REFERENCES

[1] Varonis, "157 Cybersecurity Statistics and Trends [updated 2024]." Accessed: Oct. 16, 2024. [Online]. Available: https://www.varonis.com/blog/cybersecurity-statistics

[2] Forbes, "Cybersecurity Stats: Facts And Figures You Should Know – Forbes Advisor." Accessed: Oct. 16, 2024. [Online]. Available: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/#1

[3] J. Lee and S. J. Choi, "Hospital productivity after data breaches: Difference-in-differences analysis," *J Med Internet Res*, vol. 23, no. 7, p. e26157, Jul. 2021, doi: 10.2196/26157.

[4] P. Shojaei, E. Vlahu-Gjorgievska, and Y. W. Chow, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," *Computers*, vol. 13, no. 2, p. 41, Feb. 2024, doi: 10.3390/computers13020041.

[5] J. Lee, H. Kim, and S. J. Choi, "Do hospital data breaches affect health information technology investment?," *Digit Health*, vol. 10, Jan. 2024, doi: 10.1177/20552076231224164/ASSET/IMAGES/LARGE/10.1177_20552076231224164-FIG1.JPEG.

[6] IBM, "Cost of a Data Breach Report 2024," 2024. Accessed: Oct. 17, 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[7] D. V. Dimitrov, "Medical Internet of Things and Big Data in Healthcare," *Healthc Inform Res*, vol. 22, no. 3, pp. 156–163, Jul. 2016, doi: 10.4258/HIR.2016.22.3.156.

[8] E. Dönmez *et al.*, "Readiness for health information technology is associated to information security in healthcare institutions," *Acta Informatica Medica*, vol. 28, no. 4, pp. 265–271, Dec. 2020, doi: 10.5455/AIM.2020.28.265-271.

[9] "2024 Data Breach Investigations Report | Verizon." Accessed: Oct. 16, 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/#DBIR2024NR

[10] F. Gioulekas *et al.*, "A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures," *Healthcare*, vol. 10, no. 2, p. 327, Feb. 2022, doi: 10.3390/healthcare10020327.

[11] M. Neri *et al.*, "Understanding information security awareness: evidence from the public healthcare sector," *Information and Computer Security*, vol. ahead-of-print, no. ahead-of-print, 2024, doi: 10.1108/ICS-04-2024-0094/FULL/PDF.

[12] E. H. Park, J. Kim, L. L. Wiles, and Y. S. Park, "Factors affecting intention to disclose patients' health information," *Comput Secur*, vol. 87, p. 101340, Nov. 2019, doi: 10.1016/J.COSE.2018.05.003.

[13] P. K. Yeng, M. A. Fauzi, and B. Yang, "A Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals," *Information 2022, Vol. 13, Page 335*, vol. 13, no. 7, p. 335, Jul. 2022, doi: 10.3390/INFO13070335.

[14] S. Acharya, B. Coats, A. Saluja, and D. Fuller, "From Regulations to Practice: Achieving Information Security Compliance in Healthcare," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8533 LNCS, pp. 209–220, 2014, doi: 10.1007/978-3-319-07620-1_19.

[15] J. Q. Chen and A. Benusa, "HIPAA security compliance challenges: The case for small healthcare providers," *Int J Healthc Manag*, vol. 10, no. 2, pp. 135–146, Apr. 2017, doi: 10.1080/20479700.2016.1270875.

[16] Albert. Mehrabian and J. A. . Russell, "An approach to environmental psychology," p. 266, 1976.

[17] G. Young, "Stimulus–Organism–Response Model: SORing to New Heights," *Unifying Causality and Psychology*, pp. 699–717, 2016, doi: 10.1007/978-3-319-24094-7_28.

[18] H. Chen, Y. Li, L. Chen, and J. Yin, "Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security-related conflict and fatigue," *Journal of Enterprise Information Management*, vol. 34, no. 3, pp. 770–792, Apr. 2021, doi: 10.1108/JEIM-10-2019-0318/FULL/PDF.

[19] T. Chang, Y. Wu, X. Deng, X. Wang, and Y. Yan, "The impact of environmental stimuli on the psychological and behavioral compliance of international construction employees," *Front Psychol*, vol. 15, p. 1395400, Jun. 2024, doi: 10.3389/FPSYG.2024.1395400/BIBTEX.

[20] G. White, "Generation Z: Cyber-Attack Awareness Training Effectiveness," *Journal of Computer Information Systems*, vol. 62, no. 3, pp. 560–571, May 2022, doi: 10.1080/08874417.2020.1864680.

[21] A. J. Burns, T. L. Roberts, C. Posey, R. J. Bennett, and J. F. Courtney, "Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts," *Decision Sciences*, vol. 49, no. 6, pp. 1187–1228, 2018, doi: 10.1111/deci.12304.

[22] A. AlKalbani, H. Deng, B. Kam, and X. Zhang, “Investigating the impact of institutional pressures on information security compliance in organizations,” *Proceedings of the 27th Australasian Conference on Information Systems, ACIS 2016*, pp. 1–12, 2016.

[23] I. Hwang, R. Wakefield, S. Kim, and T. Kim, “Security Awareness: The First Step in Information Security Compliance Behavior,” *Journal of Computer Information Systems*, vol. 61, no. 4, pp. 345–356, 2021, doi: 10.1080/08874417.2019.1650676.

[24] M. L. Sher, P. C. Talley, T. J. Cheng, and K. M. Kuo, “How can hospitals better protect the privacy of electronic medical records? Perspectives from staff members of health information management departments,” *http://dx.doi.org/10.1177/1833358316671264*, vol. 46, no. 2, pp. 87–95, Oct. 2016, doi: 10.1177/1833358316671264.

[25] N. K. Lankton, C. Stivason, and A. Gurung, “Information protection behaviors: morality and organizational criticality,” *Information and Computer Security*, vol. 27, no. 3, pp. 468–488, 2019, doi: 10.1108/ICS-07-2018-0092.

[26] S. M. Fahrezi and C. Candiwan, “The Influence Of Information Privacy Awareness On Privacy Protection Behavior In Facebook,” *JHSS (JOURNAL OF HUMANITIES AND SOCIAL STUDIES)*, vol. 8, no. 1, pp. 162–167, Apr. 2024, doi: 10.33751/JHSS.V8I1.8414.

[27] G. Carmi and D. Bouhnik, “The effect of rational based beliefs and awareness on employee compliance with information security procedures: A case study of a financial corporation in Israel,” *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 15, pp. 109–125, 2020, doi: 10.28945/4596.

[28] A. McIlwraith, *Information Security and Employee Behaviour*. 2016. doi: 10.4324/9781315588537.

[29] E. H. Park, J. Kim, and Y. S. Park, “The role of information security learning and individual factors in disclosing patients’ health information,” *Comput Secur*, vol. 65, pp. 64–76, Mar. 2017, doi: 10.1016/J.COSE.2016.10.011.

[30] R. Adawiyah, A. N. Hidayanto, I. Chandra Hapsari, and R. M. Samik Ibrahim, “Identification of How Health Information Security Awareness (HISA) Influence in Patient’ Health Information Protection Awareness (PHIPA),” *5th International Conference on Computing Engineering and Design, ICCED 2019*, Apr. 2019, doi: 10.1109/ICCED46541.2019.9161123.

[31] C. Candiwan, M. Azmi, and A. Alamsyah, “Analysis of Behavioral and Information Security Awareness among Users of Zoom Application in COVID-19 Era,”

International Journal of Safety and Security Engineering, vol. 12, no. 2, pp. 229–237, Apr. 2022, doi: 10.18280/IJSSE.120212.

[32] M. Frank and V. Kohn, "Understanding extra-role security behaviors: An integration of self-determination theory and construal level theory," *Comput Secur*, vol. 132, p. 103386, 2023, doi: 10.1016/j.cose.2023.103386.

[33] E. L. Deci and R. M. Ryan, "Intrinsic Motivation and Self-Determination in Human Behavior," *Intrinsic Motivation and Self-Determination in Human Behavior*, 1985, doi: 10.1007/978-1-4899-2271-7.

[34] J. G. Proudfoot, W. A. Cram, and S. Madnick, "Weathering the storm: examining how organisations navigate the sea of cybersecurity regulations," *European Journal of Information Systems*, vol. 00, no. 00, pp. 1–24, 2024, doi: 10.1080/0960085X.2024.2345867.

[35] P. K. Yeng, B. Yang, and E. A. Snekkenes, "Framework for Healthcare Security Practice Analysis, Modeling and Incentivization," *Proceedings - 2019 IEEE International Conference on Big Data, Big Data 2019*, pp. 3242–3251, Dec. 2019, doi: 10.1109/BIGDATA47090.2019.9006529.

[36] B. S. S. Raj and S. Venugopalachar, "A Survey on Healthcare Standards and Security Requirements for Electronic Health Records," *4th International Conference on Emerging Research in Electronics, Computer Science and Technology, ICERECT 2022*, 2022, doi: 10.1109/ICERECT56837.2022.10060831.

[37] B. Kim, D. Y. Lee, and B. Kim, "Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks," *Behaviour & Information Technology*, vol. 39, no. 11, pp. 1156–1175, Nov. 2020, doi: 10.1080/0144929X.2019.1653992.

[38] B. Alothman, A. Alhajraf, R. Alajmi, R. Al Farraj, N. Alshareef, and M. Khan, "Developing a Cyber Incident Exercises Model to Educate Security Teams," *Electronics (Switzerland)*, vol. 11, no. 10, 2022, doi: 10.3390/electronics11101575.

[39] O. Soultatos *et al.*, "The THREAT-ARREST Cyber-Security Training Platform," in *Computer Security*, A. P. Fournaris, M. Athanatos, K. Lampropoulos, S. Ioannidis, G. Hatzivasilis, E. Damiani, H. Abie, S. Ranise, L. Verderame, A. Siena, and J. Garcia-Alfaro, Eds., Cham: Springer International Publishing, 2020, pp. 199–214.

[40] H. N. Chua, J. S. Teh, and A. Herbland, "Identifying the Effect of Data Breach Publicity on Information Security Awareness Using Hierarchical Regression," *IEEE Access*, vol. 9, pp. 121759–121770, 2021, doi: 10.1109/ACCESS.2021.3107426.

[41] T. Tatu, C. Ament, and L. Jaeger, “Lessons learned from an information security incident: A practical recommendation to involve employees in information security,” *Proceedings of the Annual Hawaii International Conference on System Sciences*, vol. 2018-Janua, pp. 3736–3745, 2018, doi: 10.24251/hicss.2018.471.

[42] K. Mohammed and O. Saeed, “Elevating Information Security Practices within Sudanese Healthcare Establishments’ Staff,” *International Journal of Advanced Research in Computer Science*, vol. 13, no. 4, pp. 6–8, Aug. 2022, doi: 10.26483/IJARCS.V13I4.6835.

[43] M. A. Pulido, C. W. Johnson, and A. Alzahrani, “Security Awareness Level Evaluation of Healthcare Participants Through Educational Games,” *International Journal of Serious Games*, vol. 8, no. 3, pp. 25–41, Sep. 2021, doi: 10.17083/IJSG.V8I3.459.

[44] Y. Gangire, A. Da Veiga, and M. Herselman, “A conceptual model of information security compliant behaviour based on the self-determination theory,” *2019 Conference on Information Communications Technology and Society, ICTAS 2019*, 2019, doi: 10.1109/ICTAS.2019.8703629.

[45] C. Candiwan, M. Beninda, and Y. Pr, “Analysis of Information Security Audit Using ISO 27001:2013 & ISO 27002:2013 at IT Division -X Company, In Bandung, Indonesia,” Jun. 2016. doi: 10.13140/RG.2.1.1483.3044.

[46] W. Ghaban, “Integrated Information Security Policy Model for Saudi Arabia Organizations,” *Journal of Computer Science*, vol. 19, no. 4, pp. 454–466, 2023, doi: 10.3844/jcssp.2023.454.466.

[47] P. Divya Prabha, N. Suresh Kumar, N. Nandhine Shree, R. Sundaram, H. Nishanthi, and D. Pranesh, “Cybersecurity in Healthcare: Safeguarding Patient Data,” *Proceedings - 3rd International Conference on Advances in Computing, Communication and Applied Informatics, ACCAI 2024*, 2024, doi: 10.1109/ACCAI61061.2024.10602188.