MONAS: Jurnal Inovasi Aparatur
Vol. 7 No. 2 (2025): 82-91
e-ISSN: 2656-0194

Dashboard Security Awareness: Inovasi Peningkatan Kesadaran Keamanan Siber ASN di Era Digital

Dashboard Security Awareness: Innovation for Enhancing Civil Servants' Cybersecurity Awareness in the Digital Era

Nur Izzuddin[1], Andrie Yuswanto[2]
[1,2]Suku Dinas Komunikasi, Informatika dan Statistik Kota Administrasi Jakarta Barat
Jalan Kembangan Raya No. 2, Jakarta Barat 11610
[1]zudin@jakarta.go.id, [2]aan_post@jakarta.go.id

Submitted: 13-10-2025 *Accepted: 01-12-2025* *Published: 15-12-2025*

Abstrak: *Dashboard Security Awareness* (Sec-Aw) merupakan inovasi *platform* digital terpadu yang dikembangkan untuk meningkatkan kesadaran keamanan siber Aparatur Sipil Negara (ASN) di Jakarta Barat. Latar belakang penelitian ini adalah tingginya insiden keamanan siber di Indonesia yang mencapai lebih dari 330 juta serangan pada tahun 2024, dengan 60% insiden disebabkan oleh faktor kelalaian manusia. Penelitian bertujuan mengembangkan *platform* kesadaran keamanan siber yang efektif dengan fitur *self-assessment* berbasis kerangka Badan Siber dan Sandi Negara (BSSN), media edukasi interaktif, *tools* keamanan dasar, dan rekomendasi personal. Metode yang digunakan meliputi penelitian pengembangan (R&D) dengan pendekatan *mixed-method*, analisis *Fishbone* untuk identifikasi akar masalah, analisis USG (*Urgency, Seriousness, Growth*) untuk prioritas masalah, instrumen *self-assessment* mengadaptasi kerangka *Knowledge-Skill-Practice* (K-S-P) dan pendekatan *Multiple Criteria Decision Analysis* (MCDA), serta implementasi bertahap melalui fase persiapan, pengembangan, implementasi, serta evaluasi dan diseminasi. Pengukuran dilakukan dalam dua gelombang, pengukuran awal di Maret 2025 terhadap 77 pengelola TIK UKPD Jakarta Barat menghasilkan skor 2,48 (Kurang Baik), sedangkan pengukuran lanjutan pada Juni 2025 melibatkan 419 pegawai Pemerintah Kota Administrasi Jakarta Barat dan menunjukkan perbaikan menjadi 2,97 (Baik) mencerminkan kenaikan 19,8%. Meski demikian, dua area masih perlu perhatian khusus: Aduan Insiden Teknis (1,93) dan aspek Hukum/Regulasi Sosial (1,38). Penerbitan SE Walikota Jakarta Barat tentang Penyelenggaraan Keamanan SPBE menetapkan *Dashboard* Sec-Aw sebagai instrumen resmi pembinaan dan *self-assessment*, memperkuat tata kelola SPBE dan memperluas cakupan dari kantor walikota ke seluruh UKPD. *Platform* ini mendukung penguatan ketahanan digital Indonesia melalui peningkatan literasi dan budaya keamanan siber aparat pemerintah.
Kata kunci: *dashboard security awareness*, keamanan siber, ASN, inovasi pelayanan publik, bela negara digital, SPBE

Abstract: *Dashboard Security Awareness (Sec-Aw) is an integrated digital platform innovation developed to enhance cybersecurity awareness among Civil Servants (ASN) in West Jakarta. The background of this research stems from the high incidence of cybersecurity attacks in Indonesia, reaching over 330 million incidents in 2024, with 60% attributed to human negligence factors. This study aims to develop an effective cybersecurity awareness platform featuring self-assessment based on the National Cyber and Crypto Agency (BSSN) framework, interactive educational media, basic security tools, and personalized recommendations. The methodology employs Research and Development (R&D) with a mixed-method approach, Fishbone analysis for root cause identification, USG (Urgency, Seriousness, Growth) analysis for problem prioritization, self-assessment instruments adapting the Knowledge-Skill-Practice (K-S-P) framework and Multiple Criteria Decision Analysis (MCDA) approach, along with phased implementation through preparation, development, implementation, and evaluation-dissemination stages. Measurements were conducted in two waves: the initial assessment in March 2025 involving 77 ICT administrators from West Jakarta Government Work Units yielded a score of 2.48 (Poor category), while the follow-up assessment in June 2025 involving 419 employees of the West Jakarta Municipal Government demonstrated improvement to 2.97 (Good category), reflecting a 19.8% increase. Nevertheless, two areas require particular attention: Technical Incident Reporting (1.93) and Social Law/Regulation aspects (1.38). The issuance of West Jakarta Mayor's Circular regarding SPBE Security Implementation establishes Dashboard Sec-Aw as an*

Author(s). (2025). Monas: Jurnal Inovasi Aparatur, 7(2), page 82-91
https://doi.org/10.54849/monas.v7i2.298

official instrument for capacity building and self-assessment, strengthening SPBE governance and expanding coverage from the mayor's office to all work units. This platform supports the strengthening of Indonesia's digital resilience by enhancing cybersecurity literacy and culture among government officials.
Keywords: *dashboard security awareness, cybersecurity, civil servants, public service innovation, digital national defense, SPBE*

PENDAHULUAN

Era transformasi digital membawa perubahan signifikan dalam tata kelola pemerintahan dan pelayanan publik di Indonesia. Pemanfaatan teknologi informasi dalam aktivitas pemerintahan memberikan efisiensi dan kemudahan akses layanan, namun di sisi lain menghadirkan tantangan baru berupa ancaman keamanan siber yang semakin kompleks (Firmansyah & Yuswanto, 2022). Pada tahun 2024, Indonesia menghadapi lebih dari 330 juta serangan siber, menempatkan keamanan siber sebagai isu strategis nasional yang memerlukan penanganan komprehensif (BSSN, 2025).

Permasalahan keamanan siber di Indonesia tidak hanya berkaitan dengan aspek teknis dan infrastruktur teknologi, tetapi lebih dominan disebabkan oleh faktor manusia. Data menunjukkan bahwa 60% insiden keamanan siber terjadi akibat kelalaian dan rendahnya kesadaran pengguna terhadap praktik keamanan digital (Verizon, 2025). Kondisi ini diperparah dengan posisi Indonesia di peringkat 49 dari 176 negara pada National Cyber Security Index, yang mengindikasikan masih terbatasnya kapasitas keamanan siber nasional (NCSI, 2023). Literatur menunjukkan bahwa faktor manusia merupakan dimensi dominan dalam insiden keamanan informasi, sehingga pengukuran kesadaran keamanan perlu mencakup tiga dimensi yaitu pengetahuan *(knowledge*), sikap (*attitude*), dan perilaku (*behavior/practice*) untuk memetakan intervensi yang tepat sasaran (Amin, 2014).

Aparatur Sipil Negara (ASN) sebagai penyelenggara pemerintahan memiliki peran strategis dalam menjaga keamanan informasi dan data publik. Namun, tingkat kesadaran keamanan siber di kalangan ASN masih perlu ditingkatkan melalui program edukasi dan pengembangan kompetensi yang terstruktur dan berkesinambungan. Hal ini sejalan dengan konsep Bela Negara di era digital, yaitu kewajiban setiap warga negara untuk berperan aktif menjaga keamanan siber, melindungi data, dan melawan ancaman digital (Hartono, 2022; Fitri, 2025).

Penelitian sebelumnya mengenai manajemen keamanan informasi pada *Security Operation Center* (SOC) di Pemerintah Provinsi DKI Jakarta menunjukkan pentingnya pengelolaan pengetahuan dan peningkatan kapasitas SDM dalam penanganan insiden keamanan informasi (Firmansyah & Yuswanto, 2022). Namun, belum terdapat *platform* terpadu yang menyediakan fitur *self-assessment* terstandar, edukasi interaktif, *tools* keamanan, dan rekomendasi personal yang mudah diakses oleh ASN secara luas. Kontribusi orisinal penelitian ini adalah integrasi *self-assessment* Survei Kesadaran Keamanan Siber (SKKS) Badan Siber dan Sandi Negara (BSSN) dengan konten edukasi, *tools* keamanan, rekomendasi personal berbasis hasil *assessment*, dan keterhubungan kebijakan daerah melalui Surat Edaran (SE) Walikota Jakarta Barat sebagai enabler tata kelola SPBE.

Dashboard Security Awareness (Sec-Aw) dikembangkan sebagai solusi inovatif untuk menjawab kebutuhan peningkatan kesadaran keamanan siber melalui pendekatan yang komprehensif dan terukur. *Platform* ini mengintegrasikan nilai-nilai budaya kerja BerAKHLAK (Berorientasi Pelayanan, Akuntabel, Kompeten, Harmonis, Loyal, Adaptif, dan Kolaboratif) dalam konteks Bela Negara digital yang melibatkan peran aktif setiap warga negara dalam menjaga keamanan siber, serta mendukung implementasi Asta Cita Presiden, khususnya butir kedua mengenai pemantapan sistem pertahanan dan keamanan nasional serta butir keempat tentang penguatan sumber daya manusia (Subianto & Raka, 2024).

Tujuan penelitian ini adalah mengembangkan dan mengimplementasikan *Dashboard* Sec-Aw sebagai *platform* digital terpadu untuk meningkatkan kesadaran keamanan siber ASN, mengukur efektivitas *platform* melalui perbandingan *baseline* dan pasca-implementasi, serta memetakan area prioritas intervensi berdasarkan analisis dimensi keamanan siber teknis dan sosial. Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan kebijakan keamanan siber berbasis data dan menjadi model replikasi bagi instansi pemerintah lainnya di seluruh Indonesia.

METODE PENELITIAN

Penelitian ini merupakan penelitian pengembangan (*Research and Development*) dengan pendekatan *mixed-method* yang menggabungkan analisis kualitatif dan kuantitatif. Penelitian dilaksanakan di Suku Dinas Komunikasi, Informatika dan Statistik Kota Administrasi Jakarta Barat pada periode Maret 2025 hingga Juni 2025.

Penelitian menggunakan pendekatan pengembangan inovasi pelayanan publik dengan tahapan sistematis meliputi analisis kebutuhan, perancangan sistem, implementasi, dan evaluasi. Metode analisis masalah menggunakan Diagram *Fishbone* untuk mengidentifikasi akar permasalahan keamanan siber yang disebabkan faktor sumber daya manusia. Analisis prioritas masalah menggunakan metode USG (*Urgency, Seriousness, Growth*) untuk menentukan fokus penanganan yang paling strategis.

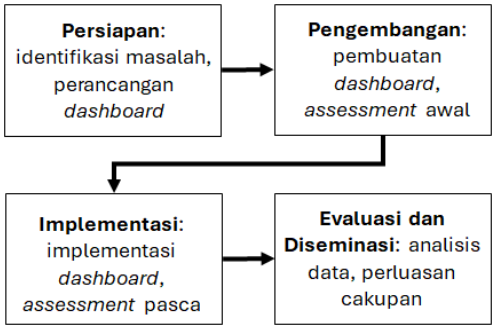
Pengukuran dilakukan dalam dua gelombang dengan komposisi responden yang berbeda. Gelombang pertama (Maret 2025) merupakan baseline assessment yang melibatkan 77 pengelola TIK UKPD Jakarta Barat, menggunakan teknik purposive sampling, menghasilkan skor rata-rata 2,48 pada skala 1-4 (kategori Kurang Baik). Gelombang kedua (Juni 2025), sebagai pasca-implementasi, mengikutsertakan 419 pegawai ASN dan Non-ASN dari Pemerintah Kota Administrasi Jakarta Barat, melebihi target minimal 378 sampel yang ditentukan berdasarkan populasi 12.000 dengan margin error 5% sesuai perhitungan Krejcie-Morgan. Perbedaan komposisi sampel ini penting dicatat sebagai limitasi metodologis sekaligus indikator perluasan cakupan adopsi *platform*. Data *baseline* digunakan sebagai konteks historis, bukan pembanding langsung antara kelompok yang homogen. Oleh karena itu, interpretasi kenaikan skor 19,8% dilakukan secara konservatif, merefleksikan perubahan kondisi organisasi dan persepsi umum, bukan perubahan perilaku individu yang sama secara longitudinal. Jumlah responden yang melebihi target mencerminkan antusiasme tinggi sekaligus meningkatkan presisi estimasi hasil survei.

Instrumen penelitian meliputi kuesioner *self-assessment* berbasis kerangka SKKS milik BSSN yang mengadaptasi dimensi *Knowledge-Skill-Practice* (K-S-P) yang dikembangkan oleh Kruger & Kearney (2006) untuk mengukur kesadaran keamanan informasi (Amin, 2014). Pengukuran kesadaran keamanan dalam penelitian ini juga mengacu pada instrumen standar seperti *Human Aspects of Information Security Questionnaire* (HAIS-Q) yang telah tervalidasi (Parsons et al., 2017). Instrumen mengukur dua dimensi utama: (1) Kesadaran Keamanan Siber Teknis, mencakup 6 indikator (Syarat dan Ketentuan Instalasi, Kata Sandi/Password, Internet dan WiFi, Keamanan Perangkat, Aduan Insiden Siber Teknis, Hukum dan Regulasi Keamanan Siber Teknis); (2) Kesadaran Keamanan Siber Sosial, mencakup 5 indikator (Rekayasa Sosial/Social Engineering, Konten Negatif, Aktivitas Media Sosial, Aduan Insiden Siber Sosial, Hukum dan Regulasi Keamanan Siber Sosial). Skala pengukuran menggunakan rentang 1-4 dengan kategorisasi: Tidak Baik (1,00-1,75), Kurang Baik (1,76-2,50), Baik (2,51-3,25), Sangat Baik (3,26-4,00). Pendekatan pengukuran mengadaptasi kerangka Multiple Criteria Decision Analysis (MCDA) yang menghitung nilai total berdasarkan bobot kriteria (Amin, 2014), dengan potensi penerapan Analytical Hierarchy Process (AHP) sebagai metode pembobotan yang telah terbukti efektif dalam analisis multi-kriteria (Brunelli, 2015; Vaidya & Kumar, 2006) untuk pembobotan area kritikal pada studi replikasi atau analisis lanjutan bersama pemangku kepentingan daerah.

Prosedur penelitian mengikuti tahapan rancang bangun inovasi yang terdiri dari empat fase:

1. Fase Persiapan: Pembentukan tim, identifikasi masalah menggunakan analisis *fishbone*, koordinasi *stakeholder*, dan penyusunan rancangan sistem.
2. Fase Pengembangan: Pelaksanaan *assessment baseline* (Maret 2025) terhadap pengelola TIK UKPD, pembuatan *dashboard*, pengembangan fitur self-*assessment* berbasis kerangka BSSN, uji coba sistem, dan implementasi awal.
3. Fase Implementasi: Sosialisasi dan publikasi, implementasi *dashboard* dengan akses media edukasi dan *tools* keamanan, pelaksanaan *assessment* pasca-implementasi (Juni 2025) terhadap seluruh pegawai Pemerintah Kota Administrasi Jakarta Barat, penyempurnaan sistem, dan update konten edukasi.
4. Fase Evaluasi dan Diseminasi: Analisis data, update konten berkelanjutan, perluasan

cakupan, serta upaya replikasi ke lingkup institusi yang lebih luas.



Gambar 1. Alur Kerja Penelitian

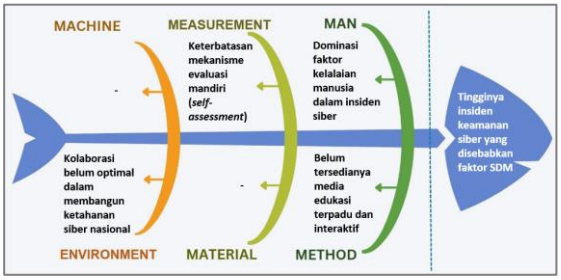
Teknik pengumpulan data menggunakan: (1) survei online melalui *platform Dashboard* Sec-Aw, (2) *focus group discussion* (FGD), (3) wawancara mendalam dengan *stakeholder* dan pengguna, (4) observasi penggunaan *platform*, dan (5) studi dokumentasi kebijakan keamanan siber dan SE Walikota.

Analisis data dilakukan dengan pendekatan deskriptif kuantitatif untuk mengukur peningkatan skor kesadaran keamanan siber sebelum dan sesudah menggunakan *platform*. Data hasil *self-assessment* diolah menggunakan statistik deskriptif untuk menghitung rata-rata skor, delta perubahan (0,49 poin atau 19,8%), dan distribusi kategori kesadaran per indikator. Analisis breakdown dilakukan pada dimensi teknis dan sosial untuk memetakan gap area rendah sebagai prioritas intervensi. Analisis kualitatif digunakan untuk mengevaluasi *feedback* pengguna, identifikasi hambatan implementasi, peran SE Walikota Jakarta Barat sebagai instrumen tata kelola, dan rekomendasi perbaikan sistem berkelanjutan. Potensi bias komposisi sampel antara *baseline* (pengelola TIK) dan pasca-implementasi (seluruh pegawai) dicatat sebagai keterbatasan dan pertimbangan dalam menafsirkan hasil; penelitian lanjutan disarankan menggunakan desain longitudinal untuk memperkuat analisis sebab-akibat.

Pendekatan Multiple Criteria Decision Analysis (MCDA) digunakan dalam penelitian ini sebagai kerangka konseptual untuk memahami pengambilan keputusan multi-kriteria dalam pengukuran *awareness*. Namun, perhitungan bobot indikator tidak dilakukan secara eksplisit pada tahap ini. Analytical Hierarchy Process (AHP) baru diposisikan sebagai rekomendasi metodologis untuk penelitian lebih lanjut dan belum diaplikasikan dalam pengolahan data penelitian ini.

HASIL DAN PEMBAHASAN

Berdasarkan analisis menggunakan metode Diagram *Fishbone*, teridentifikasi permasalahan utama yaitu tingginya insiden keamanan siber yang disebabkan faktor sumber daya manusia (SDM). Analisis mendalam menghasilkan empat akar masalah kritis: (1) dominasi faktor kelalaian manusia dalam insiden siber akibat rendahnya literasi digital dan pemahaman tentang ancaman rekayasa sosial, (2) belum tersedianya media edukasi terpadu dan interaktif yang dapat diakses luas dengan sistem pengukuran kesadaran yang terstandar, (3) keterbatasan mekanisme evaluasi mandiri (*self-assessment*) untuk memberikan gambaran akurat tingkat kesadaran keamanan siber individu, dan (4) kolaborasi yang belum optimal antara ASN dan masyarakat serta *stakeholder* dalam membangun ketahanan siber nasional.



Gambar 2. Analisis Fishbone Identifikasi Akar Masalah

Tabel 1. Analisis USG Terhadap Akar Masalah

No	Penyebab Masalah	Kriteria			Skor	Prioritas
		U	S	G		
1.	Dominasi faktor kelalaian manusia dalam insiden siber.	5	5	5	15	I
2.	Keterbatasan mekanisme evaluasi mandiri (*self-assessment*)	4	5	5	14	II
3.	Belum tersedianya media edukasi terpadu dan interaktif	4	4	5	13	III
4.	Kolaborasi belum optimal dalam membangun ketahanan siber nasional	4	4	4	12	IV

Hasil analisis prioritas menggunakan metode USG menunjukkan bahwa dominasi faktor kelalaian manusia memperoleh skor tertinggi (15) dengan nilai *Urgency, Seriousness, dan Growth* masing-masing 5, diikuti oleh keterbatasan mekanisme *self-*

assessment (skor 14), belum tersedianya media edukasi terpadu (skor 13), dan kolaborasi yang belum optimal (skor 12). Temuan ini sejalan dengan penelitian Firmansyah & Yuswanto (2022) yang menyatakan bahwa pengelolaan pengetahuan dan peningkatan kapasitas SDM merupakan kunci dalam menghadapi ancaman siber, serta Amin (2014) yang menekankan pentingnya pengukuran kesadaran keamanan informasi berbasis dimensi pengetahuan, sikap, dan perilaku.

Dashboard Sec-Aw dirancang sebagai *platform* digital terpadu yang memiliki lima komponen utama. Pertama, modul *Self-Assessment* yang memungkinkan pengguna melakukan penilaian mandiri tingkat kesadaran keamanan siber sesuai standar nasional dengan pendekatan dimensi K-S-P. Kedua, Media Edukasi Interaktif berupa video pembelajaran berupa *podcast*, infografis, dan modul materi yang mudah dipahami dan diperbarui secara berkala. Ketiga, beberapa *Tools* Keamanan Siber Dasar yang antara lain fasilitas pengecekan kekuatan password, pengecekan keamanan website, dan simulasi *phishing* untuk meningkatkan kewaspadaan pengguna. Keempat, sistem Rekomendasi Personal yang memberikan saran perbaikan aspek keamanan digital berdasarkan hasil *assessment* individual pengguna, serta memetakan hasil *assessment* berdasarkan kategori keamanan siber teknis dan sosial.

Gambar 3. Halaman Utama Dashboard Sec-Aw

Desain *platform* mengikuti prinsip *user-friendly* dengan antarmuka yang *intuitif*, aksesibilitas tinggi, dan responsif terhadap berbagai perangkat (desktop, tablet, smartphone), sejalan dengan prinsip evaluasi *context* dalam model CIPP yang menekankan kesesuaian program dengan kebutuhan pengguna (Sukoco & Kurniadewi, 2023).

Implementasi *pilot project* dilaksanakan secara bertahap melalui sosialisasi, penyediaan tutorial, pelatihan penggunaan *platform*, dan kampanye kesadaran keamanan siber kepada pegawai Pemerintah Kota Administrasi Jakarta Barat beserta masyarakat. Tahap sosialisasi melibatkan workshop dan demonstrasi *platform* yang dihadiri oleh perwakilan UKPD sebagai target pengguna awal. Proses implementasi mengintegrasikan nilai-nilai BerAKHLAK dalam setiap tahapan, khususnya nilai Berorientasi Pelayanan melalui pengembangan *platform* yang *user-centric*, Akuntabel melalui transparansi hasil *assessment*, Kompeten dengan penyediaan konten edukasi berkualitas, Harmonis melalui kolaborasi *multi-stakeholder*, Loyal pada komitmen keamanan siber nasional, Adaptif terhadap perkembangan ancaman siber, dan Kolaboratif dalam berbagi pengetahuan keamanan siber.

Hasil implementasi menunjukkan respons positif dari pengguna, dengan tingkat partisipasi *self-assessment* melebihi target responden dari 378 menjadi 419 (10,85%). Feedback pengguna mengindikasikan bahwa *platform* dinilai mudah digunakan, konten edukasi relevan dengan kebutuhan, dan fitur *self-assessment* memberikan *insight* berharga mengenai tingkat kesadaran keamanan siber personal. Temuan ini konsisten dengan penelitian Sukoco & Kurniadewi (2023) yang menyatakan bahwa kemudahan akses dan kualitas konten merupakan faktor kunci keberhasilan *platform* pembelajaran digital.

Evaluasi efektivitas *Dashboard* Sec-Aw dilakukan dengan membandingkan skor kesadaran keamanan siber pegawai sebelum dan sesudah menggunakan *platform*. Hasil *assessment* awal (Maret 2025) pada 77 pengelola TIK UKPD menunjukkan nilai rata-rata kesadaran keamanan siber sebesar 2,48 yang termasuk dalam kategori "Kurang Baik" (skala 1-4). Rincian *baseline*: dimensi Teknis 2,33; dimensi Sosial 2,65. Sub-indikator terendah adalah Aduan Insiden Siber Teknis (1,75) dan Aduan Insiden Siber Sosial (1,58), mengindikasikan hambatan signifikan dalam kultur pelaporan insiden.

Setelah periode implementasi *platform* dengan akses berkelanjutan terhadap media edukasi, *tools* keamanan, dan rekomendasi personal, dilakukan *assessment* lanjutan (Juni 2025) pada 419 pegawai Pemerintah Kota Administrasi Jakarta Barat yang menunjukkan peningkatan signifikan dengan nilai rata-rata menjadi 2,97 yang termasuk dalam kategori "Baik" (2,51-3,25). Rincian pasca-implementasi: dimensi Teknis 2,94; dimensi

Sosial 3,02. Peningkatan sebesar 0,49 poin atau 19,8% harus dipahami sebagai kenaikan skor indeks awareness pada skala ordinal 1–4, bukan sebagai peningkatan prosentase perilaku. Komposisi sampel *baseline* dan pasca-implementasi berbeda, sehingga kesimpulan tentang efektivitas lebih tepat dibaca sebagai indikasi positif dan bukan bukti kausalitas kuat. Temuan ini tetap memberi ilustrasi potensi dampak program sebagai *pilot project*, dengan batas inferensi yang jelas.

Analisis lebih mendalam terhadap komponen kesadaran keamanan siber menunjukkan peningkatan signifikan pada aspek pemahaman ancaman *phishing* yang terukur melalui indikator Rekayasa Sosial (peningkatan dari 2,72 menjadi 3,27 atau +20,2%), praktik penggunaan password yang kuat pada indikator Kata Sandi (peningkatan dari 2,39 menjadi 2,95 atau +23,4%), kesadaran keamanan perangkat (peningkatan dari 2,26 menjadi 3,20 atau +41,6%), dan kepatuhan terhadap syarat instalasi aplikasi (peningkatan dari 2,37 menjadi 3,34 atau +40,9%). Hal ini mengindikasikan efektivitas materi edukatif yang lebih mudah diaplikasikan dalam tugas sehari-hari, serta tingginya relevansi ancaman sosial engineering di lingkungan pegawai

Namun, pada aspek teknis, indikator Aduan Insiden Siber Teknis tetap merupakan yang terendah meskipun naik dari 1,75 menjadi 1,93 (+10,3%), yang mengindikasikan perlunya penyederhanaan kanal pelaporan, pelatihan alur pelaporan, dan pemberian insentif bagi pelapor. Skor rendah ini kemungkinan muncul akibat kendala teknis berupa kanal pelaporan yang masih dianggap rumit serta faktor budaya organisasi yang membuat pegawai enggan melapor karena kekhawatiran terhadap sanksi atau stigma sosial terkait pelaporan insiden. Oleh karena itu, diperlukan upaya perbaikan proses pelaporan agar lebih mudah, transparan, dan adanya jaminan perlindungan bagi pelapor.

Pada aspek sosial, indikator Hukum dan Regulasi Keamanan Siber Sosial terdapat anomali berupa penurunan tajam skor dari 2,48 menjadi 1,38 (-44,4%) setelah implementasi *platform*. Fenomena ini diduga terjadi karena dua faktor utama. Pertama, konten regulasi yang disediakan di *platform* masih bersifat umum dan belum sepenuhnya menjawab kebutuhan pegawai akan praktik keamanan yang kontekstual. Kedua, meningkatnya kesadaran akibat edukasi interaktif justru membuat responden semakin sadar akan kekurangan pengetahuan mereka (penurunan efek *social desirability*). Hal ini menunjukkan perlunya strategi konten yang lebih adaptif dan spesifik bagi kelompok pengguna dengan kebutuhan berbeda.

Tabel 2. Perbandingan Hasil Assessment Kesadaran Keamanan Siber

No	Indikator	Baseline	Pasca	Delta	Perubahan (%)	Kategori Pasca
Nilai Kesadaran Keamanan Siber Teknis		**2,33**	**2,94**	**+0,61**	**+26,2%**	**Baik**
1	Syarat dan Ketentuan Instalasi	2,37	3,34	+0,97	+40,9%	Sangat Baik
2	Kata Sandi (*Password*)	2,39	2,95	+0,56	+23,4%	Baik
3	Internet dan Wifi	2,52	2,82	+0,30	+11,9%	Baik
4	Keamanan Perangkat	2,26	3,20	+0,94	+41,6%	Baik
5	Aduan Insiden Siber Teknis	1,75	1,93	+0,18	+10,3%	Kurang Baik
6	Hukum dan Regulasi Keamanan Siber Teknis	2,69	3,10	+0,41	+15,2%	Baik
Nilai Kesadaran Keamanan Siber Sosial		**2,65**	**3,02**	**+0,37**	**+14,0%**	**Baik**
1	Rekayasa Sosial (*Social Engineering*)	2,72	3,27	+0,55	+20,2%	Sangat Baik
2	Konten Negatif	3,36	3,21	-0,15	-4,5%	Baik
3	Aktivitas Media Sosial	2,86	3,28	+0,42	+14,7%	Sangat Baik
4	Aduan Insiden Siber Sosial	1,58	2,19	+0,61	+38,6%	Kurang Baik
5	Hukum dan Regulasi Keamanan Siber Sosial	2,48	1,38	-1,10	-44,4%	Sangat Kurang Baik
Nilai Kesadaran Keamanan Siber Keseluruhan		**2,48**	**2,97**	**+0,49**	**+19,8%**	**Baik**

Interpretasi hasil perbandingan antara *baseline* dan hasil pasca-implementasi harus dilakukan secara hati-hati dengan mempertimbangkan perbedaan karakteristik dan komposisi sampel. Skor *baseline* digunakan sebagai gambaran konteks awal, sedangkan hasil survei pasca-implementasi memberikan perspektif populasi yang lebih luas setelah program berlangsung. Dengan demikian, temuan ini tidak mewakili perubahan langsung pada responden yang sama, melainkan merefleksikan perubahan kondisi organisasi dan persepsi umum terhadap kesadaran keamanan siber.

Inferensi kausal secara langsung antara intervensi dashboard dengan seluruh perubahan perilaku individu pegawai tidak dapat diambil karena terdapat perbedaan populasi antara sampel *baseline* dan pasca-program. Penelitian lanjutan dengan desain eksperimen kuasi atau longitudinal sangat dianjurkan untuk menguji pengaruh kausal secara lebih presisi

Peningkatan kesadaran keamanan siber yang signifikan ini menunjukkan bahwa program pelatihan dan edukasi berkelanjutan terbukti efektif dalam meningkatkan kepatuhan keamanan informasi (Puhakainen & Siponen, 2010), khususnya melalui pendekatan yang mengintegrasikan *self-assessment*, media edukasi interaktif, dan rekomendasi personal.

Temuan ini juga sejalan dengan penelitian Amin (2014) yang menunjukkan

bahwa gap K-S-P lazim terjadi pada dimensi keamanan informasi, di mana peningkatan pengetahuan tidak otomatis diikuti perubahan sikap dan perilaku. Pada indikator password misalnya, tantangan sering bukan pengetahuan tentang password yang kuat, melainkan sikap dan perilaku konsisten dalam mengimplementasikannya. Literatur menyarankan kombinasi edukasi, pelatihan, insentif, dan kontrol administratif untuk menutup gap K-S-P ini (Amin, 2014).

Sebagai penguatan terhadap pelaksanaan dan keberlanjutan implementasi inovasi, pada tahapan pelaksanaan aksi perubahan dilakukan penyusunan dan penerbitan SE Walikota Jakarta Barat tentang Penyelenggaraan Keamanan SPBE. SE Walikota ini menginstruksikan seluruh UKPD agar secara aktif melaksanakan langkah-langkah keamanan SPBE, termasuk peningkatan literasi dan kesadaran siber, serta melaksanakan langkah-langkah preventif seperti menggunakan antivirus pada perangkat kerja.

Penerbitan SE Walikota menetapkan *Dashboard* Sec-Aw sebagai instrumen utama pembinaan, *self-assessment*, dan rujukan rekomendasi, sekaligus menyediakan mandat formal penggunaan *platform* di semua UKPD sebagai wujud komitmen pimpinan pada penguatan tata kelola SPBE. SE Walikota ini juga menjadi dasar perluasan pelaksanaan *assessment* yang rencananya hanya di Kantor Walikota menjadi seluruh pegawai UKPD Jakarta Barat, menjadi bukti komitmen pimpinan dalam memperkuat pengelolaan keamanan SPBE secara menyeluruh dan terukur. SE Walikota berfungsi sebagai instrumen tata kelola untuk menaikkan kepatuhan dan perluasan cakupan, sekaligus akselerator adopsi *dashboard* yang memperluas populasi *assessment* dari 77 menjadi 419 responden (peningkatan 444%). Kepatuhan ASN terhadap kebijakan keamanan informasi memerlukan pendekatan komprehensif yang tidak hanya mengandalkan edukasi, tetapi juga dukungan kebijakan dan sistem monitoring (Siponen et al., 2014), sebagaimana diimplementasikan melalui penerbitan SE Walikota dalam penelitian ini.

Dashboard Sec-Aw memberikan kontribusi strategis dalam mendukung penguatan sistem pertahanan dan keamanan nasional serta pembangunan sumber daya manusia yang adaptif (Subianto & Raka, 2024). Konsep Bela Negara digital yang terintegrasi menegaskan peran aktif setiap warga negara dalam menjaga keamanan siber, melindungi data, dan melawan ancaman digital seperti hoaks dan disinformasi (Hartono, 2022; Fitri, 2025). Implementasi *platform* ini juga memperkuat kompetensi aparatur melalui materi edukasi dan evaluasi yang berkelanjutan, sekaligus mencerminkan komitmen ASN menjalankan tugas dengan integritas, profesionalisme, dan orientasi pelayanan publik yang aman dan terpercaya.

Aspek keberlanjutan *Dashboard* Sec-Aw dirancang melalui tiga strategi utama. Pertama, pengembangan berkelanjutan melalui evaluasi dan penyempurnaan sistem secara periodik, penambahan fitur responsif sesuai kebutuhan pengguna, peningkatan integrasi dengan sistem keamanan siber lainnya seperti *Computer Security Incident Response Team* (CSIRT) untuk pelaporan, serta kemitraan dengan multi sektor untuk memperkaya konten dan *tools* keamanan.

Kedua, pemanfaatan hasil *pilot project* Jakarta Barat sebagai model nasional (*best practice*) yang dapat direplikasi oleh instansi pemerintah daerah dan pusat di seluruh Indonesia. Dokumentasi proses implementasi, *lesson learned* termasuk SE Walikota sebagai lampiran kebijakan menjadi panduan replikasi yang komprehensif bagi instansi lain.

Ketiga, dukungan kebijakan dan alokasi sumber daya yang memadai untuk menjamin operasional dan pengembangan *platform* jangka panjang. Rencana ekspansi meliputi perluasan cakupan pengguna dari pegawai ASN ke masyarakat umum di Jakarta Barat, kemudian ke wilayah DKI Jakarta, dan selanjutnya replikasi nasional. Target jangka panjang adalah menjadikan *Dashboard* Sec-Aw sebagai *platform* nasional kesadaran keamanan siber yang terintegrasi dengan ekosistem keamanan siber Indonesia, mendukung pencapaian visi Indonesia Emas 2045 dengan masyarakat dan aparatur yang memiliki literasi dan kesadaran keamanan digital yang tinggi. Strategi keberlanjutan ini mengadopsi prinsip evaluasi product dalam model CIPP yang menekankan pada dampak jangka panjang dan keberlanjutan program (Sukoco & Kurniadewi, 2023).

Penelitian ini memiliki beberapa limitasi yang perlu dipertimbangkan. Pertama, perbedaan komposisi sampel antara *baseline* (pengelola TIK) dan pasca-implementasi (seluruh pegawai) membuat estimasi delta perubahan bersifat konservatif dan tidak sepenuhnya menggambarkan hubungan kausal secara langsung. Penelitian lanjutan yang

menggunakan desain dengan kelompok kontrol (pembanding) atau pengukuran ulang pada responden yang sama secara longitudinal sangat dianjurkan untuk memperkuat kesimpulan tentang hubungan sebab-akibat. Kedua, durasi implementasi 3 bulan relatif pendek untuk mengukur perubahan perilaku jangka panjang dan dampak terhadap penurunan insiden keamanan siber aktual. Ketiga, pengukuran melalui kuesioner mandiri dapat mengandung bias karena responden cenderung memberikan jawaban yang terlihat positif secara sosial (*social desirability*). Penelitian lanjutan sebaiknya mengintegrasikan pengamatan perilaku aktual dan data log sistem untuk validasi silang (triangulasi).

Artikel ini menempatkan *awareness* sebagai *leading indicator* yang umum digunakan dalam evaluasi manajemen risiko keamanan siber. Walaupun data insiden nyata di lingkungan Pemda belum dapat diukur langsung sebagai *lagging indicator*, intervensi awareness dinilai dapat memperkuat postur keamanan sebagai bagian strategi defensif. Penelitian lanjutan diharapkan dapat menyambungkan data insiden siber yang terekam oleh CSIRT dengan hasil evaluasi awareness untuk membuktikan korelasi penurunan insiden nyata.

KESIMPULAN DAN SARAN

Dashboard Security Awareness (Sec-Aw) terbukti efektif meningkatkan kesadaran keamanan siber ASN Jakarta Barat. Implementasi *pilot project* menunjukkan peningkatan skor dari 2,48 (Kurang Baik) menjadi 2,97 (Baik), atau naik 0,49 poin. Namun, tiga area masih memerlukan intervensi prioritas: Aduan Insiden Siber Teknis (1,93), Hukum dan Regulasi Keamanan Siber Sosial (1,38), dan Internet dan WiFi (2,82).

Platform ini menjawab empat akar masalah keamanan siber melalui fitur *self-assessment* terstandar (SKKS BSSN), media edukasi interaktif, tools keamanan, dan rekomendasi personal. Penerbitan SE Walikota memperkuat tata kelola SPBE dan memperluas adopsi dari 77 menjadi 419 pengguna (peningkatan 444%).

Keberhasilan *pilot project* Jakarta Barat dapat menjadi model replikasi nasional untuk memperkuat ketahanan digital Indonesia. Penelitian lanjutan dengan desain longitudinal dan integrasi data insiden aktual diperlukan untuk memperkuat validitas kausal dan mengukur dampak jangka panjang program.

Berdasarkan hasil penelitian, terdapat beberapa rekomendasi untuk pengembangan lebih lanjut: Pertama, pengembangan fitur gamifikasi dan microlearning untuk meningkatkan *engagement* dan efektivitas pembelajaran berkelanjutan. Pendekatan ini terbukti meningkatkan motivasi pengguna hingga 83% dan memperbaiki retensi pengetahuan sebesar 30-40% dalam program kesadaran keamanan siber (Le et al., 2023; Onduto, 2021). Kedua, integrasi *platform* dengan sistem manajemen keamanan informasi (ISMS) instansi dan data log insiden CSIRT untuk memperkuat *governance* keamanan siber secara holistik serta mengukur dampak terhadap penurunan insiden aktual. Ketiga, ekspansi bertahap dari *pilot project* Jakarta Barat ke instansi pemerintah daerah dan pusat lainnya sebagai model replikasi nasional. Penelitian lanjutan diperlukan untuk mengidentifikasi faktor-faktor kunci keberhasilan implementasi di berbagai konteks organisasi dan daerah. Keempat, pelaksanaan studi longitudinal dengan desain eksperimen kuasi atau kelompok kontrol untuk mengukur dampak jangka panjang terhadap perubahan perilaku keamanan digital dan memvalidasi hubungan kausal antara intervensi *platform* dengan penurunan insiden keamanan siber secara lebih presisi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Suku Dinas Komunikasi, Informatika dan Statistik Kota Administrasi Jakarta Barat yang telah mendukung penelitian dan implementasi *Dashboard* Sec-Aw. Terima kasih juga disampaikan kepada seluruh pegawai Pemerintah Kota Administrasi Jakarta Barat yang telah berpartisipasi dalam *pilot project* dan memberikan *feedback* berharga untuk penyempurnaan *platform*, serta kepada Pemerintah Kota Administrasi Jakarta Barat atas dukungan kebijakan melalui penerbitan Surat Edaran Walikota tentang Penyelenggaraan Keamanan SPBE.

DAFTAR PUSTAKA

Amin, M. (2014). Pengukuran tingkat kesadaran keamanan informasi menggunakan Multiple Criteria Decision Analysis (MCDA). Jurnal Penelitian dan Pengembangan Komunikasi dan

Informatika, 5(1), 61-80. https://jurnal.kominfo.go.id/index.php/iptekkom/article/view/306

Badan Siber dan Sandi Negara. (2024). Survei Kesadaran Keamanan Siber (SKKS): Panduan dan Hasil Nasional. https://bssn.go.id/panduan-keamanan/

Badan Siber dan Sandi Negara. (2025). Lanskap Keamanan Siber Indonesia 2024. BSSN. https://bssn.go.id/monitoring-keamanan-siber/

Brunelli, M. (2015). Introduction to the Analytic Hierarchy Process. Springer Briefs in Operations Research. Springer. https://core.ac.uk/download/pdf/80714029.pdf

Firmansyah, M., & Yuswanto, A. (2022). Manajemen pengetahuan penanganan insiden keamanan informasi pada SOC Pemprov DKI Jakarta. Monas: Jurnal Inovasi Aparatur, 4(2), 441-452. https://journal.bpsdm.jakarta.go.id/index.php/monas/article/view/321

Fitri, N. (2025). Bela negara digital: Strategi ketahanan siber nasional. Jurnal Pertahanan Nasional, 11(1), 45-62. https://jurnal.idu.ac.id/index.php/DefenseJournal

Hartono, D. (2022). Fenomena kesadaran bela negara di era digital dalam menghadapi tantangan nasional. Jurnal Lemhannas RI, 8(1), 14-33. https://doi.org/10.55960/jlri.v8i1.301

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289-296. https://doi.org/10.1016/j.cose.2006.04.002

Le, D., Matsuda, C., Pena, S., Platou, I., & Olsen, T. (2023). Effective cybersecurity training using microlearning and the drip concept: A case study of a large regional hospital. Drake Management Review, 13(2), 21-35. https://escholarshare.drake.edu/bitstreams/9c18f82a-91e3-45f4-9625-45d84a307fc4/download

National Cyber Security Index. (2023). National Cyber Security Index (NCSI). https://ncsi.ega.ee

Onduto, B. (2021). Gamification of cyber security awareness: A systematic review [Master's thesis, University of Turku]. UTUPub. https://www.utupub.fi/bitstream/handle/10024/152929/Onduto_Barack_Thesis_Final.pdf

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40-51. https://doi.org/10.1016/j.cose.2017.01.004

Peraturan Badan, Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik.

Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. (2018). Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. MIS Quarterly, 34(4), 757-778. https://doi.org/10.2307/25750704

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217-224. https://doi.org/10.1016/j.im.2013.08.006

Subianto, P., & Raka, G. R. (2024). Asta Cita 2024-2029: Visi dan Misi Presiden dan Wakil Presiden. Indonesia Baik. https://indonesiabaik.id

Sukoco, S. H., & Kurniadewi, Y. I. (2023). Pengukuran keberlanjutan pelatihan daring dengan pendekatan evaluasi model CIPP. Monas: Jurnal Inovasi Aparatur, 5(2), 122-138. https://journal.bpsdm.jakarta.go.id/index.php/monas/article/view/653

Suku Dinas Komunikasi, Informatika dan Statistik Jakarta Barat. (2025). Dashboard Security Awareness (Sec-Aw). https://barat.jakarta.go.id/security-awareness

Surat Edaran Walikota Kota Administrasi Jakarta Barat Nomor e-0009/SE/2025 tentang Penyelenggaraan Keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE). https://barat.jakarta.go.id/storage/docs/materi-security-awareness/SE%20Walikota%20Penyelenggaraan%20Keamanan%20SPBE.pdf

Vaidya, O. S., & Kumar, S. (2006). Analytic Hierarchy Process: An overview of applications. European Journal of Operational Research, 169(1), 1-29. https://doi.org/10.1016/j.ejor.2004.04.028

Verizon. (2025). Data Breach Investigations Report 2025. https://www.verizon.com/business/resources/T822/reports/2025-dbir-data-breach-investigations-report.pdf