Jurnal Mitra Manajemen (JMM Online)
URL : http://e-jurnalmitramanajemen.com

JMM Online
Vol. 3, No. 3, 314-325.

ISSN 2614-0365
e-ISSN 2599-087X

ANALISIS BUDAYA KEAMANAN INFORMASI DI KLINIK PRATAMA KOTA BANDUNG

Eka Fuji Astuti [1)] , Puspita Kencana Sari [2)]
Universitas Telkom

INFORMASI ARTIKEL

Dikirim : 13 Maret 2019
Revisi pertama : 25 Maret 2019
Diterima : 27 Maret 2019
Tersedia online : 28 Maret 2019

Kata Kunci : Keamanan Informasi, Budaya, Layanan Kesehatan

Email :
ekafujias@student.telkomuniversity.ac.id [1)],
puspitakencana@telkomuniversity.ac.id [2)]

ABSTRAK

Penggunaan sistem informasi adalah suatu keharusan dalam suatu organisasi, termasuk dalam industri perawatan kesehatan. Penggunaan data informasi kesehatan digital membuat keamanan informasi sangat penting bagi penyedia layanan kesehatan. Data kesehatan saat ini adalah target dari pelanggaran keamanan karena di nilai lebih tinggi dari informasi kartu kredit. Penelitian ini bertujuan untuk menganalisis budaya keamanan informasi pada penyedia layanan kesehatan. Penelitian ini menggunakan metode sampel dengan teknik Purposive sampling dari populasi berupa pegawai di klinik pratama Kota Bandung. Metode penelitian yang digunakan adalah metode kuantitatif dengan menggunakan teknik analisis data berupa PLS-SEM. Data dari penelitian dikumpulkan dengan cara menyebar kuesioner secara langsung kepada 150 pegawai dari dua puluh lima klinik pratama Kota Bandung. Data diolah dengan software wrapPLS 6.0 dengan melakukan evaluasi model pengukuran, model struktural dan model fit indeks. Berdasarkan hasil pengolahan data menunjukkan bahwa faktor management, knowledge, security behavior, dan attitude mempengaruhi budaya keamanan informasi di klinik pratama Kota Bandung.

PENDAHULUAN

Latar Belakang

Menurut Ponemon Institute dan Verizon data Breach Investigation Report, industri kesehatan mengalami lebih banyak pelanggaran data daripada sektor lainnya (Center for Internet Secuirty, 2018) Pelanggaran sering terjadi di sektor kesehatan dan dapat disebabkan oleh berbagai insiden, terkena serangan virus malware, karyawan yang secara sengaja atau tidak sengaja mengungkapkan informasi pasien, laptop atau perangkat lain yang hilang.

Informasi Kesehatan Pribadi (*Personal Health Information*/PHI) lebih berharga di pasar gelap dibandingkan dengan informasi kartu kredit atau Informasi Identifikasi Pribadi (Personal Identification Information) biasa. 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 mengancam korban dengan melakukan penipuan yang memanfaatkan kondisi medis korban atau tempat tinggal korban. Informasi ini dapat digunakan untuk membuat klaim asuransi palsu, memungkinkan untuk pembelian dan penjualan kembali peralatan medis. Penjahat lain menggunakan PHI secara ilegal untuk mendapatkan akses ke resep untuk digunakan atau dijual kembali. 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.

Menurut "2018 Thales Data Threat Report", 70% organisasi layanan kesehatan di seluruh dunia telah mengalami pelanggaran data (Shick, 2018). Menurut laporan tersebut, sementara transformasi digital memungkinkan perawatan kesehatan yang lebih baik melalui peningkatan efisiensi dengan biaya lebih rendah, pada saat yang sama ia memperkenalkan lebih banyak risiko keamanan melalui penggunaan cloud, big data, internet of things (IoT) dan kontainer untuk membuat, mengelola dan menyimpan data. Laporan Thales mengatakan organisasi kesehatan telah muncul sebagai target utama untuk peretas, menempatkan data medis yang berharga dalam bahaya.

Dari (Hipaajournal(c), 2018), 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%).

Maka pada penelitian ini penulis akan berfokus pada budaya keamanan informasi di fasilitas kesehatan Klinik Pratama. Klinik pratama merupakan fasilitas kesehatan tingkat pertama (FKTP) dimana semua data awal pasien berada pada faskes tingkat pertama. klinik pratama merupakan fasilitas kesehatan tingkat pertama yang memiliki jumlah populasi terbanyak di bandingkan dengan fasilitas kesehatan lainnya, maka dalam penelitian ini objek yang ambil adalah fasilitas kesehatan di Klinik Pratama di Bandung.

Rumusan Masalah

Berdasarkan *survey* dan *report* dari berbagai organisasi yang fokus pada keamanan informasi, diketahui bahwa industri kesehatan menjadi salah satu target dari pelanggaran keamanan (*security breach*) saat ini. Bahkan, informasi kesehatan personal

(PHI) dinilai lebih tinggi dibandingkan informasi identitas personal (PII) dan informasi terkait kartu kredit. Pemilik PHI maupun penyedia fasilitas layanan kesehatan dapat menjadi target cybercrime seperti scamming, ransomware, dan sebagainya. Pelanggaran keamanan informasi tersebut dapat disebabkan oleh berbagai hal seperti hacking, pencurian dan kehilangan perangkat, hingga akses yang tidak sah dan pengungkapan informasi yang dilakukan oleh pegawai yang menjadi penyebab terbesar menurut berbagai laporan. Untuk itu, diperlukan suatu mekanisme pengendalian keamanan untuk mengurangi pelanggaran yang dilakukan oleh pegawai dengan cara meningkatkan budaya dan perilaku keamanan informasi. Sebelum menetapkan mekanisme pengendalian keamanan, perlu dipelajari terlebih dahulu factor-faktor yang dapat mempengaruhi budaya dan perilaku keamanan informasi di fasilitas kesehatan agar program kesadaran lebih efektif dan efisien. Berdasarkan beberapa penelitian terdahulu (Veiga & Martins, 2017), (Alnatheer, 2015), (Flores et al., 2014), (AlHogail, 2015), (Parsons et al, 2014), (Tsohou et al, 2015), (Hassan & Ismail, 2012), (Box & Pottas, 2013), (Ahlan, Lubis, & Lubis, 2015) terdapat delapan faktor yang mempengaruhi budaya keamanan informasi yaitu *Management, Change management, organisational culture, Knowledge, Security compliance, Soft issues workplace independent , Security behaviour, Attitude.*

Tujuan Penelitian

Berdasarkan perumusan masalah di atas, maka tujuan yang akan dicapai dalam penelitian ini adalah mengetahui faktor-faktor apa saja yang mempengaruhi budaya keamaan informasi di fasilitas kesehatan klinik pratama di kota Bandung yang mengelola informasi kesehatan pasien.

KAJIAN PUSTAKA

Manajemen Keamanan Informasi

Pengertian manajemen menurut (Aziz & Irjayanti, 2014) mendefinisikan bahwa seni manajemen meliputi untuk melihat totalitas dari bagian yang terpisah-pisah serta kemampuan untuk menciptakan gambaran suatu visi.

Manajemen memiliki peran penting dalam organisasi dalam membentuk budaya yang diinginkan. Manajemen setiap organisasi perlu mendefinisikan strategi keamanan informasi dan memimpin dengan memberi arahan. (Veiga & Martins, 2017).

Keamaan informasi adalah seperangkat strategi untuk mengelola proses peralatan dan kebijakan yang diperlukan untuk mencegah, mendeteksi, mendokumentasikan dan melawan ancaman terhadap informasi digital dan non digital.

Keamanan informasi dirancang untuk melindungi kerahasiaan, integritas dan ketersediaan data sistem komputer dari mereka yang memiliki niat jahat. (Nasution, 2018).

Istilah keamanan informasi digunakan untuk menggambarkan perlindungan aset informasi, termasuk komputer dan non-komputer peralatan, fasilitas, dan data untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi melalui kebijakan aplikasi, pendidikan dan teknologi. Tujuan dari keamanan informasi adalah untuk menjamin kelangsungan bisnis, meminimalkan kerugian bisnis, dan memaksimalkan laba atas investasi. Oleh karena itu, manajemen organisasi tidak hanya diharapkan

untuk menjaga sumber daya yang aman informasi, tetapi juga diharapkan untuk menjaga organisasi agar dapat terus berfungsi setelah sistem keamanan bencana.

Keamanan informasi memiliki tiga komponen dasar yang harus dikelola, yaitu kerahasiaan informasi sensitif dari pihak yang tidak berhak; integritas informasi untuk memastikan keakuratan dan kelengkapan; dan ketersediaan informasi dan layanan penting untuk pengguna yang berwenang apabila diperlukan (Mitchell, 1999). Selain tiga tujuan dasar, keamanan informasi juga mencakup isu-isu yang dapat mengancam akuntabilitas,kehandalan, nonrepudiation, privasi, otentikasi dan kepercayaan informasi (Peltier, 2014)

Budaya Keamanan Informasi

Perilaku keamanan informasi bisa dilihat dari berbagai perspektif dan perilaku ini bisa dilihat oleh banyak penulis sebagai fungsi budaya organisasi yang diperluas, dengan berbagai intervensi, untuk menjadi budaya keamanan informasi (Box & Pottas, 2013). Perilaku keamanan informasi merupakan fungsi dari komponen keamanan informasi yang diimplementasikan sebagai seperangkat kontrol keamanan untuk mencapai keamanan. Komponen keamanan ini mempengaruhi pengguna yang menunjukkan perilaku keamanan informasi. Perilaku keamanan ini berevolusi dan menjadi perilaku organisasi de facto yang memupuk budaya keamanan informasi. Terdapat suatu hubungan timbal balik antara perilaku dan budaya. Penelitian akademis biasanya membahas faktor-faktor penentu dan hukuman dari mengendalikan perilaku keamanan pengguna, sedsngksn penelian yang lain meninjau pembangunan budaya kesadaran Keamanan Informasi dengan mengubah budaya organisasi menggunakan pembelajaran, pelatihan atau pengetahuan atau dengan memperkuatnya melalui Kebijakan Keamanan Informasi (Box & Pottas, 2013)

Tujuan dari keamanan informasi adalah perlindungan integritas dan privasi data pasien. Hal ini dapat dicapai melalui kepatuhan dengan program manajemen keamanan dimana tindakan penanggulangan keamanan di tingkat pengguna, termasuk akses dan prosedur otentikasi dan kepatuhan terhadap kebijakan keamanan. Contoh dari penelitian ada yang meneliti faktor-faktor yang memotivasi atau menghambat kepatuhan perilaku keamanan informasi (Box & Pottas, 2013). Budaya keamanan informasi diakui memiliki pengaruh terhadap kepatuhan pengguna akhir terhadap kontrol dan kebijakan keamanan informasi di dalam organisasi. Budaya keamanan informasi dapat dibentuk dengan menanamkan aspek keamanan informasi pada setiap karyawan untuk menjadikannya sebagai hal yang alami dengan cara melaksanakan pekerjaan sehari-hari mereka dalam suatu organisasi.

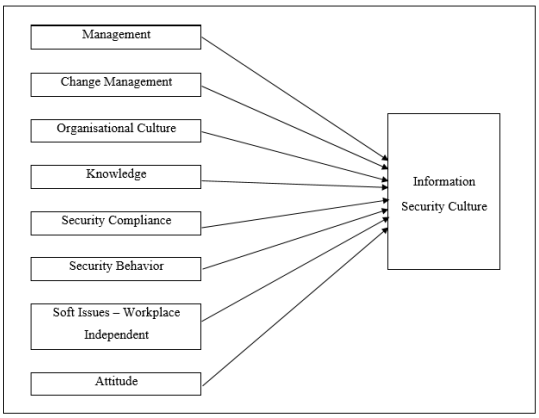
Berdasarkan *literature* bahwa kepercayaan budaya bisa ditemukan untuk mempengaruhi perilaku di antara anggota profesi yang membedakan mereka dalam sistem organisasi dan profesi yang mereka milik. Dengan demikian, fenomena ini telah mengarah ke investigasi dan pemahaman tentang penentuan menanamkan budaya keamanan informasi di organisasi kesehatan Indonesia. Hal ini penting untuk memahami dan menentukan faktor yang berkontribusi terhadap keberhasilan budaya keamanan informasi. Ini juga bisa menyediakan wawasan ke dalam kelompok profesional yang berbeda di organisasi kesehatan untuk memahami keyakinan terkait

keamanan bagi anggota mereka dalam mengimplementasikan sistem manajemen keamanan informasi (Box & Pottas, 2013).

Kerangka Pemikiran

Kerangka pemikiran pada peneitian ini dapat dilihat pada Gambar 1 dibawah ini:

Gambar 1. Kerangka Pemikiran



(*Sumber:* (Ahlan, Lubis, & Lubis, 2015), (Alnatheer, 2015), (Box & Pottas, 2013), (Flores et al., 2014), (Flores & Ekstedt, 2016), (Tsohou et al, 2015), (Veiga & Martins, 2017))

METODE PENELITIAN

Penelitian ini menggunakan metode kuantitatif, sebagaimana dijelaskan oleh Sugiyono (Sugiyono P. D., 2017, hal. 23) metode ini dapat diartikan sebagai metode penelitian yang berlandaskan pada filsafat positivisme, digunakan untuk meneliti pada populasi dan sampel tertentu, pengumpulan data menggunnakan instrumen penelitian, analisis data bersifat kuantitatif/statistik, dengan tujuan untuk menggambarkan dan menguji hipotesis yang telah ditetapkan. Berdasarkan tujuannya, penelitian ini termasuk penelitian hubungan/korelasi Menurut Sugiyono (2014: 87) metode korelasi adalah metode pertautan atau metode penelitian yang berusaha menghubung-hubungkan antara satu unsur/elemen dengan unsur/elemen lain untuk menciptakan bentuk dan wujud baru yang berbeda dengan sebelumnya. Dalam penelitian ini, teknik pengambilan sampel yang digunakan adalah *Purposive sampling*. *Purposive sampling* adalah teknik pengambilan sampel sumber data dengan pertimbangan tertentu. Penelitian ini dilaksanakan pada bulan Agustus 2018.

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 sembilan jalur, sehingga sampel minimum adalah 90 responden, dimana jumlah tersebut dianggap dapat merepresentasikan populasi dalam penelitian ini. Besar sampel minimum yang dibutuhkan yaitu sebesar 90 responden, dimana jumlah tersebut dianggap dapat merepresentasikan populasi dalam penelitian ini namun apabila sampel yang diperoleh lebih dari jumlah sampel minimum akan lebih baik.

Teknik pengolahan data menggunakan software wrapPLS 6.0 dan melakukan uji model fit dan uji hipotesis.

PEMBAHASAN

Validitas Konvergen

Validitas konvergen bertujuan untuk mengetahui validitas dari setiap hubungan antara indikator dengan konstruk atau variabel latennya. Berikut merupakan hasil uji *convergent validity* pada setiap indikator penelitian berdasarkan pada nilai *loading factor*:

Tabel 1. Nilai Combined Loadings dan Cross Loading

	M	*CM*	*OC*	*Knw*	*SC*	*SB*	*SW*	*ATT*	*ISC*	*P Value*
M1	(0.713)	0.070	0.298	0.044	-0.370	-0.059	-0.009	-0.031	-0.052	<0.001
M2	(0.701)	0.220	-0.327	-0.053	-0.063	0.055	0.202	0.062	-0.175	<0.001
M3	(0.916)	-0.127	-0.029	-0.002	0.226	0.010	-0.077	-0.009	0.099	<0.001
CM1	0.107	(0.808)	0.207	-0.179	0.043	0.053	-0.133	-0.166	0.170	<0.001
CM2	-0.176	(0.789)	-0.184	0.254	-0.170	-0.082	0.112	0.134	-0.070	<0.001
CM3	0.104	(0.600)	-0.107	-0.096	0.240	0.043	0.083	0.113	-0.249	<0.001
OC1	-0.075	0.058	(0.849)	-0.139	0.143	-0.007	-0.274	-0.056	0.186	<0.001
OC2	-0.106	-0.084	(0.874)	0.141	-0.016	0.010	-0.060	-0.080	-0.076	<0.001
OC3	0.173	0.009	(0.763)	0.029	-0.142	-0.001	0.351	0.130	-0.137	<0.001
Knw	0.206	-0.105	0.187	(0.724)	-0.236	0.015	0.288	0.187	-0.276	<0.001
Knw	-0.065	0.013	0.128	(0.785)	0.071	-0.014	-0.284	0.139	-0.142	<0.001
Knw	-0.104	0.067	-0.223	(0.816)	0.121	0.000	-0.012	-0.230	0.296	<0.001
SC	0.159	0.040	-0.126	-0.048	(0.791)	-0.288	-0.019	-0.010	0.107	<0.001
SC	-0.037	-0.064	0.146	0.143	(0.873)	0.022	-0.055	-0.036	-0.007	<0.001
SC	-0.124	0.039	-0.052	-0.132	(0.819)	0.283	0.091	0.056	-0.107	<0.001
SB1	-0.086	0.154	-0.283	0.241	0.170	(0.740)	0.006	-0.029	-0.123	<0.001
SB2	-0.011	-0.052	0.172	-0.077	0.051	(0.871)	-0.122	0.031	0.045	<0.001
SB3	0.075	-0.058	0.026	-0.095	-0.177	(0.884)	0.124	-0.011	0.043	<0.001
SW1	0.160	-0.087	-0.164	0.140	0.055	0.059	(0.856)	0.015	0.000	<0.001
SW2	-0.119	0.035	0.100	-0.030	-0.082	-0.134	(0.847)	-0.087	0.111	<0.001
SW3	-0.086	0.087	0.118	-0.176	0.025	0.091	(0.731)	0.095	-0.151	<0.001
ATT1	-0.233	0.374	-0.017	-0.253	-0.029	0.201	0.000	(0.611)	-0.125	<0.001
ATT2	0.084	-0.073	0.045	0.184	-0.351	0.125	0.084	(0.796)	-0.050	<0.001
ATT3	0.053	-0.145	-0.033	-0.031	0.351	-0.235	-0.080	(0.813)	0.119	<0.001
ISC1	-0.067	-0.122	-0.260	0.241	0.028	-0.037	0.163	0.062	(0.691)	<0.001
ISC2	-0.220	-0.125	0.469	-0.105	0.166	-0.074	-0.115	-0.275	(0.636)	<0.001

Lanjutan Tabel 1. Nilai Combined Loadings dan Cross Loading

	M	*CM*	*OC*	*Knw*	*SC*	*SB*	*SW*	*ATT*	*ISC*	*P Value*
ISC3	0.111	0.152	-0.115	0.433	-0.111	-0.154	-0.026	0.111	(0.687)	<0.001
ISC4	0.056	0.079	-0.094	0.045	-0.111	0.088	-0.033	0.114	(0.818)	<0.001
ISC5	-0.073	0.106	0.148	-0.398	0.083	-0.035	-0.077	-0.087	(0.728)	<0.001
ISC6	0.049	-0.047	-0.232	0.101	-0.124	0.146	0.060	0.068	(0.658)	<0.001
ISC7	0.099	-0.084	0.172	-0.455	0.133	0.066	0.024	-0.066	(0.646)	<0.001

Sumber: Data primer diolah (2018)

Berdasarkan pada Tabel 1, dapat dilihat nilai bahwa masing – masing nilai pada *cross-loadings Factor* telah mencapai nilai diatas 0,5 dengan p dibawah 0,001. Dengan demikian kriteria uji validitas konvergen telah terpenuhi.

Dalam penelitian ini, untuk mengukur *convergent validity* dapat dilakukan dengan melihat hasil dari wrapPLS 6.0 pada bagian *Average Variance* (AVE). Dalam pengukuran AVE tersebut, digambarkan varian atau keragaman variabel manifest yang dapat dikandung oleh konstruk laten. Kriteria penilaiannya adalah nilai AVE ≥ 0,5.

Tabel 2. Average Variance Extracted

Average Variance Extracted	Nilai	Kriteria	Keterangan
M	0.6	0.5	Valid
CM	0.5	0.5	Valid
OC	0.7	0.5	Valid
KNW	0.6	0.5	Valid
SC	0.7	0.5	Valid
SB	0.7	0.5	Valid
SW	0.7	0.5	Valid
ATT	0.6	0.5	Valid
ISC	0.5	0.5	Valid

Sumber: Data primer diolah (2018)

Tabel 2 diatas, menunjukkan bahwa nilai AVE untuk setiap konstruk dihasilkan lebih besar dari 0,5. Berdasarkan kriteria AVE, hasil tersebut telah menunjukkan validitas konvergen yang dikatakan baik.

Validitas Diskriminan

Composite Realibility

Tabel 3. Hasil Uji *Composite Reliability*

Konstruk/ Variabel	Composite Reliability	Kriteria	Keterangan
M	0.824	>= 0,7	Diterima
CM	0.779	>= 0,7	Diterima
OC	0.869	>= 0,7	Diterima

Lanjutan Tabel 3. Hasil Uji *Composite Reliability*

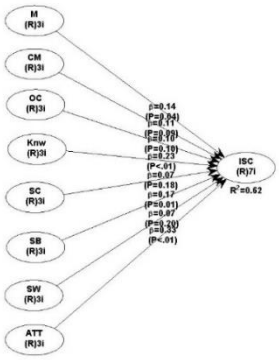
Konstruk/ Variabel	Composite Reliability	Kriteria	Keterangan
KNW	0.819	>= 0,7	Diterima
SC	0.868	>= 0,7	Diterima
SB	0.872	>= 0,7	Diterima
SW	0.854	>= 0,7	Diterima
ATT	0.787	>= 0,7	Diterima
ISC	0.868	>= 0,7	Diterima

Sumber: Data Primer diolah (2018)

Dilihat dari *composite reliability* pada tabel 4.6, masing – masing variabel memiliki tingkat *reliable* diatas kriteria *rule of thumb*, dimana seluruh variabel dinyatakan *reliable.* Dengan demikian instrumen yang digunakan dalam penelitian ini telah memenuhi semua ketentuan uji validitas.

Evaluasi Model Struktural

Gambar 2. Hasil Analisis Model wrapPLS



Uji Hipotesis dan Koefisien Regresi

Tabel 4. Hasil Uji *Composite Reliability*

	Lajur	*Koefisien*	*Nilai P*	*Ideal*	*Hasil*
H1	M -> ISC	0,14	0.04	<0,05	Diterima
H2	CM -> ISC	0,11	0,09	<0,05	Tidak Diterima
H3	OC -> ISC	0,10	0,10	<0,05	Tidak Diterima
H4	Knw -> ISC	0,23	<.01	<0,05	Diterima
H5	SC -> ISC	0,07	0,18	<0,05	Tidak Diterima
H6	SB -> ISC	0,17	0,01	<0,05	Diterima
H7	SW -> ISC	0,07	0,20	<0,05	Tidak Diterima
H8	ATT -> ISC	0,33	<.01	<0,05	Diterima

Sumber: Data Primer diolah (2018)

Model Fit Indeks

Model fit indeks dilakukan untuk mengukur kualitas hasil dari penelitian. Berikut hasil dari Uji model fit indeks:

Tabel 5. Hasil Uji Model Fit Indeks

Indeks	**Nilai**		**Kriteria**		**Keterangan**
Average path coefficient (APC)	0,155	P=0.013	P < 0,05		Diterima
Average R-squared (ARS)	0.619	P<0.001	P < 0,05		Diterima
Average adjusted R-squared (AARS)	0.598	P<0.001	P < 0,05		Diterima
Average block VIF (AVIF)	1.776		acceptable if <= 5 ideally <= 3.3	ideally <= 3.3	Diterima
Average full collinearity VIF (AFVIF)	1.849		acceptable if <= 5	ideally <= 3.3	Diterima
Tenenhaus GoF (GoF)	0.617		small >= 0.1		Diterima
			medium >= 0.25		Diterima
			large >= 0.36		Diterima
Sympson's paradox ratio (SPR)	1		acceptable if >= 0.7	ideally = 1	Diterima
R-squared contribution ratio (RSCR)	1		acceptable if >= 0.9	ideally = 1	Diterima
Statistical suppression ratio (SSR)	1		acceptable if >= 0.7		Diterima
Nonlinear bivariate causality direction ratio (NLBCDR)	1		acceptable if >= 0.7		Diterima

Sumber: Data primer diolah (2018)

Berdasarkan Tabel 5, hasil output diatas menjelaskan bahwa:

1. APC, ARS, AARS memiliki nilai yang memenuhi kriteria dapat diterima menunjukkan kualitas penjelasan signifikan memenuhi indikasi model fit.
2. AVIF dan AFVIF memiliki kriteria ideally atau kurang dari 3.3 menunjukkan bebas dari kolinearitas.
3. Nilai Tenenhaus GoF memiliki kriteria large atau luas dengan nilai 0.671 yang menunjukkan bahwa kekuatan prediksi model kuat.
4. SPR memiliki nilai 1 memiliki kriteria ideally yang berarti tidak ada masalah dengan Simpson's paradox didalam model.
5. RSCR memiliki nilai 1 yang berarti tidak ada kontribusi R-squared negatif didalam model.
6. SSR dengan nilai 1 ≥ 0.7 yang berarti bebas dari suppression instances.
7. NLBCDR dengan nilai 1 ≥ 0.7 memiliki arti model mendukung hipotesis.

Diskusi

1. Besarnya nilai koefisien total *Management* terhadap *Information Security Culture* sebesar 0,14 atau 14% dengan nilai p < 0,05 dapat dikatakan bahwa variabel *management* memiliki pengaruh yang signifikan terhadap *Information Security Culture*.

2. Besarnya nilai koefisien total *Change Management* terhadap *Information Security Culture* sebesar 0,11 atau 11% dengan nilai p > 0,05 dapat dikatakan bahwa tidak terdapat pengaruh yang signifikan dari variabel *Change Management* terhadap *Information Security Culture.*
3. Besarnya nilai koefisien total *Organisational Culture* terhadap *Information Security Culture* sebesar 0,10 atau 10% dengan nilai p > 0,05 dapat dikatakan bahwa tidak terdapat pengaruh yang signifikan antara variabel *Organisational Culture* terhadap *Information Security Culture.*
4. Besarnya nilai koefisien total *Knowledge* terhadap *Information Security Culture* sebesar 0,23 atau 23% dengan nilai p < 0,05 dapat dikatakan bahwa *Knowledge* memiliki pengaruh yang signifikan terhadap *Information Security Culture.*
5. Besarnya nilai koefisien total *Security Compliance adalah* terhadap *Information Security Culture* sebesar 0,07 atau 7% dengan nilai p > 0,05 dapat dikatakan bahwa tidak terdapat pengaruh yang signifikan variabel *Security Compliance* terhadap *Information Security Culture.*
6. Besarnya nilai koefisien total *Security Behavior* terhadap *Information Security Culture* sebesar 0,17 atau 17% dengan nilai p < 0,05 dapat dikatakan bahwa terdapat pengaruh yang signifikan *Security Behavior* terhadap *Information Security Culture*..
7. Besarnya nilai koefisien total *Soft Issues – Workplace Independent* terhadap *Information Security Culture* sebesar 0,07 atau 7% dengan nilai p > 0,05 dapat dikatakan bahwa tidak terdapat pengaruh yang signifikan terhadap *Information Security Culture.*
8. Besarnya nilai koefisien total *Attitude* terhadap *Information Security Culture* sebesar 0,33 atau 33% dengan nilai p < 0,05 dapat dikatakan bahwa terdapat pengaruh yang signifikan terhadap *Information Security Threat.*

KESIMPULAN DAN SARAN

Kesimpulan

Tujuan penelitian ini adalah penelitian ini adalah mengetahui faktor-faktor apa saja yang mempengaruhi budaya keamaan informasi di fasilitas kesehatan klinik pratama di kota Bandung. Berdasarkan hasil penelitian dan analisis yang telah dilakukan, diperoleh kesimpulan yang dapat memberikan jawaban terhadap pertanyaan penelitian dalam penelitian ini bahwa faktor *Management, Knowledge, Security Behavior* dan *Attitude* lebih mempengaruhi budaya keamanan informasi di klinik pratama Kota Bandung.

Saran

1. Saran Bagi Klinik Pratama Kota Bandung

   Dari hasil analisis yang telah dilakukan ada empat variabel yang tidak berpengaruh terhadap budaya keamanan informasi di klinik pratama Kota Bandung yaitu variabel *Change Management, Organisational Culturel, Security Compliance, Soft Issues – Workplace Independent,* penulis memberikan saran kepada fasilitas kesehatan yang menjadi tempat penelitian fasilitas kesehatan klinik pratama Kota Bandung agar dapat memperhatikan faktor – faktor yang berpengaruh terhadap *Information Security Culture* seperti faktor *Management, Knowledge, Security*

Behavior, dan Attitude untuk terus meminimalisir ataupun mengurangi dampak tidak baik terhadap budaya keamanan yang ada di masing – masing klinik pratama Kota Bandung.

2. Saran Bagi Penelitian Selanjutnya
   a. Penelitian selanjutnya diharapkan untuk dapat menambahkan variabel penelitian lainnya misalnya *Perceived Security Threat* untuk mengetahui apabila terjadi suatu ancaman akan berpengaruh terhadap Budaya Keamanan Informasi.
   b. Melakukan penelitian dibidang lain, sehingga dapat terlihat perbedaan pengaruh variabel yang diteliti.

DAFTAR PUSTAKA

Ahlan, A. R., Lubis, M., & Lubis, A. R. 2015. I*nformation Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures*. *Procedia Computer Science*, 361 – 373. Retrieved from www.sciencedirect.com

Alnatheer, M. 2015. *Information Security Culture Critical Success Factors*. *King Abdul-Aziz City for Science and Technology (KACST)*, 1-5.

Aziz, A. M., & Irjayanti, M. 2014. *Manajemen.* Bandung: Mardika Group.

Box, D., & Pottas, D. 2013. I*mproving information security behaviour in the healthcare context. Procedia Technology* , 1-11.

Center for Internet Secuirty. 2018. *Retrieved from Data Breaches: In the Healthcare* Sectors: https://www.cisecurity.org/data-breaches-in-the-healthcare-sector/

Flores et al. 2014. *Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture*. *Computer & Security, 43*, 90-110. Retrieved from http://dx.doi.org/10.1016/j.cose.2014.03.004

Flores, W. R., & Ekstedt, M. 2016. *Shaping intention to resist social engineering through transformational leadership, information security culture and awareness*. *Elsevier*, 26-44.

Hair, e. a. 2011. *PLS-SEM: Indeed a Silver Bullet, . Journal of Marketing Theory and Practice*.

Hipaajournal(c). 2018. *Retrieved from Healthcare data breach statistics:* https://www.hipaajournal.com/healthcare-data-breach-statistics/

Mitchell, R. C. 1999. *Corporate Information Security Management. New Library World Vol 100, MCB University Press. London UK ISSN*, 213-227.

Nasution, M. (2018, September). *Keamanan Informasi: Pendahuluan*. *Technical Report*.

Peltier, T. 2014. *Information Security Fundamentals, Second Edition*. *Boca Raton:: CRC Press.*

Shick, S. 2018. *Security Breaches in Healthcare*. Retrieved from 70 Percent Of Organizations Hit Globally, Report Shows: https://securityintelligence.com/news/security-breaches-in-healthcare-70-percent-of-organizations-hit-globally-report-shows/

Sugiyono, P. D. 2017. *Metode Penelitian Bisnis*. Yogyakarta: Alfabeta Bandung.

Tsohou et al. 2015. *Analyzing the role of cognitive and culture biases in the internalization of information secuirty policies: Recommendations for Information security awareness program 9. Computer & Security*, 128-141.

Veiga, A. D., & Martins, N. (2017, May). *Defining and identifying dominant information security cultures and subcultures*. *Computers & Security*, 72-94.