Pembangunan Pusat Pengendalian Operasional Keamanan Informasi (Pusdalops Kami) guna Meningkatkan Pelayanan E-Gov dari Ancaman Kejahatan Siber

Andrie Yuswanto[1], Budi Wibowo[2]
Jurusan Teknik Informatika, Fakultas Teknologi Industri, Institut Teknologi Budi Utomo[,12]
Jl. Raya Mawar Merah No., Pondok Kopi, Jakarta. [12]
E-mail : aandoct@gmail.com[,1], budiwibowo1993@gmail.com[2]

Abstract -- **The strategic issue of information security management in e-Government services at the DKI Jakarta Provincial Government is currently the most important thing in line with the increasing cyber crime, therefore a Network Information and Information Security System (SIJAKI) is needed. The purpose of this INOVASI is to build an information service web through SIJAKI, the IT Security Operation Center (SOC) or the Information Security Operations Control Center (KAMI PUSDALOPS) and Live Chat / open tickets for consultation media related to information security. To realize the goals of inovation, several short-term stages were carried out, including: forming an effective team, collecting data, creating a system, testing the system, implementing, training and monitoring the evaluation of the change project that has been carried out. SIJAKI, which has been implemented and implemented, has succeeded in reducing the number of e-Government website hacks belonging to the DKI Jakarta Provincial Government and other cyber crimes so that the e-Government services provided are safe, smooth and confidential.**

Keywords: SIJAKI, IT-SOC, cyber crime, cyber crime, information security

Abstrak -- **Isu strategis pengelolaan keamanan informasi pada layanan e-Government di Pemprov DKI Jakarta saat ini merupakan hal terpenting seiring dengan kejahatan siber/*cyber crime* yang semakin meningkat, oleh karena itu diperlukan Sistem Informasi Jaringan dan Keamanan Informasi (SIJAKI). Tujuan dari inovasi ini adalah membangun web layanan informasi melalui SIJAKI, IT Security Operation Centre (SOC) atau Pusat Pengendalian Operasi Keamanan Informasi (PUSDALOPS KAMI) dan *Live Chat/open ticket* untuk media konsultasi terkait keamanan informasi. Untuk mewujudkan tujuan inovasi dilakukan beberapa tahapan jangka pendek antara lain: pembentukan tim efektif, pengumpulan data, pembuatan sistem, uji coba sistem, implementasi, pelatihan dan monitoring evaluasi pada proyek perubahan yang sudah di lakukan. SIJAKI yang telah dilaksanakan dan diimplemetasikan berhasil menekan jumlah peretasan website layanan e-Government milik Pemprov DKI Jakarta dan kejahatan siber lainnya sehingga layanan e-Government yang diberikan menjadi aman, lancar dan terjaga kerahasiannya.**

Kata Kunci : SIJAKI, IT-SOC, *cyber crime*, kejahatan siber, keamanan informasi

I. PENDAHULUAN

Teknologi tumbuh dan berkembang sangat cepat dalam sisi keamanan menjadi topik hangat di dunia oleh karena itu Pemerintah Provinsi DKI Jakarta dalam memberikan pelayanan kepada masyarakat sangat membutuhkan sarana dan prasarana berbasis IT yang aman sehingga layanan *e-Goverment* yang diberikan menjadi lancar dan terjaga kerahasiannya.[1] *Cyber crime* atau kejahatan siber marak terjadi terutama pada website yang di kelola oleh Pemerintah[2] (kementrian, lembaga maupun pemerintah daerah/kota) termasuk website milik Pemerintah DKI Jakarta, adapun aksi pegerusakan ataupun *Hacking* biasanya dikarenakan ketidak puasan sekelompok golongan, uji coba kerentanan sistem keamanan atau bisa juga dikarenakan isu politik yang menimbulkan marak terjadi kejahatan siber (*Cyber Crime*) dan web tidak aman.[3] Dengan belum adanya pengelolaan pusat layanan keamanan informasi (PUSDALOPS KAMI) seperti Security Awareness, pencegahan, konsultasi, mitigasi dan layanan kemanan informasi lainnya.Serangan dunia maya terus meningkat komplektifitas dan frekuensi berbanding lurus dengan jumlah pertumbuhan perangkat teknologi informasi dan komunikasi yang terhubung ke internet berdampak negatif [4] pada masyarakat, pemerintah dan bisnis sangat merugikan terkait keamanan dan pertahanan nasional khususnya roda pemerintahan daerah provinsi DKI Jakarta. Badan Standarisasi Nasional menetapkan SNI ISO/IEC 71: sebagai standar nasional dalam teknologi dan keamanan informasi serta

manajemen keamanan informasi Badan Siber dan Sandi Negara (BSSN) mengeluarkan aplikasi yang digunakan sebagai alat bantu untuk menganalisa dan mengevaluasi tingkat kesiapan penerapan SNI ISO/IEC 27001:2013 yaitu indeks KAMI (Keamanan Informasi).[5]

Berdasarkan masalah kejahatan siber maka diperlukan pusat pengendalian operasional keamanan informasi (pusdalops kami) atau dalam bidang teknologi informasi biasa dikenal dengan istilah IT *Security Operation Centre (SOC)* yang merupakan tata kelola manajeman dan peralatan/perangkat pendukung keamanan informasi yang di sebut dengan Sistem Manajemen Pengamanan Informasi (SMPI), diharapkan dapat memberikan layanan dan informasi sehingga semua urusan terkait keamanan informasi dapat optimal melalui layanan *e-goverment*. tujuan inovasi ini dapat dibagi menjadi tiga tahap yaitu tujuan jangka pendek yaitu tersedianya pusdalops kami atau it-soc di pemprov dki jakarta melalui Sistem Informasi Jaringan Dan Keamanan Informasi (SIJAKI) melalui https://sijaki.jakarta.go.id tersedianya konsultasi online atau live chat terwujudnya layanan informasi keamanan informasi e-government adapun tujuan jangka menengah yaitu tersedianya "*Knowledge Management System*", sebagai percontohan dalam pembangunan it-soc dengan didukung oleh Badan Siber Dan Sandi Negara (BSSN) serta tujuan jangka panjang yaitu sebagai pendukung sertifikasi : ISO/SNI 27001 tentang "keamanan informasi", sebagai dasar kebijakan terkait peraturan gubernur tentang keamanan informasi

II. METODOLOGI PENELITIAN

Proses tinjauan pustaka pada penelitian sebelumnya tentang keamanan informasi dari ancaman siber telah dilakukan peneliti lain seperti ditunjukkan pada tabel.1 .

Tabel 1. jurnal penelitian terkait

No	Judul	Metode	Tujuan
1	A User Centric Machine Learning Framework for Cyber Security Operation Center[3]	User centric machine learning system	Detects threats and analyzes user risk identification
2	Cyber Security in the Age of covid-19: A Timeline and Analysis of Cyber-Crime and Cyber attacks during the pandemic[2]	Predictive model	Recommended that the government, media and other institutions be aware of cyber crime information
3	Challenges and Solutions of Information Security Issues in the Age of Big Data[6]	Analytic Methods	Information security is very important in the era of big data and information security protection
4	Cyber Security Operations Center characterization model and analysis[7]	Explore process methods	adopts a collaborative and coordinated operations approach To build a strong analytical foundation

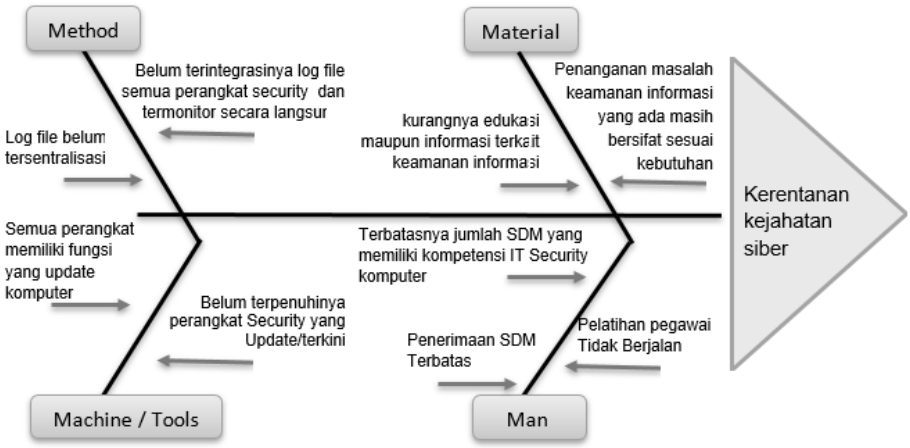
Tata kelola Teknologi informasi merupakan struktur kebijakan atau prosedur dan kumpulan proses yang memiliki tujuan untuk memastikan kesesuaian penerapan secara optimal teknologi informasi dalam hal ini mengendalikan penggunaan terhadap sumber daya teknologi informasi dan mengelola resiko yang terkait.

Penilaian dalam Indeks KAMI dilakukan dengan cakupan keseluruhan persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001:2009[8], yang disusun kembali menjadi 5 (lima) area di bawah ini:

1) Tata Kelola Keamanan Informasi
   Mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.
2) Pengelolaan Risiko Keamanan Informasi
   Mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
3) Kerangka Kerja Keamanan Informasi
   Mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
4) Pengelolaan Aset Informasi
   Mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut; dan
5) Teknologi dan Keamanan Informasi
   Mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

Alam setiap area, proses evaluasi akan membahas sejumlah aspek yang dibutuhkan untuk mencapai tujuan utama dari pengamanan di area tersebut. Setiap aspek tersebut memiliki karakteristik tersendiri terkait dengan pentahapan penerapan pengamanan sesuai dengan standar SNI ISO/IEC 27001:2009. Aspek yang dibahas (disampaikan dalam konteks pertanyaan) terdiri dari bentuk kerangka kerja dasar keamanan informasi, efektivitas dan konsistensi penerapannya, sampai dengan kemampuan untuk selalu meningkatkan kinerja keamanan

informasi.Bentuk pengamanan terakhir ini sesuai dengan kesiapan minimum yang diprasyaratkan oleh proses sertifikasi standar SNI ISO/IEC 27001:2009.



Gambar 1. *Fishbone Diagram* identifikasi permasalahan kerentanan terhadap kejahatan siber

a) Standar Internasional mengenai Keamanan Nasional

The Committee on the Administration of Justice (CAJ) mengeluarkan sebuah laporan di akhir 2012 yang berjudul "The Policing You Don't See". Laporan ini mengaris bawahi 'paralel justice system' yang saat ini beroperasi di Iralndia Utara. Ini terdiri dari kekuatan polisi yang akuntable kepada mekanisme lokal dan hal lainnya dari 'kekuatan diluar kekuatan' yang bertangung jawab kepada isu keamanan nasional yang beroprasi didalam Security Service (Mi5) London.[9]

Kepentingan nasional merupakan tujuan jangka panjang dari suatu negara yang mengikat semua elemen pemerintah dan bangsa untuk mencapainya. Oleh karena itu , sektor keamanan nasional juga diperluas dari dunia nyata ke dunia maya sehingga hasil dari analisis kebijakan standarisasi keamanan perangkat telekomunikasi untuk menunjang kebijakan pertahanan. Kekuatan untuk menghancurkan ancaman *Cyber War* saat ini hampir mencapai tahap langsung dan serius pada sistem keamanan nasional. Dalam tatanan globalisasi semua perangkat dapat mengakses informasi dimanapun sekaligus juga dapat diakses dari manapun. Kondisi ini memungkinkan penyalahgunaan informasi yang dilewatkan melalui perangkat tersebut dengan menanamkan alat untuk mengambil maupun memodifikasi informasi untuk kepentingan tertentu.[10]

b) Konsep Keamanan Teknologi Informasi dan Komunikasi Nasional

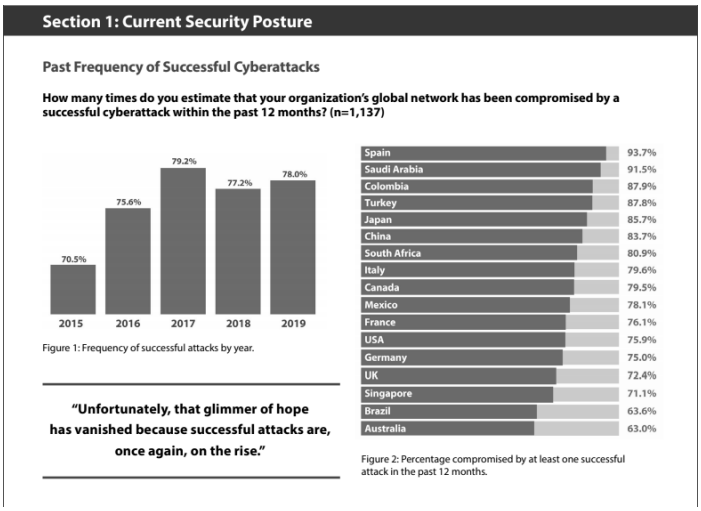
Konsep keamanan yang ada dalam ranah TIK memiliki cakupan yang sangat luas. Keamanan melingkupi empat aspek, yaitu privacy / confidentiality, integrity, authentication, dan availability. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas, terutama dalam kaitannyadengan transasksi elektronik, yaitu access control dan non-repudiation. Privacy / Confidentiality: Aspek terkait jaminan kerahasiaan isi dari informasi.

1) Authentication: Aspek yang menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses/memberikan informasi adalah betul-betul orang yang dimaksud
2) Integrity: Aspek ini menegaskan bahwa data dan informasi hanya boleh diubah seijin pemilik informasi
3) Accesibility: Aspek iniberhubungan dengan ketersediaan informasi ketika dibutuhkan
4) Access control\: Aspek ini berhubungan dengan cara pengaturan akses kepada informasi
5) Non repudiation: Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.

Masalah keamanan seringkali kurang diperhatikan terutama keamanan mengganggu performansi sistem tidak jarang tindakkan keamanan seringkali dilupakan.

c) Tantangan Keamanan Informasi di Jajaran Pemerintahan.

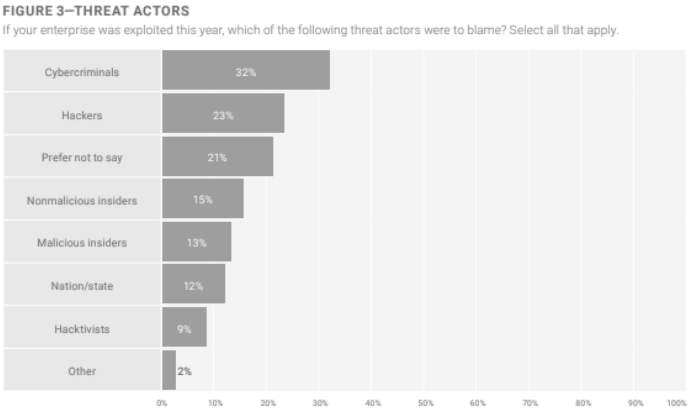
Perkembangan lingkungan strategis , Global, Regional dan Nasional era pemerintahan berbasis elektronika dimana klasifikasi informasi keseragaman tata kelola dalam aspek kerahasiaan, keaslian, keutuhan dan ketersediaan yang melibatkan semua jajaran lembaga pemerintahan.



Gambar 2. Laporan frekuensi serangan yang berhasil setiap tahun

(https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf)

Berdasarkan data dari state of cybersecurity 2019 [11] Pelaku ancaman siber tertinggi dilakukan kejahatan siber Namun, tahun ini banyak responden yang memilih tetap identitas penyerang anonim, dengan 21 persen menunjukkan bahwa mereka memilih untuk tidak mengungkapkan identitasnya dari para penyerang.



Gambar 3. Threat Actor

Dalam hal ini serangan siber di Indonesia pada Januari-Mei 2020 terus meningkat tajam jika dibandingkan periode yang sama tahun sebelumnya. Ancaman terhadap hilangnya potensi ekonomi hingga kedaulatan negara cenderung meningkat jika tren peningkatan tersebut terus berlanjut. Berdasarkan data Pusat Operasi Keamanan Siber Nasional menunjukkan pemerintah merupakan sektor yang paling banyak terkena serangan data breach yang merupakan serangan dilakukan dalam mengakses atau pengungkapan tanpa izin yang dilakukan terhadap data atau informasi rahasia dan sensitif.[12]

III. PEMBAHASAN

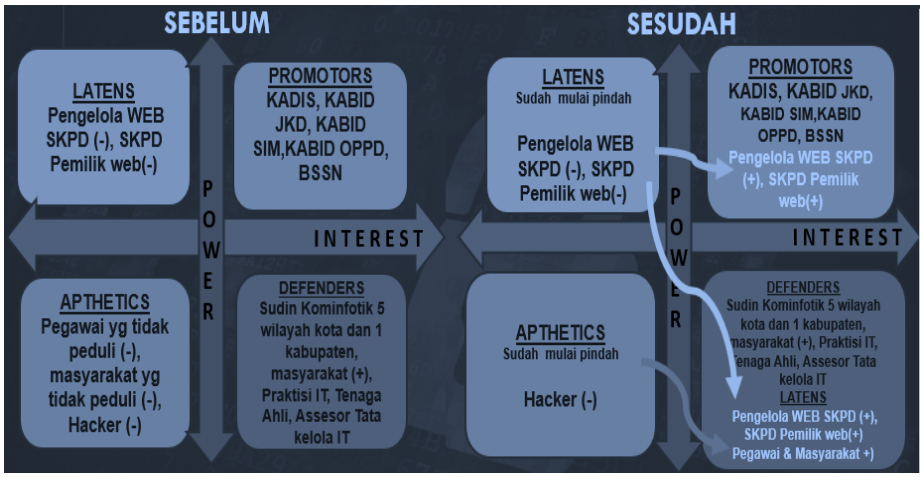
Standar Internasional Keamanan Informasi ISO 27001 dapat diterapkan pada semua jenis organisasi (perusahaan komersial, instansi pemerintah, organisasi non-profit, dsb). Standar ini menetapkan persyaratan untuk penetapan, penerapan, operasi, pemantauan, peninjauan, pemeliharaan dan peningkatan suatu ISMS terdokumentasi dalam konteks risiko organisasi bisnis secara keseluruhan. bertujuan untuk memberikan gambaran implementasi sistem manajemen keamanan informasi berstandar internasional kepada perusahaan, organisasi nirlaba, instansi atau publik agar dapat mempelajari dan mencoba mengimplementasikannya di lingkungan sendiri. Implementasi ISO 27001 pada kegiatannya juga mencoba melakukan kegiatan audit terhadap semua aspek terkait, seperti: kondisi jaringan komputer lokal, policy, manajemen SDM,organisasi keamanan informasi, dan lain-lain.

a) Rancang bangun inovasi

Rancang bangun inovasi dibagi menjadi beberapa tahap yaitu tahap jangka pendek, jangka menengah, dan jangka panjang. Tahapan tersebut ditunjukkan dalam Gambar 2. berikut ini.

Gambar 4. Tahapan Inovasi (saat ini sudah di tujuan jangka panjang)

Untuk mendukung tercapainya tujuan peta seluruh pemangku kepentingan atau *Stakeholder*, sebagai berikut :



Gambar 5. Peta Stakeholder

Strategi untuk mengatasi masalah koordinasi dengan Stakeholder yang kurang peduli/kurang mendukung terkait keamanan infromasi adalah :

1) Diadakan acara “Security Awareness” dna pendekatan personil
2) Memberikan layanan Edukasi keamanan informasi
3) Sosialisasi melalui media luar ruang/pop up website

b) Kebermanfaatan dan berkelanjutan

Manfaat yang dirasakan dari inovasi ini terbagi menjadi 3 yaitu (Internal OPD , Organisasi Pemprov DKI Jakarta dan External/masyarakat) adalah sebagai berikut :

1) Manfaat untuk Internal OPD/Diskominfotik, PUSDALOPS KAMI atau IT SOC merupakan penunjang *Keberlangsungan organisasi* terkait layanan *e-Goverment dari ancaman Cyber Crime*
2) Manfaat untuk Organisasi Pemprov DKI, tersedianya Satu Portal Layanan keamanan informasi
3) Manfaat untuk External dan masyarakat, sebagai sumber edukasi

c) Orisinaslitas ide

Ide/Inovasi ini bermula ketika belum adanya pengendalian dan monitoring terkait keamanan informasi di Pemprov DKI Jakarta seiring banyaknya kejahatan siber yang marak terjadi, kemudian mencari solusi dengan cara berkonsultasi dan berkoordinasi dengan pakar *IT Security* dan instansi terkait Berdasarkan info dari Badan Siber dan Sandi Negara (BSSN), Pemprov DKI dijadikan tempat studi banding dalam pengelolaan PUSDALOPS KAMI atau IT SOC.[13]

d) Efektivitas Pelaksanaan Inovasi

PUSDALOPS KAMI melalui SIJAKI sangat efektif untuk menekan kejahatan siber/perusakan/Hacking pada layanan web E Government Pemprov DKI Jakarta dari >10 kali kejadian menjadi 0 kejadian dan kesadaran terkait keamanan informasi website meningkat dari 322 website yang suah diamani menjadi 356 website, terdapat peningkatan sebanyak 44. (data 2018)

IV. KESIMPULAN & SARAN

Penerapan standar keamanan perangkat telekomunikasi yang ada saat ini hanya mencakup perangkat untuk kebutuhan umum sementara perangkat untuk kebutuhan khusus belum memiliki standar keamanan tersendiri. Saat ini regulasi bidang standardisasi keamanan perangkat telekomunikasi masih belum memadai terutama yang ditujukan bagi perangkat telekomunikasi untuk kebutuhan khusus. Tidak ada yang aman sepenuhnya salah satunya pertahanan Sederhana lebih mudah untuk mengamankan eamanan sebuah sistem informasi harus dinomor satukan karena keamanan sebuah sistem yang menjaga informasi akan memberi rasa aman terhadap informasi yang dimiliki. Ancaman terhadap keamanan sistem dapat diatasi apabila dalam pengoperasian keamanan sistem selalu dipantau.

Keamanan adalah sutu proses bukan produk kekuatan keamanan informasi berada pada rantai terlemah jadi Dalam mencapai goal standarisasi keamanan perangkat telekomunikasi khususnya untuk menunjang kebijakan hankamnas masih banyak diperlukan upaya lebih lanjut untuk mewujudkannya.

V. DAFTAR PUSTAKA

[1] S. Methmali, “Perception of internet usage and its impact on cyber-crime in Sri Lanka internet usage and relationship with cyber-crime,” *Int. Conf. Signal Process. Commun. Power Embed. Syst. SCOPES 2016 - Proc.*, pp. 674–690, 2017.

[2] H. S. Lallie *et al.*, “Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the paandemic,” *arXiv*, pp. 1–20, 2020.

[3] X. Zheng, IEEE ITSS, and Institute of Electrical and Electronics Engineers, “IEEE ISI 2017 : IEEE International Conference on Intelligence and Security Informatics: Security and Big Data : July 22-24, 2017 - Beijing, China,” pp. 173–175, 2017.

[4] M. Mutemwa, J. Mtsweni, and N. Mkhonto, “Developing a cyber threat intelligence sharing platform for South African organisations,” *2017 Conf. Inf. Commun. Technol. Soc. ICTAS 2017 - Proc.*, 2017.

[5] A. R. Riswaya, A. Sasongko, and A. Maulana, “Menggunakan Indeks Kami Untuk Persiapan Standar Sni Iso / Iec 27001 (Studi Kasus : Stmik Mardira Indonesia),” vol. 14, no. 1, pp. 10–18, 2020.

[6] M. Yang, X. Zhou, J. Zeng, and J. Xu, “Challenges and solutions of information security issues in the age of big data,” *China Commun.*, vol. 13, no. 3, pp. 193–202, 2016.

[7] S. Kowtha, L. A. Nolan, and R. A. Daley, “Cyber security operations center characterization model and analysis,” *2012 IEEE Int. Conf. Technol. Homel. Secur. HST 2012*, pp. 470–475, 2012.

[8] N. Hidayati, “Kajian Tata Kelola It Berdasarkan Indeks Kami Pada Universitas Pakuan Bogor,” *J. Paradig.*, vol. XVI, no. 2, 2014.

[9] I. Amaritasari, “Keamanan Nasional dalam Konsep dan Standar Internasional,” *J. Keamanan Nas.*, vol. I, p. 173, 2015.

[10] W. Pradono and Y. Yourdan, “Analisis kebijakan standardisasi keamanan perangkat telekomunikasi untuk menunjang kebijakan pertahanan dan keamanan nasional (Policy analysis on telecommunication devices security standardization to support national security and defence policy),” *Bul. Pos dan Telekomun.*, vol. 13, no. 2, p. 151, 2015.

[11] WIPRO, “State of Cybersecurity 2019,” no. November 2018, pp. 1–21, 2019.

[12] BSSN, “Laporan Tahunan Honeynet Project BSSN IHP 2018.” p. 40, 2018.

[13] P. Gubernur *et al.*, “Gubernur Provinsi Daerah Khusus Ibukota Jakarta,” vol. 7, pp. 583–606, 2005.

[14] Peraturan Daerah Provinsi DKI Jakarta Nomor 5 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Daerah Khusus Ibu Kota Jakarta.

[15] Peraturan Gubernur Provinsi DKI Jakarta Nomor 265 Tahun 2016 tentang Organisasi dan Tata Kerja Dinas

Komunikasi Informatika dan Statistik.
[16] Peraturan Gubernur Provinsi DKI Jakarta Nomor 39 Tahun 2012 tentang Sistem Informasi Manajemen Daerah.
[17] Peraturan Gubernur Pemprov DKI Jakarta No 69 Tahun 2018 Penggunaan Sertifikat Elektronik
[18] Website resmi Badan Siber dan Sandi Negara *https://bssn.go.id/*
[19] *Website resmi Kemenkominfo RI https://www.kominfo.go.id/*