In Search

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

ANALISIS BUDAYA KEAMANAN INFORMASI DI RUMAH SAKIT DI KOTA BANDUNG

Farisha Pratami Tallei[1)], Puspita Kencana Sari,[2)]Candiwan[3)], Adhi Prasetio.[4)]

Fakultas Ekonomi dan Bisnis, Telkom University
email: farishatallei@student.telkomuniversity.ac.id, puspitakencana@telkomuniversity.ac.id, candiwan@telkomuniversity.ac.idadhipras@telkomuniversity.ac.id

Abstrak

Penelitian menganalisis faktor-faktor yang memengaruhi budaya keamanan informasi di Rumah Sakit di Kota Bandung. Penelitian ini menggunakan kuesioner yang disebarkan ke rumah sakit yang terdaftar di Badan Penyelenggara Jaminan Sosial Kesehatan (BPJS) sebanyak 169 kuesioner. Penelitian menggunakan sampel sejumlah rumah sakit di Kota Bandung. Metode penelitian adalah metode kuantitatif dengan teknik analisis data *Partially Least Square Structural Equation Modelling (PLS-SEM)*. Data penelitian adalah data primer melalui kuisioner kepada pegawai rumah sakit. Berdasarkan penelitian terdahulu, budaya keamanan informasi dipengaruhi oleh berbagai faktor dan budaya organisasi secara keseluruhan. Penelitian diharapkan memberikan wawasan tentang budaya dan perilaku keamanan informasi di rumah sakit Kota Bandung dan mendukung strategi e-kesehatan nasional oleh Kementerian Kesehatan Republik Indonesia. Penelitian ini dimulai dengan jumlah variabel sebanyak 14, yaitu *management*, *workplace capabilities*, *risk and response factors*, *operational management*, *change management*, *organisational culture*, *knowledge*, *security compliance*, *security behavior*, *soft issues – workplace independent*, *training and awareness*, *information security policies*, *perceived security threat* dan *attitude*. Namun, yang berpengaruh terhadap *Information Security Culture (ISC)* adalah *organisational culture*, *knowledge*, *information security policies*, *perceived security threat* dan *attitude*.

Abstract

This study to analyze the factors that influence the information security culture in hospitals in Bandung. This study used a questionnaire distributed to hospitals in Bandung that was registered in the Social Insurance Administration Organization of Health (BPJS) of 169 questionnaires. The study used a sample of hospitals in Bandung. The research method is a quantitative method with Partially Least Square Structural Equation Modeling (PLS-SEM) data analysis techniques. Research data are primary data through questionnaires for a number of hospital employees. Based on previous research, information security culture is influenced by various factors and overall organizational culture. Research is expected to provide insight into the culture and behavior of information security in Bandung City hospitals and support the national e-health strategy by the Ministry of Health of the Republic of Indonesia. This research began with 14 variables, namely management, workplace capabilities, risk and response factors, operational management, change management, organizational culture, knowledge, security compliance, security behavior, independent workplace issues, training and awareness, information security policies, perceived security threat and attitude. However, it turns out that the one that affects Information Security Culture (ISC) is organizational culture, knowledge, information security policies, perceived security threat and attitude.

Keywords: *Information Security, Culture, Hospital.*

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

1. PENDAHULUAN

Program Jaminan Kesehatan Nasional (JKN) bertujuan untuk memberikan layanan kesehatan kepada masyarakat melalui fasilitas kesehatan, baik dari pemerintah ataupun swasta. Ada lebih dari 20,000 fasilitas kesehatan yang bias memberikan layanan kesehatan bagi masyarakat se-Indonesia. Dalam pelayanannya, setiap fasilitas kesehatan akan menghasilkan, menyimpan, mengelola dan menggunakan data-data kesehatan milik pasien menggunakan sistem informasi, baik yang disediakan oleh BPJS Kesehatan atau yang dikembangkan secara mandiri. Pasien yang dirawat bukan hanya pasien yang berpartisipasi dalam JKN, melainkan juga pasien umum yang menggunakan asuransi swasta atau pasien yang menggunakan dana sendiri (swadana).

Berdasarkan Menurut Keputusan Menteri Kesehatan Republik Indonesia Nomor 340/MENKES/PER/III/2010 adalah, "Rumah sakit adalah institusi pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perorangan secara paripurna yang menyediakan pelayanan rawat inap, rawat jalan dan gawat darurat".

Berikut adalah informasi mengenai jumlah dan data rumah sakit di Kota Bandung yang akan diteliti di Tabel 1.

Tabel 1 Objek Penelitian

Nama	Klasifikasi
Rumah Sakit Umum Pindad	Tipe C
Rumah Sakit Khusus Gigi dan Mulut	Tipe C
Rumah Sakit Khusus Ibu dan Anak	Tipe C
Rumah Sakit Humana Prima	Tipe B
Rumah Sakit Muhammadiyah	Tipe C
Rumah Sakit Mata Cicendo	Tipe A
Rumah Sakit Hermina Arcamanik	Tipe C
Rumah Sakit Umum Melinda 2	Tipe C

Sumber: Hasil Olahan Data

2. KAJIAN PUSTAKA

2.1 Keamanan Informasi Kesehatan

Berdasarkan Pusat Data dan Informasi milik Kementerian Kesehatan Republik Indonesia (Pusdatin Kemkes, 2015), keamanan informasi merupakan upaya untuk melindungi, mengamankan aset informasi dari ancaman yang mungkin akan timbul sehingga dapat membahayakan aset informasi tersebut. Keamanan informasi adalah suatu penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan aktivitas perusahaan, meminimalisir risiko dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis ataupun kegiatan di dalam bidang industri lainnya.

2.2 Budaya Keamanan Informasi

Menurut penelitian terdahulu (Box & Pottas, 2013), perilaku keamanan informasi merupakan fungsi dari komponen keamanan informasi yang diimplementasikan sebagai seperangkat kontrol keamanan untuk mencapai keamanan. Komponen keamanan ini memengaruhi pengguna yang menunjukan 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. Perilaku keamanan informasi dapat dilihat dari berbagai sudut dan perilaku tersebut dapat dilihat oleh banyak penulis sebagai fungsi yang diperluas dari budaya organisasi, dengan berbagai

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

intervensi, untuk menjadi budaya keamanan informasi *(Information Security/IS Culture)*.

2.3 Faktor-Faktor Budaya Keamanan Informasi

Berdasarkan penelitan dari beberapa peneliti terdahulu, disimpulkan terdapat empat belas faktor yang memengaruhi budaya kemanan informasi *(Information Security Culture)* dalam informasi pemeliharaan kesehatan yaitu *Management*, *Workplace Capabilities*, *Risk and Response Factors*, *Operational Management*, *Change Management*, *Organisational Culture*, *Knowledge*, *Security Compliances*, *Soft Issues – Workplace Independent*, *Security Behavior*, *Training and Awareness*, *Information Security (IS) Policies*, *Perceived Security Threat* dan *Attitude*.

Berdasarkan penelitian terdahulu (Alnatheer, 2015), (Flores & Ekstedt, 2016) dan (Da Veiga & Martin, 2017), *management* merupakan faktor keamanan informasi untuk membentuk budaya yang diinginkan oleh perusahaan berdasarkan kepemimpinan atau peran mereka dalam organisasi.

Menurut (Da Veiga & Martin, 2017), *workplace capabilities* merupakan kemampuan internal organisasi yang dapat memengaruhi budaya/aspek seperti kegunaan sistem, perputaran karyawan, ketergantungan pada karyawan sementara, kompetensi karyawan dan efektivitas prosedur pemantauan, kepuasan kerja, tekanan tugas, signifikansi tugas, praktik keamanan, prosedur pendisiplinan, pemantauan keamanan, pengawasan, kinerja serta penghargaan.

Salah satu faktor yang paling kuat pengaruhnya terhadap keamanan informasi adalah *risk and response factors*, berdasarkan (Flores et al., 2014), (Parsons et al., (2014), (Da Veiga & Martin, 2017), berfokus pada budaya risiko keamanan informasi untuk meminimalkan risiko keamanan informasi. Cara dimana organisasi mengidentifikasi, mencegah, mendeteksi dan menanggapi insiden keamanan berdampak pada budaya keamanan informasi.

Melalui faktor *operational management*, organisasi harus memiliki pendekatan yang komprehensif untuk mengelola dan mengatur Keamanan Informasi berdasarkan pendekatan penilaian risiko. Manajemen, tinjauan, audit, dan pemantauan yang tepat akan membantu mengarahkan budaya positif keamanan informasi (Shameli-Sendi et al, 2015), (Da Veiga & Martin, 2017).

Menurut (Parsons et al, 2014), *change management* adalah perubahan terhadap teknologi dalam suatu organisasi membantu meningkatkan keamanan, kualitas, efisiensi, dan keandalan, yang memiliki dampak signifikan pada fungsi, kegunaan, keangkuhan, dan keamanan data. Perubahan proses manajemen harus dimasukkan ke dalam perubahan teknologi dan membantu karyawan dengan integrasi dan penerimaan perubahan untuk itu menjadi bagian dari budaya.

Faktor *knowledge* berdasarkan penelitian (Da Veiga & Martins, 2017) adalah pengetahuan keamanan informasi diciptakan melalui cara implisit dan eksplisit untuk menanamkan ketaatan pada keamanan. Individu memiliki pengetahuan dan pemahaman mereka sendiri tentang keamanan informasi, yang memengaruhi cara mereka memproses informasi dan menggunakan kontrol keamanan informasi.

Security Compliance merupakan pengetahuan intrinsik tenaga kerja tentang kebijakan keamanan informasi dan prosedur akan memiliki dampak positif pada sikap mereka terhadap kebijakan keamanan informasi dan kepatuhan. Dalam sebuah organisasi di mana ada budaya keamanan informasi yang kuat atau sehat, orang akan mengharapkan kepatuhan sebagai ciri yang terlihat dari budaya (Parsons et al, 2014), (Tsohou et al., 2015), (Alnatheer, 2015) dan (Da Veiga & Martins, 2017).

Faktor *Soft Issues – Work Independent*, masalah-masalah ringan yang berkaitan dengan

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

karyawan juga dapat berdampak pada budaya keamanan informasi, seperti paparan kehidupan nyata, insiden yang berhubungan dengan keamanan, liputan media, manfaat pribadi, manfaat dan kesadaran kelompok atau masyarakat, penerimaan kebijakan, kompetensi, etiket, komitmen, kepatuhan, penolakan diri dan etika. Norma subkultur juga dapat memengaruhi budaya keamanan informasi (Parsons et al., 2015).

Security behavior menerapkan komponen keamanan berdampak pada interaksi karyawan dengan aset informasi, akibatnya menunjukkan perilaku tertentu yang disebut sebagai perilaku keamanan. Tujuannya adalah untuk menanamkan perilaku keamanan yang kondusif untuk perlindungan aset informasi berdasarkan kebijakan organisasi (Hassan Ismail, 2016), (Box and Pottas, 2013) dan (Ahlan, 2015).

Training and awareness merupakan faktor yang paling sering muncul di penelitian-penelitian terdahulu, pelatihan dan kesadaran keamanan informasi dilaksanakan untuk mendidik karyawan untuk memahami risiko terhadap informasi dan kontrol yang relevan untuk menggunakan kebijakan untuk dipatuhi. Pelatihan dan kesadaran telah terbukti memiliki dampak positif pada budaya informasi dari waktu ke waktu (Hassan & Ismail, 2016), (Hovav and D'Arcy, 2013), (Box and Pottas, 2013), (Parsons et al., 2014), (Safa et al., 2015), (Alnatheer, 2015), (Da Veiga & Martins, 2015), (Ahlan et al, 2015) dan (Flores & Ekstedt, 2016).

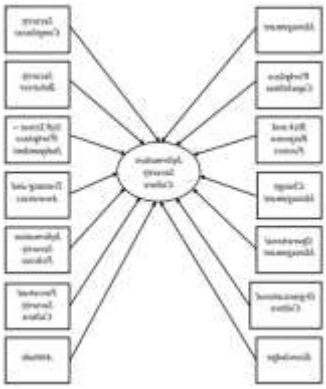
Information security policies, pengetahuan dan persepsi karyawan atas aturan dan prosedur kebijakan keamanan informasi dapat secara positif memengaruhi budaya keamanan informasi. Kebijakan ini merupakan landasan penting untuk mengarahkan budaya keamanan informasi dan berfungsi sebagai landasan untuk menciptakan nilai dan keyakinan bersama (Box & Pottas, 2013), (Da Veiga, 2015), (Parsons et al., 2014) dan (Hassan & Ismail, 2016).

Perceived security threat menjelaskan bahwa sejauh mana seseorang memiliki persepsi atau paradigma akan sebuah ancaman keamanan (Ahlan et al, 2015) dan (Wardani, 2017).

Menurut (Ahlan, 2015), *attitude* merupakan faktor umumnya, sikap dapat diubah melalui persuasi sebagai tanggapan terhadap komunikasi. Secara teoritis, sikap positif terhadap perubahan perilaku dapat dicapai jika kekuatan pendorong lebih besar daripada kekuatan yang melawan dan sebaliknya.

2.4 Kerangka Pemikiran

Kerangka berpikir adalah suatu bentuk konseptual mengenai bagaimana teori yang ada memiliki hubungan dengan berbagai faktor yang telah diidentifikasi sebagai suatu masalah yang krusial (Sugiyono, 2017:60). Penelitian ini dilakukan di Rumah Sakit di Kota Bandung yang telah terdaftar di Badan Penyelenggara Jaminan Sosial Kesehatan. Variabel independen adalah *management*, *workplace capabilities*, *risk and response factors*, *operational management*, *change management*, *organisational culture*, *knowledge*, *security compliance*, *security behavior*, *soft issues – workplace independent*, *training and awareness*, *information security policies*, *perceived security threat* dan *attitude*, serta variabel dependennya adalah budaya keamanan informasi.



Gambar 1. Kerangka Pemikiran
Sumber: Hasil Olahan Data

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

3. METODE PENELITIAN

3.1 Karakteristik Penelitian

Penelitian ini menggunakan metode kuantitatif, seperti yang dijelasnkan oleh Sugiyono (2014:13), metode ini disebut metode kuantitatif karena data penelitian berupa angka-angka dan analisis menggunakan statistik dengan tujuan untuk menguji hipotesis yang telah ditetapkan.

Tabel 2. Karakteristik Penelitian

Karakteristik Penelitian	Jenis
Berdasarkan metode	Kuantitatif
Berdasarkan tujuan	Konklusif
Berdasarkan tipe penyelidikan	Korelasional
Berdasarkan keterlibatan peneliti	Tidak mengintervensi data
Berdasarkan unit analisis	Individual
Berdasarkan waktu penelitian	*Cross-sectional*

Sumber: Hasil Olahan Data

3.2 Operasional Variabel

Variabel endogen terdiri dari *management*, *workplace capabilities*, *risk and response factors*, *operational management*, *change management*, *organisational culture*, *knowledge*, *security compliance*, *security behavior*, *soft issues – workplace independent*, *training and awareness*, *information security policies*, *perceived security threat* dan *attitude*, serta variabel eksogen adalah budaya keamanan informasi.

3.3 Tahapan Penelitian

Tahapan penelitian dimulai dengan mengidentifikasi fenomena mengenai budaya keamanan informasi di sektor kesehatan. Kemudian, memilih salah satu objek dari fasilitas kesehatan yang terdaftar di Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, yaitu rumah sakit. Setelah itu, mengidentifikasi faktor-faktor apa saja yang memengaruhi *information security culture* atau budaya keamanan rumah sakit dan menelaah penelitian-penelitian sebelumnya dari jurnal-jurnal mengenai keamanan informasi serta menyusun kerangka pemikiran. Lalu, hipotesis dibuat berdasarkan variabel-variabel yang telah ditentukan dilanjutkan dengan membuat kuisioner. Setelah kuisioner dibuat, dilakukan uji validitas dan uji reliabilitas. Setelah kuisioner diuji, terbukti bahwa kuisioner valid dan reliabel, penelitian dilanjutkan dengan meminta izin kepada tiap-tiap rumah sakit di Kota Bandung untuk melakukan penelitian dan penyebaran kuisioner terhadap pegawai-pegawai di rumah sakit. Setelah diberi izin oleh Kepala Rumah Sakit/Bagian Direksi, data responden didapatkan untuk dianalisis. Kemudian, dilakukan pembahasan dan membuat kesimpulan serta saran dari penelitian yang telah dilakukan.

3.4 Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah menggunakan kuisioner yang disebarkan kepada sejumlah responden, yaitu kepada sejumlah instrumen pegawai di rumah sakit.

Adapun yang menjadi responden dari penelitian ini adalah pegawai atau karyawan dari rumah sakit yang menggunakan sistem informasi pada objek dalam penelitian ini, yaitu Kepala Rumah Sakit/Direktur/Manajer/Kepala Bagian, Dokter Spesialis, Dokter Umum/Dokter Gigi, Perawat, Pegawai IT dan Bagian Administrasi (yang berhubungan dengan data dan informasi mengenai riwayat kesehatan dan rekam medis milik pasien).

3.5 Teknik Analisis Data

Metode penelitian yang digunakan dalam penelitian ini adalah metode kuantitatif. Pada tahap awal akan dilakukan studi literatur untuk meneliti variabel apa saja yang akan menjadi

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

kandidat sebagai *antecedent* dari *information security culture*. Setelah diperoleh kandidat variabel maka penelitian dilanjutkan dengan melakukan pengujian terhadap model yang dihasilkan dengan menggunakan metode kuantitatif.

Data penelitian ini menggunakan data primer yang diambil melalui kuisioner kepada sejumlah pegawai di rumah sakit di Kota Bandung yang dijadikan sampel. Pengumpulan data akan dilakukan dengan cara penyebaran kuesioner kepada responden. Teknik sampling yang digunakan adalah *nonprobability sampling*. Jumlah sampel minimum yang diperlukan adalah sepuluh kali dari jumlah jalur terbanyak yang menuju ke sebuah variabel (Hair, 2011).

Dalam penelitian ini jumlah jalur terbanyak adalah jalur yang menuju ke variabel *information security culture*, yaitu 14 jalur, sehingga sampel minimum adalah 140 sampel. Data yang terkumpul akan dianalisis lebih lanjut dengan teknik analisis *Partially Least Square Structural Equation Modeling (PLS- SEM)*.

3.6 Pengujian Hipotesis

Pengujian validitas dan reliabilitas dalam penelitian ini dilakukan dengan cara sebagai berikut:

1. Uji validitas butir pertanyaan dilakukan dengan menghitung korelasi item total.
2. Uji reliabilitas kuisioner menggunakan *cronbach's alpha*.

3.6.1 Uji Validitas

Penelitian ini menggunakan korelasi item total *(item total correlation)* sebagai pengujian validitas. Statistic uji untuk metode pengujian tersebut adalah sebagai berikut:

1. Korelasi item total (rxi) jika jumlah butir pertanyaan (i) > 30. Perhitungan rxi menggunakan rumus berikut ini (Kusnendi, 2008, p. 94).

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

X = skor butir; Y = skor total; n = jumlah butir pertanyaan. Kriteria pengujian dinyatakan memenuhi validitas adalah:
rxi positif dengan *P-value* < 0.05.

3.6.2 Hasil Uji Validitas

Uji validitas dengan korelasi item total menggunakan SPSS.

Tabel 3.1 Hasil Uji Validitas

Variabel	Hasil (r hitung)	Kriteria (r tabel)
Mng1	0.546	0.361
Mng2	0.368	0.361
Mng3	0.459	0.361
WoCa1	0.392	0.361
WoCa2	0.630	0.361
WoCa3	0.647	0.361
RRF1	0.617	0.361
RRF2	0.647	0.361
RRF3	0.705	0.361
OpMng1	0.618	0.361
OpMng2	0.661	0.361
OpMng3	0.627	0.361
ChaMng1	0.568	0.361
ChaMng2	0.723	0.361
ChaMng3	0.408	0.361
OrgCult1	0.624	0.361
OrgCult2	0.727	0.361
OrgCult3	0.727	0.361
Knowldg1	0.405	0.361
Knowldg2	0.723	0.361
Knowldg3	0.638	0.361
SecCom1	0.524	0.361
SecCom2	0.417	0.361
SecCom3	0.654	0.361
SecBehv1	0.720	0.361
SecBehv2	0.626	0.361
SecBehv3	0.630	0.361
SIWI1	0.728	0.361
SIWI2	0.543	0.361
SIWI3	0.663	0.361

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

TAA1	0.396	0.361
TAA2	0.643	0.361
TAA3	0.602	0.361
ISP1	0.643	0.361
ISP2	0.810	0.361
ISP3	0.617	0.361
PST1	0.643	0.361
PST2	0.696	0.361
PST3	0.709	0.361
Attitd1	0.558	0.361
Attitd2	0.477	0.361
Attitd3	0.676	0.361
ISC1	0.694	0.361
ISC2	0.638	0.361
ISC3	0.463	0.361
ISC4	0.778	0.361
ISC5	0.796	0.361
ISC6	0.642	0.361
ISC7	0.620	0.361

Sumber: Hasil Olahan Data

Berdasarkan pengujian validitas menggunakan SPSS, nilai dari semua variabel dinyatakan valid karena nilainya lebih dari 0.361.

3.7 Uji Reliabilitas

Uji reliabilitas kuisioner pada penelitian ini menggunakan rumus *Cronbach's Alpha*. *Cronbach's Alpha* adalah rumus matematis yang digunakan untuk menguji tingkat reliabilitas ukuran. Berikut adalah rumus dari *Cronbach's Alpha* (Kusnendi, 2008, p. 97).

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

Keterangan :

α = koefisien reliabilitas instrumen Alpha Cronbach

N = banyaknya pertanyaan

σ^2_{item} = variance dari pertanyaan

σ^2_{total} = variance dari skor

Tabel berikut merupakan kriteria keputusan untuk uji reliabilitas suatu variabel berdasarkan nilai koefisien dari *Cronbach's Apha*.

Tabel 3.2 Kriteria Keputusan Reliabilitas

Koefisien *Cronbach's Alpha*	Keputusan
≥ 0.70	Reliabel
< 0.70	Tidak Reliabel

Sumber: Kusnendi, 2008, p. 96

3.7.1 Hasil Uji Reliabilitas

Uji reliabilitas menggunakan 30 responden dengan SPSS.

Tabel 3.3 Hasil Uji Reliabilias

Variabel	Hasil (r hitung)	Kriteria (r tabel)
Mng	0.803	≥ 0.70
WoCa	0.768	≥ 0.70
RRF	0.882	≥ 0.70
OpMng	0.709	≥ 0.70
ChaMng	0.710	≥ 0.70
OrgCult	0.923	≥ 0.70
Knowldg	0.719	≥ 0.70
SecCom	0.717	≥ 0.70
SecBehv	0.788	≥ 0.70
SIWI	0.768	≥ 0.70
TAA	0.823	≥ 0.70
ISP	0.827	≥ 0.70
PST	0.885	≥ 0.70
Attitd	0.782	≥ 0.70
ISC	0.889	≥ 0.70

Sumber: Hasil Olahan Data

Berdasarkan pengujian reliabilitas menggunakan SPSS, nilai dari semua variabel dinyatakan reliabel karena nilainya lebih dari 0.70.

4. HASIL DAN PEMBAHASAN

4.1 Karakteristik Responden

Responden adalah pegawai Runah Sakit di Kota Bandung, meliputi Kepala Rumah Sakit/Direktur/Manajer/Kepala Bagian, Dokter Spesialis, Dokter Umum/Dokter Gigi, Perawat, Pegawai IT dan Administrasi.

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

a. Jenis Kelamin

Tabel 4.1 Jenis Kelamin Responden

Jenis Kelamin	
Pria	Wanita
70	99

Sumber: Hasil Kuisioner

Dari 169 data responden, terdapat pria sejumlah 70 orang atau 41% dari total jumlah dan wanita sejumlah 99 orang atau 59% dari total jumlah.

b. Usia

Tabel 4.2 Usia Responden

Usia			
≤ 18	19~29	30~39	≥ 40
0	73	60	36

Sumber: Hasil Kuisioner

Terdapat usia 19 - 29 tahun sejumlah 73 orang atau 43%, usia 30 - 39 tahun sejumlah 60 orang atau 36% dan usia lebih dari 40 tahun sejumlah 36 orang atau 21% dari total jumlah.

c. Latar Belakang Pendidikan

Tabel 4.3 Latar Belakang Pendidikan Responden

Latar Belakang Pendidikan Responden				
SMP	SMA/SMK	D1/D2/D3	S1	S2/S3
0	32	63	58	16

Sumber: Hasil Kuisioner

Terdapat lulusan SMA/SMK sejumlah 32 orang atau 19%, D1/D2/D3 sejumlah 63 orang atau 37%, S1 sejumlah 58 orang atau 34% dan S2/S3 sejumlah 16 orang atau 10% dari total jumlah.

d. Lama Bekerja

Tabel 4.4 Lama Bekerja Responden

Lama Bekerja Responden			
<1	1~5	5~10	>10
13	68	35	53

Sumber: Hasil Kuisioner

Terdapat pengalaman kerja <1 tahun sejumlah 13 orang atau 8%, 1 – 5 tahun sejumlah 68 orang atau 40%, 5 – 10 tahun sejumlah 35 orang atau 21% dan > 10 tahun sejumlah 53 orang atau 31% dari total jumlah.

e. Posisi Pekerjaan

Tabel 4.5 Posisi Pekerjaan Responden

Jabatan Pekerjaan	Jumlah
Kepala Rumah Sakit/Direktur/Manajer/Kepala Bagian	19
Dokter Umum/Dokter Gigi	8
Dokter Spesialis	5
Administrasi	71
Perawat	48
Pegawai IT	13
Analisis Kesehatan	3
Analisis Laboratorium	2

Sumber: Hasil Kusioner

Posisi kerja sebagai Kepala Rumah Sakit/Direktur/Manajer/Kepala Bagian ada 19 orang atau 11%, Dokter Spesialis ada 5 orang atau 3%, Dokter Umum/Dokter Gigi ada 8 orang atau 5%, Perawat ada 48 orang atau 28%, Pegawai IT ada 13 orang atau 8% dan Administrasi ada 71 orang atau 42%.

f. Pengelolaan Informasi

Tabel 4.6 Pengelolaan Informasi oleh Responden

Pengelolaan Informasi		
Manual	Elektronik	Campuran
12	14	143

Sumber: Hasil Kuisioner

Terdapat pengelolaan informasi secara campuran *(paper-based dan computer-based)* dilakukan oleh 143 orang atau 85% dari total jumlah, pengelolaan informasi secara elektronik *(computer-based)* dilakukan oleh 14 orang atau 8% dari total jumlah dan pengelolaan informasi secara manual *(paper-based)* dilakukan oleh 12 orang atau 8% dari total jumlah.

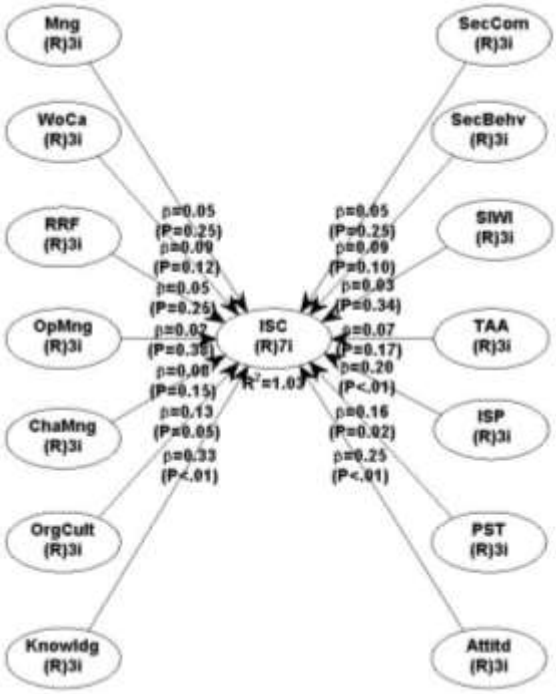
p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

g. Kebijakan Keamanan Informasi

Berdasarkan hasil penyebaran dari kuisioner, semua responden memiliki kebijakan terkait keamanan informasi.

4.2 Evaluasi Model

Pengujian hipotesis pada penelitian ini dilakukan dengan menguji 14 variabel dengan metode analisis SEM-PLS menggunakan WarpPLS versi 6.0.



Gambar 4.1 Hasil Pengujian Hipotesis Model 1
Sumber: Hasil Olahan Data

Pengujian hipotesis menunjukkan bahwa semua variabel memengaruhi budaya keamanan informasi.

4.2.1 Evaluasi Model Pengukuran

4.2.1.1 Validitas Konvergen

Tabel 4.7 *Loading Factors and Cross-Loadings*

Pengaruh Antar Variabel		Hasil
X1.1		0.891
X1.2	X1	0.901
X1.3		0.864
X2.1		0.830
X2.2	X2	0.848
X2.3		0.771
X3.1		0.873
X3.2	X3	0.885
X3.3		0.838
X4.1		0.839
X4.2	X4	0.812
X4.3		0.724
X5.1		0.853
X5.2	X5	0.863
X5.3		0.768
X6.1		0.873
X6.2	X6	0.878
X6.3		0.857
X7.1		0.867
X7.2	X7	0.878
X7.3		0.826
X8.1		0.852
X8.2	X8	0.919
X8.3		0.916
X9.1		0.868
X9.2	X9	0.838
X9.3		0.836
X10.1		0.863
X10.2	X10	0.890
X10.3		0.873
X11.1		0.883
X11.2	X11	0.876
X11.3		0.738
X12.1		0.863
X12.2	X12	0.862
X12.3		0.872
X13.1		0.778
X13.2	X13	0.850
X13.3		0.818
X14.1		0.819
X14.2	X14	0.715
X14.3		0.676
Y1		0.732
Y2		0.751
Y3	Y	0.766
Y4		0.668
Y5		0.812
Y6		0.816
Y7		0.811

Sumber: Hasil Olahan Data

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

Hasil pengujian validitas konvergen menunjukkan bahwa semua variabel yang diuji adalah valid, karena semua nilai dari *cross-loading* lebih besar dari 0.5 dan semua nilai dari *loading factor* lebih kecil dari 0.5.

4.2.1.2 Validitas Diskriminan

Tabel 4.8 *Average Variance Extracted (AVE)*

Variabel	AVE	Kriteria
X1	0.886	≥ 0.5
X2	0.817	≥ 0.5
X3	0.865	≥ 0.5
X4	0.793	≥ 0.5
X5	0.829	≥ 0.5
X6	0.869	≥ 0.5
X7	0.857	≥ 0.5
X8	0.896	≥ 0.5
X9	0.847	≥ 0.5
X10	0.875	≥ 0.5
X11	0.835	≥ 0.5
X12	0.865	≥ 0.5
X13	0.816	≥ 0.5
X14	0.739	≥ 0.5
Y	0.767	≥ 0.5

Sumber: Hasil Olahan Data

Hasil pengujian validitas diskriminan menunjukkan bahwa semua variabel yang diuji adalah valid, karena seluruh nilai dari AVE lebih besar dari 0.5.

4.2.1.3 Reliabilitas

Tabel 4.9 *Composite Reliability*

Variabel	*Composite Reliable*	Kriteria
X1	0.916	≥ 0.7
X2	0.858	≥ 0.7
X3	0.899	≥ 0.7
X4	0.835	≥ 0.7
X5	0.868	≥ 0.7
X6	0.903	≥ 0.7
X7	0.892	≥ 0.7
X8	0.924	≥ 0.7
X9	0.884	≥ 0.7
X10	0.908	≥ 0.7
X11	0.873	≥ 0.7
X12	0.900	≥ 0.7
X13	0.856	≥ 0.7
X14	0.782	≥ 0.7
Y	0.909	≥ 0.7

Sumber: Hasil Olahan Data

Hasil pengujian *composite reliability* menunjukkan bahwa semua variabel yang diuji adalah reliabel karena selurun nilai dari *composite reliability* lebih dari 0.7.

4.2.2 Evaluasi Model Struktural

4.2.2.1 Uji Hipotesis dan Koefisien Regresi

Tabel 4.10 Uji Hipotesis dan Koefisien Regresi

Pengaruh Antar Variabel		*Path Coefficients (β)*	*P-values*
X1	Y	0.052	0.249
X2		0.089	0.121
X3		0.051	0.253
X4		0.023	0.383
X5		0.078	0.153
X6		0.127	0.046
X7		0.334	< 0.001
X8		0.052	0.247
X9		0.095	0.105
X10		0.031	0.342
X11		0.071	0.174
X12		0.205	0.003
X13		0.157	0.018
X14		0.246	< 0.001

Sumber: Hasil Olahan Data

Berdasarkan hasil pengujian hipotesis dan koefisien regresi yang telah dilakukan, kesimpulannya adalah:

1. *Management* tidak memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan informasi
2. *Workplace Capability* tidak memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan informasi.
3. *Risk and Response Factors* tidak memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan informasi.

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

4. *Operational Management* tidak memiliki pengaruh yang positif dan signfikan terhadap budaya keamanan informasi.
5. *Change Management* tidak memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan informasi.
6. *Organisational Culture* memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan informasi.
7. *Knowledge* memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan informasi.
8. *Security Compliance* tidak memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan informasi.
9. *Security Behavior* tidak memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan informasi.
10. *Soft Issues – Workplace Independent* tidak memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan informasi.
11. *Training and Awareness* tidak memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan informasi.
12. *Information Security Policies* memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan informasi.
13. *Perceived Security Threat* memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan informasi.
14. *Attitude* memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan informasi.

4.2.2.2 Model Fit Indeks

Tabel 4.11 Model Hit Indeks

Indeks	Hasil	Kriteria
Average Path Coefficient (APC)	0.115 P = 0.032	P < 0.05
Average R-squared (ARS)	1.035 P < 0.001	P < 0.05
Average adjusted R-squared (AARS)	1.038 P < 0.001	P < 0.05
Average block VIF (AFIV)	2.528	*acceptable if ≤ 5 ideally if ≤ 3.3*
Average full collinearity VIF (AFVIF)	2.699	*acceptable if ≤ 5 ideally ≤ 3.3*
Tenenhaus GoF (GoF)	0.853	*small ≥ 0.1 medium ≥ 0.25 large ≥ 0.36*
Sympson's paradox ratio (SPR)	1	*acceptable if ≥ 0.7 ideally = 1*
R-squared contribution ratio (RSCR)	1	*acceptable if ≥ 0.9 ideally = 1*
Statistical suppression ratio (SSR)	1	*acceptable if ≥ 0.7*
Nonlinear bivariate causality direction ratio (NLBCDR)	1	*acceptable if ≥ 0.7*

Sumber: Hasil Olahan Data

Berdasarkan hasil pengujian model fit indeks menunjukkan bahwa semua kriteria telah dipenuhi karena seluruh nilai dari semua indeks telah diterima.

4.3 Bahasan Penelitian

Faktor-faktor yang memengaruhi budaya keamanan informasi di rumah sakit di Kota Bandung adalah *organisational culture*, *knowledge*, *information security policies*,

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

perceived security threat dan *attitude*. Sedangkan *management*, *workplace capabilities*, *risk and response factors*, *operational management*, *change management*, *security compliances*, *security behaviour*, *soft issues – workplace independent* dan *training and awareness* tidak memengaruhi.

Organisational culture memengaruhi budaya keamanan informasi di rumah sakit menggambarkan bahwa rumah sakit menjunjung tinggi keterbukaan dan transparansi yang bebas dari arus informasi yang mengalir di organisasi. Oleh karena itu, rumah sakit tidak membatasi informasi yang tersebar dan hal ini berdampak pada bagaimana cara informasi diproses serta dilindungi, lalu akhirnya memengaruhi budaya keamanan informasi (Sherif et al, 2015), Flores et al, 2014), (Alfawaz et al, 2010), (Dojkovski et al, 2010).

Knowledge di rumah sakit menjelaskan mengenai pengetahuan dan pemahaman pegawai-pegawai di rumah sakit mengenai keamanan informasi, hal tersebut dapat menyebabkan pengaruh bagaimana cara mereka memroses informasi sampai dengan menggunakan kontrol untuk keamanan informasi. Pengetahuan mereka mengenai keamanan informasi dapat disampaikan melalui cara yang implisit atau eksplisit untuk menanamkan ketaatan terhadap kebijakan keamanan informasi (Da Veiga & Martins, 2017).

Information security policies yang memengaruhi budaya keamanan informasi merupakan pengetahuan dan sudut pandang pegawai-pegawai di rumah sakit terhadap aturan dan prosedur kebijakan keamanan informasi. Hal tersebut dapat memengaruhi budaya keamanan informasi secara positif yang penting sebagai landasan untuk mengarahkan budaya keamanan informasi dan menciptakan nilai serta keyakinan bersama (Box & Pottas, 2013), (Da Veiga, 2015), (Parsons et al, 2014), (Hassan & Ismail, 2016).

Perceived security threat menjelaskan sejauh mana pegawai-pegawai di rumah sakit memiliki persepsi atau paradigma (cara pandang terhadap sesuatu) mengenai ancaman keamanan informasi. Hal tersebut akan memengaruhi budaya keamanan informasi (Wardani, 2017), (Ahlan et al, 2015).

Attitude merupakan faktor umum bagaimana sikap dan pendirian dari pegawai-pegawai di rumah sakit dapat dikendalikan melalui persuasi sebagai reaksi atau sambutan terhadap komunikasi. Sikap yang positif terhadap keamanan informasi dapat dicapai jika ada kekuatan penggerak untuk mematuhi kebijakan keamanan informasi di rumah sakit (Ahlan, 2015).

Semua faktor tersebut dapat menjadi dasar atau landasan untuk mengukur budaya keamanan informasi sehingga dapat menganalisis langkah-langkah apa saja yang perlu diambil untuk mencegah serangan dan ancaman keamanan informasi.

5. KESIMPULAN

Berdasarkan rumusan permasalahan penelitian dan pembahasan hasil penelitian, maka dapat disimpulkan bahwa hasil dari penelitian adalah sebagai berikut:

1. Tidak terdapat pengaruh yang signifikan dari *Management* terhadap *Information Security Culture*.
2. Tidak terdapat pengaruh yang signifikan dari *Workplace Capabilities* terhadap *Information Security Culture.*
3. Tidak terdapat pengaruh yang signifikan dari *Risk and Response Factors* terhadap *Information Security Culture.*
4. Tidak terdapat pengaruh yang signifikan dari *Operational Management* terhadap *Information Security Culture.*
5. Tidak terdapat pengaruh yang signifikan dari *Change Management* terhadap *Information Security Culture*.

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

6. Terdapat pengaruh yang signifikan dari *Organisational Culture* terhadap *Information Security Culture*.
7. Terdapat pengaruh yang signifikan dari *Knowledge* terhadap *Information Security Culture*.
8. Tidak terdapat pengaruh yang signifikan dari *Security Compliances* terhadap *Information Security Culture*.
9. Tidak terdapat pengaruh yang signifikan dari *Soft Issues – Workplace Independent* terhadap *Information Security Culture*.
10. Tidak terdapat pengaruh yang signifikan dari *Security Behavior* terhadap *Information Security Culture*.
11. Tidak terdapat pengaruh yang signifikan dari *Training and Awareness* terhadap *Information Security Culture*.
12. Terdapat pengaruh yang signifikan dari *Information Security Policies* terhadap *Information Security Culture*.
13. Terdapat pengaruh yang signifikan dari *Perceived Security Threat* terhadap *Information Security Culture*.
14. Terdapat pengaruh yang signifikan dari *Attitude* terhadap *Information Security Culture*.

6. REFERENSI

Ashford, Warwick. 2018. *Most healthcare organisations have been breached, report shows.*

BINUS University. 2019. Sistem Informasi Manajemen Rumah Sakit (SIMRS).

Box, Debra & Pottas, Dalenca. 2013. *Improving information security behaviour in the healthcare context.* Procedia Technology 9, pp.1093 – 1103.

BPJS Kesehatan. 2019. Jumlah Rumah Sakit di Indonesia.

Center for Internet Security. 2018. Data Breaches: *In the Healthcare Sectors*.

CNN Indonesia. 2018. Serangan WannaCry Peringatan untuk Rumah Sakit.

Detik News. 2019. Serangan WannaCry, 30 Persen Komputer di RS Dharmais Terpaksa Offline.

Detik News. 2019. Imbas Serangan WannaCry, Antrean Panjang Terlihat di RS Dharmais.

Forbes. 2017. *The Real Threat of Identity Theft Is in Your Medical Records, Not Credit Cards.*

Hair, Joe F., Ringle, Christian M. & Sarstedt, Marko. 2011. *PLS-SEM: Indeed a Silver Bullet, Journal of Marketing Theory and Practice*, 19:2, 139-152.

Hassan, Noor Hafizah & Ismail, Zuraini. 2016. *Information Security Culture in Healthcare Informatics: A Preliminary Investigation.* Journal of Theoretical and Applied Information Technology Vol.88. No.2, pp. 202 – 209

Hipaajournal(a). 2018. *Report healthcare data breach in Q1 2018*.

Hipaajournal(b). 2018. *Analysis Q4 2017 healthcare security breaches*.

Hipaajournal(c). 2018. *Healthcare data breach statistics.*

Kementerian Kesehatan. 2018. Data Rumah Sakit Online.

Kementerian Kesehatan. 2019. SIMRS untuk Rumah Sakit.

Kock, N. 2017. *WarpPLS 6.0 User Manual*. Laredo, Texas, USA.

Kruger, Hennie., et al. 2010. *A vocabulary Test to Assess Information Security Awareness*.

South African Information Security Multi-conference in Port Elizabeth, South Africa.

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

Tribun News. 2019. Kepala BSSN Ungkap Ancaman yang Dihadapi Sejumlah Negara.

Kruger, H.A. & Kearney, W.D. 2006. *A Protoype for Assessing Information Security Awareness*. Elsevier Journal: Computers & Security. page 289-296.

Kusnendi. 2008. Model-model Persamaan Struktural. Bandung: Alfabeta.

Latan, H., & Ghozali, I. 2012. Partial Least Squares Konsep, Metode dan Aplikasi WarpPLS 2.0. Semarang: Badan Penerbit - UNDIP.

Masrom, Maslin; Rahimly, Ailar. 2015. *Overview od Data Security Issues in Hospital Information Systems*, Pacific Asia Journal of the Association for Information Systems Vol. 7 No. 4, pp.51-66

Mitchell, Ruth C. Et al. 1999. *Corporate Information Security Management*. New Library World Vol 100, Number 1150 pp 213-227. MCB University Press. London UK ISSN 0307-4803

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

Peraturan Menteri Kesehatan (2018) Klasifikasi Rumah Sakit.

Pusat Data dan Informasi Kementerian Kesehatan. 2018. Sistem Manajemen Keamanan Informasi.

Schick, Shane. 2018. Security Breaches in Healthcare*: 70 Percent of Organizations Hit Globally*, Report Shows.

Sekaran, Uma. 2011. Metodologi Penelitian Untuk Bisnis, Edisi 4. Jakarta: Salemba Empat.

Sugiyono. 2014. Metode penelitian bisnis. Bandung: Alfabeta

Tempo.co. 2019. Diserang Virus Ransomware, Komputer Rumah Sakit Dharmais Lumpuh.