



Dampak Sosial dan Ekonomi dari insiden-insiden Keamanan Informasi Studi kasus KPU Provinsi Jambi

Ahmad Affan¹, Fahmi Hidayat², Gilang Ramadhan³

^{1,2,3} Sistem Informasi, Fakultas Sains & Teknologi, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi, Indonesia

afan22635@gmail.com , fahmihidayat0403@gmail.com , gilangramadhan@gmail.com

Jl. Jambi Ma.Bulian KM.16 Simpang Sungai Duren, Kabupaten Muaro Jambi,
Provinsi Jambi, Indonesia, 36361

Abstract. :Information security incidents within government institutions have become a critical issue due to their potential impact on public trust and socio-economic stability. This study examines the social and economic impacts of information security incidents at the General Election Commission (KPU) of Jambi Province. The research aims to identify the types of security incidents that occurred, analyze their social and economic consequences, and evaluate mitigation efforts implemented by the institution. This study employs a qualitative case study approach, using data collection techniques including document analysis, media reports, and interviews with relevant stakeholders. The findings indicate that information security incidents significantly affect public trust in electoral institutions, increase public anxiety regarding personal data protection, and generate additional economic costs related to system recovery, security enhancement, and administrative delays. Furthermore, the incidents also indirectly affect voter participation and institutional reputation. The study highlights the importance of strengthening information security governance, improving human resource awareness, and implementing comprehensive risk management strategies. The results of this research are expected to contribute to the development of more resilient information security policies in public sector institutions, particularly in electoral management bodies.

Keywords: Data Protection, Election Commission, Information Security Incident, Public Trust, Socio-Economic Impact.

Abstrak. :Insiden keamanan informasi pada lembaga pemerintahan menjadi isu penting karena dampaknya terhadap kepercayaan publik dan stabilitas sosial ekonomi. Penelitian ini bertujuan untuk menganalisis dampak sosial dan ekonomi dari insiden-insiden keamanan informasi yang terjadi pada Komisi Pemilihan Umum (KPU) Provinsi Jambi. Fokus penelitian meliputi identifikasi jenis insiden keamanan informasi, analisis dampak sosial dan ekonomi yang ditimbulkan, serta evaluasi upaya penanganan dan mitigasi yang dilakukan oleh KPU Provinsi Jambi. Metode penelitian yang digunakan adalah pendekatan kualitatif dengan desain studi kasus. Teknik pengumpulan data dilakukan melalui analisis dokumen, telaah pemberitaan media, dan wawancara dengan pihak-pihak terkait. Hasil penelitian menunjukkan bahwa insiden keamanan informasi berdampak pada menurunnya tingkat kepercayaan masyarakat terhadap penyelenggara pemilu, meningkatnya kekhawatiran publik terkait perlindungan data pribadi, serta munculnya beban ekonomi tambahan berupa biaya pemulihan sistem, peningkatan infrastruktur keamanan, dan keterlambatan proses administrasi. Selain itu, dampak tidak langsung juga terlihat pada reputasi kelembagaan dan potensi penurunan partisipasi pemilih. Penelitian ini menegaskan pentingnya penguatan tata kelola keamanan informasi, peningkatan kesadaran sumber daya manusia, serta penerapan manajemen risiko yang komprehensif. Temuan penelitian diharapkan dapat menjadi bahan pertimbangan dalam perumusan kebijakan keamanan informasi yang lebih efektif pada institusi sektor publik, khususnya lembaga penyelenggara pemilu.

Kata kunci: Dampak Sosial Ekonomi, Insiden Keamanan Informasi, Kepercayaan Publik, KPU, Perlindungan Data.

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah mendorong terjadinya transformasi digital dalam berbagai sektor, termasuk dalam penyelenggaraan administrasi pemerintahan dan proses demokrasi. Digitalisasi sistem pemilu menjadi salah satu strategi

penting untuk meningkatkan efisiensi, akurasi, transparansi, serta akuntabilitas dalam pengelolaan data pemilih dan hasil pemungutan suara. Komisi Pemilihan Umum (KPU) sebagai lembaga negara yang memiliki mandat konstitusional dalam penyelenggaraan pemilu telah mengadopsi berbagai sistem informasi berbasis teknologi digital, seperti sistem informasi data pemilih, sistem rekapitulasi hasil penghitungan suara, serta kanal informasi publik berbasis daring (Kotler & Lee, 2021; Norris, 2022).

Namun demikian, pemanfaatan sistem informasi digital dalam penyelenggaraan pemilu juga membawa konsekuensi meningkatnya risiko keamanan informasi. Ancaman seperti peretasan sistem, serangan siber, kebocoran data pribadi pemilih, serta gangguan terhadap ketersediaan layanan menjadi tantangan serius yang harus dihadapi oleh lembaga penyelenggara pemilu (Kuzior et al., 2024; Tobondo, 2024). Keamanan informasi tidak hanya berkaitan dengan aspek teknis, tetapi juga mencakup perlindungan terhadap integritas data, kerahasiaan informasi pribadi, dan keandalan sistem dalam mendukung proses demokrasi yang kredibel (Whitman & Mattord, 2021).

Insiden keamanan informasi pada lembaga publik memiliki dampak multidimensional. Dari sisi sosial, kebocoran data dan gangguan sistem pemilu dapat menurunkan tingkat kepercayaan publik terhadap institusi penyelenggara negara serta memicu keresahan dan ketidakpastian di masyarakat (Bator et al., 2022; Imran, 2024). Kepercayaan publik merupakan elemen fundamental dalam legitimasi hasil pemilu, sehingga gangguan keamanan informasi berpotensi melemahkan kualitas demokrasi secara keseluruhan (Norris, 2022).

Dari perspektif ekonomi, insiden keamanan informasi menimbulkan beban biaya yang signifikan, baik biaya langsung maupun tidak langsung. Biaya langsung meliputi pemulihan sistem, peningkatan infrastruktur keamanan, serta penanganan hukum dan administratif. Sementara itu, biaya tidak langsung dapat berupa terganggunya layanan publik, penurunan produktivitas institusi, serta kerugian reputasi yang berdampak jangka panjang (Cobos & World Bank, 2023; IBM Security, 2023). Laporan global menunjukkan bahwa sektor publik termasuk salah satu sektor dengan kerugian tertinggi akibat insiden siber, terutama yang berkaitan dengan data sensitif warga negara.

Dalam konteks Indonesia, isu keamanan informasi pemilu menjadi perhatian serius seiring dengan meningkatnya penggunaan sistem digital oleh KPU. Beberapa kasus dugaan kebocoran data dan serangan siber terhadap sistem KPU yang dilaporkan oleh media nasional maupun internasional menunjukkan adanya kerentanan dalam tata kelola keamanan informasi

pemilu (KPU RI, 2023; Reuters, 2024; Rizki, 2024). Kondisi ini menegaskan pentingnya evaluasi menyeluruh terhadap kebijakan dan implementasi keamanan informasi di lingkungan penyelenggara pemilu.

Pada tingkat daerah, KPU Provinsi Jambi sebagai bagian dari sistem penyelenggara pemilu nasional juga menghadapi tantangan serupa. Keterbatasan sumber daya, kapasitas teknis, serta kompleksitas pengelolaan data pemilih di daerah berpotensi meningkatkan risiko terjadinya insiden keamanan informasi. Beberapa gangguan sistem yang terjadi menjelang dan setelah tahapan pemilu menunjukkan adanya kesenjangan antara kebutuhan akan sistem informasi yang andal dengan kemampuan pengelolaan keamanan informasi yang tersedia (Andrianika, 2023; Utama, 2024).

Berdasarkan uraian tersebut, penelitian ini memiliki urgensi untuk mengkaji secara mendalam dampak sosial dan ekonomi dari insiden keamanan informasi yang terjadi di KPU Provinsi Jambi. Penelitian ini bertujuan untuk menganalisis bentuk-bentuk insiden keamanan informasi, mengidentifikasi dampak sosial dan ekonomi yang ditimbulkan, serta mengevaluasi upaya mitigasi dan penguatan tata kelola keamanan informasi yang telah dilakukan. Hasil penelitian diharapkan dapat memberikan kontribusi teoritis dan praktis dalam pengembangan kebijakan keamanan informasi pada lembaga penyelenggara pemilu, khususnya di tingkat daerah..

2. KAJIAN TEORITIS

Bagian Keamanan informasi didefinisikan sebagai upaya untuk melindungi informasi dari ancaman yang dapat mengganggu aspek kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability). Insiden keamanan informasi terjadi ketika terdapat pelanggaran terhadap salah satu atau lebih prinsip tersebut. Dalam konteks organisasi publik, keamanan informasi memiliki peran strategis karena berkaitan langsung dengan kepercayaan masyarakat dan legitimasi institusi.

Dampak sosial dari insiden keamanan informasi sering kali tercermin dalam menurunnya kepercayaan publik, meningkatnya kecemasan sosial, serta perubahan perilaku masyarakat terhadap penggunaan layanan digital pemerintah. Sementara itu, dampak ekonomi mencakup biaya langsung seperti perbaikan sistem dan penguatan infrastruktur, serta biaya tidak langsung seperti penurunan produktivitas, kerugian reputasi, dan potensi penurunan partisipasi publik.

Beberapa penelitian sebelumnya menunjukkan bahwa lemahnya tata kelola keamanan informasi dan rendahnya kesadaran sumber daya manusia menjadi faktor utama terjadinya insiden keamanan informasi di sektor publik. Kajian-kajian tersebut menjadi landasan bagi penelitian ini dalam menganalisis kasus yang terjadi di KPU Provinsi Jambi.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan desain studi kasus. Pendekatan ini dipilih untuk memperoleh pemahaman yang mendalam mengenai fenomena insiden keamanan informasi dan dampaknya dalam konteks organisasi publik. Lokasi penelitian adalah KPU Provinsi Jambi, dengan fokus pada pengelolaan sistem informasi dan kejadian insiden keamanan informasi yang terjadi pada periode penyelenggaraan pemilu terakhir.

Teknik pengumpulan data dilakukan melalui wawancara semi-terstruktur, analisis dokumen, dan telaah pemberitaan media. Wawancara dilakukan terhadap informan kunci yang terdiri atas anggota atau staf KPU Provinsi Jambi yang terlibat dalam pengelolaan teknologi informasi, serta pihak pendukung teknis. Wawancara bertujuan untuk menggali informasi terkait jenis insiden keamanan informasi, dampak yang dirasakan, serta langkah-langkah penanganan yang dilakukan. Selain itu, data sekunder diperoleh dari laporan resmi KPU, dokumen kebijakan, dan berita media daring yang relevan.

Analisis data dilakukan dengan menggunakan teknik analisis tematik melalui tahapan reduksi data, penyajian data, dan penarikan kesimpulan. Validitas data dijaga melalui teknik triangulasi sumber, yaitu membandingkan hasil wawancara dengan data dokumentasi dan pemberitaan media. Pendekatan ini diharapkan mampu menghasilkan temuan yang komprehensif dan kredibel.

4. HASIL DAN PEMBAHASAN

A. Bagian Identifikasi Insiden Keamanan Informasi

Hasil penelitian menunjukkan bahwa insiden keamanan informasi yang terjadi meliputi gangguan sistem, potensi kebocoran data, dan ancaman siber terhadap infrastruktur teknologi informasi. Insiden tersebut sebagian besar dipicu oleh keterbatasan sistem pengamanan dan faktor kelalaian manusia.

B. Dampak Sosial

Dari aspek sosial, insiden keamanan informasi menyebabkan menurunnya tingkat kepercayaan masyarakat terhadap KPU Provinsi Jambi. Masyarakat menjadi lebih waspada dan cenderung meragukan keamanan data pribadi yang dikelola oleh institusi publik. Kondisi ini berpotensi memengaruhi partisipasi masyarakat dalam proses demokrasi.

C. Dampak Ekonomi

Dari sisi ekonomi, insiden keamanan informasi menimbulkan biaya tambahan untuk pemulihan sistem dan peningkatan keamanan. Selain itu, keterlambatan layanan dan proses administrasi juga berdampak pada efisiensi kerja dan penggunaan anggaran.

D. Implikasi dan Upaya Mitigasi

Penelitian ini menunjukkan bahwa penguatan kebijakan keamanan informasi, peningkatan kapasitas sumber daya manusia, serta penerapan standar keamanan yang lebih ketat merupakan langkah penting untuk meminimalkan dampak insiden di masa depan.

KESIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa insiden keamanan informasi di KPU Provinsi Jambi memberikan dampak signifikan terhadap aspek sosial dan ekonomi. Dampak sosial tercermin dari menurunnya kepercayaan publik, sementara dampak ekonomi terlihat dari meningkatnya biaya operasional dan pemulihan sistem. Oleh karena itu, KPU Provinsi Jambi disarankan untuk memperkuat tata kelola keamanan informasi, meningkatkan kesadaran dan kompetensi sumber daya manusia, serta menerapkan manajemen risiko yang berkelanjutan. Penelitian selanjutnya diharapkan dapat menggunakan pendekatan kuantitatif atau memperluas objek penelitian pada KPU di provinsi lain.

DAFTAR REFERENSI

- Andrianika, S. (2023). Keamanan data pemilu di era cybercrime. *Jurnal Pengawasan Pemilu*, 5(2), 45–62.
- Bator, J., Bryan, D., & Schultz, T. (2022). Public trust and cybersecurity incidents in government institutions. *Journal of Public Administration*, 18(3), 211–228.

- Cobos, E. V., & World Bank. (2023). *A review of the economic costs of cyber incidents*. World Bank Publications.
- IBM Security. (2023). *Cost of a data breach report 2023*. IBM Corporation.
- Imran, M. F. (2024). Public awareness on data protection: A case in Indonesian elections. *Jurnal Organisasi dan Governance*, 10(3), 101–118.
- Kotler, P., & Lee, N. (2021). *Social marketing: Influencing behaviors for good* (6th ed.). Sage Publications.
- KPU Republik Indonesia. (2023). *Siaran pers terkait dugaan kebocoran data pemilu*. <https://www.kpu.go.id>
- Kuzior, A., Tiutiunyk, I., & et al. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of Information Security*, 12(4), 1–18.
- Norris, P. (2022). *Why electoral integrity matters*. Cambridge University Press.
- Reuters. (2024). Indonesia says it has begun recovering data after major ransomware attack. *Reuters News*.
- Rizki, M. (2024). Data breach of the General Elections Commission. *Jurnal JustInfo*, 2(1), 12–27.
- Tobondo, Y. A. (2024). Analysis of cybersecurity implementation in Indonesia. *Jurnal Hukum & Siber*, 3(1), 34–50.
- Utama, F. S. (2024). Data leakage of the Indonesian elections commission. *Majalah Ilmu Informasi*, 8(1), 77–90.
- Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.
- World Economic Forum. (2023). *Global cybersecurity outlook 2023*. WEF.
- Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.