REFERENCES

Adedoyin Tolulope Oyewole, Chinwe Chinazo Okoye, Onyeka Chrisanctus Ofodile, & Chinonye Esther Ugochukwu. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, *21*(3), 625–643. https://doi.org/10.30574/wjarr.2024.21.3.0707

Agustian, K., Mubarok, E. S., Zen, A., Wiwin, W., & Malik, A. J. (2023). The Impact of Digital Transformation on Business Models and Competitive Advantage. *Technology and Society Perspectives (TACIT)*, *1*(2), 79–93. https://doi.org/10.61100/tacit.v1i2.55

Ali, M. H., Jaber, M. M., Abd, S. K., Rehman, A., Awan, M. J., Damaševičius, R., & Bahaj, S. A. (2022). Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT). *Electronics (Switzerland)*, *11*(3). https://doi.org/10.3390/electronics11030494

Al-Sada, B., Sadighian, A., & Oligeri, G. (2024). Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database. *IEEE Access*, *12*, 1217–1234. https://doi.org/10.1109/ACCESS.2023.3344680

Anggi Muliawati. (2024, February 14). *KPU Sebut Situsnya Terima Ratusan Juta Serangan saat Pencoblosan* . DetikNews.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. In *Electronics (Switzerland)* (Vol. 12, Issue 6). MDPI. https://doi.org/10.3390/electronics12061333

Betancourt, V. P., Glock, T., Kharitonov, A., Kern, M., Liu, B., Sax, E., & Becker, J. (2020, August 24). Linking intrusion detection system information and system model to redesign security architecture. *SYSCON 2020 - 14th Annual IEEE International Systems Conference, Proceedings*. https://doi.org/10.1109/SysCon47679.2020.9275862

Bishop, M., & Goldman, E. (2003). The strategy and tactics of information warfare. *Contemporary Security Policy*, *24*(1), 113–139. https://doi.org/10.1080/13523260312331271839

Butun, I., Osterberg, P., & Song, H. (2020). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Communications Surveys and Tutorials*, *22*(1), 616–644. https://doi.org/10.1109/COMST.2019.2953364

Chevendra, A., Sindhwad, P. v., Kulkarni, R., Samant, M., Deegoju, S., & Kazi, F. (2024). System Architecture and Threat Modelling of Advanced Metering Infrastructure. *Power Research - A Journal of CPRI*, 27–33. https://doi.org/10.33686/pwj.v20i1.1164

Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber Threats Classifications and Countermeasures in Banking and Financial Sector. *IEEE Access*, *11*, 125138–125158. https://doi.org/10.1109/ACCESS.2023.3327016

Dumitriu, D., & Popescu, M. A. M. (2020). Enterprise architecture framework design in IT management. *Procedia Manufacturing*, *46*, 932–940. https://doi.org/10.1016/j.promfg.2020.05.011

Dupont, B. (2019a). The cyber-resilience of financial institutions: Significance and applicability. In *Journal of Cybersecurity* (Vol. 5, Issue 1). Oxford University Press. https://doi.org/10.1093/cybsec/tyz013

Dupont, B. (2019b). The cyber-resilience of financial institutions: Significance and applicability. In *Journal of Cybersecurity* (Vol. 5, Issue 1). Oxford University Press. https://doi.org/10.1093/cybsec/tyz013

Ekonomi dan Perbankan Syariah, J., Fitriani, R., Subagiyo, R., Nur Asiyah, B., & Sayyid Ali Rahmatullah Tulungagung, U. (2023). *Mitigating IT Risk of Bank Syariah Indonesia: A Study of Cyber Attack on May 8, 2023*. *15*(1), 86–100. https://doi.org/10.24235/amwal.v%vi%i.14124

Fernández Blánquez, P. (n.d.). *Malware attack prevention, detection, response and recovery*.

Framework for Threat Analysis and AttackModelling of Network Security Protocols. (n.d.).

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9). https://doi.org/10.3390/s21093267

Ghelani, D., Kian Hua, T., Kumar, S., & Koduru, R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *American Journal of Computer Science and Technology*, *x, No. x*, x–x. https://doi.org/10.22541/au.166385206.63311335/v1

GUIDE TO CYBER THREAT MODELLING. (2021).

Habler, E., Bitton, R., & Shabtai, A. (2022). *Evaluating the Security of Aircraft Systems*. http://arxiv.org/abs/2209.04028

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains Dan Teknologi*, *2*(02), 55–62. https://doi.org/10.56741/bst.v2i02.353

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). *Financial crime and fraud in the age of cybersecurity*.

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, *21*(6), 1285–1305. https://doi.org/10.1007/s10796-019-09959-1

Jimmy, F. (2024). Cybersecurity Threats and Vulnerabilities in Online Banking Systems. *International Journal of Scientific Research and Management (IJSRM)*, *12*(10), 1631–1646. https://doi.org/10.18535/ijsrm/v12i10.ec10

Kabundi, A., de Simone, F. N., & Bank, W. (2019). *Monetary Policy and Systemic Risk-taking in the Euro Area Banking Sector*.

Kesharwani, A., & Bisht, S. S. (2012). The impact of trust and perceived risk on internet banking adoption in India: An extension of technology acceptance model. *International Journal of Bank Marketing*, *30*(4), 303–322. https://doi.org/10.1108/02652321211236923

Kinnunen, J. (2022). *Threat Detection Gap Analysis Using MITRE ATT&CK Framework*.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*, *105*. https://doi.org/10.1016/j.cose.2021.102248

Leclair, B. (n.d.). *Threat Modelling in Virtual Assistant Hub Devices Compared With User Risk Perceptions*.

Legoy, V., Caselli, M., Seifert, C., & Peter, A. (2020). *Automated Retrieval of ATT&CK Tactics and Techniques for Cyber Threat Reports*. http://arxiv.org/abs/2004.14322

Lis, P., & Mendel, J. (2019). Cyberattacks on Critical Infrastructure: an Economic Perspective. *Economics and Business Review*, *5*(2), 24–47. https://doi.org/10.18559/ebr.2019.2.2

Luo, Y. (2022). A general framework of digitization risks in international business. *Journal of International Business Studies*, *53*(2), 344–361. https://doi.org/10.1057/s41267-021-00448-9

Mauri, L., & Damiani, E. (2022a). Modeling Threats to AI-ML Systems Using STRIDE †. *Sensors*, *22*(17). https://doi.org/10.3390/s22176662

Mauri, L., & Damiani, E. (2022b). Modeling Threats to AI-ML Systems Using STRIDE †. *Sensors*, *22*(17). https://doi.org/10.3390/s22176662

Mergel, I., Edelmann, N., & Haug, N. (2019a). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, *36*(4). https://doi.org/10.1016/j.giq.2019.06.002

Mergel, I., Edelmann, N., & Haug, N. (2019b). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, *36*(4). https://doi.org/10.1016/j.giq.2019.06.002

Mike Levi, & Melvin Soudijn. (2020). *Understanding the laundering of organized crime money* (Vol. 1).

Natesan, Dr. G. (2024). PREVENTION OF CYBER FRAUDS IN THE BANKING SECTOR. *International Scientific Journal of Engineering and Management*, *03*(03), 1–22. https://doi.org/10.55041/isjem01341

Nurkamiden, M. (2024). SiRekap : Tantangan dan Potensi Kekeliruan Proses Rekapitulasi Pemilu Serentak di Indonesia SiRekap: Challenges and Potential Errors in the Recapitulation Process of Simultaneous Elections in Indonesia. In *SOSIOLOGI: Jurnal Penelitian dan Pengabdian Kepada Masyarakat* (Vol. 1, Issue 2).

Pell, R., Moschoyiannis, S., Panaousis, E., & Heartfield, R. (2021). *Towards Dynamic Threat Modelling in 5G Core Networks Based on MITRE ATT&CK*. http://arxiv.org/abs/2108.11206

pojk 13-2020. (n.d.).

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. In *Sensors* (Vol. 23, Issue 8). MDPI. https://doi.org/10.3390/s23084060

Rouland, Q., Hamid, B., & Jaskolka, J. (2021). Specification, detection, and treatment of STRIDE threats for software components: Modeling, formal methods, and tool support. *Journal of Systems Architecture*, *117*. https://doi.org/10.1016/j.sysarc.2021.102073

Santos, D. R. dos, Dagrada, M., & Costante, E. (2019). *Leveraging Operational Technology and the Internet of Things to Attack Smart Buildings*. http://arxiv.org/abs/1912.02480

Sean Peek. (2023, April 14). *Features of Business Security Systems*. Business.Com.

Slavković, M., Pavlović, K., Mamula Nikolić, T., Vučenović, T., & Bugarčić, M. (2023). Impact of Digital Capabilities on Digital Transformation: The Mediating Role of Digital Citizenship. *Systems*, *11*(4). https://doi.org/10.3390/systems11040172

Soares Cruzes, D., Gilje Jaatun, M., Bernsmed, K., & Tondel, I. A. (2018). Challenges and experiences with applying microsoft threat modeling in agile development projects. *Proceedings - 25th Australasian Software Engineering Conference, ASWEC 2018*, 111–120. https://doi.org/10.1109/ASWEC.2018.00023

Souri, A., Hussien, A., Hoseyninezhad, M., & Norouzi, M. (2022). A systematic review of IoT communication strategies for an efficient smart environment. *Transactions on Emerging Telecommunications Technologies*, *33*(3). https://doi.org/10.1002/ett.3736

Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry*, *13*(4). https://doi.org/10.3390/sym13040597

Stene, H. A. (n.d.). *Threat analysis of mobile banking platforms*.

Straub, J. (2020). Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATTCK and STRIDE Frameworks as Blackboard Architecture Networks. *Proceedings - 2020 IEEE International Conference on Smart Cloud, SmartCloud 2020*, 148–153. https://doi.org/10.1109/SmartCloud49737.2020.00035

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (n.d.). *MITRE ATT&CK®: Design and Philosophy*.

Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., Whitley, S. M., & Wolf, R. D. (2017). *Finding Cyber Threats with ATT&CK™-Based Analytics*.

Syrotynskyi, R., Tyshyk, I., Kochan, O., Sokolov, V., & Skladannyi, P. (2024). *Methodology of network infrastructure analysis as part of migration to zero-trust architecture ⋆*.

Systemic Risk Board, E. (2020). *Systemic cyber risk*. https://doi.org/10.2849/566567

Tete, S. B. (2024). *Threat Modelling and Risk Analysis for Large Language Model (LLM)-Powered Applications*. http://arxiv.org/abs/2406.11007

Van Landuyt, D., & Joosen, W. (2022). A descriptive study of assumptions in STRIDE security threat modeling. *Software and Systems Modeling*, *21*(6), 2311–2328. https://doi.org/10.1007/s10270-021-00941-7

View of Impact of Cyber-Attacks on Banking Institutions in India_ A Study of Safety Mechanisms and Preventive Measures. (n.d.).

Vitorio Mantalean. (2024, February 14). *KPU Klaim Situsnya Alami Ratusan Juta Serangan Artikel ini telah tayang di Kompas.com dengan judul "KPU Klaim Situsnya Alami Ratusan Juta Serangan", Klik untuk baca: https://nasional.kompas.com/read/2024/02/14/22094771/kpu-klaim-situsnya-alami-ratusan-juta-serangan. Kompascom+ baca berita tanpa iklan: https://kmp.im/plus6 Download aplikasi: https://kmp.im/app6*. Kompas.Com.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wewege, L., Lee, J., & Thomsett, M. C. (2020). Disruptions and Digital Banking Trends. In *Journal of Applied Finance & Banking* (Vol. 10, Issue 6). online) Scientific Press International Limited. https://www.researchgate.net/publication/343050625

Williams, L. (2019). *Secure Software Lifecycle*. http://heartbleed.com/

Wong, W. P., Tan, H. C., Tan, K. H., & Tseng, M. L. (2019). Human factors in information leakage: mitigation strategies for information sharing integrity. *Industrial Management and Data Systems*, *119*(6), 1242–1267. https://doi.org/10.1108/IMDS-12-2018-0546

Xin, T., & Xiaofang, B. (2014a). Online banking security analysis based on STRIDE threat model. *International Journal of Security and Its Applications*, *8*(2), 271–282. https://doi.org/10.14257/ijsia.2014.8.2.28

Xin, T., & Xiaofang, B. (2014b). Online banking security analysis based on STRIDE threat model. *International Journal of Security and Its Applications*, *8*(2), 271–282. https://doi.org/10.14257/ijsia.2014.8.2.28

Yousseef, A., Satam, S., Latibari, B. S., Pacheco, J., Salehi, S., Hariri, S., & Satam, P. (2024). *Autonomous Vehicle Security: A Deep Dive into Threat Modeling*. http://arxiv.org/abs/2412.15348

Zhang, Z., Nan, G., & Tan, Y. (2020). Cloud Services vs. On-Premises Software: Competition under Security Risk and Product Customization. *Information Systems Research*, *31*(3), 848–864. https://doi.org/10.1287/ISRE.2019.0919

Zolkover, A., Kharkiv, S. K., Stashkevych, O., & Mehdizade, M. M. (2022). BENEFITS AND RISKS OF DIGITAL BUSINESS TRANSFORMATION: THE EXAMPLE OF EASTERN EUROPE COUNTRIES Olesia Iastremska. *JOURNAL OF EASTERN EUROPEAN AND CENTRAL ASIAN RESEARCH*, *9*(2). https://doi.org/10.15549/jeecar.9i2.910