

Are people the biggest risk in cyber security? experience tells us unfortunately this tends to be the case people are frequently the weak link in security “Recent research has established that at least five elements are required to mould people’s behaviour in relation to security and control” (Jeimy J 2019)

* Preparation
* Responsibility
* Management
* Social elements
* Regulation

Risks can also be overcome using technology and polices.

**Access control** restricting physical access to the underlying servers running the services though with the increase in the use of SAAS, IAAS local physical access control is no longer enough. An organization also need to partner with a cloud vendor who has good datacentre security made up of the following.

* Secure Perimeter
* Building Signage
* Building Access
* Security Operations Centre
* Restricted Access to Data Centre Floor
* Secure Hard Disk Destruction (Google 2019)

**Audit** while this will not stop incidents it allows us to log the 4 W’s (Who, What, Where and When) we would want our system audit and logging system to use a daemon such as syslog where logs can be offloaded onto a secondary server this prevents the altering of logs if a machine is comprised. Audit should also feed into the organizations IDS to proactively identify threat behaviour so that an early response can take place to prevent further breech of security.

**Authentication** is the process of proving identity to a system or process such as logging on to a workstation. An account is authenticated by a means of an authentication method (Password, Token, Biometrics) once authenticated the users account is permitted to logon to the device. We can overcome the human element by forcing Authentication to carry out tasks that have a security impact.

**Policy** an organization should have a policy in regard to IT security including mandatory training of all staff in security best practice this will limit a security incident being caused by the human factor due to the staff being aware of security risks and their own responsibility in helping preventing breeches of security.

**Risk Assessment** we can mitigate against some of the risk down to the human factor by identifying the areas that have the potential to be exploited and thus enable organizations to put in measures to prevent this an example of this for example is putting in dual authorization so that a single person cannot take an action that could be a potential security breech without the signoff of a second person. The risk assessment can be done as an internal review or as part of an annual pentest security review.

**References**

**ISO** [**https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en**](https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en) **[Accessed 15.03.2022]**

**Google** [**https://cloud.google.com/docs/security/infrastructure/design**](https://cloud.google.com/docs/security/infrastructure/design) **[Accessed 15.03.2022]**

**Microsoft Authentication Process** [**https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication**](https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication) **[Accessed 15.03.2022]**

# **Jeimy J The Human Factor in Information Security** [**https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security**](https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security) **[Accessed 15.03.2022]**