The Human Factor – Individual Essay – Michael Geiger

The Queens Medical Centre is a community clinic and as such collects personal information about its patients. Therefore, the clinic is subject to the GDPR and, according to Art. 5 f, must process the data in a way that represents appropriate security and protects them against loss, destruction, damage and unauthorised or unlawful processing (GDPR, 2022). These protective measures relate to a technical as well as organisational and thus human level.

The 2019 Cyber Security Breaches Survey found that 80% of businesses and 81% of charities surveyed that were breached were affected by fraudulent emails or being directed to fraudulent websites (Department for Digital, Culture, Media & Sport, 2019). 49% of businesses and 63% of charities declared theses as most disruptive cyber security breach. Based on the 2020 Data Breach Investigations Report (Langlois, 2020) it can be stated that after hacking, the human factors 'social' and 'human error' are the most common reasons for a security breach as shown in figure 1 below.

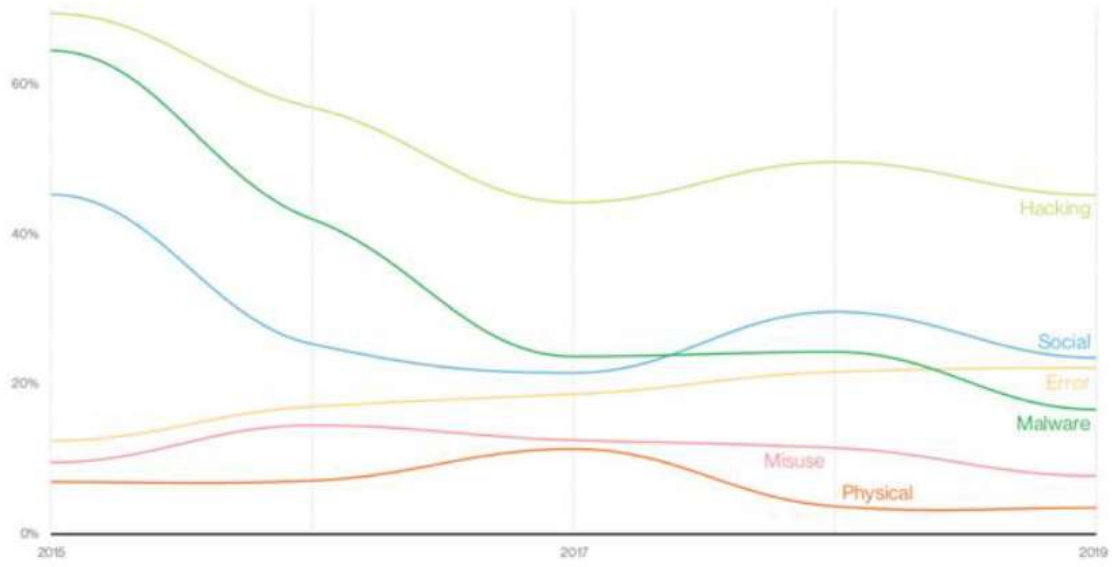

Figure 1: Actions over time in breaches (Langlois, 2020)

With the danger of ‘misuse’, which, like ‘social’ and ‘human error’, is based on human factors, these factors together represent the greatest threat of a breach and must therefore be included in cyber security planning in order to mitigate risks.

Under the social threats factor can be listed phishing and pretexting aimed at fraudulently obtaining unauthorised information by the attacker posing as an authorised person or trusted entity (Jagatic et al., 2007). Various studies suggest that phishing is a well-established threat, but one that is growing in potential danger. A study by the Gartner Group in 2004 found that 19% of the participants surveyed clicked on a link in a phishing email and 3% provided personal or financial information (Jagatic et al., 2007, as cited in Gartner Group, 2004). A study from 2017 came to the conclusion that 20% of the test participants opened phishing emails and thus the risk of phishing via emails remained constant (Benenson et al., 2017). However, it was also found that 42.5% of the participants clicked on a malicious link on Facebook. It can therefore be seen that the risk of becoming a victim of phishing attacks has increased through social networks.

This can be due to various causes. On the one hand, users behave less cautiously in social networks, user curiosity is a driving factor here (Benenson et al., 2017). On the other hand, users share private information about themselves and acquaintances with the public through social networks, which enables personalised phishing attacks (Coronges et al., 2012). Through social engineering and spear phishing, potential victims can be specifically examined for their usage preferences and behaviour and thus targeted phishing attacks can be carried out, which makes it more difficult to identify a malicious link. Potential victims of such an attack are not only the employees in all areas of the clinic, but also their patients.

The human error factor refers to accidental or incorrect execution of tasks. This includes erroneous active as well as omitted executions. Causes that favour human errors can be classified as latent failures arising from poor workplace and organization conditions and active failures based on user misconduct (Sasse & Rashid, 2019). Factors that promote latent failure of the clinic's employees can be traced back to causes that have a negative impact on the working atmosphere and thus lead to cognitive overload. Johnson (2021) states that external stimuli such as noise, hectic work environments and time pressure, which are often encountered in a clinic, lead to stress, thereby increasing the potential for error. Because people have limited mental capacity and distraction and stress negatively affect short-term memory skills and work performance, erroneous active actions and decisions can be made, which can lead to misconfigurations, loss or incorrect processing of information.

Latent and active failures arise in most cases from an intertwining of several factors, which is shown in the accident causation model figure 2.

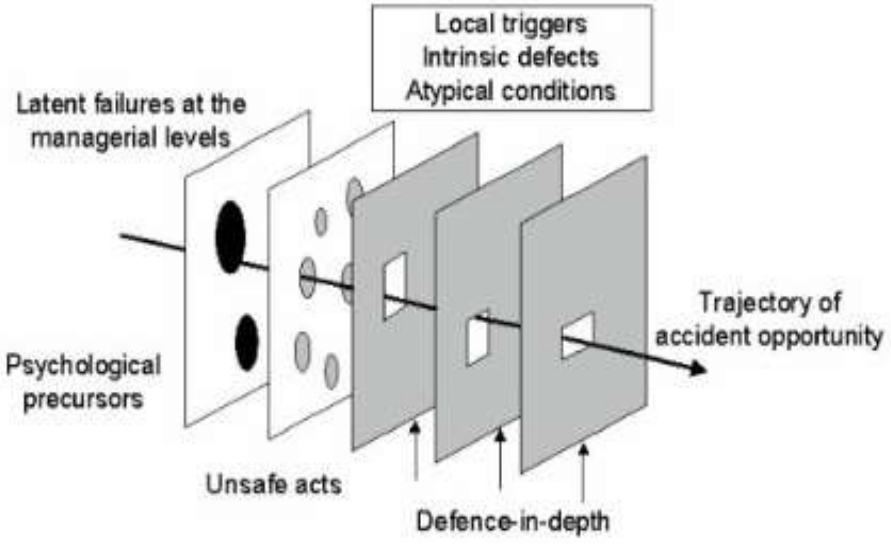

Figure 2: Accident causation model (Reason, 1990)

Changes in the work environment, including the implementation of ASMIS, require employees to adapt to the new circumstances, rethink the work patterns they have already learned and learn new skills in dealing with the new technical equipment and applications. Especially at the beginning of the change, a higher cognitive workload for receptionists and doctors is to be expected and thusalso increases the risk of human error (Johnson, 2021).

On the one hand, misuse can be traced back to accidental misconduct and can therefore be viewed under the aspects of human error. On the other hand, misuse can be caused by intentional and malicious actions, which could lead to data mishandling, privilege abuse and knowledge abuse. Maasberg et al. (2020) lists various psychological factors and personal traits that may indicate a malicious insider, a list is shown in Figure 3.

Key Characteristics	Machiavellianism	Narcissism	Psychopathy
Duplicity	×	×	×
Self-promotion	×	×	×
Aggressiveness	×	×	×
Interpersonal coldness	×	×	×
Tendency to manipulate and exploit others	×	×	×
Sense of superiority	×	×	×
Low empathy	×	×	×
Callousness/lack of conscience	×	×	×
Attention to reputation	×	×	
Cynical world view	×		
Strategic calculation	×		
Sense of entitlement		×	
Sense of grandiosity		×	
Ego-reinforcement all-consuming motive		×	
Thrill-seeking			×
Low anxiety			×
Lack of impulse control			×

Figure 3: Psychological factors and personal traits (Maasberg et al., 2020)

It should be emphasized that malicious actions often arise due to dissatisfied employees. Subjective insufficient recognition of work and poor working conditions are causes that can lead to an employee committing malicious misuse.

In summary, it can be stated that the threats social, human error and misuse are due to human factors and these must be considered when implementing ASMIS in order to prevent cyber breaches.

References:

Benenson, Z., Gassmann, F. & Landwirth, R. (2017) Unpacking Spear Phishing Susceptibiliy. *Lecture Notes in Computer Science.* 10323: 601-726. Available from: https://link.springer.com/chapter/10.1007/978-3-319-70278-0_39 [Accessed 30 June 2022].

Coronges, K., Dodge, R., Mukina, C., Radwick, Z., Shevchik, J. & Rovira, E. (2012) The influences of social networks on phishing vulnerability. *International Conference on System Sciences*. 2366-2373. IEEE. Available from: https://ieeexplore.ieee.org/abstract/document/6149301 [Accessed 30 June 2022].

Department for Digital, Culture, Media & Sport (2019) Cyber Security Breaches Survey 2019. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950063/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised_V2.pdf [Accessed 27 June 2022].

GDPR (2022) Principles relating to processing of personal data. Available from: https://gdpr-info.eu/art-5-gdpr/ [Accessed 27 June 2022].

Jagatic, T. N., Johnson, N. A., Jakobsson, M & Menczer, F. (2007) Social Phishing. *Communictions of the ACM*. 50(10): 94-100. Available from: https://cacm.acm.org/magazines/2007/10/5556-social-phishing/fulltext [Accessed 29 June 2022].

Johnson, J. (2021) Designing with the Mind in Mind. Available from: https://essexonline.vitalsource.com/reader/books/9780128182031/pageid/273 [Accessed 26 June 2022].

Langlois, P. (2020) 2020 Data Breach Investigations Report. Available from: https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/files/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf [Accessed 28 June 2022].

Maasberg, M., Van Slyke, C., Ellis, S. & Beebe, N. (2020) The dark triad and insider threats in cyber security. *Communications of the ACM*. *63*(12): 64-80. Available from: https://dl.acm.org/doi/fullHtml/10.1145/3408864 [Accessed 01 July 2022].

Reason, J. (1990) Human error. *Cambridge university press*.

Sasse, M. A. & Rashid, A. (2019) Human Factors Knowledge Area. Available from: https://www.cybok.org/media/downloads/Human_Factors_issue_1.0.pdf [Accessed 27 June 2022].