Summary Post

It has been interesting reading the view points from my fellow classmates. I have enjoyed reading such a diverse list of examples of possible security breaches, ranging from the transport to the oil industry. The examples all seem to have a consistent pattern and I agree that whenever technology is involved there is a potential risk of an attack.

My initial post, went into details on the number of attacks that UK business have faced from a survey conducted in 2021. My one important takeaway from this discussion, is that this issue is not just limited to one organisation or to one country. This is a worldwide issue and needs a global shift from organisations and individuals to tackle security attacks.

Companies need to invest in their people both within Information Technology roles and outside and instill security at the core of any business decision, from planning a disaster recovery site to building a new application. They need to follow a framework where the life cycle of any decision takes into account who, what, when, where and how a security breach or attack may occur. Bruce Schneier has a fascinating article on attack trees that all organistion should take into account.

Senior management needs to force software development life cycles to incorporate security at the beginning when the requirement gathering stage is taking place. Individuals responsible for building these requirements need to ensure they empower the business decision makers to know the risk’s from the very beginning. As the project ripples through each stage of the development cycle, security needs to be at the forefront. The OWASP have been present for so many years and have a top 10 application security list. It is interesting to see that security risks that were at the top of the list in 2017 such as A01:2017-Injection are still present in 2021 (A03:2021 injection). In 2017, the data was driven by incidence rate and team discussion based on exploitability, detectability and technical impact. In 2021, the data was judged on exploitability and technical impact.

As a closing summary, security is such an important factor that organisations not only need to think of physical security, but need to consider all aspects of security from Operating Systems, Software Development, networks and hardware security such as firewalls. Sensitive Data is one of the most important assets any organistation has and they need to ensure the information is accurate, up to date, used for purpose and kept secure.

REFERENCES:

B.Scneier(1999) Attack Trees Available from: https://www.schneier.com/academic/archives/1999/12/attack_trees.html [Access 26 March 2022]

OWASP Top 10:2021 (2021) Available from:https://owasp.org/www-project-top-ten/ [Accessed 26 March 2021]

Singh, R(2020) OWASP Top 10 Web Application Security Risks and Vulnerabilities to Watch Out for in 2020 Available from: https://www.indusface.com/blog/owasp-top-10-web-application-security-risks-and-vulnerabilities-to-watch-out-for-in-2020/ [Accessed 26 March 2021]

The Data Protection Act Available from : https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018%20is%20the%20UK's%20implementation%20of,used%20fairly%2C%20lawfully%20and%20transparently

[Accessed 26 March 2021]