Cybersecurity is one the main key areas where the organisations are focusing over the last years.

Cybersecurity can be exploited by many factors and one of those is the internal risk of being exposed to cybersecurity breaches and attacks from the inside.

The last couple of years our society was subject to a radical change of habits due to the COVID 19 pandemic and this affected the different work environments. Most people was forced to work from home and this exposed organisations to a series of cybersecurity threats due to the lack of **competence** of some individuals in assuring to work in a secure home computing environment. Many people was using their own devices to check work emails and connect to the office IT infrastructure. This behaviour exposed organisations to possible cyberattacks due to virus and malware on the employees devices (Li, Xin and Siponen, 2021).

The lack of competence, in addition to other factors, made the organisations concerned on the scenario of cyber attacks from the inside and to prevent or mitigate any incidents they can adopt a series of **measures**.

Many organisation set up cyber awareness trainings as a **requirement** for their employees to continue to work. The scope is to help the individuals in how to recognize and deal with cyber threats (Li, Xin and Siponen, 2021).

Organisations can review their **access control** policies by checking who has access to certain assets/information, how they are using it and with which frequency. In this way it is possible to evaluate if certain users should continue to have access permissions and eventually revoke it to who does not need it.

Moreover, reviewing the access control policies helps organisations to assess the

right level of **availability** to data. It is important that individuals should not have access to more data than what is actually necessary to perform their duties in accordance to their role.

REFERENCES

Li, Y., Xin, T. and Siponen, M. (2021). Citizens' Cybersecurity Behavior: Some Major Challenges. *IEEE Security & Privacy*, pp.2–9. doi:10.1109/msec.2021.3117371. [Accessed 27 June 2022].