CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 3, No. 2, November 2020, hlm. 28-33

MODEL PERILAKU KEAMANAN SIBER PADA PENGGUNA SISTEM INFORMASI KESEHATAN PADA MASA PANDEMI COVID-19

Penggalih Mahardika Herlambang[1], Sylvia Anjani[2], Hendro Wijayanto[3], Murni[4]

[1]Fakultas Kedokteran Universitas Wahid Hasyim Semarang
[2]Fakultas Kesehatan Universitas Dian Nuswantoro Semarang
[3]Program Studi Informatika STMIK Sinar Nusantara Surakarta
[4]Fakultas Kesehatan Masyarakat Universitas Diponegoro Semarang
Email: [1]dr.penggalih@unwahas.ac.id, [2]sylvia.anjani@dsn.dinus.ac.id, [3]hendro@sinus.ac.id, [4]murniprima80@gmail.com

(Naskah masuk: 23 Oktober 2020, diterima untuk diterbitkan: 31 November 2020)

Abstrak

Penggunaan Sistem Informasi Kesehatan memunculkan resiko kebocoran data yang terbanyak disebabkan oleh pihak internal fasilitas kesehatan. Untuk itu diperlukan sebuah instrumen yang dapat mengukur perilaku pengguna yang berisiko terhadap sistem informasi kesehatan yang digunakan untuk meminimalisir potensi kebocoran tersebut. Penelitian ini terdiri dari tiga tahap meliputi kajian pustaka mengenai aspek yang berpengaruh terhadap keamanan sistem informasi kesehatan. Tahap kedua penyusunan desain kuesioner mengenai risiko serangan siber pada sistem informasi kesehatan. Kemudian tahap ketiga pengujian reliabilitas dan validitas kuesioner. Berdasarkan penelitian terdapat 4 aspek yang berpengaruh terhadap keaman sistem informasi kesehatan yaitu penggunaan perangkat elektronik, akses sistem informasi kesehatan, perilaku ber-internet, dan kejadian tidak wajar di fasilitas kesehatan. Kuesioner yang dikembangkan terdiri dari 27 item pertanyaan yang terbagi dalam 4 aspek tersebut. Pada uji validitas keseluruhan item valid (r hitung > r tabel). Sedangkan pada uji reliabilitas kuesioner reliabel dengan nilai *Cronbach's Alpha* sebesar 0,777. Desain kuesioner yang dikembangkan dapat diterapkan untuk menilai risiko serangan siber pada sistem informasi kesehatan di fasilitas kesehatan. Penelitian lanjutan diperlukan untuk mengimplementasikan desain kuesioner tersebut.

Kata kunci: *keamanan siber, system informasi kesehatan, perilaku keamanan siber, kejahatan siber, covid-19*

CYBER SECURITY BEHAVIOR MODEL ON HEALTH INFORMATION SYSTEM USERS DURING COVID-19 PANDEMIC

Abstract

The use of the Health Information System raises the risk of data leakage which is mostly caused by internal health facilities. For this reason, an instrument is needed that can measure the behavior of users who are at risk for the health information system used to minimize the potential for these leaks. Develop and test the validity and reliability of the questionnaire based Human Aspect of Information Security Questionaire (HAIS-Q), Risky Security Behavior Scale (RScB), and the tendency of Internet users in Indonesia. Based on the research 4 aspects that affect the security of Health Information System, namely the use of electronic devices, access to health information systems, internet behavior, and unusual events in health facilities. The questionnaire developed consisted of 27 question items was valid (r count> r table) and reliable (Alfa Chronbach value of 0.777). The developed questionnaire design can be applied to assess the risk of cyber attacks on Health Information Systems in health facilities. Further research is needed to implement the design of the questionnaire.

Keywords: *cyber security, health information systems, cyber security behavior, cyber crime, covid-19*

1. PENDAHULUAN

Peta Jalan Kementrian Kesehatan tentang Sistem Informasi Kesehatan Nasional (SIKNAS) menargetkan seluruh fasilitas pelayanan kesehatan (FASYANKES) akan saling tehubung lewat internet pada fase satu (Kementerian Kesehatan Republik Indonesia, 2015). Efisiensi waktu, biaya dan sumberdaya manusia dalam pengelolaan FASYANKES merupakan beberapa faktor yang mendorong budaya kerja menjadi *paperless* dengan penggunaan sistem informasi kesehatan (SIK).

Berbagai bentuk SIK berbagai macam, untuk fasilitas kesehatan tingkat primer (FKTP) seperti Puskesmas sistem informasi manajemen puskesmas (SIMPUS), sistem informasi pelaporan dinas kesehatan (SIP/SP3), sistem pembiayaan kesehatan *P-Care*, dan sejenisnya. Sedangkan untuk fasilitas kesehatan rujukan tingkat lanjut (FKRTL) terdapat sistem informasi manajemen Rumah Sakit (SIMRS) yang dapat terintegrasi dengan sistem pembiayaan kesehatan dari BPJS seperti SEP (Surat Eligibilitas Peserta), e-Klaim dan V-Klaim.

Dengan pengguna internet di Indonesia sekitar 175.4 juta orang atau sekitar 64% penduduk, kebutuhan akan tenaga fasyankes yang melek internet untuk menjalankan berbagai SIK seharusnya dapat terpenuhi dapat dipenuhi (Hootsuite, 2020). Penggunaan SIK tentunya memiliki konsekwensi. Ancaman serangan siber di fasilitas pelayanan kesehatan meningkat sejak tahun 2017 (IndoTelko, 2019). Bentuk serangan dapat berupa *Phising*, *Distribute Denial of Service (DDoS), Ransomware*, *Malware*, hingga kebocoran data oleh pihak internal . Dampak dari serangan tersebut dapat berupa perusakan data, pencurian data hingga penyanderaan data (Samuel, 2018).

Kebocoran data merupakan salah satu ancaman dalam pengelolaan data kesehatan. *Verizon* melaporkan bahwa 59% kejadian kebocoran data kesehatan disebabkan oleh pihak internal pengelola sistem informasi kesehatan (Widup, 2019). Data kesehatan yang dicuri atau bocor dapat diperjualbelikan oleh peretas dengan nilai hingga $1000 di *darkweb*. Harga yang tinggi disebabkan karena data kesehatan seperti rekam medis berisi informasi nama ibu kandung, tanggal lahir, hingga nomer identitas dapat dimanfaatkan pihak-pihak lain untuk melakukan penipuan atau pencurian lain (Kamaliah, 2020).

Pada bulan Juli Tahun 2018, terjadi kasus kebocoran data pribadi warga Singapura yang disimpan pada institusi kesehatan *SingHealth*. Kasus kebocoran data tersebut diperkirakan mengakibatkan 1,5 juta data rekam medis warga Singapura tersebar luas. Kasus kebocoran data pada *SingHealth* (Singapura) ini menandakan bahwa data pribadi mengenai kesehatan juga menjadi primadona bagi serangan tertarget (BSSN, 2020a). Kasus lain juga ditemukan celah keamanan pada perangkat medis *Medtronic* yang menandakan bahwa isu keamanan siber pada sektor kesehatan juga menyentuh pada permasalahan *supply chain*, kemudian serangan *cyber security* sektor kesehatan di USA, dan serangan *defacement web* terhadap laman penyelenggara sektor kesehatan di Indonesia yang dilakukan oleh *hacker* dari dan luar Indonesia, serta serangan *ransomware* terhadap beberapa rumah sakit di Indonesia.

Dalam hasil evaluasi Indeks KAMI yang dilakukan oleh BSSN terhadap sektor kesehatan pada tahun 2018/2019, mengindikasikan bahwa kesiapan sektor kesehatan masih kurang dan perlu upaya perbaikan berkelanjutan. Sebanyak 69% sistem informasi kesehatan memiliki status tidak layak keamanannya apabila dinilai dari 3 area Indeks KAMI yaitu pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi serta tata kelola keamanan informasi.

Healthcare Information and Management System Society (*HIMSS*) menyebutkan bahwa phising email dan kelalaian pegawai masih menjadi perilaku berisiko terbesar untuk celah kerawanan pada organisasi kesehatan. Perilaku berisiko serta literasi digital yang rendah mengenai pengelolaan SIK diantaranya merupakan penyebab kebocoran data kesehatan.

Untuk itu diperlukan instrumen berupa pengembangan kuesioner perilaku berisiko pengguna SIK agar dapat meminimalisir risiko tersebut diatas.

2. TINJAUAN PUSTAKA

Keamanan sistem informasi penting dijaga agar sistem tersebut terhindar dari segala ancaman yang membahayakan keamanan data informasi dan keamanan pelaku sistem (ISO 27799:2008, 2008). Ancaman ini dapat berupa ancaman internal dan eksternal, yaitu berbagai jenis perilaku karyawan seperti ketidaktahuan karyawan, kecerobohan, mengambil sandi karyawan lain dan memberikan *password* untuk karyawan lain atau *virus* dan serangan *spyware*, *hacker* dan penyusup di tempat.

Hasil penelitian yang menghasilkan *Policy Brief* oleh (Wijayanto, 2020) mengatakan bahwa keamanan siber dari sisi pengguna dapat dipengaruhi oleh perilaku penggunaan password, bersosial media, akses perangkat internet dan jaringan, perilaku akses data informasi serta perilaku penggunaan smartphone. Hal ini didasari kegiatan-kegiatan inilah yang sering dilakukan oleh pengguna internet.

Hasil Indeks KAMI juga menunjukkan bahwa sebagian besar pengelola keamanan siber tidak memiliki kompetensi yang cukup. Rendahnya kesadaran keamanan dan kompetensi sumber daya manusia kesehatan di bidang teknologi keamanan siber menjadikan penggunaan perangkat elektronik yang tidak aman (BSSN, 2020c). Dikutip dari CNN Money, Rabu (17/5/2017), komputer dengan *software* kadaluwarsa yang kebanyakan berada di fasilitas kesehatan, menjadi alasan kuat mengapa

banyak fasilitas kesehatan menjadi sasaran malware (Damar, 2017).

Aspek lain yang mempengaruhi keamanan sistem informasi kesehatan adalah akses terhadap sistem informasi kesehatan. Peraturan Pemerintah Nomor 46 Tahun 2014 Pasal 24 (1) menyatakan bahwa untuk menjaga keamanan dan kerahasiaan Informasi Kesehatan, harus ada kriteria dan batasan hak akses pengguna Informasi Kesehatan (Kementerian Kesehatan Republik Indonesia, 2014). Selain itu keamanan juga berhubungan dengan orang (personel), termasuk identifikasi, dan profil resiko dari orang yang mempunyai akses (pekerja). Kelemahan dari keamanan sistem informasi seperti ini yaitu menyebabkan adanya teknik "*social engineering*" yang digunakan oleh kriminal untuk berpura-pura sebagai orang yang berhak mengakses informasi dan berpura-pura lupa *password*nya dan minta agar diganti menjadi kata lain sehingga data kesehatan dapat terakses dengan bebas (Wijayanto, Muhammad, & Hariyadi, 2020).

Dalam penjaminan keamanan informasi kesehatan di fasilitas kesehatan diperlukan kesadaran seluruh tenaga kesehatan dalam berperilaku ber-*internet*. Perilaku ber-internet yang beresiko yang dilakukan tenaga difaskes mampu memengaruhi keamanan sistem informasi kesehatan yang ada. Dalam (Jogiyanto, 2007) menyebutkan bahwa kesalahan penerimaan informasi pada *SIMRS* bukan disebabkan kualitas teknik melainkan aspek keperilakuan (*behavioral*) sumber daya manusia. Perilaku pengabaian tata cara pengoperasian sistem informasi kesehatan juga masih sering terjadi. Survei yang dilakukan (Hadlington, 2017a) hasilnya juga menunjukkan bahwa perilaku keamanan siber yang berisiko berkorelasi negatif dengan impulsif non-perencanaan. Hal ini juga menguatkan bahwa aspek perilaku *cybersecurity berisiko (RScB)* dapat memperbesar peluang masalah keamanan sistem informasi.

Kejadian atau kerusakan tidak wajar pada perangkat elektronik di fasilitas kesehatan juga menjadi salah satu aspek yang dapat mempengaruhi keamanan sistem informasi kesehatan. Pasalnya perangkat elektronik yang digunakan tidak selalu aman, karena tidak semua dilengkapi perangkat lunak antivirus yang mampu mencegah, mendeteksi, dan menghapus malware, termasuk virus komputer, worm komputer, *Trojan horse*, *spyware*, dan *adware* dll. Kurang amannya browser yang digunakan untuk mengakses website menyebabkan masuknya *botnet* dan *malware* dan mengakibatkan kebocoran data (Sendari, 2019).

3. METODOLOGI

Dalam penelitian ini secara garis besar pengembangan kuesioner perilaku online berisiko dilakukan dalam tiga tahap. yaitu:

3.1. Tahap Studi Pustaka

Studi pustaka dilakukan untuk mengetahui aspek yang berperan dalam risiko terjadinya serangan siber pada sistem informasi. Prosiding, jurnal, artikel ilmiah dan hasil riset Tahun 2010 - 2020 dengan kata kunci: "*Cybersecurity*", "*Health Information System*", dan "*Cyber Risk Assessment*.

3.2. Tahap Penyusunan Kuesioner

Kuesioner disusun berdasarkan beberapa referensi antara lain *Human Aspect of Information Security Questionaire (HAIS-Q)*, *Risky Security Behavior Scale (RScB)* (Hadlington, 2017b) dan penambahan item kuesioner sesuai kondisi dan kebutuhan di Indonesia.

3.3. Tahap Pengujian Kuesioner

Kuesioner yang telah disusun kemudian diuji reliabilitas dan validitasnya kepada 35 responden yang bekerja di beberapa fasilitas kesehatan di Indonesia. Pengujian dilakukan pada masa pandemi Covid-19 antara bulan Agustus- September 2019. Uji validitas dan reliabilitas dilakukan dengan menggunakan *product moment Pearson Corelation* dengan item kuesioner dikatakan valid jika *r* hitung lebih besar daripada *r* tabel. Sedangkan uji reliabilitas menggunakan uji Alpha Chroncbach instrumen dikatakan reliabel jika *Alfa Chronbach* lebih dari 0,6

4. HASIL DAN PEMBAHASAN

Kuesioner disusun berdasarkan referensi dua alat ukur mengenai perilaku beresiko terhadap sistem informasi yaitu:

1. *Human Aspect of Information Security Questionaire (HAIS-Q)*
2. *Risky Security Behavior Scale (RScB)*

Dari dua alat tersebut kemudian disusun kuesioner dan disesuaikan dengan kondisi fasyankes di Indonesia pada umumnya. Dimana pada penelitian ini keempat aspek yaitu penggunaan perangkat elektronik, akses sistem informasi kesehatan, perilaku ber-internet dan kejadian tidak wajar dikembangkan menjadi kuesioner yang terdiri dari 27 item pertanyaan yang terbagi dalam 4 aspek tersebut, ditunjukkan pada Tebel 1.

Tabel 1. Kuesioner Perilaku Beresiko dalam Penggunaan SIK

	A. Penggunaan Perangkat
1.	Saya bekerja menggunakan perangkat elektronik (laptop/ komputer/ tablet/ dsb) yang terhubung dengan jaringan di faskes.
2.	Selain perangkat elektronik dari kantor, kadang saya juga menggunakan perangkat elektronik pribadi (hp/ tablet/ laptop) di faskes.
3.	Saya pernah menggunakan perangkat elektronik kantor untuk mengakses internet diluar urusan faskes.
4.	Saya pernah mengkases internet lewat hp/ tablet/ laptop pribadi menggunakan WiFi/ akses internet faskes.
5.	Saya pernah menyimpan data dari laptop/ komputer faskes ke USB flasdisk/hard disk eksternal milik saya.

6.	Saya pernah menyimpan data dari laptop/ komputer faskes ke penyimpanan cloud gratis. (dropbox, googledrive, dsb)
7.	Perangkat elektronik dari faskes (laptop/ komputer/ tablet, dsb) digunakan oleh lebih dari 1 pengguna.
8.	Perangkat elektronik dari kantor (laptop/ tablet/ komputer) belum terinstall antivirus.
	B. Akses Sistem Informasi Kesehatan
9.	Saya memiliki akses ke perangkat lunak sistem informasi kesehatan di faskes (SIMRS,SIMPUS,e-Claim,SEP, P-Care, dsb)
10.	Saya bekerja menggunakan lebih dari satu aplikasi sistem informasi kesehatan.
11.	Saya memakai password yang sederhana (nama, tanggal lahir, nomer hp, dsb) untuk mengakses sistem infromasi kesehatan tersebut.
12.	Saya pernah berbagi password tersebut dengan rekan kerja.
13.	Saya menggunakan password yang sama untuk beberapa sistem informasi kesehatan di faskes.
	C. Perilaku ber-internet
14.	Saya pernah membuka email lewat laptop/komputer faskes.
15.	Saya pernah meng-klik link/tautan tak dikenal dari email ketika mengakses lewat laptop/komputer faskes.
16.	Saya pernah membuka lampiran (attachment) tak dikenal dari email ketika mengakses lewat laptop/ komputer faskes.
17.	Saya pernah mengirimkan email berupa informasi penting dari faskes ke pihak yang tidak saya kenal.
18.	Saya pernah mengunduh/men-download film, lagu, software gratisan lewat komputer/ laptop faskes.
19.	Saya memiliki lebih dari 2 akun media sosial (Facebook, Youtube, dsb).
20.	Saya pernah mengakses media sosial (Facebook, Youtube, dsb) pribadi menggunakan komputer/ laptop faskes.
21.	Saya pernah mem-posting informasi penting faskes di media sosial pribadi.
22.	Saya pernah berkomunikasi lewat instant messaging (WhatsApp, Telegram, dsb) menggunakan komputer/ laptop faskes.
23.	Saya pernah berbagi informasi penting mengenai faskes melalui instant messaging (WhatsApp, Telegram, dsb) menggunakan komputer/laptop faskes.
24.	Saya pernah berbelanja online menggunakan laptop/komputer faskes.
	D. Kejadian tidak wajar
25.	Komputer/laptop faskes sering menjadi lambat /hang setelah mengakses website tertentu.
26.	Sering muncul peringatan dari antivirus di komputer/laptop faskes.
27.	Pernah muncul tampilan tertentu di layar komputer/laptop faskes sehingga tidak dapat diakses.

Kuesioner ini menggunakan skala linkert untuk mengetahui skala sikap dari responden. Dalam instrumen ini skala jawaban terdiri dari (Sangat Tidak Setuju=5, Tidak Setuju=4, Netral=3, Setuju=2 dan Sangat Setuju=1).

Evaluasi kuesioner dalam penelitian ini dilakukan dengan pengujian validitas dan reliabel pada kuesioner yang dikembangkan.

Tabel 2. Uji validitas Kuesioner Perilaku Beresiko dalam Penggunaan SIK

No Item	*r hitung*	*r tabel*
X1A	.495**	0.334
X1B	.715**	0.334
X1C	.727**	0.334
X1D	.733**	0.334
X1E	.690**	0.334
X1F	.707**	0.334
X1G	.444**	0.334
X1H	.499**	0.334
X2A	.425*	0.334
X2B	.730**	0.334
X2C	.850**	0.334
X2D	.682**	0.334
X2E	.789**	0.334
X3A	.688**	0.334
X3B	.497**	0.334
X3C	.527**	0.334
X3D	.628**	0.334
X3E	.804**	0.334
X3F	.674**	0.334
X3H	.814**	0.334
X3I	.735**	0.334
X3J	.780**	0.334
X3K	.708**	0.334
X3L	.693**	0.334
X4A	.865**	0.334
X4B	.841**	0.334
X4C	.933**	0.334

Tabel 2 menunjukan hasil uji validitas pada instrumen yang dikembangkan dalam penelitian. R tabel pada *p=0,05* dengan uji 2 sisi dan *n=35*, didapat *r* tabel sebesar *0,334*. Pada uji validitas ini, keseluruhan item memiliki *r* hitung > *r* tabel. Hal tersebut bermakna bahwa masing-masing item dalam kuesioner yang dikembangkan valid.

Hasil uji reliabilitas kuesioner ini ditunjukkan pada Tabel 3 yang menunjukan nilai *Alfa Chronbach* = 0,777. Ini bermakna bahwa butir-butir instrument yang disusun dalam penelitian ini reliabel atau konsisten.

Tabel 3. Uji Reliability Kuesioner Perilaku Beresiko dalam Penggunaan SIK

Reliability Statistics	
Cronbach's Alpha	N of Items
0.777	35

Seperti halnya pada masa pandemi *Corona Virus Disease* 2019 (*COVID-19*) saat ini. Kondisi tersebut dimanfaatkan oleh *threat actor* untuk menyebarkan malware (*virus*, *ransomware*, dan lainnya) dan spam email ke berbagai pihak. Penyebaran malware ini sangat berpotensi menyebabkan kebocoran data sensitif pasien (*COVID-19*) (BSSN, 2020b). Di Tiongkok kebocoran data *Covid-19* muncul dari data *National University of Defence Technology* yang bocor kepada 100 *Reporters* dan menyebabkan data pasien *Covid-19* di Tiongkok tersebar di *Twitter* (Sinuhaji, 2020). Di Indonesia kebocoran data juga terjadi, dimana akun atas nama *Database Shopping* mengklaim > 200.000 data pribadi pasien *Covid-19*. Data tersebut berisi data sensitif pasien *Covid-19*, yang berisi indentitas lengkap dari pasien *Covid-19* dan akan dijual ke *RaidForums* (Mukharomah, 2020).

Penelitian lain terkait keamanan penggunaan sistem informasi kesehatan, sebagian besar meneliti terkait ruang lingkup keamanan sistem informasi kesehatan (*organization, people, process and technology*). Dimana dalam penelitiannya meneliti perilaku sumber daya manusia secara umum (kemampuan, tanggung jawab, kepatuhan prosedur dan lainnya) dan belum menilai perilaku beresiko dalam penggunaan sistem informasi kesehatan. Oleh karena itu kuesioner perilaku beresiko dalam penggunaan SIK pada penelitian ini sangat penting untuk dikembangkan.

Hasil dari uji validitas dan reliabel ini juga menjadi dasar bahwa kuesioner yang dikembangkan pada penelitian ini layak untuk diimplementasikan/ diterapkan untuk menilai risiko serangan siber pada Sistem Informasi Kesehatan.

5. KESIMPULAN

Desain kuesioner yang dikembangkan dapat diterapkan untuk menilai risiko serangan siber, meminimalisir kebocoran data atau pencurian yang terjadi pada Sistem Informasi Kesehatan di fasilitas kesehatan. Saran untuk penelitian selanjutnya adalah adanya penelitian lanjutan untuk mengimplementasikan desain kuesioner tersebut.

Desain kuesioner ini dapat digunakan untuk pengujian di Rumah Sakit atau fasilitas kesehatan lainnya. Penelitian selanjutnya juga dapat memodifikasi kuesioner dari *likert scale* menjadi skoring dengan juga melakukan uji validitas dan reliabilitas.

Penelitian selanjutnya perlu dilakukan studi tentang penyusunan kebijakan-kebijakan mitigasi keamanan siber serta standar operasional prosedur dalam penggunaan teknologi informasi dan komputer dilingkungan kesehatan.

DAFTAR PUSTAKA

BSSN. (2020a). *Buku Putih Keamanan Siber Sektor Kesehatan*. Jakarta: Badan Siber dan Sandi Negara (BSSN).

BSSN. (2020b). *Buku Putih Mitigasi Insiden Siber Saat Pandemi Covid-19*. Jakarta: Badan Siber dan Sandi Negara (BSSN).

BSSN. *Indeks Keamanan Informasi (KAMI)*. , (2020).

DAMAR, A. M. (2017). Mengapa WannaCry Serang Komputer di Fasilitas Kesehatan? Retrieved September 5, 2020, from Liputan 6 website: https://www.liputan6.com/tekno/read/2955041/mengapa-wannacry-serang-komputer-di-fasilitas-kesehatan

HADLINGTON, L. (2017a). *Cybercognition: Brain, behaviour and the digital world*. New York: SAGE.

HADLINGTON, L. (2017b). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

HOOTSUITE, W. A. S. (2020). *Digital 2020. Indonesia*. Retrieved from https://datareportal.com/reports/digital-2020-indonesia

INDOTELKO. (2019). Serangan siber target layanan kesehatan di Indonesia. Retrieved September 2, 2020, from IndoTelko website: https://www.indotelko.com/read/1568065603/serangan-keseshatan

ISO 27799:2008. *Health informatics — Information security management in health using ISO/IEC 27002*. , (2008).

JOGIYANTO. (2007). *Model Kesuksesan Sistem Teknologi Informasi*. Yogyakarta: Andi Publisher.

KAMALIAH, A. (2020). Data Pribadi Marak Dijual di Dark Web, Kalau Kena Bagaimana?

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA. *Peraturan Pemerintah Republik Indonesia. Nomor 46 Tahun 2014. Tentang. Sistem Informasi Kesehatan*. , (2014).

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA. *Peraturan Menteri Kesehatan No 97 Tahun 2015*. , (2015).

MUKHAROMAH, V. F. (2020). Data Pasien Covid-19 Diduga Bocor, Mengapa Hal Ini Bisa Terjadi? Retrieved September 5, 2020, from Kompas website: https://www.kompas.com/tren/read/2020/06/20/180500065/data-pasien-covid-19-diduga-bocor-mengapa-hal-ini-bisa-terjadi?page=all

SAMUEL, R. (2018). Serangan Masif Cyber Attack Global. Retrieved September 2, 2020, from KOMITE.ID website: https://www.komite.id/2018/06/26/serangan-masif-cyber-attack-global/

SENDARI, A. A. (2019). 12 Jenis Virus Komputer yang Perlu Diwaspadai, Bisa Rusak komputer.

SINUHAJI, J. (2020). Data Bocor, Kasus COVID-19 di Tiongkok Disebut 8 Kali Lebih Banyak dari yang Dilaporkan. Retrieved September 5, 2020, from Pikiran Rakyat website: https://www.pikiran-rakyat.com/internasional/pr-01383375/data-bocor-kasus-covid-19-di-tiongkok-disebut-8-kali-lebih-banyak-dari-yang-dilaporkan

WIDUP, S. (2019). *2019 Verizon Data Breach Investigations Report*. United State.

WIJAYANTO, H. (2020). *Policy Brief : Kesiapan Perguruan Tinggi Wilayah Jawa Tengah Dalam Menghadapi Serangan Siber*. Indonesia: Lembaga Penelitian dan Pengabdian pada Masyarakat Universitas Dian Nuswantoro.

WIJAYANTO, H., MUHAMMAD, A. H., & HARIYADI, D. (2020). Analisis Penyalahgunaan Data Pribadi Dalam Aplikasi Fintech Ilegal Dengan Metode Hibrid. *Jurnal Ilmiah SINUS*, *18*(1), 1–10. https://doi.org/10.30646/sinus.v18i1.433