**Turnitin Submission Number:1888884432**

20 hours ago

According to Verizon (2022), the Data Breach Investigations Report highlights that 82% of data breaches in 2022 are related to human factors such as phishing, error, misuse, and use of stolen credentials, where internal actors present 39% of data breaches in the healthcare sector. Human factors are defined as information about human behavior, abilities, and limitations that need to be considered during the design of systems for reliable and safe human use (Ayereby, 2018). Yeo & Banfield (2022) studied healthcare data breach records between 2015 – 2020 and found that 73.1% of data breaches were caused by unintentional human factors such as failing victims to phishing and ransomware, carelessness, and negligence.

Phishing attacks are a kind of exploitation of human behavior traits that enable the attacker to influence the user to do the desired (Karakasiliotis et al., 2006). Phishing emails rely on the inability of users to differentiate the legitimate and illegitimate senders and try to convince them that they are revealing their confidential information while they trust that they are connected to the legal network or website (Alseadoon, 2014). Frauenstein & Flowerday (2020) examined phishing susceptibility for 215 respondents by sending phishing emails from Facebook accounts and found that such traits as agreeableness, neuroticism, and openness had a positive influence on heuristic processing in the contrast, conscientiousness had a negative which is less susceptible to phishing on social networks.

Phishing attacks impact negatively on individuals and entities; for example, identity theft as an influence of phishing could cause not only financial loss but also influence people's psychology and emotion (Vučković et al., 2018). In September 2020 Anthem Inc. paid $16 million in penalties for HIPPA violations beside that Anthem paid a $48.2 million multistate settlement in penalties (Steve Alder, 1 October 2020). Anthem announced a data breach of 78.8 million records due to a cyber-attack because a user opened a phishing email (California Department of Insurance, N.D).

Stolen credentials are mostly caused by weak or reused passwords, brute-force, and password sharing. The inability to remember due to human memory limitations could cause people to choose simple/weak, reuse passwords, or one-time passwords. Herley (2009) highlighted that the user tends to use an easy password instead of a strong password, which is hard to remember, moreover reusing the same password on many websites is common. Because individuals have many accounts that require many passwords consequently, forgetting passwords increases which make people tend to use a combination of names, birthday, and address. Fernández-Alemána et al. (2015) evaluated the security behavior in a real clinic and found that 62.2% of respondents reported weak passwords, moreover, because too many systems required passwords, infrequent use, and complexity of passwords weak passwords can be found as a result. ASMIS expect to have a strong authentication system and support multi-factor authentication technique.

According to Rajah et.al. (2020) poor password habits such as weak and reuse passwords have a significant positive impact on personal data breach that enables hackers to gain unauthorized access which could be used in illegitimate activities. Personal information and stolen credentials could be to access a user's bank account or online accounts and cause financial and reputation loss. In 2012, Dropbox announced that email information for 68 million user credentials was hacked and for sale on the dark net because an employee reused a password hacked on another website (Karen Turner, 7 September 2016). More than 50 million credit cards and emails were stolen from Home Depot by a hacker who used a stolen credential (Artiningsih & Sasmita, 2016), Home Depot paid $134.5 million to credit card as a penalty (Michael Hill, 16 August 2022).

Privilege abuse is a kind of insider threat related to human misuse, the privileged user who is authorized to access the system or network depends on his function. Insider threats could be employees, customers, or business partners, privileged abuse can be caused by disgruntled employees or other reasons, privileges such as reading, writing, and execution for users per their functions (Elifoglu et al., 2018). ASMIS should not give privileges to all at the same level. A system administrator is a legitimate user who has full admin privileges to all system resources that pose threat to the organization because of the trust given and the high level of access (Magklaras & Furnell, 2001). Data should be protected and restricted access on role-based instead of access by all, Hospitals should apply role-based control for a different level of access, therefore, privileges of doctors, nurses, and administrative employees should be different (Cobia, 2019).

The damage that comes from insiders caused by administrators or who have power privileges is high and can affect the whole system, damage from insiders such as privileged employees can be stolen or compromised confidential or customer information which could cause financial and reputation loss (Elifoglu et al., 2018). One of the famous cases of privilege abuse is the NSA contractor Edward Snowden who downloaded sensitive NSA files using a USB stick (Howe, 2019).

Queen medical center management during the implementation of the ASMIS system to ensure that is usable and secure, should be considered breaches caused by phishing, the use of stolen credentials, and privilege abuse/misuse which are human factors, where humans play a major role in data breaches.

References

Alder, S. (October 1, 2020) Anthem Inc. Settles State Attorneys General Data Breach Investigations and Pays $48.2 Million in Penalties. *HIPAA Journal*. Available from: https://www.hipaajournal.com/anthem-inc-settles-state-attorneys-general-data-breach-investigations-and-pays-48-2-million-in-penalties/ [Accessed 23 August 2022].

Alseadoon, I. (2014) *The impact of users' characteristics on their ability to detect phishing emails*. Ph.D. dissertation, Queensland University of Technology. Available from: https://core.ac.uk/download/pdf/33491513.pdf [Accessed 26 August 2022].

Artiningsih, A. & Sasmita, A. (2016) Data Breaches and Identity Theft: A Case Study of U.S. Retailers and Banking. *Jurnal Universitas Paramadina*. 13 (2016). Available from: https://journal.paramadina.ac.id/index.php/upm/article/view/112 [Accessed 26 August 2022].

Ayereby, M. (2018) *Overcoming Data Breaches and Human Factors in Minimizing Threats to Cyber-Security Ecosystems*. Ph.D. dissertation, Walden University. Available from: https://scholarworks.waldenu.edu/dissertations/6163/ [Accessed 26 August 2022].

California Department of Insurance (n.d.) Anthem Data Breach. Available from: https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm [Accessed 24 August 2022].

Cobia, A. (2019) *Privileged Access Management*. Master. thesis, La Salle University. Available from: https://digitalcommons.lasalle.edu/ecf\_capstones/34/ [Accessed 26 August 2022].

Elifoglu, I., Abel, I. & Tas¸seven, Ö. (2018) Minimizing Insider Threat Risk with Behavioral Monitoring. *INTERDISCIPLINARY JOURNAL ON RISK AND SOCIETY*. 38 (2): 61-73. Available from: https://www.stjohns.edu/sites/default/files/uploads/review-of-business-382-june\_2018.pdf#page=66 [Accessed 23 August 2022].

Fernández-Alemán, J., Sánchez-Henarejos, A., Toval, A., Sánchez-García, A., Hernández-Hernández, I. & Fernandez-Luque, L. (2015) Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International Journal of Medical Informatics*. 84 (6): 454-467. Available from: https://doi.org/10.1016/j.ijmedinf.2015.01.010 [Accessed 17 August 2022].

Frauenstein, E. & Flowerday, S. (2020) Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security*. 94. Available from: https://doi.org/10.1016/j.cose.2020.101862 [Accessed 23 August 2022].

Herley, C. (2009) So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. *NSPW '09*. 2009: 133–144. Available from: https://doi.org/10.1145/1719030.1719050 [Accessed 23 August 2022].

Hill, M. (August 16, 2022) The 12 biggest data breach fines, penalties, and settlements so far. *CSO*. Available from: https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html [Accessed 25 August 2022].

Howe, D. (2022) Deciphering How Edward Snowden Breached the NSA [Five Years Later]. *Venafi*. Available from: https://www.venafi.com/blog/deciphering-how-edward-snowden-breached-the-nsa [Accessed 24 August 2022].

Karakasiliotis, A., Furnell, S. & Papadaki, M. (2006) Assessing end-user awareness of social engineering and phishing. *7th Australian Information Warfare and Security Conference*. 2006, School of Computer and Information Science. Australia. Available from: https://ro.ecu.edu.au/isw/12/. [Accessed 16 August 2022].

Magklaras, G. & Furnell, S. (2001) Insider Threat Prediction Tool: Evaluating the probability of IT misuse. *Computers & Security*. 21 (1): 62-73. Available from: https://doi.org/10.1016/S0167-4048(02)00109-8 [Accessed 24 August 2022].

Rajah, P., Dastane, O., Bakon, K. & Johari, Z. (2020) The Effect of Bad Password Habits on Personal Data Breach*. International Journal of Emerging Trends in Engineering Research*. 8 (10): 6950-6960. Available from: https://doi.org/10.30534/ijeter/2020/538102020 [Accessed 22 August 2022].

Turner, K. (September 7, 2016) Hacked Dropbox login data of 68 million users is now for sale on the dark Web. *The Washington Post*. Available from: https://www.washingtonpost.com/news/the-switch/wp/2016/09/07/hacked-dropbox-data-of-68-million-users-is-now-or-sale-on-the-dark-web/ [Accessed 25 August 2022].

Verizon (2022) *2022 Data Breach Investigations Report*. Available from: https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf [Accessed 19 August 2022].

Vučković, Z., Vukmirović, D., Milenković, M., Ristić, S. & Prljić, K. (2018) Analyzing of e-commerce user behavior to detect identity theft. *Physica A: Statistical Mechanics and its Applications*. 511: 331-335. Available from: https://www.sciencedirect.com/science/article/pii/S0378437118309312 [Accessed 21 August 2022].

Yeo, L. & Banfield, J. (2022) Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives in Health Information Management*. 19 (Spring). Available from: https://pubmed.ncbi.nlm.nih.gov/35692854/ [Accessed 21 August 2022].

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Response 200 words