Jurnal Kesehatan Vokasional, Vol. 4 No. 2 (Mei 2019)
ISSN 2541-0644 (print), ISSN 2599-3275 (online)
DOI https://doi.org/10.22146/jkesvo.44409

Analisis Budaya Keamanan Informasi Di Puskesmas Kota Bandung

Syaza Syauqina[1], Puspita Kencana Sari[2], Adhi Prasetio[3], Candiwan[4]
Prodi S1 MBTI, Fakultas Ekonomi dan Bisnis, Universitas Telkom[1,2,3,4]
emailsyau@gmail.com[1]

Diajukan 24 Maret 2019 *Diperbaiki* 13 Mei 2019 *Diterima* 28 Mei 2019

ABSTRAK

Latar Belakang: Penggunaan sistem informasi saat ini menjadi kebutuhan dalam organisasi, termasuk di bidang kesehatan karena besarnya data pasien yang harus dikelola. 95% warga Kota Bandung berhak atas layanan fasilitas kesehatan yang telah bemitra dengan BPJS, salah satunya Puskesmas. Puskesmas mengelola data kesehatan pasien menggunakan SIMPus berbasis komputer. Informasi kesehatan pribadi rentan terhadap ancaman keamanan informasi baik dari internal maupun eksternal. Oleh karena itu dibutuhkan keamanan informasi untuk mengurangi tingkat pelanggaran keamanan dan menjaga informasi kesehatan pasiennya.

Tujuan: Tujuan penelitian ini adalah untuk mengetahui faktor - faktor yang mempengaruhi Budaya Keamaan Informasi di Puskesmas Kota Bandung.

Metode: Metode penelitian yang digunakan adalah metode kuantitatif dengan Teknik analisis data PLS-SEM menggunakan Software WarpPLS 6.0, dengan Evaluasi Model yang terdiri dari Model Pengukuran,Model Struktural dan Pengujian Hipotesis. Data penelitian ini menggunakan data primer yang diambil melalui kuisioner kepada 154 pegawai di yang dijadikan sampel.

Hasil: Sebagian besar pegawai puskesmas adalah wanita, usia terbanyak adalah 19-29 tahun, jabatan terbanyak adalah Administrasi/Rekam Medis, Pendidikan pegawai adalah S1, Lama Bekerja pegawai adalah 1-5 tahun. Dalam proses pengelolaan informasi, Puskesmas telah menggunakan *Computer Based*. Puskesmas memiliki Kebijakan Keamanan Informasi. Berdasarkan Evaluasi Model dapat diketahui bahwa model sudah baik karena sudah memenuhi kriteria *Rule of Thumb*.

Kesimpulan: Dapat disimpulkan bahwa variabel yang mempengaruhi Budaya Kemanan Informasi di Puskesmas Kota Bandung adalah *Management, Change Management, Knowledge, Soft Issue-Workplace Independent* dan *Attitude*.

Kata Kunci: budaya keamanan informasi; layanan kesehatan; pls-sem

ABSTRACT

Background: *The utilization of information systems is neccesary in organizations, including in the health sector. 95% of Bandung City citizens are entitled to health facility services (Puskesmas) that have been partnered with BPJS Kesehatan. It is manages using computer-based; SIMPus, personal health information which is vulnerable to security threats both from internal and external. Needed to build information security to reduce the level of security violations and maintain the health information.*

Objective: *To determine the factors that influence the Culture of Information Security in Puskesmas Bandung .*

Methods: *The research method used is a quantitative method with PLS-SEM data analysis technique using WarpPLS 6.0 software with model evaluation consisting of Measurement Models, Structural Models and Hypothesis Testing. It uses primary data taken through questionnaires to 154 employees who were sampled*

Results: *The majority of health center employees are women, the highest age is 19-29 years, the most positions are Administration / Medical Records, Education of employees is S1, lenght of work of Employees is 1-5 years. In the information management process, the Puskesmas has used Computer Based. The Puskesmas has an Information Security Policy. Based on the Evaluation Model, it can be seen that the model is fit, because it meets the Rule of Thumb criteria.*

Conclusion: *It can conclude that the variables that influence the Information Security Culture in Bandung City Health Center are Management, Change Management, Knowledge, Soft Issue-Workplace Independent and Attitude.*

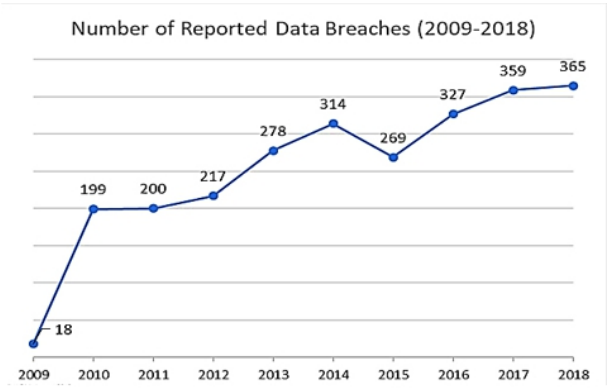
Keywords: *information security culture; healthcare; pls-sem*

PENDAHULUAN

Menurut Ponemon Institute dan Verizon Data Breach Investigations Report, industri kesehatan mengalami lebih banyak pelanggaran data daripada sektor lainnya (Center for Internet Security, 2018) Pelanggaran pada sektor kesehatan disebabkan oleh berbagai jenis insiden, yaitu pencurian oleh *malware*, karyawan yang secara sengaja atau tidak sengaja mengungkapkan data pasien, dan laptop atau perangkat lain yang hilang.

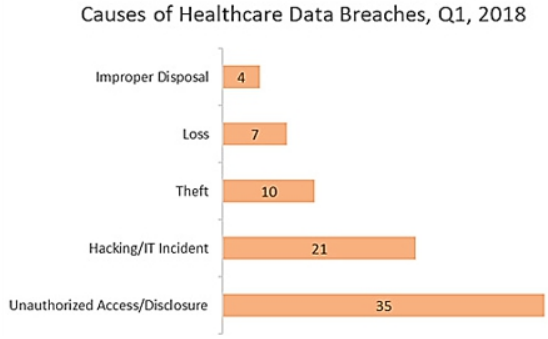
Informasi Kesehatan Pribadi *(Personal Health Information/PHI*) lebih berharga di pasar gelap daripada informasi kartu kredit atau Informasi Identifikasi Pribadi (*Personal Identification Information*) biasa. Oleh karena itu, ada insentif yang lebih tinggi bagi para penjahat *cyber* untuk menargetkan database medis, sehingga mereka dapat menjual PHI atau menggunakannya untuk keuntungan pribadi mereka. Informasi kartu kredit dan data pribadi dijual seharga $1 - $2 di pasar gelap, tetapi PHI dapat dijual sebesar $363 menurut *Infosec Institute*. PHI berharga karena pelaku kriminal dapat menggunakannya untuk menargetkan korban dengan penipuan yang memanfaatkan kondisi medis korban atau permukiman korban. Ini dapat digunakan untuk membuat klaim asuransi palsu, memungkinkan untuk pembelian dan penjualan kembali peralatan medis. Penjahat lain menggunakan PHI untuk secara ilegal mendapatkan akses ke resep untuk digunakan atau dijual kembali.

Menurut "2018 Thales Data Threat Report", 70% organisasi layanan kesehatan di seluruh dunia telah mengalami pelanggaran data (Shick, 2018). Laporan Thales mengatakan organisasi kesehatan telah muncul sebagai target utama untuk peretas, menempatkan data medis yang berharga dalam bahaya. Verizon "*2018 Protected Health Information Data Breach Report (PHIDBR)*" mengungkapkan bahwa hampir 6 dari 10 pelanggaran keamanan dalam layanan kesehatan berasal dari karyawan yang jahat atau lalai. Penelitian lain dari firma konsultan Accenture menemukan bahwa hampir seperempat karyawan layanan kesehatan AS mengetahui setidaknya satu rekan kerja yang secara ilegal telah menjual nama pengguna, kata sandi atau informasi pribadi lainnya kepada pihak luar yang tidak sah.



Gambar 1. Pelanggaran Keamanan Informasi Pada Penyedia Layanan Kesehatan di AS

Dilihat dari *www.hipaajournal.com* antara tahun 2009 dan 2017 ada 2.181 pelanggaran data kesehatan yang melibatkan lebih dari 500 rekaman (*record*). Pelanggaran tersebut telah mengakibatkan pencurian / pemaparan dari 176,709,305 catatan kesehatan atau setara dengan lebih dari 50% populasi Amerika Serikat (54,25%).



Gambar 2. Sumber Pelanggaran Data di Penyedia Layanan Kesehatan

Dapat dilihat dari Gambar 2 antara 1 Januari hingga 31 Maret 2018, sebanyak 1.073.766 orang mengalami pencurian atau pengungkapan PHI mereka, jauh lebih banyak dibandingkan dengan pelanggaran di Q4, 2017 sebanyak 520.141 orang (HIPAA Journal (b), 2018).

Di industri lain, peretasan / insiden IT mendominasi laporan pelanggaran; namun,

industri kesehatan berbeda karena pelanggaran data lebih banyak disebabkan oleh orang dalam (karyawan). Di Indonesia sendiri, serangan cybercrime terhadap industri kesehatan terjadi di pertengahan tahun 2017 dimana dua rumah sakit besar diserang oleh Ransomware WannyCry (CNN Indonesia, 2017). Laporan KompasTV pada bulan Oktober 2018, telah terjadi kehilangan computer di Puskesmas Gebang, Kab, Cirebon Jawa Barat. Akibat dari serangan ini, semua aktivitas pelayanannya terganggu, hal ini tentunya merugikan baik dari pihak Fasilitas Kesehatan dann juga Pasien.

Berdasarkan data BPJS Kesehatan mencatat, sampai dengan 1 September 2018, sebanyak 201.660.548 jiwa penduduk di Indonesia telah menjadi peserta JKN-KIS. Jumlah ini hampir mencakup seluruh populasi masyarakat Indonesia. Pasien yang ingin mendapatkan pelayanan kesehatan menggunakan BPJS Kesehatan harus melalui Faskes Tingkat Pertama (FKTP) terlebih dahulu. Jika membutuhkan rawatan lebih lanjut, maka pasien akan dirujuk ke Faskes Rujukan Tingkat Lanjut (FKRTL). Pada penelitian ini, objek penelitian dibatasi pada Faskes yang terdaftar di BPJS Kesehatan yang ada di Kota Bandung. Di antara Fasilitas Kesehatan yang ada penulis memilih Puskesmas yang merupakan Faskes Tingkat Pertama sebagai objek penelitian karena menurut data BPJS sebaran FKTP terbanyak di Indonesia pada Data BPJS Kesehatan tahun 2018 adalah Puskesmas yaitu sebesar 6.436 Puskesmas. Puskesmas merupakan *gatekeeper* atau sebagai kontak pertama pada pelayanan kesehatan formal dan penapis rujukan sesuai dengan pedoman pelayanan medik. Puskesmas juga sebagai layanan primer yang letaknya berada paling dekat di tengah-tengah masyarakat dan mudah dijangkau dibandingkan dengan unit pelayanan kesehatan lainnya.

Dalam pelayanannya, tiap Puskesmas akan men-*generate*, menyimpan, mengelola, dan menggunakan data kesehatan pasien mulai dari administrasi hingga catatan kesehatan pasien, menggunakan SIMPus yang berbasis elektronik / komputer. Dengan demikian, informasi kesehatan pribadi (PHI) peserta JKN tersebut rentan terhadap ancaman keamanan informasi baik dari internal maupun dari eksternal. Maka dari itu dalam upaya melindungi aset informasi, di perlukan keamanan informasi. Tujuan dari keamanan informasi adalah untuk memastikan keberlangsungan organisasi dan untuk meminimalisir kerugian organisasi dengan mencegah dan meminimilisir dampak dari insiden keamanan (Kruger, Drevin, dan Steyn, 2010). Keamanan informasi memiliki tiga komponen dasar yang harus dikelola, yaitu Kerahasiaan (*confidentiality*), Integritas (*integrity*) dan Ketersediaan (*availability*).

Salah satu bagian terpenting dari manajemen keamanan informasi adalah program kesadaran keamanan informasi. Menurut Kruger dan Kearney (2006) sasaran utama dari *information security awareness* adalah memastikan bahwa pengguna komputer sadar akan risiko-risiko terkait penggunaan teknologi informasi dan juga pemahaman terhadap kebijakan dan prosedur yang berlaku. Program kesadaran informasi ini perlu dilakukan oleh pemilik sistem sebagai bagian dari manajemen teknologi informasi.

Seperti yang dikatakan oleh Peltier (2014) bahwa pemilik sistem bertangggung jawab untuk memberikan pengetahuan yang mumpuni mengenai keberadaan dan tingkat umum pengendalian yang berlaku sehingga semua pengguna yakin bahwa sistem tersebut aman. Selain meningkatkan keamanan aplikasi dan jaringan melalui berbagai mekanisme kendali teknis, pelatihan tentang penggunaan dan penanganan PHI yang tepat dianjurkan untuk mengurangi pelanggaran data yang disebabkan oleh kesalahan karyawan, seperti perangkat yang hilang atau pengungkapan yang tidak disengaja.

Untuk itu, penelitian ini bertujuan untuk mengetahui variabel apa saja yang mempengaruhi Budaya Keamaan Informasi

secara signifikan di Puskesmas Kota Bandung . Berikut adalah Kerangka Pemikiran dari penelitian ini

Gambar 4. Kerangka Pemikiran

METODE

Penelitian ini menggunakan metode kuantitatif. Berdasarkan tujuannya, penelitian ini termasuk penelitian hubungan/korelasi. Berdasarkan tipe penyelidikan penelitian ini adalah penelitian kausal. Dalam penelitian ini peneliti tidak mengintervensi data dan waktu pelaksanaan penelitian ini adalah cross-sectional. Penelitian ini dilaksanakan selama 4 bulan terhitung mulai bulan September 2018 sampai dengan Februari 2019 yang dilakukan di 22 Puskesmas Kota Bandung.

Pada penelitian ini model budaya keamanan informasi diukur melalui 14 variabel eksogen dan 1 variabel endogen. Variabel eksogen terdiri dari *Management, Workplace Capabilities, Risk and Response Factors, Operational Management, Change Management, Organizational Culture, Knowledge, Security Compliance, Soft Issues - Workplace Independent , Security Behaviour, Training and Awareness, Information Security Culture, Perceived Security Threats,* dan *Attitude.* Sedangkan variable endogen terdiri atas *Information Security Culture.*

Data penelitian ini menggunakan data primer yang diambil melalui kuisioner di Puskesmas telah dijadikan sample. Populasi dari penelitian ini adalah seluruh pegawai Puskesmas di Kota Bandung. Pengumpulan data akan dilakukan dengan cara penyebaran kuesioner kepada 154 pegawai yang menjadi responden.

Teknik sampling yang digunakan adalah *nonprobability sampling.* Jumlah sampel minimum yang diperlukan adalah sepuluh kali dari jumlah jalur terbanyak yang menuju ke sebuah variable (Hair, 2011). Dalam penelitian ini jumlah jalur terbanyak adalah jalur yang menuju ke variable *Information Security* culture yaitu 14 jalur, sehingga sampel minimum adalah 150 sampel. Data yang terkumpul akan dianalisis lebih lanjut dengan teknik analisis *Partially Least Square Structural Equation Modeling* (PLS-SEM).

Uji validitas item pertanyaan dilakukan dengan menghitung korelasi item total karena jumlah item pertanyaan (i) > 30.

Perhitungan rxi menggunakan rumus berikut ini (Kusnendi, 2008:94).

$$r_{xi} = \frac{n\sum XY - (\sum X)(\sum Y)}{\sqrt{[n\sum X^2 - (\sum X^2][n\sum X^2 - (\sum X^2)]}}$$

di mana :

X = skor item ,

Y = skor total

n = jumlah item pertanyaan

Dalam uji validitas setiap item pertanyaan membandingkan r_{hitung} dengan r_{tabel}. Penentuan r_{tabel} dengan menggunakan tabel harga titik dari Pearson Product Moment dengan jumlah sampel (n) sebanyak 30 orang dan taraf signifikan 0,05 adalah sebesar 0,361.

Kriteria batas minimal butir pernyataan yang diterima adalah r_{tabel} 0,361, sehingga diketahui

- Jika $r_{hitung} > r_{tabel}$ maka instrumen dianggap valid.
- Jika $r_{hitung} < r_{tabel}$ maka instrumen dianggap tidak valid (drop), sehingga instrumen tidak dapat digunakan dalam penelitian.

Dari hasil pengujian Validitas dapat diketahui bahwa kuesioner dinyatakan valid sebanyak dengan 49 pernyataan, karena setiap item pernyataan tersebut memiliki r_{hitung} lebih besar dari r_{tabel} (0,361), sehingga pernyataan tersebut dapat dijadikan sebagai alat ukur

untuk variabel yang diteliti. Uji reliabilitas kuesioner menggunakan *Cronbach's Alpha*. Berikut adalah rumus dari Cronbach's Alpha menurut Kusnendi (2008:97) :

$$\alpha = \left(\frac{N}{(N-1)}\right)\left(1 - \frac{\sum \sigma^2_{item}}{\sigma^2_{total}}\right)$$

α = koefisien reliabilitas instrument Cronbach'sAlpha
N = banyaknya pertanyaan
σ^2item = variance dari pertanyaan
σ^2total = variance dari skor

Dari hasil perhitungan di atas, diketahui bahwa hasil uji reliabilitas dengan rumus *Cronbach's Alpha* memiliki nilai ≥ 0.7. Hal ini menunjukkan bahwa semua instrumen reliabel. Setelah model dibuat diagramnya, maka model siap diproses untuk estimasi dan evaluasi. Evaluasi model pada PLS-SEM yang menggunakan WarpPLS dapat dilakukan dengan mengevaluasi hasil dari Pengukuran Model.

Penelitian ini menggunakan indikator reflektif, sehingga penilaian hasil model pengukuran dilakukan melalui analisis faktor konfirmatori dengan cara menguji validitas dan reliabilitas konstruk laten. Langkah evaluasi selanjutnya adalah melakukan pengujian signifikansi untuk menguji pengaruh antar konstruk dan model fit.

Model Pengukuran

Measurement model atau *outer model* merupakan model pengukuran yang bersifat *reflective* dan menunjukkan bagaimana variabel *manifest* atau *observed variabel* merepresentasi konstruk laten. Pengujiannya dilakukan dengan melakukan uji validitas dan reliabilitas dari indikator-indikator pembentuk konstruk laten tersebut melalui analisis faktor konfirmatori (Ghozali & Latan, 2014).

Uji validitas yang dilakukan dalam evaluasi model pengukuran PLS-SEM adalah uji validitas internal, validitas internal (*internal validity*) menunjukkan kemampuan dari instrumen penelitian untuk mengukur apa yang seharusnya diukur dari suatu konsep.. Pengukuran model melalui analisis faktor konfirmatori adalah dengan menggunakan pendekatan *Multi Trait-Multi Method* dengan menguji Validitas *Convergent* dan *Discriminant (Ghozali & Latan, 2014)*

Model Struktural

Kualitas model yang dihasilkan dalam penelitian ini akan diukur dengan menggunakan model *fit* indeks. WarpPLS versi 6.0 menyajikan beberapa indeks untuk mengukur model *fit*.

Meskipun demikian, interpretasi indeks model *fit* tergantung pada tujuan dari analisis SEM. Jika tujuannya adalah untuk menguji hipotesis, maka indeks model *fit* berguna untuk mengatur langkah-langkah yang terkait dengan kualitas model (Kock, 2018). Tabel 1 akan menunjukkan *Rule Of Thumb Pengujian* Model *Fit* sebagaimana disampaikan oleh (Kock, 2018).

Tabel 1. *Rule Of Thumb* Pengujian Model Fit

Index	Kriteria
Average Path Coefficient (APC)	P = 0.05
Average R-Squared (ARS)	P = 0.05
Average Adj R-Squared (AARS)	P = 0.05
Average Block VIF (AVIF)	acceptable if = 5, ideally =3.3
Average Full Collinearity VIF (AFVIF)	acceptable if = 5, ideally =3.3
Tenenhaus Gof (Gof)	small = 0.1 , medium =0.25, large = 0.36
Sympson's Paradox Ratio (SPR)	acceptable if = 0.7 ,ideally = 1
R-Squared Contribution Ratio(RSCR)	acceptable if = 0.9 ,ideally = 1
Statistical Suppression Ratio(SSR)	acceptable if = 0.7
Nonlinear Bivariate Causality Direction Ratio (NLBCDR)	acceptable if = 0.7

Uji hipotesis dalam penelitian ini digunakan untuk membuktikan ada atau tidaknya pengaruh antara masing - masing variabel terhadap variabel yang lain.

Software WarpPLS 6.0 juga menyajikan nilai koefisien regresi untuk masing-masing hubungan antar konstruk. Koefisien ini dapat menunjukkan seberapa besar pengaruh dari variabel satu ke variabel yang lainnya. Pengujian hipotesis dalam analisis SEM ini dilakukan dengan melihat nilai *probability* (P), jika P< 0,05 maka Hipotesis akan diterima.

HASIL DAN PEMBAHASAN

Berdasarkan data BPJS Tahun 2018 jumlah Puskesmas di Kota Bandung yang terdaftar di BPJS adalah sebanyak 73 Puskesmas. Pada penelitian ini, penulis hanya menggambil 22 Puskesmas dengan hal ini di karenakan minimum sample adalah 150 responden. Jadi dengan mengambil responden dari 22 Puskesmas, maka jumlah sampel minimum sudah terpenuhi. Berikut adalah Daftar Puskesmas yang penulis jadikan objek penelitian :

Tabel 2. Daftar Puskesmas

Nama Puskesmas	Kecamatan
UPT Puskesmas Sukajadi	Sukajadi
UPT Puskesmas Paskal	Cicendo
UPT Puskesmas Garuda	Andir
UPT Puskesmas Salam Puskesmas Taman Sari	Bandung Wetan
UPT Puskesmas Tamblong Puskesmas Balai Kota	Sumur Bandung
UPT Puskesmas Padasuka	CibeunyingKidul
UPT Puskesmas BB Sari Puskesmas BB Surabaya	Kiaracondong
Puskesmas Ibrahim Aji Puskesmas Ahmad Yani Puskesmas Talagabodas	Batununggal
Puskesmas Suryalaya Puskesmas Cijagra Baru Puskesmas Cijagra Lama	Lengkong
UPT Puskesmas Pasundan	Regol
UPT Puskesmas Pagarsih Puskesmas Astana Anyar	Astana Anyar
Puskesmas Sukapakir	Bojongloa Kaler
UPT Puskesmas Kopo	Bojongloa Kidul
UPT Puskesmas Caringin	Babakan Ciparay

Karakteristik Responden

Detail demografi responden dapat dilihat pada tabel di bawah ini :

Tabel 3. Profil Responden

Keterangan		Jumlah
Jenis Kelamin	Pria	25(16%)
	Wanita	129(84%)
Usia	=18 Tahun	0
	19 – 29 Tahun	64 (42%)
	30 – 39 Tahun	43 (27%)
	=40 Tahun	48 (31%)
Pendidikan Terakhir	SMA/SMK	10 (6%)
	D1/D2/D3	61 (40%)
	S1	78 (51%)
	S2/S3	5 (3%)
Jabatan	Administrasi / Rekam Medis	40
	Dokter Umum / Dokter Gigi	38
	Perawat	30
	Bidan	25
	Ka.Puskesmas / Manajer / KaBagian	14
	Pegawai IT	6
	Dokter Spesialis	1
Lama Bekerja	< 1 Tahun	32 (20%)
	1 - 5 Tahun	60 (39%)
	5 – 10 Tahun	19 (13%)
	> 10 Tahun	43 (28%)
Pengelolaan Informasi	Manual / Paper Based	0
	Elektronik / Computer Based	0
	Campuran	154(100%)
Kebijakan Keamanan Informasi	Ya	154(100%)
	Tidak	0

Untuk analisis penelitian ini penulis menggunakan Teknik analisis PLS-SEM dengan menggunakan bantuan *Software WarpPLS 6.0* dengan dua tahap analisis, yaitu Analisis Model Pengukuran dan Analisis Model Struktural.

Evaluasi Model Pengukuran Outer ini menggunakan 3 evaluasi model yaitu :

1. *Convergent Validity*. Dari model pengukuran dapat dilihat dari korelasi antara skor indikator dengan skor kontruknya

(loading *Factor*) dengan kriteria nilai loading *Factor* dari setiap indikator lebih besar dari 0.5 dapat dikatakan valid (Kock, 2018). Hasil perhitungan *WarpPLS 6.0* menunjukkan bahwa masing - masing nilai pada *Cross-Loadings Factor* telah mencapai nilai diatas 0.5 dengan nilai P < 0,001. Dengan demikian kriteria uji validitas konvergen telah terpenuhi. Hal ini berarti semua indikator - indikator diatas valid serta dapat digunakan dalam model. Dalam penelitian ini, untuk mengukur *Convergent Validity* dapat dilakukan dengan melihat hasil dari *WarpPLS 6.0* pada bagian *Average Variance Extracted* (AVE). Kriteria penilaiannya adalah nilai AVE > 0.5 . Hasil dari konstruk – konstruk tersebut menunjukan bahwa nilai AVE dari semua kontruk yang dihasilkan lebih besar dari 0.5. Berdasarkan kriteria AVE, hasil tersebut telah menunjukan *Convergent Validity* yang dikatakan baik.

2. Validitas Diskriminan , Untuk Uji ini menggunakan perbandingan akar dari AVE dengan korelasi antar variabel. Nilai AVE konstruk seharusnya lebih tinggi dibandingkan dengan korelasi antar variabel *Laten* (Kock 2018). Hasil perhitungan *WarpPLS 6.0* menunjukkan bahwa nilai akar AVE variabel yang sama telah lebih tinggi dari pada nilai akar AVE pada variabel yang berbeda.Hal ini menunjukkan bahwa kriteria uji validitas diskriminan telah terpenuhi. Dengan demikian instrumen yang digunakan dalam penelitian ini telah memenuhi semua ketentuan uji validitas.
3. Uji Reabilitas , Masing – masing konstruk memiliki realibility yang tinggi dimana hal ini dapat dilihat dari nilai *Composite Realibility* seluruh konstruk lebih besar dari 0.70 (Kock, 2018).

Setelah melakukan Evaluasi Model Pengukuran dimana *Convergent Validity*, *Discriminant Validity*, dan *Composite Realibility* telah memenuhi syarat, tahap selanjutnya adalah melakukan Evaluasi Struktural . Uji kecocokan model (model *fit*) ini digunakan untuk mengetahui apakah suaru model memiliki kecocokan dengan data.

Tabel. 4 ***Model fit and Quality Indices***

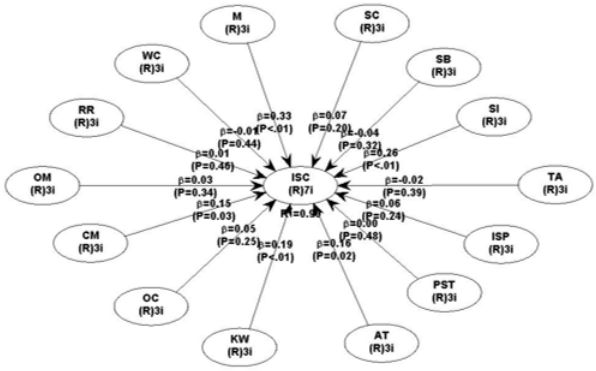
Kriteria	Nilai	Ket
APC	0.099 , P=0.05	Terima
ARS	0.904 , P<0.001	Terima
AARS	0.894 , P<0.001	Terima
AVIF	3.924	Terima
AFVIF	3.734	Terima
GoF	0.795	Terima, Large
SPR	0.786	Terima
RSCR	0.952	Terima
SSR	1	Terima
NLBCDR	1	Terima

Dari hasil *output* general result pada tabel diatas dapat dilihat bahwa :

- Model mempunyai *fit* yang baik, dimana nilai *P-Value* untuk APC, ARS, dan AARS lebih kecil atau sama dengan dari 0.05 dengan nilai APC = 0.099, ARS = 0.904,AARS= 0.894.
- Begitu juga dengan nilai AVIF (3.924) dan AFVIF (3.734), yang di hasilkan yaitu ≤ 5, *ideally* ≤ 3.3, yg berarti bahwa tidak ada masalah m*ultikolonieritass* antar *indicator* dan antar *variable eksogen*.
- GoF yang dihasilkan yaitu 0.795 > 0.36 yang berarti *fit* model sangat baik.
- Untuk index SPR (0.786), RSCR (0.952), SSR (1), NLBCDR (1) yang berarti tidak ada *problem* kausalitas didalam model.

Kesimpulannya adalah model sudah *fit* dengan data sehingga dapat melanjutkan pengujian berikutnya.

Berikut merupakan gambar model penelitian, beserta hasil yang telah diperoleh berdasarkan pengolahan data dengan menggunakan program *WarpPLS 6.0* :



Gambar 5. Model SEM

Dari model tersebut dapat diperoleh nilai Adjusted R-squared sebesar 0.894. Ini brarti termasuk dalam kategori besar dan menunjukkan variasi Information Security Culture yang dapat dijelaskan oleh 14 variabel eksogen sebesar 89.4% dan sisanya 10.6% di pengaruhi oleh variabel lain diluar model.

Untuk mengevaluasi hubungan struktural antar variabel Laten, harus dilakukan pengujian hipotesis terhadap koefisien jalur antara variabel dengan membandingkan angka P-Value dengan 0.05. Besarnya P-Value diperoleh dari output pada WarpPLS 6.0. Pengujian seluruh hipotesis akan dianalisis berdasarkan hasil yang diperoleh dari pengolahan data pada tabel berikut :

Tabel 5. ***Direct Effect***

Hub	(β)	*P-Values*	Keputusan
MGT→ISC	0.329	0.001	Signifikan
WC → *ISC*	-0.011	0.443	Tidak
RR → *ISC*	0.009	0.457	Tidak
OM → *ISC*	0.034	0.338	Tidak
CM → *ISC*	0.146	0.032	Signifikan
OC→ *ISC*	0.053	0.252	Tidak
KW → *ISC*	0.189	0.008	Signifikan
SC → *ISC*	0.068	0.196	Tidak
SB → *ISC*	-0.037	0.323	Tidak
SW → *ISC*	0.264	0.001	Signifikan
TA → *ISC*	-0.023	0.388	Tidak
ISP → *ISC*	0.055	0.245	Tidak
PST → *ISC*	0.003	0.484	Tidak
AT→ *ISC*	0.158	0.022	Signifikan

KESIMPULAN

Berdasarkan hasil analisis yang telah dilakukan, diperoleh kesimpulan yang dapat memberikan jawaban terhadap pertanyaan penelitian dan tujuan pada penelitian ini. Dari 14 variabel yang mempengaruhi Budaya Kemanan Informasi *(Information Security Culture)*, terdapat 5 variabel yang memiliki pengaruh yang signifikan terhadap Information Security Culture di Puskesmas Kota Bandung yaitu: *Management* (M), *Change Management* (CM), *Knowledge* (K), *Soft Issue –Workplace Independent* (SI) dan *Attitude* (AT).

Faktor-faktor yang memiliki pengaruh terhadap Budaya Kemanan Informasi *(Information Security Culture) ini yaitu Management* (M) dan *Change Management* (CM) berasal dari eksternal individu, dalam kasus ini merupakan instalasi atau divisi di Puskesmas. Knowledge (K) bisa didapatkan dari pengaruh internal dan eksternal individu dari Puskesmas. Sedangkan *Soft Issue - Workplace Independent* (SI) dan *Attitude* (AT). berasal dari Internal individu disuatu organisasi, hal ini mencerminkan tindakan / penerapan dan pengalaman masing-masing individu di Puskesmas.

Saran Bagi Puskesmas Kota Bandung :

Puskesmas di Kota Bandung secara umum perlu meningkatkan keamanan informasi mereka dengan melihat dari 2 aspek yaitu dari Organisasi dan Individu.

- Untuk organisasi , tentunya perlu ditingkatkan dimulai dari Top Management dari Puskesmas itu sendiri agar bisa langsung mengarahkan ke personil-personil di puskesmas agar kebijakan-kebijakan terkait keamanan Informasi dapat disadari oleh para-personil-personilnya.
- Untuk Individu, tentunya penting bagi para pegawai Puskesmas untuk memiliki kesadaran dan pengetahuan tentang pentingnya perlindungan sebuah asset informasi. Hal ini karena para pegawai inilah yang secara langsung berhubungan dengan data-data pasien.

Maka dari itu diharapkan bagi seluruh personil Puskesmas yang ada agar dapat menyadari akan pentingnya Keamanan informasi dan menerapkan kebijakan-

kebijakan terkait keamanan informasi di Puskesmas tempat mereka bekerja.

Saran Bagi Penelitian Selanjutnya :

1. Dalam penelitian ini penulis masih belum memasukkan seluruh faktor-faktor yang dikemukakan oleh beberapa peneliti sebelumnya dikarenakan keterbatasan bahasa yang mana dasar utama penelitian ini menggunakan beberapa penelitian sebelumnya yang dilakukan di luar negeri. Hal ini sejalan dengan hasil output Adj R-squared pada WarpPLS yang mana sebesar 10.6% ISC dipengaruhi oleh variabel lain diluar model. Maka dari itu diharapkan pada penelitian selanjutnya dapat mencari faktor-faktor lainnya yang mempengaruhi ISC, karena belum tentu semua faktor akan berpengaruh terhadap Information Security Culture.
2. Meskipun dalam penelitian ini jumlah sampel telah memenuhi persyaratan representativeness dan sample size rules, diharapkan pada penelitian selanjutnya samplena perlu diperbesar sehingga hasilnya dapat digunakan untuk mengeneralisir kondisi Fasilitas Kesehatan yang ada di Indonesia.
3. Dasar utama penelitian ini menggunakan beberapa penelitian sebelumnya yang dilakukan di luar negeri dan objeknya selain bidang kesehatan. Diharapkan pada penelitian selanjutnya untuk dapat mengangkat objek pada bidang lainnya khususnya di Indonesia sehingga dapat terlihat perbedaan pengaruh terhadap *Information Security Culture.*

DAFTAR PUSTAKA

Ashford, W. (2018) Most healthcare organisations have been breached, report shows, ComputerWeekly.com. Available at:https://www.computerweekly.com/news/252436215/Most-healthcare-organisations-have-been-breached-report-shows.

Box, D. and Pottas, D. (2013) 'Improving Information Security Behaviour in the Healthcare Context', Procedia Technology. Elsevier B.V., 9, pp. 1093–1103. doi: 10.1016/j.protcy.2013.12.122.

BPJS Kesehatan (2018) Data Fasilitas Kesehatan BPJS Kesehatan, https://faskes.bpjs-kesehatan.go.id. Available at: https://faskes.bpjs-kesehatan.go.id/aplicares/#/app/peta.

Center for Internet Security (2018) Data Breaches: In the Healthcare Sectors, www.cisecurity.org. Available at: www.cisecurity.org/data-breaches-in-the-healthcare-sector/.

CNN Indonesia and Kertopati, L. (2017) Dua Rumah Sakit di Jakarta Kena Serangan Ransomware WannaCry, www.cnnindonesia.com. Available at: https://www.cnnindonesia.com/teknologi/20170513191519-192-214642/dua-rumah-sakit-di-jakarta-kena-serangan-ransomware-wannacry (Accessed: 3 November 2018).

Da Veiga, A. and Martins, N. (2017) 'Defining and identifying dominant information security cultures and subcultures', Computers and Security, 70, pp. 72–94. doi: 10.1016/j.cose.2017.05.002.

Da Veiga, A. and Martins, N. (2015) 'Improving the information security culture through monitoring and implementation actions illustrated through a case study', Computers and Security, 49(December 2017), pp. 162–176. doi: 10.1016/j.cose.2014.12.006.

Ghozali, I. and Latan, H. (2014) Partial Least Square Konsep, Metode dan Aplikasi Menggunkan Program Aplikasi WarpPLS 5.0. Semarang: Universitas Diponegoro.

Hair, J. F., Christian, M. and Sarstedt, M. (2011) 'PLS-SEM : Indeed a Silver Bullet', Journal of Marketing Theory and Practice, 19(2), pp. 139–152.

Hassan, N. H. and Ismail, Z. (2016) 'Information security culture in healthcare informatics:

A preliminary investigation', Journal of Theoretical and Applied Information Technology, 88(2), pp. 202–209. doi: doi:10.1817/jatit.2016.04.

HIPAA Journal (a) (2018) Report: Healthcare Data Breaches in Q1, 2018, www.hipaajournal.com. Available at: https://www.hipaajournal.com/report-healthcare-data-breaches-in-q1-2018/.

HIPAA Journal (b) (2018) Analysis of Q4 2017 Healthcare Security Breaches, www.hipaajournal.com. Available at: https://www.hipaajournal.com/analysis-q4-2017-healthcare-security-breaches/.

HIPAA Journal (c) (2018) Healthcare Data Breach Statistics, www.hipaajournal.com. Available at: https://www.hipaajournal.com/healthcare-data-breach-statistics/.

Kock, N. (2018) WarpPLS User Manual Version 6.0.

KompasTV (2018) 6 Komputer Puskesmas di Cirebon Hilang, Pelayanan Terganggu, www.kompas.com. Available at: https://www.kompas.tv/article/34067/6-komputer-puskesmas-di-cirebon-hilang-pelayanan-terganggu (Accessed: 2 November 2018).

Kruger, H. A., Drevin, L. and Steyn, T. (2010) 'A vocabulary test to assess information security awareness', Information Management & Computer Security, 18(5), pp. 316–327. doi: 10.1108/09685221011095236.

Kruger, H. A. and Kearney, W. D. (2006) 'A Prototype for Assesing Information Security Awareness', Elsevier Journal : Computers & Security, pp. 289–296. doi: 10.1016/j.cose.2006.02.008.

Kusnendi (2008) Model-Model Persamaan Struktural. Bandung: ALFABETA.

Menteri Kesehatan RI (2013) 'Peraturan Menteri Kesehatan RI No. 71 Tahun 2013 Tentang Pelayanan Kesehatan pada Jaminan Kesehatan Nasional'.

Menteri Kesehatan RI (2014) Peraturan Menteri Kesehatan RI No. 75 Tahun 2014 Tentang Puskemas.

Peltier, T. R. (2014) Information Security Fundamentals. 2nd edn. Auerbach Publications.

Shick, S. (2018) Security Breaches in Healthcare: 70 Percent Of Organizations Hit Globally, Report Shows, https://securityintelligence.com. Available at: https://securityintelligence.com/news/security-breaches-inhealthcare-70-percent-of-organization-hit-globally-report-shows.

Sugiyono (2018) Metode Penelitian Kuantitatif. Bandung: ALFABETA.

Verizon (2018) Protected Health Information Data Breach Report. Available at: http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf.