Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 1, No. 9, September 2017, hlm. 783-792 http://j-ptiik.ub.ac.id

Analisis Hubungan Kesadaran Keamanan, Privasi Informasi, dan Perilaku Keamanan Pada Para Pengguna Media Sosial *Line*

Irfan Arif Afandi[1], Ari Kusyanti[2], Niken Hendrakusma Wardani[3]

Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]13515S0401111074@mail.ub.ac.id, [2]ari.kusyanti@ub.ac.id, [3]niken13@ub.ac.id

Abstrak

LINE merupakan aplikasi pengirim pesan yang kerap kali dijadikan sebagai media perbuatan yang tidak normatif dan dijadikan sebagai lahan mencari keuntungan tertentu secara sepihak oleh para pelaku tindak kejahatan berbasis jejaring internet *(cyber crime)*. Penelitian ini bertujuan untuk menganalisis lebih mendalam mengenai faktor apa saja yang memengaruhi perilaku keamanan pada pengguna *LINE*. Model penelitian ini terdiri dari 8 konstruk. Adapun konstruk model terdiri dari *Security Awareness, Self–Effiacy in Information Security, Expectation, Security Behavior, Cues to Action, Perceived Susceptibility/Perceived Severity*, *Perceived Security Threat,* dan *Internet Users Information Privacy Concerns*. Analisis data pada penelitian ini bersumber pada hasil kuesioner yang dibagikan pada para pengguna *LINE*. Analisis korelasi dan kekuatan korelasi antara variabel laten atau konstruk menggunakan *Structural Equation Modeling* (SEM). Dari hasil penelitian menunjukan bahwa variabel *Cues to Action* memiliki hubungan positif dan berpengaruh signifikan terhadap variabel *Perceived Security Threat;* variabel *Self–Efficacy in Information Security* memiliki hubungan positif dan berpengaruh signifikan terhadap variabel *Expectations;* variabel *Perceived Security Threat* memiliki hubungan positif dan berpengaruh signifikan terhadap variabel *Internet Users' Information Privacy Concerns*; variabel *Perceived Security Threat* memiliki hubungan positif dan berpengaruh signifikan terhadap variabel *Security Behavior*.

Kata kunci: *LINE, Structural Equation Modeling, Internet Users Information Privacy Concerns (IUIPC), Security Belief Model, Perilaku Keamanan*

Abstract

LINE is the messaging application that often used as a way to non-normative act and used as media is looking for profit or benefit unilaterally by the peoples who work in cyber crime. This research attempted to explore the main factors affecting security behavior of LINE users. The research model comprised of eight constructs. The constructs were security awareness, self–effiacy in information security, expectation, security behavior, cues to action, perceived susceptibility/perceived severity, perceived security threat, and internet users information privacy concerns. It analyzed data collected from qustionnaire survey on users of LINE. Correlations and strength of corelations between laten constructs were identified using Structural Equation Modeling (SEM). The result of this research show that Cues to Action have significant and positive influence on Perceived Security Threat; Self–Efficacy in Information Security have significant and positive influence on Expectations; Perceived Security Threat have significant and positive influence on Internet Users Information Privacy Concerns; and Perceived Security Threat have significant and positive influence on Security Behavior.

Keywords: *LINE, Structural Equation Modeling, Internet Users Information Privacy Concerns (IUIPC), Security Belief Model, Security Behavior*

1. PENDAHULUAN

Dengan layanan canggih yang tersedia pada teknologi informasi dengan berbasis internet memudahkan manusia untuk saling berkomunikasi dan berinteraksi satu sama lain. Bahkan dengan adanya teknologi informasi berbasis internet, proses bisnis pun dapat dengan mudah dijalankan. Namun, pemanfaatan teknologi informasi, media, dan komunikasi telah mengubah perilaku masyarakat maupun

peradaban manusia secara global.

Meskipun kerapkali pemanfaatan teknologi informasi dijadikan sebagai tindakan yang tidak normatif, tingkat ketergantungan masyarakat terhadap teknologi informasi terlebih pada situs jejaring media sosial semakin meningkat. Menurut Kementerian Komunikasi dan Informatika (Kekominfo) tercatat 63 juta penduduk indonesia menggunakan internet, dan dari angka tersebut terbilang 95% menggunakan internet untuk mengakses layanan jejaring sosial (Kominfo, 2017).

LINE, merupakan situs jejaring media sosial yang sangat populer, khusunya di Indonesia. Menurut *Managing Director LINE* Indonesia tercatat pengguna *LINE* 88.000.000 per juni 2016, di Indonesia (Bohang, F.K., 2016). *LINE* juga dapat dioperasikan di berbagai *platform*, termasuk *notebook, tablet*, dan komputer. *LINE* semakin populer dibuktikan dengan kesuksesan menjadi aplikasi *messenger* yang paling laris di 42 negara, termasuk Indonesia (Chandrataruna, M & Ngazis, A. R, 2013).

Tanpa disadari ada beberapa kemungkinan buruk atau risiko yang tidak terduga bisa terjadi begitu saja. Beberapa kasus yang sempat membuat pengguna *LINE* merasa terganggu adalah adanya himbauan dari *CEO NH Corporation* untuk melakukan perubahan *password* dan *username* secara berkala, serta untuk tidak menggunakan *username* dan *password* yang sama dengan situs jejaring internet lainnya, hal tersebut dilakukan untuk mengantisipasi adanya tindakan pembajakan *(hacked)* oleh oknum yang tidak bertanggung jawab (Susilo, R., 2014). Pada pertengahan tahun 2014, tepatnya dibulan juni di Tokyo, Jepang, sedikitnya 303 pemilik akun *LINE* mengadu kepada polisi telah tertipu oleh akun yang seolah dia kenal. Selain itu tepat di akhir bulan Mei 2014, beberapa warga Korea yang menggunakan *LINE* mengalami kejadian penipuan yang sama. Setelah kasus tersebut diselidiki oleh pihak yang berwajib ternyata akun tersebut dari pembajak untuk menipu pengguna *LINE* supaya membeli *web-money* (uang elektronik) yang ditawarkan oleh pelaku yang tidak bertanggung jawab (Susilo, Richard, 2014).

Aplikasi *LINE* dituduh oleh pemerintah Thailand secara sengaja membuka peluang bagi pihak ketiga untuk mengakses dan melihat percakapan penggunanya. Sejumlah pakar teknologi di Thailand telah melakukan tes untuk menguji kemanan data privasi pengguna *LINE*, dan hasilnya mereka berhasil 'mengintip' sejumlah sesi percakapan pengguna *LINE* dengan mudah. Disebutkan bahwa para pakar tersebut hanya memerlukan sebuah *software* khusus yang menurut mereka umum dimiliki oleh para penyelenggara jasa telekomunikasi seperti operator seluler dan penyedia layanan *Internet Service Provider* (ISP) (Maulana, 2013).

Menyadari risiko keamanan personal informasi yang disebabkan oleh perilaku membagikan informasi di media sosial atau situs jejaring internet, banyak penelitian yang telah dilakukan. Salah satunya adalah penelitian dengan judul "*Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer Users"* oleh Edwards (2015), namun penelitian tersebut memiliki kelemahan dalam menganalisis praktik *security awareness*, *information privacy*, dan *security behavior* yang masih menggunakan metode *concern for information privacy* (CFIP). Sebelumnya, metode CFIP ditentang oleh Malhotra, Kim & Agarwal (2004), mereka beranggapan bahwa model CFIP masih ada beberapa kekurangan.

Berdasarkan hal di atas, penulis tertarik untuk membuat analisis pemahaman dan mencari faktor apa saja yang memengaruhi kesadaran pengguna media sosial *LINE* dalam praktik perilaku keamanan *(security behavior)* dengan menerapkan model *internet users' for information privacy concern* (IUIPC) yang merupakan metode yang sudah baku dan lebih modern (Malhotra et al, 2004).

2. DASAR TEORI

A. *Structural Equation Modeling* (SEM)

Structural Equation Modeling (SEM) merupakan salah satu analisis multivariat yang mampu menganalisis hubungan antarvariabel secara lebih kompleks. Teknik analisis multivariat dengan menggunakan SEM digunakan para peneliti untuk melakukan pengujian hubungan antara variabel laten dan variabel manifes (persamaan pengukuran), hubungan antara variabel laten yang satu dengan variabel laten yang lain (persamaan struktural), serta memaparkan kesalahan pengukuran. Variabel laten adalah variabel yang memerlukan indikator untuk melakukan pengukuran atau pengujian (Sarjono & Julianita, 2015).

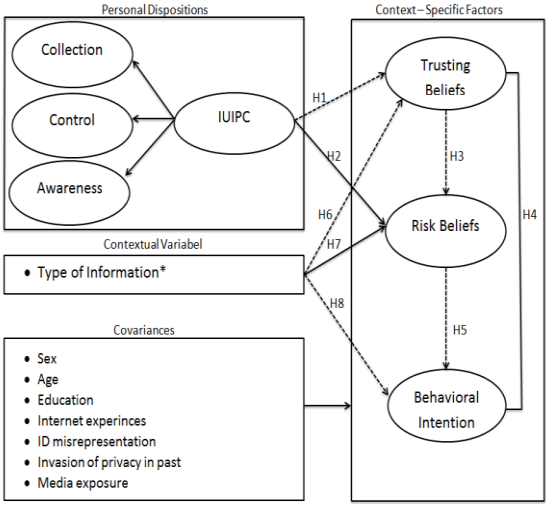
Sedangkan Variabel Manifes merupakan variabel yang berperan sebagai indikator dalam sebuah model penelitian SEM, atau variabel yang dikenal sebagi variabel yang dapat diamati dan diukur secara langsung (Sarjono & Julianita, 2015). Variabel manifes berfungsi sebagai indikator bagi variabel laten.

B. *Internet Users' Information Privacy Concerns* (IUIPC)

Internet Users' Information Privacy Concerns (IUIPC) adalah model kerangka kerja yang memasalahkan secara inti dengan merujuk ke dalam konteks pandangan subyektif kewajaran bagi setiap individu dalam berinteraksi dan menggunakan jaringan internet terlebih dalam praktik privasi informasi personal (Malhotra et al, 2004).

Internet Users' Information Privacy Concerns (IUIPC) merupakan pengembangan dari model *concern for information privacy* (CFIP) yang digagas oleh Stewart dan Segars (2002) dengan memformulasikan dimensi pembentuk atas privasi informasi personal dengan pengkoleksian (*collection*), kesalahan (*errors*), penggunaan pihak sekunder takterotorisasi (*unauthorized secondary used*) dan akses tidak sah (*improper access*) (Malhotra et al, 2004). Namun seiring dengan perkembangan internet yang begitu cepat, Malhotra et al (2004) menentang terhadap model CFIP dengan mengemukakan formulasi model baru yang lebih modern, yakni *internet users' for information privacy concern* (IUIPC). Formulasi dimensinya dikerangkakan dalam pengkoleksian *(collection)*, pengendalian *(control)* dan kesadaran terhadap praktik privasi informasi (*awareness of privacy practices*).

Malhotra et al (2004) mengkonstruksikan IUIPC yang mengkaitkan ketiga dimensi dengan keyakinan kepercayaan *(trusting beliefs)*, keyakinan risiko *(risk beliefs)* dan intensi keperilakuan *(behavioral intention)*. Berdasarkan penjelasan diatas, maka didapatkan model IUIPC yang tersaji pada Gambar 1.

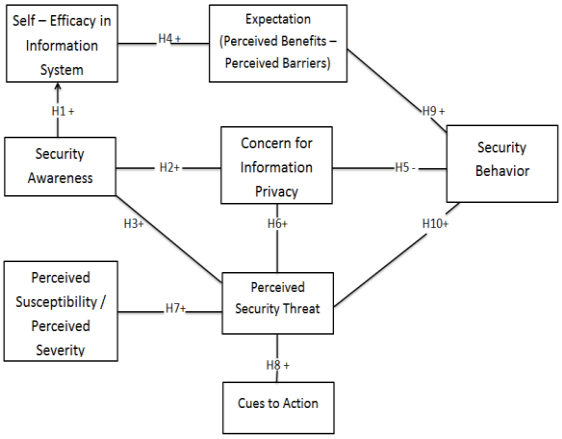


Gambar 1. Model *IUIPC*

C. *Security Belief Model*

Security Belief Model merupakan model yang dibuat untuk menganalisa perilaku pengguna personal komputer untuk melakakukan tindakan sadar yang sewajarnya akan keamanan saat sedang mengakses jaringan internet (Edwards, 2015).

Model formulasi dari hasil penelitian Edwards (2015) didasarkan atas sebuah keyakinan bahwa kesadaran terhadap keamanan *(security awareness) memiliki* dampak pada tingkat pemahaman atau pengetahuan pengguna terkait keamanan informasi *(self-efficacy in information security)* saat sedang mengakses jaringan internet. Pemahaman atau pengetahuan pengguna terkait keamanan informasi *(self-efficacy in information security)* saat sedang mengakses jaringan internet memiliki dampak positif terhadap harapan pengguna *(user's expectations)*, dan harapan pengguna *(user's expectations)* akan memiliki dampak positif terhadap kemauan pengguna untuk berperilaku yang baik atas tindakan keamanan. Selain itu kesadaran terhadap keamanan *(security awareness)* seharusnya memiliki dampak positif terkait persepsi ancaman pengguna *(user's threat perception)* dan kesadaran terkait praktik *information privacy (concern for information privacy).* Dan kesadaran terkait praktik *information privacy (concern for information privacy)* memiliki dampak negatif terhadap perilaku pengguna atas keamanan *(user's seccurity behavior)*. Model *Security Belief Model* dapat dilihat pada Gambar 2.



Gambar 2. *Security belief model*

3. MODEL PENELITIAN DAN RUMUSAN HIPOTESIS

A. Definisi Konstruk Penelitian

Security Awareness (SA)

Security awareness bisa didefinisikan bahwa seseorang memiliki pengetahuan atau kemampuan yang baik dalam melakukan praktik keamanan pada saat menggunakan situs jejaring internet dan memahami arti penting melindungi data pribadi dan atau data kelompok atas nama sebuah organisasi ketika memutuskan akan menggunakan sebuah situs jejaring internet.(Edwards, 2015).

Self–efficacy in Information Security (SEIS)

Self–Efficacy in Informtion Security dapat disimpulkan sebagai kepercayaan pada kemampuan diri sendiri bahwa tanpa meminta bantuan orang lain, seseorang tersebut mampu untuk melindungi personal informasi dan sistem informasi dari pengungkapan yang tidak sah, modifikasi, kehilangan, kerusakan, dan kurangnya ketersediaan atau pengkoleksian data oleh penyedia atau pengembang layanan situs jejaring internet (Rhee et al, 2009).

Expectations (Perceived Benefits–Perceived Barriers) (EPB)

Menurut Edwards (2015) *perceived barriers* dan *perceived benefit* merupakan variabel yang sama-sama memiliki dampak secara langsung untuk memengaruhi perilaku keamanan seseorang dalam menggunakan sebuah layanan jejaring internet. Maka dari itu, *perceived barriers* dan *perceived benefits* dijadikan dalam satu konstruk yaitu variabel *expectations*, sebab dua variabel tersebut memiliki kesamaan arti. *Perceived Barriers* adalah sejauh mana seseorang memprediksikan hambatan dalam melakukan sebuah aktifitas. (Glanz et al, 2008). *Perceived Benefits* adalah sejauh mana seseorang meyakini tentang keefektivitasan atau manfaat apa yang diperoleh ketika telah melakukan sebuah aktifitas. (Ng et al, 2009).

Security Behavior (SB)

Security Behavior adalah perilaku atau aktifitas melindungi data pribadi dan atau data kelompok atas nama sebuah organisasi ketika memutuskan akan menggunakan sebuah situs jejaring internet dalam melakukan aktifitas tertentu. (Edwards, 2015).

Cues to Action (CTA)

Cues to Action adalah sebuah kegiatan yang ditujukan untuk dapat memotivasi atau memicu perubahan perilaku atau persepsi seseorang ketika memutuskan untuk menggunakan sebuah situs jejaring internet untuk sadar akan pentingnya melakukan tindakan menjaga keamanan privasi informasi. (Ng, Xu, 2007 ; Edwards, 2015).

Perceived Susceptibility / Perceived Severity (PS)

Perceived Susceptability adalah keyakinan seseorang akan adanya suatu risiko ketika sedang melakukan sebuah aktifitas atau seseorang memiliki kerentanan risiko yang buruk ketika memberikan sebuah privasi informasinya ke situs jejaring internet (Ng et al, 2009 ; Edwards, 2015). *Perceived Severity* adalah keyakinan seseorang terhadap hal–hal buruk yang akan terjadi padanya ketika dia terpengaruh pada isu–isu tertentu (Glanz et al, 2008).

Perceived Security Threat (PCT)

Perceived Security Therat adalah sejauh mana seseorang memiliki persepsi atau paradigma akan sebuah ancaman keamanan (Liang & Xue, 2010).

Internet User's Information Privacy Concerns (IUIPC)

Internet Users' Information Privacy Concerns (IUIPC) adalah model kerangka kerja yang memasalahkan secara inti dengan merujuk ke dalam konteks pandangan subyektif kewajaran bagi setiap individu dalam berinteraksi dan menggunakan jaringan internet terlebih dalam praktik privasi informasi personal

(Malhotra, Kim & Agarwal ,2004).

B. Rumusan Hipotesis

Berdasarkan penjelasan konstruk penelitian diatas, terdapat sembilan konstruk yang digunakan dalam penelitian dengan 10 rumusan hipotesis, yaitu :

H1 Ada hubungan antara kesadaran terhadap keamanan *(security awareness)* (SA) dan pengetahuan pengguna dalam memahami praktik keamanan informasi *(self-efficacy in information security)* (SEIS).

H2 Ada hubungan antara kesadaran terhadap keamanan *(security awareness)* (SA) dan tingkat perhatian pengguna *LINE* terhadap data privasi informasi saat mereka berikan ketika berinteraksi dan menggunakan jaringan internet terlebih dalam praktik privasi informasi *(internet users' information privacy concerns)* (IUIPC).

H3 Ada hubungan positif antara kesadaran terhadap keamanan *(security awareness)* (SA) dan persepsi pengguna terhadap ancaman keamanan *(perceived security threat)* (PCT).

H4 Ada hubungan antara pengetahuan pengguna dalam memahami praktik keamanan informasi *(self-efficacy in information security)* (SEIS) dan harapan pengguna (persepsi kemanfaatan – persepsi hambatan *(expectations perceived benefits–perceived barriers)* (EPB).

H5 Ada hubungan antara tingkat perhatian pengguna *LINE* terhadap data privasi informasi saat mereka berikan ketika berinteraksi dan menggunakan jaringan internet terlebih dalam praktik privasi informasi *(internet users' information privacy concerns)* (IUIPC). dan perilaku keamanan *(Security Behavior)* (SB).

H6 Ada hubungan antara persepsi pengguna terhadap ancaman keamanan *(perceived security threat)* (PCT) dan kewajaran pengguna dalam berinteraksi dan menggunakan jaringan internet terlebih dalam praktik privasi informasi personal informasi *(internet users' information privacy concerns)* (IUIPC).

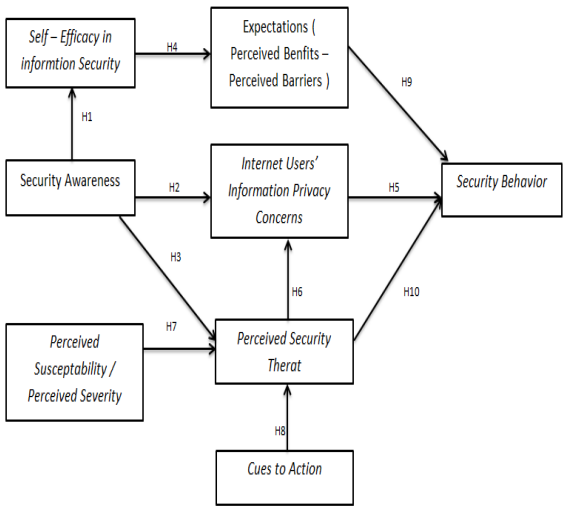
H7 Ada hubungan antara persepsi kelemahan/persepsi keparahan *(perceived susceptability/perceived severity)* (PS) dan persepsi pengguna terhadap ancaman keamanan *(perceived security threat)* (PCT).

H8 Ada hubungan antara aktifitas yang memotivasi untuk merubah perilaku pengguna *(cues to action)* (CTA) dan persepsi pengguna terhadap ancaman keamanan *(perceived security threat)* (PCT).

H9 Ada hubungan antara harapan pengguna (persepsi kemanfaatan–persepsi hambatan *(expectations perceived benefits–perceived barriers)*) (EPB) dan perilaku keamanan *(security behavior)* (SB).

H10 Ada hubungan antara persepsi pengguna terhadap ancaman keamanan *(perceived security threat)* (PCT) dan perilaku keamanan *(security behavior)* (SB).

Berdasarkan rumusan hipotesis diatas, maka untuk model yang digunakan pada penelitian bisa dilihat pada Gambar 3



Gambar 3. Model perilaku keamanan

4. ANALISIS DATA

4.1 Missing Data

Uji *missing data* dilakukan untuk mengetahui data yang kosong. Setelah dilakukan uji *missing* data pada penelitian ini tidak ditemukan *missing* data. Total jumlah responden sebesar 263

4.2 Uji *Levene*

Uji Levene digunakan untuk menguji apakah terdapat perbedaan varians yang signifikan atau untuk mengetahui data bersifat homogeny (Thoifah, 2015). Data dikatakan homogen jika nilai signifikan > 0,01(Levene, 1960 disitasi dalam Gastwrith et al , 2009, p.346). Untuk mengetahui data bersifat homogen akan disajikan dalam Tabel 1

Tabel 1. Hasil uji *levene*

Varians	Sig.	Varians	Sig.
PS1	,504	SB1	,498
PS2	,021	SB2	,183
PS3	,017	SB3	,620
PCT1	,098	SB4	,841
PCT2	,071	SEIS1	,325
PCT3	,048	SEIS2	,345
EPB1	,599	SEIS3	,115
EPB2	,092	SEIS4	,396
EPB3	,631	IUIPC1	,206
EPB4	,105	IUIPC2	,150
EPB5	,380	IUIPC3	,837
EPB6	,323	IUIPC4	,571
EPB7	,262	IUIPC5	,893
CTA1	,240	IUIPC6	,070
CTA2	,254	IUIPC7	,314
CTA3	,984	IUIPC8	,956
CTA4	,836	IUIPC9	,761

Berdasarkan hasil uji data yang disajikan dalam Tabel 1 data yang didapatkan dinyatakan homogen. Arti dari kata homogen yang dimaksud dalam penelitian ini adalah responden yang berjumlah 263, memiliki karekteristik kemampuan pemahaman yang sama dalam menafsirkan atau memahami kuesioner.

4.3 Uji Validitas dan Reliabilitas

Uji validitas digunakan untuk mengetahui sejauh mana alat ukur yang digunakan mampu memberikan hasil yang sesuai dengan tujuan yang hendak dicapai, menghasilkan data yang memiliki relevansi yang tinggi, serta mampu menjalankan fungsi sebagaimana mestinya (Wiyono, 2011). Sedangkan uji reliabilitas untuk mengetahui bahwa variabel manifes yang digunakan untuk penelitian memiliki presisi yang tinggi, dapat dipercaya, dan dapat diandalkan (Thoifah, 2015). Untuk mengetahui hasil uji validitas variabel manifes akan disajikan dalam Tabel 2. Uji validitas dalam penelitian ini menggunakan metode uji *bivariate pearson*. Untuk menentukan nilai koefisien dari *bivariate pearson* yaitu dengan cara mengidentifikasi derajat kebebasan *(degree of freedom)* (df), setelah diketahui hasil dari *degree of freedom* (df) maka langkah berikutnya adalah melihat nilai r tabel. Nilai koefisien dari r tabel pada penelitian ini adalah 0,101. Sedangkan untuk mengetahui tingkat reliabilitas variabel laten digunakan nilai *Cronbach Alpha* sebagai acuan bahwa variabel dapat dikatakan reliabel. Nilai *Cronbach Alpha* yang dihasilkan pada uji reliabilitas harus lebih besar dari 0,6 agar variabel bisa memenuhi standar reliabilitas. Hasil uji reliabilitas bisa dilihat dalam Tabel 2.

Tabel 2. Hasil uji validitas

Index	R	Hasil	Index	R	Hasil
PS2	,317**	Valid	SEIS1	,386**	Valid
PS3	,515**	Valid	SEIS2	,245**	Valid
PCT1	,469**	Valid	SEIS3	,348**	Valid
PCT2	,522**	Valid	SEIS4	,508**	Valid
PCT3	,575**	Valid	SA1	,639**	Valid
EPB1	,427**	Valid	SA2	,154*	Valid
EPB2	,473**	Valid	SA3	,386**	Valid
EPB3	,504**	Valid	SA4	,329**	Valid
EPB4	,503**	Valid	SA5	,485**	Valid
EPB5	,340**	Valid	IUIPC1	,412**	Valid
EPB6	,317**	Valid	IUIPC2	,481**	Valid
EPB7	,269**	Valid	IUIPC3	,593**	Valid
CTA1	,562**	Valid	IUIPC4	,520**	Valid
CTA2	,538**	Valid	IUIPC5	,449**	Valid
CTA3	,582**	Valid	IUIPC6	,537**	Valid
CTA4	,573**	Valid	IUIPC7	,600**	Valid
SB1	,361**	Valid	IUIPC8	,548**	Valid
SB2	,579**	Valid	IUIPC9	,646**	Valid
SB3	,529**	Valid	SB4	,491**	Valid

Berdasarkan Tabel 2 dapat ditarik kesimpulan bahwa nilai r hitung lebih besar dari nilai r tabel yang artinya semua variabel manifes yang digunakan dalam penelitian dinyatakan valid. Untuk uji reliabilitas dapat dilihat dalam Tabel 4.3. Uji reliabilitas dalam penelitian ini ditemukan dua variabel yang dinyatakan tidak reliabel. Adapun variabel tersebut adalah *security awareness* dan *perceived susceptability/perceived severity*. Ketika variabel dinyatakan tidak reliabel maka variabel atau suatu alat ukur tersebut tidak dapat digunakan untuk mengukur kebenaran suatu hasil penelitian dan tidak dapat digunakan untuk mengungkap ciri atau keadaan yang sesungguhnya dari obyek ukur (Hair, J.F et al, 2010; Matondang, Z, 2009).

4.4 Uji *Outlier* Data

Outlier adalah sebuah data yang memiliki nilai sangat berbeda dengan rata–rata data yang lainya (Santoso, 2015). Umunya adanya data *outlier* dapat mengganggu pengolahan data sehingga dapat menghasilkan kesimpulan yang bias. Uji *data outlier* pada penelitian ini, yaitu

dengan mencari nilai *mahalanobis distance* terlebih dahulu. Batas nilai *mahalanobis distance* dengan taraf kesalahan 0,001 menghasilkan nilai *mahalanobis distance* sebesar 72,054. Setelah diketahui batas nilai maka data yang memiliki nilai *mahalanobis distance* lebih dari 72,054 disebut data *outlier* dan harus dihilangkan. Dari data responden yang berjumlah 263, ditemukan sebanyak 18 data yang dinyatakan data *Outlier*.

Tabel 3. Hasil uji reliabilitas

Variabel	*Cronbach Alpha*
Security Awareness	0,559
Self - efficacy in information security	0,711
Expectations	0,669
Security Behavior	0,701
Cuest to Action	0,748
Perceived Susceptebility/ Perceived Severity	0,566
Perceived Security Threat	0,717
Internet Users' Information Privacy Concerns	0,865

4.5 Uji Normalitas Data

Uji normalitas pada penelitian ini menggunakan uji normalitas *skewness* dan *kurtosis*, yang dimana data akan dikatakan berdistribusi normal jika nilai *skewness* berkisar -2 sampai 2 (S, Supardi U, 2013), sedangkan untuk *kurtosis* yaitu berkisar -3 sampai 3 (Chandio, 2011). Pada penelitian ini, hasil uji normalitas menunjukan bahwa data yang didapatkan berdistribusi normal, untuk lebih jelasnya, hasil uji normalitas akan disajikan dalam Tabel 4.

Tabel 4. Hasil uji normalitas

Varians	Skewness	Kurtosis
	Statistic	Statistic
PCT1	-0,319	-0,227
PCT2	-0,359	-0,319
PCT3	-0,987	0,899
EPB1	0,042	-0,083
EPB2	-0,379	-0,337
EPB3	-0,397	-0,115
EPB4	-0,737	0,189
EPB5	-0,473	-0,429
EPB6	-0,134	-0,316
EPB7	-0,111	-0,839
SB1	-0,080	-0,565
SB3	-0,501	-0,034
SB4	-0,012	-0,562
SEIS1	-0,421	0,25
SEIS2	-0,021	-0,44
SEIS3	-0,233	-0,465
SEIS4	-0,664	0,574
IUIPC1	-0,312	0,033
IUIPC2	-0,208	-0,06
IUIPC3	-0,439	0,064
IUIPC4	-0,233	-0,135
IUIPC5	-0,301	0,045
IUIPC6	-0,338	0,01
IUIPC7	-0,399	0,381
IUIPC8	-0,132	-0,374
IUIPC9	-0,317	-0,317
SB2	-0,373	-0,208
CTA1	-0,302	-0,329
CTA2	-0,375	-0,104
CTA3	-0,314	-0,245
CTA4	-0,371	-0,312

Berdasarkan Tabel 4 dapat ditarik kesimpulan bahwa, data yang didapat dinyatakan berdistribusi normal.

4.6 Uji *Kaiser Mayer Olkin* (KMO)

Tujuan dari uji KMO adalah untuk memenuhi asumsi bahwa data yang didapat saat melakukan penelitian terpenuhi dan mampu untuk dilakukan analisis faktor (Field, 2009; Chandio, 2011) Nilai KMO dianggap mencukupi jika lebih dari 0,5 (Hidayat, 2014; Yong & Pearce, 2013). Untuk mengetahui nilai KMO pada data penelitian ini, akan disajikan dalam Tabel 5.

Tabel 5. Uji *Kaiser Mayer Olkin* (KMO)

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,877
Bartlett's Test of Sphericity	Approx. Chi-Square	3689,929
	Df	741
	Sig.	0,000

Berdasarkan Tabel 5, diketahui bahwa nilai KMO sebesar 0,887 yang artinya bahwa data yang didapatkan telah memenuhi asumsi kecukupan sampel untuk dilakukan analisis faktor.

4.7 Hasil Uji *Measurement Model Spesification and Confirmatory Factor Analysis*

Pada penelitian ini, *confirmatory Factor Analysis* digunakan untuk mengukur kesesuaian data dengan model dan menilai hubungan antara konstruk atau variabel dan indikator. Untuk menguji model yang digunakan dalam penelitian ini, digunakan metode *Structural Equationn Modeling* (SEM), yang dimana hasil dari uji CFA dapat dilihat dalam Tabel 6.

Tabel 6. *Goodness of Fit Indices*

Indeks	Batas	Nilai	Hasil
X^2	> 0,05	329,6	Fit
X^2/DF	< 3	1,577	Fit
GFI	> 0,9	0,902	Fit
AGFI	> 0,08	0,871	Fit
RMSEA	< 0,08	0,047	Fit
NFI	> 0,08	0,854	Fit
CFI	>0,9	0,94	Fit

Berdasarkan Tabel 6 dapat disimpulkan bahwa model penelitian yang digunakan dinyatakan *Fit.* Maksud dari kata *fit* adalah model mampu secara realistis mempresentasikan data (Chandio, 2011).

4.8 Uji *Structural Model* dan Hipotesis

Bagian yang paling penting dalam melakukan uji *structural model* adalah nilai dari parameter *estimate coefficient* (Chandio, 2011). *Estimate coefficient* digunakann untuk menguji dan mengevaluasi dari hipotesis yang telah dimodelkan. Hipotesis dinyatakan diterima ketika saat dilakukan pengujian nilai dari *critical ratio* (CR or *t–value*) lebih dari 1,96 dan *p–value* kurang dari 0,05. Hasil dari uji *structural model* dapat dilihat dalam Tabel 7.

Tabel 7. Hasil uji *structural model*

Index	Estimate	C.R	P
PCT<-CTA	1,066	7,806	***
EPB<-SEIS	0,267	1,984	0,047
APP<-PCT	0,875	7,864	***
CTL<-PCT	0,72	6,909	***
CL<-PCT	0,604	6,255	***
SB<-PCT	2,356	3,685	***
SB<-EPB	0,676	1,441	0,15
SB<-APP	0,011	0,102	0,919
SB<-CTL	-2,228	-2,571	0,1
SB<-CL	0,039	0,363	0,717

Berdasarkan dalam Tabel 7 dapat ditarik kesimpulan bahwa, terdapat sebanyak 4 rumusan hipotesis yang dinyatakan diterima, 2 hipotesis dinyatakan tidak signifikan, dan 4 hipotesis dinyatakan tidak bisa dilakukan pengujian karena terdapat variabel yang dinyatak tidak reliabel saat dilakukan pengujian reliabilitas, yang artinya bahwa 4 hipotesis tersebut dinyatakan ditolak.

5. HASIL

Berdasarkan Tabel 7 maka hubungan antar variabel yang memiliki nilai lebih dari 0,5 atau *p-value* kurang dari 0,05(*) dinyatakan memiliki hubungan yang kuat dan hipotesis dapat dinyatakan diterima.

5.1 Pembahasan Hipotesis

1. Pembahasan Hipotesis H1.

Berdasarkan hasil uji hipotesis yang telah dilakukan, hipotesis yang menyatakan bahwa ada hubungan antara kesadaran terhadap keamanan *(security awareness)* (SA) dan pengetahuan pengguna dalam memahami praktik keamanan informasi *(self-efficacy in information security)* (SEIS) dinyatakan tidak ada hubungan yang saling memengaruhi. Hal ini dikarenakan variabel laten *security awareness* tidak reliabel ketika dilakukan uji reliabilitas. Ketika variabel dinyatakan tidak reliabel maka variabel tersebut tidak dapat dilakukan uji data ketahap berikutnya, termasuk uji hipotesis. Menurut Hair et al (2010), Matondang, Z, (2009) mengatakan bahwa ketika variabel atau suatu alat ukur dinyatakan tidak reliabel maka tidak dapat digunakan untuk mengukur kebenaran suatu hasil penelitian dan tidak dapat digunakan untuk mengungkap ciri atau keadaan yang sesungguhnya dari obyek ukur, sebab variabel tersebut tidak mampu menghasilkan nilai yang konsisten atau tidak dapat diandalkan dalam memberikan jawaban.

2. Pembahasan Hipotesis H2.

Berdasarkan hasil uji hipotesis yang telah dilakukan, hipotesis yang menyatakan bahwa ada hubungan antara kesadaran terhadap keamanan *(security awareness)* (SA) dan pengguna dalam mengakses jaringan internet terkait praktik privasi informasi *(internet users' information privacy concerns)* (IUIPC) dinyatakan tidak ada hubungan yang saling memengaruhi. Hal ini dikarenakan variabel *security awarenes* dinyatakan tidak reliabel,

ketika variabel dinyatakan tidak reliabel maka variabel tersebut tidak dapat dilakukan uji SEM. Jadi ketika suatu variabel dinyatakan tidak reliabel, rumusan hipotesis yang berhubungan dengan variabel yang dinyatakan tidak reliabel maka secara statistik hasilnya tidak signifikan atau ditolak (Sarjono, H., Julianita, W., 2015)

3. Pembahasan Hipotesis H3.

Berdasarkan hasil uji hipotesis yang telah dilakukan, hipotesis yang menyatakan bahwa ada hubungan antara kesadaran terhadap keamanan *(security awareness)* (SA) dan persepsi pengguna terhadap ancaman keamanan *(perceived security threat)* (PCT) dinyatakan tidak ada hubungan yang saling memengaruhi. Permasalahan pada hipotesis H3 ini juga dialami pada hipotesis H1 dan H2, sebab nilai reliabilitas variabel *security awareness* sebesar 0,559 yang tidak memenuhi standard nilai *cronbach alpha*, yaitu harus lebih besar 0,6.

4. Pembahasan Hipotesis H4.

Berdasarkan hasil uji hipotesis yang telah dilakukan, hipotesis yang menyatakan bahwa ada hubungan antara pengetahuan pengguna dalam memahami praktik keamanan informasi *(self-efficacy in information security)* (SEIS) dan harapan pengguna (persepsi kemanfaatan–persepsi hambatan *(expectations perceived benefits–perceived barriers)* (EPB) dinyatakan ada hubungan positif yang signifikan, hal tersebut dapat dibuktikan dengan nilai *estimate* yang dihasilkan sebesar 0,267, *critical ratio* sebesar 1,98, dan *p-value* sebesar 0,047. Artinya bahwa dengan memiliki pengetahuan dan mampu memahami praktik keamanan informasi, para pengguna *LINE* berharap mendapatkan sebuah manfaat, keuntungan dalam berperilaku keamanan ketika memutuskan untuk menggunakan *LINE* serta berharap tidak ada hambatan atau gangguan ketika mereka berperilaku keamanan untuk menjaga privasi informasinya yang dipublikasikan atau dibagikan ke *LINE*.

5. Pembahasan Hipotesis H5.

Berdasarkan hasil uji hipotesis yang telah dilakukan, hipotesis yang menyatakan bahwa ada hubungan antara tingkat perhatian pengguna *LINE* terhadap data privasi informasi saat mereka berikan ketika berinteraksi dan menggunakan jaringan internet terlebih dalam praktik privasi informasi *(internet users' information privacy concerns)* (IUIPC) dan perilaku keamanan (*Security Behavior)* (SB) dinyatakan ada hubungan negatif yang tidak signifikan, hal ini dikarenakan nilai dari *estimate* yang dihasilkan sebesar -0,727, *critical ratio* sebesar -0,702, dan *p-value* sebesar 0,54. Artinya bahwa responden tidak akan melakukan perilaku keamanan dalam menggunakan *LINE*, responden menganggap aktifitas yang dikerjakan dengan bantuan media *LINE* bahkan privasi informasi yang dia berikan pada *LINE* masih dalam batas kewajaran. Dengan kata lain, responden tidak akan melakukan tindakan preventif untuk menjaga privasi informasinya selama menurutnya masih aman dan tidak ada gangguan yang membuat dirinya merasa terganggu.

6. Pembahasan Hipotesis H6.

Berdasarkan hasil uji hipotesis yang telah dilakukan, hipotesis yang menyatakan bahwa ada hubungan antara persepsi pengguna terhadap ancaman keamanan *(perceived security threat)* (PCT) dan tingkat perhatian pengguna *LINE* terhadap data privasi informasi saat mereka berikan ketika berinteraksi dan menggunakan jaringan internet terlebih dalam praktik privasi informasi *(internet users' information privacy concerns)* (IUIPC) dinyatakan ada hubungan positif yang signifikan, hal ini dikarenakan nilai dari *estimate* yang dihasilkan sebesar 0,733, *critical ratio* sebesar 7, dan *p-value* kurang dari ≤ 0,001. Artinya bahwa ketika pengguna merasa ada sebuah risiko atau ada ancaman terhadap keamanan pada data privasi informasinya, responden akan melakukan tindakan preventif, akan mengurangi beberapa aktifitas yang berhubungan dengan penggunaan layanan *LINE*, hal ini dilakukan unuk menjaga data privasi informasinya dan akan melakukan perilaku keamanan sesuai dengan prosedur yang diberlakukan.

7. Pembahasan Hipotesis H7.

Berdasarkan hasil uji hipotesis yang telah dilakukan, hipotesis yang menyatakan bahwa ada hubungan antara persepsi kelemahan/persepsi keunggulan *(perceived susceptability/perceived severity)* (PS) dan persepsi pengguna terhadap ancaman keamanan *(perceived security threat)* (PCT) dinyatakan tidak ada hubungan yang saling memengaruhi. Hal ini dikarenakan nilai reliabilitas dari variabel laten *perceived susceptability/perceived severity* sebesar 0,566 yang artinya tidak reliabel dan

tidak memenuhi standard dari nilai *cronbach alpha*.

8. Pembahasan Hipotesis H8.

Berdasarkan hasil uji hipotesis yang telah dilakukan, hipotesis yang menyatakan bahwa ada hubungan antara aktifitas yang memotivasi untuk merubah perilaku pengguna *(cues to action)* (CTA) dan persepsi pengguna terhadap ancaman keamanan *(perceived security threat)* (PCT) dinyatakan ada hubungan positif yang signifikan, hal ini dikarenakan nilai dari *estimate* yang dihasilkan sebesar 1,066, *critical ratio* sebesar 7,806, dan *p-value* kurang dari ≤0,001. Artinya bahwa, responden akan merubah perilakunya terkait tindakan menjaga keamanan data privasi informasi yang telah mereka telah berikan atau publikasikan ke *LINE* ketika mereka tau ada sebuah ancaman keamanan yang bisa membahayakan dirinya. Hal serupa juga dikatakan oleh Edwards (2015)

9. Pembahasan Hipotesis H9

Berdasarkan hasil uji hipotesis yang telah dilakukan, hipotesis yang menyatakan bahwa ada hubungan antara harapan pengguna (persepsi kemanfaatan–persepsi hambatan) *(expectations (perceived benefits–perceived barriers))* (EPB) dan perilaku keamanan *(security behavior)* (SB) dinyatakan ada hubungan positif yang tidak signifikan, hal ini dikarenakan nilai dari *estimate* yang dihasilkan sebesar 2,356, *critical ratio* sebesar 3,685, dan *p-value* sebesar ≤0,001. Artinya bahwa ketika responden memiliki harapan dengan menggunakan sebuah *LINE* bisa mendapatkan sebuah manfaat dan bisa mengetahu hambatan apa saja ketika mereka beraktifitas menggunakan *LINE* tidak ada implikasi dalam hal perilaku keamanan.

10. Pembahasan Hipotesis H10

Berdasarkan hasil uji hipotesis yang telah dilakukan, hipotesis yang menyatakan bahwa ada hubungan antara persepsi pengguna terhadap ancaman keamanan *(perceived security threat)* (PCT) dan perilaku keamanan *(security behavior)* (SB) dinyatakan ada hubungan positif yang signifikan, hal ini dikarenakan nilai dari *estimate* yang dihasilkan sebesar 2,356, *critical ratio* sebesar 3,685, dan *p-value* sebesar ≤0,001. Artinya bahwa dengan adanya sebuah ancaman keamanan ketika responden menggunakan *LINE* dalam menunjang aktifitas berkomunikasi dan yang lain sebagainya akan berpengaruh dengan perilaku keamanan dalam menjaga data privasi informasinya. Perilaku keamanan responden akan menjadi sangat baik ketika ancaman keamanan yang mereka ketahui pernah terjadi atau sedang terjadi pada orang terdekat, rekan kerja, atau bahkan dirinya sendiri ketika pernah menggunakan media sosial yang serupa.

6. KESIMPULAN

Berdasarkan hasil analisis data, faktor yang memengaruhi perilaku keamanan *(security behavior)* pada pengguna *LINE* adalah persepsi pengguna terhadap ancaman keamanan *(perceived security threat).* Dengan adanya sebuah ancaman keamanan ketika responden menggunakan *LINE* dalam menunjang aktifitas berkomunikasi dan yang lain sebagainya akan berpengaruh dengan perilaku keamanan dalam menjaga data privasi informasinya. Perilaku keamanan pada pengguna *LINE* akan menjadi sangat baik ketika ancaman keamanan yang mereka ketahui pernah terjadi atau sedang terjadi pada orang terdekat, rekan kerja, atau bahkan dirinya sendiri ketika pernah menggunakan media sosial yang serupa.

DAFTAR PUSTAKA

Bohang, F. K. Di Indonesia Jumlah Pengguna *LINE* pepet *Facebook.* [online] Tersedia di: http://tekno.kompas.com/read/2016/09/03/09490637/di.indonesia.jumlah.pengguna.line.pepet.facebook [Diakses, 13 April 2016]

Chandio, F. H., 2011. Studying Acceptance of Online Banking Information System: A Structural Equation Model. *Thesis : Brunel Business School, Brunel University London.*

Chandrataruna, M., & Ngazis, A. R. 2013. Pengguna *LINE* Tembus 300 Juta. Tersedia di: <http://teknologi.news.viva.co.id/news/read/461580-pengguna-line-tembus-300-juta> [diakses 13 April 2016].

Edwards, K. 2015. *Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer User. Disertation:* College of Engineering and Computing Nova Southeastern University.