UNIVERSITAS
GADJAH MADA
**Analisis Sosio - Teknis Tata Kelola Keamanan Siber Sektor Publik Indonesia (Studi Kasus pada Badan
Kepegawaian Negara)**
ANINDA ISNAINI, Dr. Bevaola Kusumasari, M.Si.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR PUSTAKA

Adristi, I. F., & Ramadhani, E. (2024). Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede. *Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen*, *02*(06), 196–212. https://journal.uii.ac.id/selma/index

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers and Security*, *99*. https://doi.org/10.1016/j.cose.2020.102030

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2022). Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. *Government Information Quarterly*, *39*(4). https://doi.org/10.1016/j.giq.2022.101721

Al-Hawamleh, A. M. (2024). Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the KSA. *Digital Policy, Regulation and Governance* , *26*(3), 317–336. https://doi.org/10.1108/DPRG-11-2023-0168

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028

Appelbaum, S. H. (1997). Socio-technical systems theory: an intervention strategy for organizational development. In *Management Decision* (Vol. 35, Number 6, pp. 452–463). https://doi.org/10.1108/00251749710173823

Backman, S. (2023). Risk vs. threat-based cybersecurity: the case of the EU. *European Security*, *32*(1), 85–103. https://doi.org/10.1080/09662839.2022.2069464

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, *23*(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

Bongiovanni, I., Slapnicari, S., Axelseni, M., & Stockdalei, D. (2024). *The Three Lines Model in Cybersecurity Governance and Risk Management FEATURE FEATURE*. www.isaca.org

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

UNIVERSITAS
GADJAH MADA
**Analisis Sosio - Teknis Tata Kelola Keamanan Siber Sektor Publik Indonesia (Studi Kasus pada Badan
Kepegawaian Negara)**
ANINDA ISNAINI, Dr. Bevaola Kusumasari, M.Si.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

BSSN. (2025). *Laporan Hasil Monitoring*. 2025. https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html

Burns, A. J. (2019). Security Organizing: A Framework for Organizational Information Security Mindfulness. *SIGMIS Database*, *50*(4), 14–27. https://doi.org/10.1145/3371041.3371044

Burton, S. L. (2024). Securing Tomorrow: Synergizing Change Management and Cybersecurity in the Digital Era. *HOLISTICA – Journal of Business and Public Administration*, *15*(1), 1–20. https://doi.org/10.2478/hjbpa-2024-0001

Busetti, S., & Scanni, F. M. (2025). Evaluating incident reporting in cybersecurity. From threat detection to policy learning. *Government Information Quarterly*, *42*(1), 102000. https://doi.org/https://doi.org/10.1016/j.giq.2024.102000

Cherns, A. (1976). The Principles of Sociotechnical Design. *Human Relations*, *29*(8), 783–792. https://doi.org/https://doi.org/10.1177/001872677602900806

Cherns, A. (1987). Principles of Sociotechnical Design Revisted. *Human Relations*, *40*(3), 153–162. https://doi.org/https://doi.org/10.1177/001872678704000303

Clegg, C. W. (2000). Sociotechnical principles for system design. *Applied Ergonomics*, (31). https://doi.org/https://doi.org/10.1016/S0003-6870(00)00009-0

Creswell, J. W., & Creswell, J. D. (2018). *RESEARCH DESIGN Qualitative, Quantitative, and Mixed Methods* (5th ed.). SAGE Publications, Inc.

CSIS. (2025). *Significant Cyber Incidents Since 2006*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-06/250610_Significant_Cyber_Incidents.pdf?VersionId=IAAkHurCCF.s7dd26zpWQUXbumz3JXsq

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. In *TQM Journal* (Vol. 33, Number 7, pp. 76–105). Emerald Group Holdings Ltd. https://doi.org/10.1108/TQM-09-2020-0202

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers and Security*, *92*. https://doi.org/10.1016/j.cose.2020.101713

Dunleavy, P., & Margetts, H. (2025). Data science, artificial intelligence and the third wave of digital era governance. *Public Policy and Administration*, *40*(2), 185–214. https://doi.org/10.1177/09520767231198737

UNIVERSITAS
GADJAH MADA
**Analisis Sosio - Teknis Tata Kelola Keamanan Siber Sektor Publik Indonesia (Studi Kasus pada Badan
Kepegawaian Negara)**
ANINDA ISNAINI, Dr. Bevaola Kusumasari, M.Si.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

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

Fahey, E. (2024). The evolution of EU–US cybersecurity law and policy: on drivers of convergence. *Journal of European Integration*, *46*(7), 1073–1088. https://doi.org/10.1080/07036337.2024.2411240

Fan, B., & Pan, T. (2023). Does information technology–organizational resource interaction affect E-government performance? Moderating roles of environmental uncertainty. *Government Information Quarterly*, *40*(3). https://doi.org/10.1016/j.giq.2023.101830

Figueroa, V., Sánchez Crespo, L. E., Santos-Olmo, A., Rosado, D. G., & Fernández-Medina, E. (2025). Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals. *International Journal of Information Security*, *24*(3). https://doi.org/10.1007/s10207-025-01024-0

Frandell, A., & Feeney, M. (2022). Cybersecurity Threats in Local Government: A Sociotechnical Perspective. *American Review of Public Administration*, *52*(8), 558–572. https://doi.org/10.1177/02750740221125432

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers and Security*, *121*. https://doi.org/10.1016/j.cose.2022.102840

Garcia-Perez, A., Sallos, M. P., & Tiwasing, P. (2023). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective. *Journal of Intellectual Capital*, *24*(2), 465–486. https://doi.org/10.1108/JIC-06-2021-0166

Geels, F. W. (2004). From sectoral systems of innovation to socio-technical systems: Insights about dynamics and change from sociology and institutional theory. *Research Policy*, *33*(6–7), 897–920. https://doi.org/10.1016/j.respol.2004.01.015

Gil-Garcia, J. R., Dawes, S. S., & Pardo, T. A. (2018). Digital government and public management research: finding the crossroads. In *Public Management Review* (Vol. 20, Number 5, pp. 633–646). Taylor and Francis Ltd. https://doi.org/10.1080/14719037.2017.1327181

Hassandoust, F., & Johnston, A. C. (2023). Peering through the lens of high-reliability theory: A competencies driven security culture model of high-reliability organisations. *Information Systems Journal*, *33*(5), 1212–1238. https://doi.org/10.1111/isj.12441

UNIVERSITAS
GADJAH MADA
Analisis Sosio - Teknis Tata Kelola Keamanan Siber Sektor Publik Indonesia (Studi Kasus pada Badan Kepegawaian Negara)
ANINDA ISNAINI, Dr. Bevaola Kusumasari, M.Si.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ISO/IEC. (2022). *ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.

Jaber, A. (2025). Cybersecurity governance and political structures: Comparing centralized and decentralized approaches to cyber defense. *Comparative Strategy*. https://doi.org/10.1080/01495933.2025.2507310

James Norcross, by S., Benavides, A., McCaskill, J. R., Searing, E., & Ho, K. K. (2025). *CYBERSECURITY CHALLENGES AND STRATEGIES IN PUBLIC AFFAIRS*.

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. In *Government Information Quarterly* (Vol. 32, Number 3, pp. 221–236). Elsevier Ltd. https://doi.org/10.1016/j.giq.2015.07.001

Kanaan, A., Al-Hawamleh, A., Abulfaraj, A., Al-Kaseasbeh, H. M., & Alorfi, A. H. (2023). The effect of quality, security and privacy factors on trust and intention to use e-government services. *International Journal of Data and Network Science*, *7*(1), 185–198. https://doi.org/10.5267/j.ijdns.2022.11.004

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*. https://doi.org/10.1016/j.inffus.2023.101804

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). *Learning from "Shadow Security": Why understanding non-compliant behaviors provides the basis for effective security*. https://doi.org/10.14722/usec.2014.23<007

Liu, C. W., Huang, P., & Lucas, H. C. (2020). Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems*, *37*(3), 758–787. https://doi.org/10.1080/07421222.2020.1790190

Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: investigations, approaches, measures, and trends. *International Journal of Information Security*, *24*(4). https://doi.org/10.1007/s10207-025-01097-x

Mahmood, S., Chadhar, M., & Firmin, S. (2024). Addressing Cybersecurity Challenges in Times of Crisis: Extending the Sociotechnical Systems Perspective. *Applied Sciences (Switzerland)*, *14*(24). https://doi.org/10.3390/app142411610

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security*, *27*(2), 233–272. https://doi.org/10.1108/ICS-03-2018-0031

UNIVERSITAS
GADJAH MADA
Analisis Sosio - Teknis Tata Kelola Keamanan Siber Sektor Publik Indonesia (Studi Kasus pada Badan Kepegawaian Negara)
ANINDA ISNAINI, Dr. Bevaola Kusumasari, M.Si.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

Mayer, P., Gerber, N., McDermott, R., Volkamer, M., & Vogt, J. (2017). Productivity vs security: Mitigating conflicting goals in organizations. *Information and Computer Security*, *25*(2), 137–151. https://doi.org/10.1108/ICS-03-2017-0014

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers and Security*, *120*. https://doi.org/10.1016/j.cose.2022.102820

Patton, M. Q. (2015). *Qualitative Research & Evaluation Methods* (Fourth Edition). SAGE Publications, Inc.

Prasetyo, A., Aji, R. F., & Wibowo, W. S. (2025). Assessing Information Security Awareness Among Indonesian Government Employees: A Case Study of the Meteorology, Climatology, and Geophysics Agency. *Journal of Information Systems Engineering and Business Intelligence*, *11*(2), 126–142. https://doi.org/10.20473/jisebi.11.2.126-142

Preis, B., & Susskind, L. (2022). Municipal Cybersecurity: More Work Needs to be Done. *Urban Affairs Review*, *58*(2), 614–629. https://doi.org/10.1177/1078087420973760

Pullin, D. W. (2018). Cybersecurity: Positive Changes Through Processes and Team Culture. *Frontiers of Health Services Management*, *35*(1), 3–12. https://doi.org/10.1097/hap.0000000000000038

Safi, R., Browne, G. J., & Jalali Naini, A. (2021). Mis-spending on information security measures: Theory and experimental evidence. *International Journal of Information Management*, *57*. https://doi.org/10.1016/j.ijinfomgt.2020.102291

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4

Sensuse, D. I., Putro, P. A. W., Rachmawati, R., & Sunindyo, W. D. (2022). Initial Cybersecurity Framework in the New Capital City of Indonesia: Factors, Objectives, and Technology. In *Information (Switzerland)* (Vol. 13, Number 12). MDPI. https://doi.org/10.3390/info13120580

Sugiyono. (2013). *METODE PENELITIAN KUANTITATIF KUALITATIF R&D* (19th ed.). ALFABETA, CV.

Tempo. (2024). *Data Pribadi PNS di BKN Diduga Bocor, Dijual Rp 160 juta di BreachForums*. https://www.tempo.co/ekonomi/data-pribadi-pns-di-bkn-diduga-bocor-dijual-rp-160-juta-di-breachforums-26828

UNIVERSITAS
GADJAH MADA
**Analisis Sosio - Teknis Tata Kelola Keamanan Siber Sektor Publik Indonesia (Studi Kasus pada Badan
Kepegawaian Negara)**
ANINDA ISNAINI, Dr. Bevaola Kusumasari, M.Si.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal getting. In *Clinician in Management* (Vol. 9, Number 4, pp. 235–237). https://doi.org/10.1177/001872675100400101

Trist, E. L., Higgin, G. W., Murray, H., & Pollock, A. B. (2013). *ORGANIZATIONAL CHOICE Capabilities of Groups At The Coal Face Under Changing Technologies The Loss, Re-Discovery & Transformation of a Work Tradition* (Vol. 28). Routledge.

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Walker, G. H., Stanton, N. A., Salmon, P. M., & Jenkins, D. P. (2008). A review of sociotechnical systems theory: A classic concept for new command and control paradigms. *Theoretical Issues in Ergonomics Science*, *9*(6), 479–499. https://doi.org/10.1080/14639220701635470

Wirtz, B. W., & Weyerer, J. C. (2017). Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. *International Journal of Public Administration*, *40*(13), 1085–1100. https://doi.org/10.1080/01900692.2016.1242614

Woods, D. W., & Seymour, S. (2023). Evidence-based cybersecurity policy? A meta-review of security control effectiveness. *Journal of Cyber Policy*, *8*(3), 365–383. https://doi.org/10.1080/23738871.2024.2335461

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). SAGE Publications, Inc.

Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, *16*(4), 490–513. https://doi.org/10.1080/19361610.2021.1918995

Zhang, H., Tang, Z., & Jayakar, K. (2018). A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services. *Telecommunications Policy*, *42*(5), 409–420. https://doi.org/10.1016/j.telpol.2018.02.004

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269