Volume 8 Issue 3 (2023) Pages 336 - 343
Jurnal Mirai Management
ISSN : 2598-8301 (Online)

Manajemen Penggunaan Sistem Informasi dalam Pertahanan dan Keamanan

St. Nurhayati Azis[1], Abdillah Ala Sabnur[2], Fitri Hasrianti[3], Satriani[4]
[1,2,3,4] *Pascasarjana Universitas Muslim Indonesia*

Abstrak

Artikel ini membahas tentang system informasi dalam pertahan dan keamanan, dimana Informasi merupakan aset yang strategis bagi setiap organisasi.Inilah yang menyebabkan mengapa banyak pemerintahan ataupun badan tertentu menghabiskan jutaan bahkan miliaran dollar untuk mendapatkan informasi mengenai segala sesuatu yang berkaitan dengan ancaman potensial bagi keamanan mereka.Tanpa informasi yang tepat dapat menyebabkan kegagalan khususnya dalam bidang pertahanan, sehingga kemampuan untuk menyediakan informasi potensial merupakan faktor yang sangat menentukan dari kekuatan pertahanan suatu negara. Sistem komunikasi beperan penting dalam menjaga keamanan dan kedaulatan negara.Terutama jika satelit digunakan untuk keperluan intelijen, pencitraan dan *reconnaissance*. Diperlukan adanya sistem komunikasi satelit yang selalu siap sedia, mumpuni tanpa bergantung pada satelit pihak ketiga. Berdasarkan teori informasi yang dikemukakan Sun Tzu, keamanan informasi sangat menentukan menang dan kalahnya sebuah pertempuran. Karena dengan informasi, strategi, taktik dan teknik operasional dibangun.

Kata Kunci: system Informasi, Pertahanan, Keamanan

Abstract

This article discusses information systems in defense and security, where information is a strategic asset for every organization. This is the reason why many governments or certain agencies spend millions or even billions of dollars to obtain information about everything related to potential threats to their security. Without proper information it can lead to failure, especially in the defense sector, so the ability to provide potential information is a very determining factor in a country's defense strength. Communication systems play an important role in maintaining the security and sovereignty of the country. Especially if satellites are used for intelligence, imaging and reconnaissance purposes. It is necessary to have a satellite communications system that is always ready, capable without relying on third party satellites. Based on the information theory put forward by Sun Tzu, information security determines the victory and defeat of a battle. Because with information, strategies, tactics and operational techniques are built.

Keywords: Information systems, Defense, Security,

Copyright (c) 2023 St. Nurhayati Azis

✉ Corresponding author :
Email Address : **stnurhayati.azis@umi.ac.id**

PENDAHULUAN

Masalah keamanan merupakan salah satu aspek penting bagi sebuah sistem informasi, sayang sekali masalah keamanan ini kurang mendapat perhatian dari pemilik dan pengelola sistem informasi.Seringkali masalah keamanan berada di urutan kedua, atau bahkan diurutkan terakhir dalam daftar ha-hal yang di anggap penting.Apabila mengganggu performasi dari sistem, seringkali keamanan di kurangi atau bahkan di tiadakan. Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting, kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahaan, maupun individual. Hal ini dimungkinkan dengan perkembangan pesat di bidang tekhnologi komputer dan telekomunikasi.Sangat pentingnya nilai sebuah informasi seringkali informasi diinginkan hanya boleh di akses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Sebagai contoh, banyak informasi dalam sebuah perusahaan yang hanya diperbolehkan diketahui oleh orang-orang tertentu di dalam perusahaan tersebut, seperti misalnya informasi tentang produk yang sedang dalam development, algoritma-algoritma dan teknik-teknik yang di lakukan untuk menghasilkan produk tersebut, untuk itu keamanan dari system informasi yang di gunakan harus terjamin dalam batas yang dapat diterima.

Perkembangan teknologi informasi pada abad ke-21 ini telah memberikan kepraktisan bagi masyarakat modern untuk melakukan berbagai kegiatan komunikasi secara elektronik, salah satunya dalam bidang bisnis seperti perdagangan dan perbankan. Kegiatan berbisnis secara elektronik ini dikenal dengan namae-commerce. Dengan teknologi informasi, khususnya dengan jaringan komputer yang luas seperti Internet, barang dan jasa dapat dipromosikan secara luas dalam skala global.Kepada calon konsumen pun diberikan pula kemudahan-kemudahan yang memungkinkan mereka mengakses dan membeli produk dan jasa yang dimaksud secara praktis, misalnya pelayanan kartu kredit.Perkembangan ini rupanya membawa serta dampak negatif dalam hal keamanan.Praktek-praktek kejahatan dalam jaringan komputer kerap terjadi dan meresahkan masyarakat, misalnya pencurian sandi lewat dan nomor rahasia kartu kredit. Akibat dari hal seperti ini, aspek keamanan dalam penggunaan jaringan komputer menjadi hal yang krusial.Terdapat teknik serangan yang mendasarkan pada bunyi yang dihasilkan dari peralatan seperti keyboard PC. Yaitu dengan membedakan bunyi yang dikeluarkan.Sehingga metode ini dapat mengetahui tombol-tombol yang ditekan.Dalam pengaplikasian lebih lanjut dapat diterapkan pada mesin komputer notebook, telepon, sampai mesin ATM.Serangan menggunakan metode ini murah dan tidak langsung.Murah karena selain tambahan komputer, yang dibutuhkan hanyalah sebuah microphone parabolic.Disebut tidak langsung karena tidak membutuhkan adanya serangan fisik langsung ke sistem, bunyi dapat direkam menggunakan peralatan tambahan.

MATERI DAN METODE

A. Manajemen keamanan informasi

Aktifitas untuk menjaga agar sumber daya informasi tetap aman disebut manajemen keamanan informasi. Pada bentuk paling dasar manajemen keamanan informasi terdiri atas empat tahap :

1. Mengidentifikasi ancaman yang dapat menyerang sumber daya informasi perusahaan
2. Mendefinisikan risiko yang dapat disebabkan oleh ancaman-ancaman tersebut, menentukan kebijakan keamanan informasi.
3. Menentukan kebijakan keamanan informasi**.**

B. keamanan sistem informasi

Jika kita berbicara tentang keamanan sistem informasi, selalu kata kunci yang dirujuk adalah pencegahan dari kemungkinan adanya virus, *hacker, cracker* dan lain-lain. Menurut G.J Simons, Kemanan sistem informasi adalah bagaimana usaha untuk dapat mencegah penipuan *(cheating)* atau bisa mendeteksi adanya penipuan pada system yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.

Padahal berbicara masalah keamanan sistem informasi maka kita akan berbicara kepada kemungkinan adanya resiko yang muncul atas sistem tersebut (lihat tulisan strategi pendekatan manajemen resiko dalam pengembangan sistem informasi). Sehingga pembicaraan tentang keamanan sistem tersebut maka kita akan berbicara 2 masalah utama yaitu *Threats* (Ancaman) atas sistem dan *Vulnerability* (Kelemahan) atas sistem

Masalah tersebut pada gilirannya berdampak kepada 6 hal yang utama dalam sistem informasi yaitu : Efektifitas & Efisiensi, Kerahaasiaan, Integritas, Keberadaan (*availability*), Kepatuhan (*compliance*), Keandalan (*reliability*).

Untuk menjamin hal tersebut maka keamanan sistem informasi baru dapat terkriteriakan dengan baik. Adapun kriteria yang perlu di perhatikan dalam masalah keamanan sistem informasi membutuhkan 10 domain keamanan yang perlu di perhatikan yaitu : Akses kontrol sistem yang digunakan, Telekomunikasi dan jaringan yang dipakai, Manajemen praktis yang di pakai, Pengembangan sistem aplikasi yang digunakan, Cryptographs yang diterapkan, Arsitektur dari sistem informasi yang diterapkan, Pengoperasian yang ada, *Busineess Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP), Kebutuhan Hukum, bentuk investigasi dan kode etik yang diterapkan dan Tata letak fisik dari sistem yang ada.

C. Ancaman keamanan sistem informasi

Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Ancaman yang mungkin timbul dari kegiatan pengolahan informasi berasal dari 3 hal utama, yaitu :

1. Ancaman Alam

   Yang termasuk dalam kategori ancaman alam terdiri atas :

   a. Ancaman air, seperti : banjir, tsunami, intrusi air laut, kelembaban tinggi, badai, pencairan salju.
   b. Ancaman Tanah, seperti : longsor, gempa bumi, gunung meletus
   c. Ancaman Alam lain, seperti : kebakaran hutan, petir, tornado, angin ribut

2. Ancaman Manusia

   Yang dapat dikategorikan sebagai ancaman manusia, diantaranya adalah :

   a. Malicious code
   b. Virus, Logic bombs, Trojan horse, Worm, active contents, Countermeasure
   c. Social engineering

d. *Hacking, cracking*, akses ke sistem oleh orang yang tidak berhak, DDOS, backdoor
e. Kriminal
f. Pencurian, penipuan, penyuapan, pengkopian tanpa ijin, perusakan
g. Teroris
h. Peledakan, Surat kaleng, perang informasi, perusakan

3. Ancaman Lingkungan
   Yang dapat dikategorikan sebagai ancaman lingkungan seperti :
   a. Penurunan tegangan listrik atau kenaikan tegangan listrik secara tiba-tiba dan dalam jangka waktu yang cukup lama
   b. Polusi
   c. Efek bahan kimia seperti semprotan obat pembunuh serangga, semprotan anti api, dll
   d. Kebocoran seperti A/C, atap bocor saat hujan

   Besar kecilnya suatu ancaman dari sumber ancaman yang teridentifikasi atau belum teridentifikasi dengan jelas tersebut, perlu di klasifikasikan secara matriks ancaman sehingga kemungkinan yang timbul dari ancaman tersebut dapat di minimalisir dengan pasti.Setiap ancaman tersebut memiliki probabilitas serangan yang beragam baik dapat terprediksi maupun tidak dapat terprediksikan seperti terjadinya gempa bumi yang mengakibatkan sistem informasi mengalami mall function.

D. Kelemahan keamanan sistem informasi

Adalah cacat atau kelemahan dari suatu sistem yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh pelaku yang mencoba menyusup terhadap sistem tersebut. Cacat sistem bisa terjadi pada prosedur, peralatan, maupun perangkat lunak yang dimiliki, contoh yang mungkin terjadi seperti : Seting firewall yang membuka telnet sehingga dapat diakses dari luar, atau Seting VPN yang tidak di ikuti oleh penerapan kerberos atau NAT. Suatu pendekatan keamanan sistem informasi minimal menggunakan 3 pendekatan, yaitu :

1. Pendekatan *Preventif* yang bersifat mencegah dari kemungkinan terjadikan ancaman dan kelemahan
2. Pendekatan *Detective* yang bersifat mendeteksi dari adanya penyusupan dan proses yang mengubah sistem dari keadaan normal menjadi keadaan abnormal
3. Pendekatan *Corrective* yang bersifat mengkoreksi keadaan sistem yang sudah tidak seimbang untuk dikembalikan dalam keadaan normal

Tindakan tersebutlah menjadikan bahwa keamanan sistem informasi tidak dilihat hanya dari kaca mata timbulnya serangan dari virus, *mallware, spy ware* dan masalah lain, akan tetapi dilihat dari berbagai segi sesuai dengan domain keamanan sistem itu sendiri.

E. Pengendalian Dalam manajeman Keamanan Informasi

Pengamanan sistem informasi

Mengamankan Sistem informasi dapat dikategorikan menjadi 2 jenis : pencegahan (*preventif*) dan pengobatan (*recovery*).

1. Kriptografi merupakan ilmu dan seni untuk menjaga pesan agar aman.

2. Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak.

Pengendalian (*Control*)

Merupakan mekanisme yang diterapkan, baik untuk melindungi perusahaan dari risiko atau untuk meminimalkan dampak risiko tersebut pada perusahaan jika risiko tersebut terjadi.Pengendalian terbagi menjadi 3 kategori, yakni:

Sistem Deteksi Gangguan

Logika dasar dari sistem deteksi gangguan adalah mengenali upaya pelanggaran keamanan sebelum memiliki kesempatan untuk melakukan perusakan.

Contoh:Peranti lunak proteksi virus (virus protection software).Peranti lunak yang didesain untuk mencegah rusaknya keamanan sebelum terjadi.

Firewall

Suatu Filter yang membatasi aliran data antara titik-titik pada suatu jaringan-biasanya antara jaringan internal perusahaan dan Internet.Berfungsi sebagai:

a. Penyaring aliran data
b. Penghalang yang membatasi aliran data ke dan dari perusahaan tersebut dan internet.

Jenis Firewall:

a. Firewall Paket
b. Firewall Tingkat Sirkuit
c. Firewall Tingkat Aplikasi

F. **Pentingnya Keamanan sistem**

Sistem Informasi diperlukan karena:

a. Teknologi Komunikasi Modern yang membawa beragam dinamika dari dunia nyata ke dunia virtual. Contohnya adalah: dalam bentuk transaksi elektronik seperti e-banking, dan pembawa aspek positif maupun negative, misalnya: pencurian, pemalsuan, dan penggelapan menggunakan internet.
b. Kurangnya Keterampilan Pengamanan yang dimiliki oleh Pemakai
   Contoh: Pemakai kurang menguasai computer.
c. Untuk menjaga objek kepemilikan dari informasi yang memiliki nilai ekonomis.
   Contoh: dokumen rancangan produk baru, kartu kredit, dan laporan keuangan perusahaan

G. Manfaat keamanan sistem informasi

Sistem Informasi dalam suatu perusahaan bertujuan untuk mencapai 3 manfaat : **Kerahasiaan**. Untuk melindungi data dan informasi dari pengguna yang tidak semestinya oleh orang-orang yang tidak memiliki otoritas. Sistem informasi eksekutif, sumber daya manusia, dan sistem pengolahan transaksi, adalah sistem-sistem yang terutama harus mendapat perhatian dalam keamanan informasi. **Ketersediaan**. Supaya data dan informasi perusahaan tersedia bagi pihak-pihak yang memiliki otoritas untuk menggunakannya. **Integritas.** Seluruh sistem informasi harus memberikan atau menyediakan gambaran yang akurat mengenai sistem fisik yang mereka wakili.

H. Jenis ukuran-ukuran keamanan sistem informasi

Untuk melindungi sumberdaya organisasi, suatu perusahaan harus menerapkan beragam jenis ukuran keamanan, antara lain: Melindungi fasilitas komputernya dan

fasilitas fisik lainnya, Menjaga integritas dan kerahasiaan file data. Menghindari kerusakan serius atau kerugian karena bencana

Untuk keamanan fokus pada: keamanan fisik dan keamanan data informasi Keamanan fisik dikelompokkan atas: keamanan untuk sumber daya fisik selain fasilitas komputer, keamanan untuk fasilitas perangkat keras komputer.

Untuk setiap keamanan fisik dan keamanan data/informasi, maka ukuran-ukuran keamanan harus ditetapkan untuk : Melindungi dari akses yang tidak diijinkan , Perlindungan terhadap bencana, Perlindungan terhadap kerusakan, Perlindungan dari akses yang tidak terdeteksi, Perlindungan terhadap kehilangan atau perubahan-perubahan yang tidak seharusnya, Pemulihan atau rekonstruksi data yang hilang.

METODE

Penelitian ini menggunakan pendekatan kualitatif yang bersifat studi pustaka atau library research. Objek penelitiannya adalah system keamanan dan pertahan negara.. Jenis data yang digunakan adalah data sekunder. Ruang lingkup data yang digunakan adalah artikel jurnal penelitian tentang system informasi kemanan dan pertahanan negara. Sumber pengambilan data berasal dari penelusuran jurnal nasional terakreditasi Sinta melalui website Garuda (Garba Rujukan Digital) dan software Perish/Harzing. Teknik pengumpulan data meliputi: (1) membuka sofware Perish/Harzing, lalu mencari jurnal berdasarkan kategori title words berkata kunci "manajemen system keamanan dan pertahanan" mengumpulkan data judul dan mengidentifikasi judul.

HASIL PENELITIAN

Teknologi informasi dan komunikasi, atau disingkat TIK, saat ini telah menjadi bagian dalam setiap aspek kehidupan masyarakat, baik dalam aspek ekonomi, sosial, budaya, pendidikan, dan kesehatan. Sektor TIK di Indonesia berkembang dengan sangat pesat, terutama dalam hal penggunaan internet. Pada kuartal kedua tahun 2020, Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) memperkirakan 196,7 juta orang, atau 73,7 persen, dari populasi Indonesia akan menggunakan internet (Asosiasi Penyelenggara Jasa Internet Indonesia, 2020). Jika dibandingkan dengan tahun 2018, angka ini naik 64,8%. Di satu sisi, meningkatnya kemampuan masyarakat untuk beradaptasi dengan kemajuan teknologi didukung oleh peningkatan pengguna internet. Namun, meningkatnya jumlah pengguna yang masih awam dengan keamanan siber juga meningkatkan risiko keamanan. Pelaku kejahatan siber telah tertarik dengan peningkatan lalu lintas internet, yang menyebabkan banyaknya serangan siber di Indonesia. Menurut Badan Siber dan Sandi Negara (BSSN), jumlah serangan siber pada tahun 2020 mencapai 495,3 juta, naik 41% dari tahun 2019 yang mencapai 290,3 juta (Badan Siber dan Sandi Negara, 2021).

Serangan siber adalah upaya untuk menguasai atau mendapatkan akses tidak sah ke sistem komputer atau jaringan komputer (Marshall & Saulawa, 2015). Sebaliknya, kejahatan siber adalah aktivitas ilegal yang memanfaatkan atau menargetkan jaringan atau sistem komputer (International Telecommunication Union, 2012). Menurut pernyataan yang berbeda, istilah "cybercrime" mengacu pada tindakan kriminal yang menggunakan komputer atau jaringan komputer sebagai alat, target, atau lokasi dan menimbulkan kerugian materiil maupun imateriil bagi pihak-pihak yang menjadi sasaran (Wilson, 2008). Menurut laporan data anomali trafik BSSN, terdapat 495,3 juta serangan siber di Indonesia pada tahun 2020, meningkat 41% dari tahun sebelumnya yang berjumlah 290,3 juta (Badan Siber dan Sandi Negara, 2021). Dengan total 7.311.606 anomali, tanggal 10 Desember 2020 merupakan tanggal dengan anomali trafik terbanyak. Anomali dengan jumlah tertinggi adalah Trojan.

Selama tahun 2020, negara dengan jumlah serangan anomali terbanyak adalah Amerika Serikat, dan Indonesia juga menjadi negara dengan jumlah serangan anomali terbanyak yang berasal dari Indonesia sendiri (dengan alamat IP Indonesia). Laporan tersebut juga menemukan sebanyak 2.549 kasus email phishing, dengan peningkatan jumlah kasus email phishing pada bulan Maret sampai Mei 2020. Ancaman cyber atau ancaman terhadap keamanan data di komputer sangat meresahkan semua pihak saat ini. Ketika berbicara tentang keamanan data dan informasi, tidak ada institusi atau organisasi yang dikecualikan. Tentu saja, hal ini membutuhkan banyak penelitian dan perhatian untuk mengukur daya tahan dan keamanan data komputer organisasi. Perlindungan data di komputer menjadi topik yang semakin populer di seluruh dunia. Hal ini tidak hanya berdampak negatif dalam bentuk malware atau virus, tetapi juga dapat berakibat fatal, seperti terbongkarnya rahasia negara dan lumpuhnya lembaga- lembaga penting negara (Czosseck, C. et al, 2013).

Menyusul terjadinya kebocoran data di sejumlah instansi, kasus kebocoran data akhir-akhir ini menjadi perhatian. Insiden kebocoran data yang pernah terjadi di Indonesia adalah sebagai berikut (Clinten, 2022): kebocoran data pengguna aplikasi eHAC Kementerian Kesehatan, kebocoran data BPJS kesehatan, kebocoran data nasabah BRI Life, kebocoran data Daftar Pemilih Tetap (DPT) Pemilu KPU, kebocoran data pengguna Tokopedia, dan kebocoran data 26 juta riwayat pengguna IndiHome. Berdasarkan kasus kebocoran data tersebut diatas, maka pemanfaatan TI secara optimal menjadi hal yang penting dalam pelaksanaan Sistem Pemerintahan Berbasis Elektronik (SPBE) di instansi pemerintahan. Sesuai dengan Peraturan Presiden No. 95 Tahun 2018, SPBE adalah penyelenggaraan pemerintahan yang memberikan layanan kepada pengguna SPBE melalui pemanfaatan teknologi informasi dan komunikasi. Ketika instansi pemerintah menggunakan TI untuk mengimplementasikan SPBE, mereka harus mempertimbangkan keterbatasan sumber daya seperti data, teknologi, fasilitas, dan sumber daya manusia, serta fakta bahwa TI relatif mahal untuk digunakan.

SIMPULAN

Masa sekarang ini banyak perusahaan/organisasi yang semakin peduli akan pentingnya menjaga sistem keamanan informasi agar aman dari ancaman baik dari dalam maupun dari luar. Ancaman Keamanan Informasi (Information Security Threat) merupakan orang, organisasi, mekanisme, atau peristiwa yang memiliki potensi untuk membahayakan sumber daya informasi perusahaan. Pada kenyataannya, ancaman dapat bersifat internal serta eksternal dan bersifat disengaja dan tidak disengaja.

Resiko Keamanan Informasi (Information Security Risk) didefinisikan sebagai potensi output yang tidak diharapkan dari pelanggaran keamanan informasi oleh Ancaman keamanan informasi. Pengendalian (control) adalah mekanisme yang diterapkan baik untuk melindungi perusahaan dari resiko atau untuk meminimalkan dampak resiko tersebut pada perusahaan jika resiko tersebut terjadi. Pengendalian dibagi menjadi tiga kategori, yaitu : teknis, formal dan informal. Namun, pada intinya dapat disimpulkan bahwa keamanan sistem informasi untuk mencegah dari adanya dari kemungkinan adanya virus, hacker, cracker dan lain-lain.

Kebutuhan akan tata kelola TI untuk mengendalikan bagaimana TI digunakan dalam organisasi pemerintah tumbuh sebagai akibat dari sumber daya yang terbatas. Berdasarkan Peraturan Presiden No. 95 Tahun 2018, implementasi SPBE instansi pemerintah harus dipantau dan dievaluasi untuk mengukur dan meningkatkan kualitasnya. Menurut peraturan di atas, maka semua instansi pemerintahan yang memanfaatkan penggunaan TI dalam proses bisnisnya memiliki kewajiban untuk melakukan evaluasi pemanfaatan TI dalam pelaksanaan SPBE. Salah satu kementerian di Indonesia yang memiliki urgensi untuk melakukan evaluasi pelaksanaan SPBE ialah Badan Siber dan Sandi Negara (BSSN). Sesuai dengan Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara,

BSSN mempunyai tugas menyelenggarakan urusan pemerintahan di bidang keamanan siber dan persandian untuk membantu Presiden dalam menyelenggarakan pemerintahan negara.

Referensi :

Ardiyanti, Handrini. 2014. "Cyber-Security dan Tantangan Pengembangannya di Indonesia". Jurnal Politica. Vol. 5. No. 1 . Juni.

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., &Ekhsan, M. (2019).Cybercrime Business Digital in Indonesia.In *E3S Web of Conferences* (Vol. 125, p. 21001).EDP Sciences.

Indrawan, Raden Mas Jerry dan Efriza. 2017. "Bela Negara Sebagai Metode Pencegahan Ancaman Radikalisme di Indonesia". Jurnal Pertahanan dan Bela Negara. Universitas Pertahanan Indonesia. Vol. 7.No. 3. Desember.

M. Arsyad. 2005. Hukum Teknologi dan Informasi. Bandung: Tim Kemas Buku. Vivian, John. 2008.Teori Komunikasi Massa. Jakarta: Kencana. Thompson, Ronald & William Cats Barril. 2003. Information Technology and Management. New York: Mc Graw Hill

Menthe, D. 1998. "Jurisdiction in Cyberspace: A Theory of International Space". Michigan Telecommunications and Technology Law Review. 23 April. Sanusi,

Parashakti, R. D., &Ekhsan, M. (2020). The Effect of Discipline and Motivation *Research in Business, Economics, and Education*, *2*(3), 653-660.

Parashakti, R. D., Fahlevi, M., Ekhsan, M., &Hadinata, A. (2020, April).The Influence of Work Environment and Competence on Motivation and Its Impact on Employee Performance in Health Sector.In *3rd Asia Pacific International Conference of Management and Business Science (AICMBS 2019)* (pp. 259-267).Atlantis Press.