Blog Post: Question 2

Living in an interconnecting world has its advantages. However, the more we cyber-connect, the more opportunities arise for cybersecurity crimes.

Monitoring, identifying, and resolving security risks can be challenging but can be done following specific procedures. But how can you solve the challenges arising from your own organisation? How do you manage people?

Most companies are suffering from both external and internal cybersecurity threats. However, in nine cases out of ten, the threat was created from a human error (Nel, n.d). Data leak incidents originating from within a company are not uncommon and can happen either willingly or accidentally (ERMProtect, n.d).

Malicious employees or "Turncloak" are individuals who maliciously and intentionally use their own credentials to leak data from within the organisation. Financial or personal reasons can lead an employee to become malicious (imperva, n.d).

On the other hand, data leaks can occur from pure mistakes. Even one mistake can result in leaving a system exposed to external threats. This is common to companies with limited or no cybersecurity training, where an employee is much more possible to click a malicious URL and infect the system (imperva, n.d).

Monitoring and preventing employees from leaking sensitive data is tough and time-consuming but with the appropriate **risk analysis** and **risk management** it can be achieved.

- Employers can differentiate the access levels their employees have. By limiting access to the strictly necessary for employees to perform the work, the employers can mitigate the risks of an extensive data leak (ERMProtect, n.d). Additionally, **authentication** systems can be introduced to log all actions performed and shield the systems from external threats (ISO, 2018).
- Cyber-security training can be organised to raise awareness to employees for potential cybersecurity threats the organisation might come across and what steps can be taken to mitigate the risk. This can include theoretical training to all-known threats or showcases of previous threats the organisation has dealt with (ERMProtect, n.d).

- Frequent **audit** controls can take place to monitor and review the system and the employee's profiles. These controls can review the type of activities, any activities that might have occurred at an unusual time, the level of access of the employees, etc. (imperva, n.d).

While people are the most important part of a company, they are the riskiest as well. By making sure that frequent controls are taking place and clear policies are drafted, companies and organisations can mitigate – or even eliminate the risk of potential data breaches.

References:

ERMProtect (n.d.) External vs. Internal Cybersecurity Risks: Know the Difference Available from: https://ermprotect.com/blog/external-vs-internal-cybersecurity-risks-know-difference/ [Accessed 16 May 2021].

Imperva (n.d.) What Is an Insider Threat Available from: https://www.imperva.com/learn/application-security/insider-threats/ [Accessed 16 May 2021].

ISO.org (2018). ISO/IEC 27000:2018(en) Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed 16 May 2021].

Nel, M. (n.d.) 90% of Security Breaches Are Due to Human Error Available from: https://www.360smartnetworks.com/90-of-security-breaches-are-due-to-human-error/ [Accessed 16 May 2021].