discover data breaches, cyber threats, and other system flaws. It's a proactive cybersecurity approach that can assist IT teams in sorting through cyber events to evaluate which ones constitute a risk to data or systems.

A **policy** is a set of principles that an organisation uses to make decisions. These guidelines can help senior management make better decisions and guide employees in their daily tasks. A password policy is an excellent illustration of the latter.

Audits are about assessing compliance. A cybersecurity audit can determine whether or not they have the necessary security procedures in place, as well as whether or not they are in accordance with relevant rules and security standards.

References:

CYDEF, (2021). The Human Factor: The Hidden Problem of Cybersecurity. Available from https://cydef.ca/blog/the-human-factor-the-hidden-problem-of-cybersecurity [Accessed 14 May 2022]

Mark Hall. (2016). Why people are key to cyber-security. Network Security,Volume 2016, Issue 6,Pages 9-10. Available from https://www.sciencedirect.com/science/article/abs/pii/S1353485816300575 [Accessed 14 May 2022]