Nusantara Journal of Multidisciplinary Science
Vol. 3, No. 8, Maret 2026
Hal 1150-1157
E-ISSN : 3024-8752
P-ISSN : 3024-8744
Site : https://jurnal.intekom.id/index.php/njms

Analisis Faktor Penyebab Kebocoran Data Di Lembaga Pemerintah Dengan Metode *Nist Cybersecurity Framework*

Tarreq Azis Khomaeni[1]
[1]Fakultas Teknik & Informatika, Universitas Bina Sarana Informatika, Jakarta, Indonesia

Article Info

Article history:

Received Februari 28, 2026
Revised Maret 1, 2026
Accepted Maret 3, 2026

Kata Kunci:

Kebocoran Data,
Keamanan Informasi,
NIST Cybersecurity Framework,
Lembaga Pemerintah

Keywords:

Data Breach,
Information Security,
NIST Cybersecurity Framework,
Government Institutions

ABSTRAK

Perkembangan teknologi informasi di lingkungan pemerintahan meningkatkan ketergantungan terhadap sistem digital dalam pengelolaan data dan layanan publik. Namun, kondisi tersebut juga diiringi dengan meningkatnya risiko kebocoran data, sebagaimana terjadi pada kasus kebocoran data Pusat Data Nasional (PDN) dan Badan Kepegawaian Negara (BKN) tahun 2024. Kebocoran data ini menunjukkan adanya kelemahan dalam pengelolaan keamanan sistem informasi di lembaga pemerintah. Penelitian ini bertujuan untuk mengidentifikasi faktor utama penyebab kebocoran data, menganalisis kelemahan sistem informasi dan manajemen keamanan data, serta memberikan rekomendasi strategis perbaikan keamanan data di lembaga pemerintah. Dalam penelitian ini, dilakukan studi kasus terhadap kasus kebocoran data PDN 2024 dan kebocoran data BKN 2024. Metode penelitian yang digunakan adalah metode kualitatif dengan teknik studi dokumentasi terhadap sumber-sumber publik yang relevan. Analisis dilakukan menggunakan kerangka kerja NIST *Cybersecurity Framework* (CSF) versi 2.0, yang mencakup fungsi *Govern, Identify, Protect, Detect, Respond, dan Recover*. Hasil penelitian menunjukkan bahwa faktor utama penyebab kebocoran data adalah lemahnya tata kelola keamanan siber, tidak optimalnya manajemen aset dan data, serta kurangnya penerapan kontrol akses, deteksi, respons, dan pemulihan insiden keamanan. Penerapan NIST CSF 2.0 terbukti efektif dalam mengidentifikasi kelemahan keamanan secara sistematis dan terstruktur. Penelitian ini diharapkan dapat menjadi bahan evaluasi dan acuan bagi lembaga pemerintah dalam meningkatkan keamanan data dan sistem informasi secara berkelanjutan.

ABSTRACT

The development of information technology within the government sector has increased reliance on digital systems for data management and public service. However, this condition is accompanied by a growing risk of data breaches, as evidenced by the data breach incidents at the National Data Center (Pusat Data Nasional/PDN) and the National Civil Service Agency (Badan Kepegawaian Negara/BKN) in 2024. These incidents indicate weaknesses in information system security management within government institutions. This study aims to identify the main factors contributing to data breaches, analyze weaknesses in information systems and data security management, and provide strategic recommendations for improving data security in government institutions. This research employs a case study approach focusing on the PDN 2024 and BKN 2024 data breach incidents. A qualitative research method is applied using documentation study techniques on relevant public sources. The analysis is conducted using the NIST Cybersecurity Framework (CSF) version 2.0, which consists of the

Govern, Identify, Protect, Detect, Respond, and Recover functions. The results indicate that the primary causes of data breaches include weak cybersecurity governance, suboptimal asset and data management, and inadequate implementation of access control, detection, incident response, and recovery mechanisms. The application of NIST CSF 2.0 has proven effective in systematically and structurally identifying security weaknesses. This study is expected to serve as an evaluation reference and guideline for government institutions in enhancing data and information system security on a sustainable basis.

Corresponding Author:

Tarreq Azis Khomaeni
Fakultas Teknik & Informatika, Universitas Bina Sarana Informatika,
Jakarta, Indonesia
Email: tarreq.azis20@gmail.com

1. PENDAHULUAN

Di era digital yang semakin berkembang seperti saat ini, penggunaan teknologi sudah terintegrasi dengan kegiatan sehari-hari baik itu digunakan sebagai akses informasi, transaksi, pekerjaan, ataupun hiburan. Transformasi digital telah menjadi pilar utama dalam pembangunan nasional dan reformasi birokrasi di berbagai negara berkembang [1], [2]. Penggunaan teknologi yang kian memberikan kemudahan ini juga membawa perubahan besar dalam pengelolaan data dan sistem informasi di berbagai bidang, salah satunya di sektor pemerintahan. Implementasi e-government terbukti mampu meningkatkan efisiensi layanan publik dan kualitas tata kelola pemerintahan [3]. Pemerintah Indonesia melalui berbagai instansi telah mengadopsi sistem yang terintegrasi guna memfasilitasi pelayanan publik secara digital, baik dari segi administrasi, keuangan, data kependudukan dan layanan publik lainnya. Digitalisasi tersebut diharapkan mampu meningkatkan efektivitas kinerja pemerintah serta transparansi dalam pelayanan publik, sebagaimana ditegaskan dalam berbagai studi mengenai digital governance dan public value [4].

Dibalik kemudahan yang diberikan oleh perkembangan teknologi, adapun berbagai ancaman bahaya yang timbul seperti pencurian informasi penting atau sensitif, manipulasi data, sabotase sistem, ataupun serangan terhadap infrastruktur penting. Meningkatnya kompleksitas sistem digital pemerintah juga meningkatkan risiko serangan siber yang bersifat sistemik [5]. Hal ini dapat merugikan berbagai pihak baik pribadi ataupun umum. Laporan terbaru menunjukkan bahwa sektor publik merupakan salah satu target utama serangan ransomware dan data breach secara global [6]. Kondisi tersebut tercermin pada insiden serangan siber yang menimpa Pusat Data Nasional (PDN) pada Juni 2024. Serangan ransomware menyebabkan terganggunya sejumlah layanan publik karena data pada sistem PDN tidak dapat diakses. Fenomena ransomware pada infrastruktur kritis pemerintah telah banyak dikaji sebagai ancaman serius terhadap keamanan nasional dan kontinuitas layanan publik [7]. Insiden ini menunjukkan bahwa sistem yang berfungsi sebagai pusat integrasi data nasional masih memiliki celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab, terutama apabila manajemen risiko siber belum diimplementasikan secara menyeluruh [8].

Selain kasus PDN, pada Agustus 2024 muncul dugaan kebocoran data yang melibatkan Badan Kepegawaian Negara (BKN). Data kepegawaian dalam jumlah besar dilaporkan tersebar melalui forum online, yang mengindikasikan adanya kelemahan dalam pengelolaan dan perlindungan data aparatur sipil negara. Studi sebelumnya menegaskan bahwa lemahnya tata kelola keamanan informasi dan

kurangnya kontrol akses menjadi faktor dominan dalam kebocoran data sektor publik [9]. Kebocoran tersebut tidak hanya menimbulkan risiko terhadap privasi individu, tetapi juga berdampak pada kepercayaan publik terhadap institusi pemerintah. Kepercayaan publik sangat dipengaruhi oleh persepsi keamanan dan perlindungan data dalam layanan digital pemerintah [10].

Berdasarkan peristiwa tersebut, dapat diketahui bahwa keamanan informasi pada lembaga pemerintah masih memerlukan perhatian serius. Oleh karena itu, penelitian ini dilakukan dengan tujuan untuk menganalisis faktor apa saja yang menjadi penyebab terjadinya kebocoran data dan juga menyusun rekomendasi perbaikan terhadap sistem keamanan informasi di lembaga pemerintah. Pendekatan manajemen risiko berbasis kerangka kerja keamanan siber dinilai efektif dalam meningkatkan ketahanan sistem informasi pemerintah [11]. Penelitian sebelumnya membahas kebocoran data secara umum dan belum secara spesifik menggunakan kerangka kerja NIST Cybersecurity Framework. NIST Cybersecurity Framework telah banyak digunakan sebagai standar internasional dalam penguatan keamanan infrastruktur kritis dan organisasi publik [12], [13]. Implementasi NIST CSF terbukti membantu organisasi dalam mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan dari insiden keamanan siber secara sistematis [14], [15]. Diharapkan penelitian ini dapat memberikan rekomendasi yang strategis yang dimana dapat diaplikasikan pada keamanan sistem di lembaga pemerintah.

2. METODE

2.1 Jenis dan Pendekatan Penelitian

Penelitian ini menerapkan pendekatan kualitatif deskriptif dengan metode studi kasus, yang digunakan untuk memperoleh pemahaman mendalam mengenai fenomena kebocoran data yang terjadi pada lembaga pemerintah. Pendekatan kualitatif dipilih karena penelitian ini tidak berfokus pada pengukuran kuantitatif, melainkan pada analisis kondisi, pola, serta faktor penyebab terjadinya insiden kebocoran data berdasarkan informasi yang tersedia.

Objek kajian dalam penelitian ini mencakup dua kasus kebocoran data yang terjadi di Indonesia, yaitu insiden kebocoran data pada Pusat Data Nasional (PDN) pada Juni 2024 dan Badan Kepegawaian Negara (BKN) pada Agustus 2024. Metode studi kasus digunakan karena memungkinkan peneliti untuk menelaah suatu peristiwa secara mendalam dan kontekstual melalui pengumpulan data dari berbagai sumber, seperti dokumen resmi pemerintah, publikasi ilmiah, serta pemberitaan media massa.

Analisis dilakukan dengan menggunakan kerangka kerja NIST CSF sebagai panduan dalam mengevaluasi tingkat keamanan siber. NIST *Cybersecurity Framework* (CSF) adalah sebuah perangkat panduan perlindungan keamanan siber dari National Institute of Standards and Technology (NIST). Kerangka kerja ini dipilih karena menyediakan pendekatan sistematis dalam menilai tata kelola, pengelolaan risiko, serta kesiapan organisasi dalam menghadapi dan menangani insiden keamanan siber melalui enam fungsi utama, yaitu *Govern, Identify, Protect, Detect, Respond,* dan *Recover.*

2.2 Instrumen Penelitian

Menurut (Sugiyono, 2022), instrumen penelitian merupakan suatu alat yang digunakan untuk mengukur sebuah fenomena alam ataupun sosial yang diamati. Sedangkan, menurut **(**Komang & Atmaja, 2020) instrumen penelitian merupakan alat yang digunakan untuk mengumpulkan data pada penelitian. Berdasarkan pengertian diatas, dapat disimpulkan bahwa instrumen penelitian adalah alat atau cara yang digunakan untuk mengumpulkan data-data yang berkaitan dengan keperluan penelitian. Pada penelitian ini, instrumen penelitian yang digunakan berupa panduan observasi dan studi dokumentasi yang disusun berdasarkan enam fungsi utama dari NIST CSF 2.0.

2.3 Metode Pengumpulan Data

Pengumpulan data dilakukan guna mendapatkan informasi-informasi yang dibutuhkan untuk menjawab penelitian yang dilakukan. Untuk mengumpulkan data yang diperlukan, maka perlu menerapkan metode pengumpulan data. Metode pengumpulan data menurut (Makbul, 2021) merupakan suatu teknik, metode atau cara yang digunakan oleh peneliti untuk mengumpulkan data yang berkaitan dengan penelitian.

2.4 Analisis Data

Analisis data pada penelitian ini dilakukan dengan menggunakan analisis deskriptif kualitatif berdasarkan tujuh tahapan implementasi NIST (NIST, 2018). Tahapan ini digunakan untuk memastikan bahwa analisis dilakukan secara sistematis dan terstruktur. Langkah-langkah tersebut meliputi:

1. Menentukan Prioritas dan Ruang Lingkup *(Prioritize and Scope)*

   Menentukan tujuan organisasi serta ruang lingkup. Pada tahap ini, organisasi mengidentifikasi sistem, aset, data, dan layanan yang akan dianalisis. Penentuan prioritas didasarkan pada tingkat risiko dan dampak terhadap operasional organisasi.
2. Orientasi Konteks Organisasi dan Risiko *(Orient)*

   Mengidentifikasi lingkungan bisnis, regulasi yang berlaku, aset penting, ancaman yang mungkin terjadi, serta kerentanan yang ada. Tahap ini bertujuan untuk memahami kondisi internal dan eksternal yang mempengaruhi keamanan informasi.
3. Menyusun Profile Kondisi Saat Ini *(Create Current Profile)*

Pada tahap ini dilakukan pemetaan kondisi keamanan yang sedang berjalan berdasarkan fungsi utama NIST CSF 2.0. Hasilnya adalah gambaran nyata mengenai tingkat kematangan keamanan siber organisasi saat ini.

4. Melakukan Nilai Risiko *(Conduct Risk Assessment)*

   Menganalisis kemungkinan terjadinya ancaman serta dampak yang ditimbulkan terhadap aset dan layanan penting. Penilaian risiko ini menjadi dasar dalam menentukan langkah pengamanan yang diperlukan.
5. Menyusun Profil Target *(Create Target Profile)*

   Menetapkan kondisi keamanan yang ingin dicapai. Profil target ini menggambarkan tingkat keamanan ideal yang sesuai dengan kebutuhan dan toleransi risiko organisasi.
6. Menentukan dan Memprioritaskan Kesenjangan *(Determine, Analyze, and Prioritize Gaps)*

   Membandingkan profil saat ini dengan profil target untuk mengidentifikasi kesenjangan *(gap).* Setiap celah kemudian dianalisis dan diprioritaskan berdasarkan tingkat risiko serta urgensi perbaikannya.
7. Menyusun dan Mengusulkan Rencana Perbaikan *(Implement Action Plan)*

   Menyusun dan melaksanakan rencana aksi untuk menutup kesenjangan yang telah diidentifikasi. Implementasi dapat berupa pembaruan kebijakan, peningkatan teknologi keamanan, pelatihan SDM, atau perbaikan prosedur operasional.

3. HASIL DAN PEMBAHASAN

Hasil analisis pada penelitian ini diperoleh melalui penerapan kerangka kerja NIST CSF 2.0 terhadap dua studi kasus, yaitu insiden kebocoran data pada Pusat Data Nasional (PDN) dan Badan Kepegawaian Negara (BKN). Analisis dilakukan melalui tujuh tahapan implementasi, mulai dari *prioritize and scope* hingga *implement action plan*. Secara umum, hasil analisis menunjukkan bahwa kedua organisasi memiliki tingkat kematangan keamanan siber yang masih rendah, dengan mayoritas berada pada *Tier 1 (Partial).* Hal ini mengindikasikan bahwa praktik keamanan yang dilakukan masih bersifat reaktif, tidak terstandarisasi, serta belum berbasis manajemen risiko yang terstruktur.

Pada kasus PDN, hasil analisis menunjukkan bahwa kelemahan paling dominan terletak pada aspek ketersediaan layanan *(availability)* dan ketahanan sistem *(resilience).* Tidak tersedianya sistem

backup yang memadai, tidak adanya DRP *(Disaster Recovery Plan)*, serta lemahnya mekanisme pemantauan keamanan menyebabkan organisasi tidak memiliki kemampuan untuk mempertahankan layanan ketika terjadi gangguan. Hal ini terbukti dari dampak insiden yang mengakibatkan terganggunya berbagai layanan publik berbasis digital secara luas.

Dari perspektif fungsi NIST CSF 2.0, kelemahan pada PDN dapat dijelaskan sebagai berikut. Pada fungsi *govern*, tidak ditemukan adanya kebijakan keamanan yang terdokumentasi seperti IRP *(Incident Response Plan)*, DRP *(Disaster Recovery Plan)* dan BCP *(Business Continuity Plan)* yang seharusnya menjadi dasar dalam pengelolaan keamanan siber. Pada fungsi *identify*, tidak adanya inventaris aset yang terstruktur menyebabkan rendahnya visibilitas terhadap aset kritikal yang harus dilindungi. Kondisi ini berimplikasi pada fungsi *protect*, di mana kontrol akses dan perlindungan data tidak diterapkan secara optimal karena tidak adanya prioritas yang jelas.

Pada fungsi *detect,* tidak ditemukannya implementasi teknologi seperti SIEM *(Security Information and Event Management)* dan EDR *(Endpoint Detection and Response)* menyebabkan organisasi tidak mampu melakukan pemantauan secara *real-time*. Akibatnya, ancaman tidak dapat dideteksi sejak dini dan berkembang menjadi insiden yang berdampak besar. Ketika insiden terjadi, kelemahan pada fungsi *respond* terlihat dari tidak adanya prosedur respons yang terdokumentasi, sehingga penanganan dilakukan secara ad-hoc. Hal ini diperparah oleh kelemahan pada fungsi *recover*, di mana tidak terdapat rencana pemulihan yang terstruktur sehingga waktu pemulihan menjadi lebih lama dan berdampak pada kontinuitas layanan.

Pada kasus BKN, hasil analisis menunjukkan bahwa kelemahan utama terletak pada aspek kerahasiaan data *(confidentiality).* Tidak adanya klasifikasi data menyebabkan seluruh data diperlakukan secara seragam tanpa mempertimbangkan tingkat sensitivitasnya. Hal ini meningkatkan risiko kebocoran data, terutama terhadap data pribadi ASN yang bersifat sensitif.

Dari sisi fungsi NIST CSF pada fungsi *govern,* tidak terdapat kebijakan formal terkait klasifikasi dan pengelolaan data. Pada fungsi *identify,* aset data dan sistem belum terinventarisasi secara menyeluruh sehingga organisasi tidak memiliki pemahaman yang jelas terhadap sumber daya yang dimiliki. Pada fungsi *protect,* implementasi MFA *(Multi-Factor Authentication)* belum dilakukan secara menyeluruh serta belum terdapat mekanisme enkripsi data yang memadai.

Kelemahan ini diperburuk oleh fungsi *detect,* yang belum berjalan optimal dengan ditandai tidak adanya sistem *monitoring* keamanan yang terintegrasi. Akibatnya, kebocoran data justru diketahui oleh pihak eksternal, bukan melalui mekanisme deteksi internal. Pada fungsi *respond,* respons insiden masih bersifat reaktif dan tidak didukung oleh prosedur teknis yang terdokumentasi. Sedangkan pada fungsi *recover,* tidak terdapat informasi mengenai proses pemulihan yang terstruktur, yang menunjukkan rendahnya kesiapan organisasi dalam menghadapi insiden lanjutan.

Hasil *risk assessment* pada kedua kasus menunjukkan bahwa sebagian besar risiko berada pada kategori tinggi hingga sangat tinggi. Pada kasus PDN, risiko utama berkaitan dengan gangguan layanan publik, kehilangan data, serta kegagalan pemulihan sistem. Sementara pada kasus BKN, risiko utama berkaitan dengan kebocoran data pribadi, penyalahgunaan data, serta penurunan kepercayaan publik. Selanjutnya, hasil *gap analysis* menunjukkan adanya kesenjangan signifikan antara kondisi aktual dengan kondisi ideal yang ditetapkan pada *Tier 3 (Repeatable).* Kesenjangan tersebut meliputi tidak adanya kebijakan keamanan yang terstruktur, lemahnya manajemen aset dan risiko, tidak optimalnya kontrol akses dan perlindungan data, ketiadaan sistem deteksi dini serta belum adanya rencana respons dan pemulihan yang formal.

Secara keseluruhan, hasil analisis menunjukkan bahwa kelemahan pada masing-masing fungsi tidak berdiri sendiri, melainkan saling berkaitan dan membentuk suatu rantai kerentanan. Kegagalan pada satu fungsi akan mempengaruhi efektivitas fungsi lainnya, sehingga meningkatkan risiko terjadinya insiden dengan dampak yang lebih besar.

3.1 Pembahasan

Berdasarkan hasil analisis yang telah dilakukan terhadap kasus PDN dan BKN, dapat dipahami bahwa permasalahan keamanan siber di lingkungan pemerintahan memiliki karakteristik yang kompleks dan multidimensional. Permasalahan tidak hanya disebabkan oleh keterbatasan teknologi, tetapi juga oleh lemahnya tata kelola, kurangnya manajemen risiko, serta belum terbentuknya budaya keamanan siber dalam organisasi.

Salah satu temuan utama dalam penelitian ini adalah bahwa fungsi *govern* merupakan fondasi utama dalam keamanan siber. Pada kedua kasus, tidak adanya kebijakan keamanan yang terdokumentasi menyebabkan seluruh implementasi keamanan berjalan tanpa arah yang jelas. Tanpa adanya tata kelola yang kuat, organisasi tidak memiliki standar dalam menerapkan kontrol keamanan, sehingga setiap fungsi berjalan secara parsial dan tidak terintegrasi. Kelemahan pada fungsi *govern* ini kemudian berdampak pada fungsi *identify*, di mana organisasi tidak memiliki visibilitas yang memadai terhadap aset dan data yang dimiliki. Ketidakjelasan ini menyebabkan organisasi tidak mampu menentukan prioritas perlindungan secara tepat. Akibatnya, kontrol keamanan pada fungsi *protect* tidak dapat diterapkan secara efektif, karena tidak didasarkan pada tingkat kritikalitas aset.

Lebih lanjut, kelemahan pada fungsi *protect* membuka peluang bagi terjadinya ancaman keamanan. Namun, ancaman tersebut tidak dapat segera diidentifikasi karena lemahnya fungsi *detect* yang ditandai dengan tidak adanya sistem *monitoring real-time.* Kondisi ini menyebabkan insiden berkembang tanpa terdeteksi hingga mencapai skala yang lebih besar. Ketika insiden terjadi, kelemahan pada fungsi *respond* menyebabkan proses penanganan menjadi lambat dan tidak terkoordinasi. Tidak adanya prosedur respons yang terdokumentasi membuat organisasi bergantung pada keputusan situasional, yang sering kali tidak efektif dalam kondisi krisis. Selanjutnya, kelemahan pada fungsi *recover* memperpanjang dampak insiden karena organisasi tidak memiliki strategi pemulihan yang matang.

Dari sudut pandang konseptual, hasil penelitian ini menegaskan bahwa keamanan siber merupakan suatu sistem yang terintegrasi, di mana setiap fungsi dalam NIST CSF 2.0 saling bergantung satu sama lain. Fungsi *govern* berperan sebagai landasan strategis, *identify* sebagai dasar pengenalan aset dan risiko, *protect* dan *detect* sebagai mekanisme pertahanan, serta *respond* dan *recover* sebagai upaya penanganan dan pemulihan. Selain itu, penelitian ini juga menunjukkan adanya perbedaan karakteristik risiko antara kedua kasus. Pada PDN, fokus risiko berada pada aspek *availability* karena gangguan layanan berdampak langsung pada operasional pemerintahan. Sementara pada BKN, fokus risiko berada pada aspek *confidentiality* karena kebocoran data berdampak pada privasi dan keamanan informasi individu.

Perbedaan ini menunjukkan bahwa pendekatan keamanan siber harus disesuaikan dengan karakteristik organisasi dan jenis aset yang dikelola. Namun demikian, kedua kasus tetap menunjukkan pola kelemahan yang serupa yaitu rendahnya tingkat kematangan keamanan dan belum diterapkannya pendekatan berbasis risiko. Secara keseluruhan, penelitian ini menegaskan bahwa peningkatan keamanan siber tidak dapat dilakukan secara parsial atau hanya berfokus pada teknologi semata. Diperlukan pendekatan yang komprehensif yang mencakup aspek tata kelola, proses, teknologi serta sumber daya manusia. Implementasi kerangka kerja seperti NIST CSF 2.0 menjadi penting sebagai panduan dalam membangun sistem keamanan yang terstruktur, terintegrasi, dan berkelanjutan. Dengan adanya perbaikan yang menyeluruh pada seluruh fungsi, organisasi diharapkan dapat meningkatkan tingkat kematangan keamanan siber, mengurangi risiko insiden, serta meningkatkan ketahanan dalam menghadapi ancaman siber di masa mendatang..

4. KESIMPULAN

Terkait dengan rumusan masalah mengenai kondisi keamanan siber pada saat insiden terjadi, hasil analisis menunjukkan bahwa tingkat kematangan keamanan siber pada kedua instansi masih berada pada

Tier 1 (Partial). Kondisi ini mencerminkan bahwa praktik keamanan yang diterapkan belum terstruktur, belum terdokumentasi secara formal serta belum berbasis pada pendekatan manajemen risiko. Pada kasus PDN kelemahan utama terletak pada aspek *availability*, yang ditunjukkan dengan tidak adanya sistem backup yang memadai serta ketiadaan DRP *(Disaster Recovery Plan)* dan BCP *(Business Continuity Plan)* sehingga berdampak pada terganggunya layanan publik secara luas. Sementara itu pada kasus BKN kelemahan utama terletak pada aspek *confidentiality*, yang ditandai dengan tidak adanya klasifikasi data dan lemahnya kontrol akses sehingga meningkatkan risiko kebocoran data pribadi.

Terkait dengan rumusan masalah mengenai penerapan kerangka kerja NIST CSF 2.0 dalam menganalisis keamanan siber, hasil penelitian menunjukkan bahwa kerangka kerja ini mampu memberikan pendekatan yang sistematis dan komprehensif dalam mengidentifikasi kelemahan pada setiap fungsi keamanan siber. Melalui pemetaan terhadap fungsi *govern, identify, protect, detect, respond* dan *recover* dapat diketahui bahwa kelemahan paling mendasar pada kedua kasus terletak pada fungsi *govern* yang dimana tidak adanya kebijakan keamanan yang formal dan terintegrasi. Kelemahan ini berdampak secara sistemik terhadap fungsi lainnya, karena tidak adanya landasan dalam pengelolaan risiko dan penerapan kontrol keamanan.

Terkait dengan rumusan masalah mengenai kesenjangan antara kondisi aktual dan kondisi ideal, hasil *gap analysis* menunjukkan adanya perbedaan signifikan antara kondisi saat ini *Tier 1(Partial)* dengan kondisi yang diharapkan *Tier 3 (Repeatable).* Kesenjangan tersebut mencakup tidak adanya tata kelola keamanan yang terstruktur, lemahnya visibilitas aset dan manajemen risiko, belum optimalnya kontrol akses dan perlindungan data, tidak adanya sistem deteksi dini serta belum tersedianya prosedur respons dan pemulihan yang formal.

Terkait dengan rumusan masalah mengenai upaya peningkatan keamanan siber, hasil penelitian menunjukkan bahwa peningkatan harus dilakukan secara terintegrasi dan berbasis risiko pada seluruh fungsi dalam NIST CSF 2.0. Perbaikan tidak dapat dilakukan secara parsial, melainkan harus dimulai dari penguatan tata kelola *(govern)* sebagai fondasi utama, yang kemudian diikuti dengan peningkatan kemampuan pada *fungsi identify, protect, detect, respond* dan *recover* secara berkesinambungan.

Secara keseluruhan, penelitian ini menegaskan bahwa kelemahan pada satu fungsi keamanan siber akan berdampak pada fungsi lainnya sehingga diperlukan pendekatan yang holistik dalam meningkatkan ketahanan siber organisasi. Tanpa adanya tata kelola yang kuat, implementasi kontrol teknis tidak akan berjalan secara optimal dan tidak mampu mengurangi risiko secara signifikan

REFERENSI

[1] A. Mergel, N. Edelmann, and N. Haug, "Defining digital transformation: Results from expert interviews," *Government Information Quarterly*, vol. 38, no. 4, 2021, doi: 10.1016/j.giq.2021.101587.
[2] Y. K. Dwivedi et al., "Impact of digital transformation on public sector performance," *International Journal of Information Management*, vol. 60, 2021, doi: 10.1016/j.ijinfomgt.2021.102397.
[3] M. A. Wirtz and D. Müller, "E-government and public service value creation," *Public Management Review*, vol. 24, no. 6, 2022, doi: 10.1080/14719037.2021.1895228.
[4] T. Cordella and F. Tempini, "E-government and organizational change," *Government Information Quarterly*, vol. 39, no. 2, 2022, doi: 10.1016/j.giq.2021.101653.
[5] S. Ransbotham et al., "Cybersecurity risk management in the public sector," *MIS Quarterly Executive*, vol. 20, no. 4, 2021, doi: 10.17705/2msqe.00045.
[6] A. ENISA, "Threat landscape for ransomware attacks," *Computer Fraud & Security*, vol. 2022, no. 7, 2022, doi: 10.1016/S1361-3723(22)00074-5.
[7] M. K. Rogers and K. Seigfried-Spellar, "Ransomware and critical infrastructure protection," *Journal of Cybersecurity*, vol. 7, no. 1, 2021, doi: 10.1093/cybsec/tyab012.
[8] S. Shackelford, "Managing cybersecurity risk in public institutions," *Journal of National Security Law & Policy*, vol. 12, no. 2, 2022, doi: 10.2139/ssrn.4104325.
[9] H. Bada and A. Nurse, "Developing cybersecurity capability in public sector organisations," *Information & Computer Security*, vol. 29, no. 3, 2021, doi: 10.1108/ICS-09-2020-0141.

[10] J. Bélanger and L. Carter, "Trust and risk in e-government adoption," *Government Information Quarterly*, vol. 38, no. 3, 2021, doi: 10.1016/j.giq.2021.101575.
[11] R. Sabillon, J. Serra-Ruiz, and J. Cavaller, "Cybersecurity frameworks evaluation in public organizations," *Computers & Security*, vol. 108, 2021, doi: 10.1016/j.cose.2021.102384.
[12] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity 2.0," *NIST Special Publication*, 2024, doi: 10.6028/NIST.CSWP.29.
[13] S. M. Furnell and K. Shah, "Cybersecurity governance and standards adoption," *Computer Law & Security Review*, vol. 44, 2022, doi: 10.1016/j.clsr.2021.105655.
[14] M. A. Ali and R. Awad, "Adoption of NIST cybersecurity framework in government institutions," *IEEE Access*, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3156789.
[15] D. S. Setiadi and B. Pratama, "Information security risk assessment in public sector using NIST framework," *Procedia Computer Science*, vol. 197, 2022, doi: 10.1016/j.procs.2021.12.130.