HUBUNGAN *RISK TOLERANCE* DAN *RISK PERCEPTION* TERHADAP PERILAKU KEAMANAN INFORMASI

THE CORRELATION OF RISK TOLERANCE AND RISK PERCEPTION TO INFORMATION SECURITY BEHAVIOR

Dewi Hernikawati
Peneliti pada Balai Pengkajian dan Pengembangan Komunikasi
dan Informatika Jakarta, Jln. Pegangsaan Timur No. 19 B Jakarta Pusat, Provinsi DKI Jakarta, Indonesia,
No HP : 0815 8762 573- dewi--nika@gmail.com
(Naskah diterima 15 September 2016, Submit catatan editor ke penulis 20 September 2016; Submit ke-2 penulis ke editor 6 Oktober 2016, submit editor ke Mitra Bestari 20 Oktober 2016, submit mitra bestari ke editor 6 November 2016; submit editor ke penulis 7 November 2016; submit penulis ke editor, 8 November 2016; disetujui terbit November 2016)

ABSTRACT

Today, Information is an important asset for organization. The speed of internet access makes information easy to get, on the other side it cause a threat and vulnerability for the information. Therefore, information security becomes important. This study will find the relationship between risk perception and risk tolerance variable to Information security. Quantitative method is used to answer the research questions. Population of this study is civil officer (PNS) in Central Jakarta City Administration. Data analyze with SPSS to see the correlation. Result of this study is risk tolerance and risk perception affect to Information Security. The lower of risk perception, the higher information security for individu. Similarly, the lower risk tolerance, the higher information security for individu.
Keywords : Risk Perception, Risk Tolerance, Information Security

ABSTRAK

Informasi merupakan asset yang penting bagi organisasi saat ini. Dengan kecepatan akses internet menjadikan informasi mudah diperoleh, namun hal ini menimbulkan ancaman dan kerawanan terhadap informasi tersebut. Oleh karena itu keamanan informasi menjadi penting. Dalam penelitian ini akan dilihat hubungan antara variabel *risk perception* dan *risk tolerance* terhadap perilaku keamanan informasi. Metode kuantitatif digunakan untuk menjawab pertanyaan penelitian. Penelitian dilakukan dengan populasi PNS di Kota Administrasi Jakarta Pusat. Data dianalisis dengan bantuan SPSS untuk melihat korelasinya. Hasil dari penelitian ini adalah variabel Perilaku Keamanan Informasi dipengaruhi oleh variabel *risk tolerance* dan *risk perception*. Semakin rendah *risk perception* seseorang maka akan semakin tinggi Kemanan Informasi orang tersebut. Begitu pula semakin rendah *risk tolerance* seseorang maka akan semakin tinggi Kemanan Informasi orang tersebut.
Kata-kata kunci : *Risk Perception, Risk Tolerance*, Keamanan Informasi

I. A. PENDAHULUAN

1. Latar Belakang dan Permasalahan

Informasi merupakan data yang diolah sehingga mempunyai arti bagi penggunanya. Informasi tersebut dapat memberikan pengetahuan kepada penggunanya. Saat ini informasi menjadi aset yang sangat berharga. Informasi digunakan sebagai pendukung dalam pengambilan keputusan pimpinan dalam organisasi tidak hanya bagi perusahaan yang komersial namun juga bagi pemerintah, dunia pendidikan maupun individu. Oleh karena itu kemampuan untuk menyediakan informasi menjadi sangat penting. Informasi dianggap sebagai asset yang berharga menyebabkan informasi ini hanya diperbolehkan untuk diakses bagi orang-orang tertentu dan berhak. Informasi yang jatuh ke pihak lain seperti lawan bisnis atau lawan politik bisa menyebabkan kerugian bagi pemiliknya. Berdasarkan hal tersebut maka informasi perlu untuk dilindungi.

Internet dengan kecepatan tinggi disertai perkembangan infrastruktur pendukung yang ada saat ini memudahkan informasi diakses oleh seluruh masyarakat. Dengan adanya kemudahan akses informasi ini memberikan kelebihan dan kelemahan-kelemahan. Informasi menjadi mudah diperoleh dan tidak mengenal jarak dan waktu merupakan salah satu kelebihan adanya internet. Namun dibalik kelebihan tersebut, terdapat ancaman-ancaman yang akan timbul

terhadap informasi antara lain informasi hilang karena dicuri atau dihack, informasi disalahgunakan oleh pengakses yang tidak berwenang, fraud, spam, *denial of service* dsb.

Ancaman-ancaman yang mungkin timbul terhadap informasi tersebut menjadikan pentingnya untuk menjaga informasi, sehingga keamanan informasi menjadi sesuatu kebutuhan untuk melindungi informasi. Saat ini masih banyak yang belum menyadari pentingnya keamanan informasi dan menganggap informasi merupakan asset yang tidak perlu dilindungi. Keamanan Informasi adalah bagaimana dapat mencegah penipuan atau paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Kemanan informasi menurut ISO 27000:2012 meliputi kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi. Kerahasiaan (*confidentiality*) dapat diartikan bahwa jaminan bahwa hanya yang berhak yang bisa mengakses informasi tertentu. Keutuhan (*integrity*) adalah jaminan terhadap kelengkapan data dan tidak ada data yang hilang atau korup, kerusakan atau ancaman lain yang menyebabkan data bisa berubah dari aslinya. Ketersediaan (*availability*) adalah jaminan informasi dapat diakses tanpa ada gangguan.

Banyak faktor-faktor yang mempengaruhi keamanan informasi baik dari segi manusia (pengguna), sistem, dan prosesnya. Dari segi sistem bisa jadi sistem yang dibangun rawan untuk di hack atau ada celah-celah yang memungkinkan adanya kesalahan dan eror. Contoh serangan dari segi proses yaitu sniffing dan spoofing. Sniffing merupakan penyadapan terhadap lalulintas pada jaringan komputer. Misalnya jika seseorang akan mengirimkan email dari kantor dan dikirimkan kepada temannya yang berada di luar kantor. Email ini bisa dibajak pada saat melalui server dari jaringan komputer kantor dan bisa dilakukan oleh administratot jaringan yang mengendalikan server. Aktivitas sniffing ini bisa membaca email yang dikirimkan kepada orang lain. Spoofing adalah teknik yang dipakai untuk mengakses computer atau informasi yang tidak sah dan dilakukan dengan memalsukan bahwa mereka adalah host yang bisa dipercaya. Dari segi pengguna bisa berupa ketidaktahuan, tidak perduli, belum sadar dan memiliki persepsi yang berbeda-beda akan pentingnya melindungi informasi. Individu memiliki resiko dalam keamanan informasi pada saat menggunakan komputer (Pattison & Anderson (2006)). Dari ketiga faktor tersebut, manusia merupakan faktor yang sangat penting karena rentan terhadap kesalahan (*human error*) dan sebagai kunci dalam melaksanakan keamanan informasi.

Oleh karena itu pada penelitian ini hanya akan membahas keamanan informasi terkait manusia. Permasalahan dalam penelitian yang akan dibahas adalah : 1) Apakah *risk tolerance* berpengaruh positif terhadap Perilaku Keamanan Informasi ? ; 2) Apakah *risk perception* berpengaruh positif dengan Perilaku Keamanan Informasi?

2. Signifikansi

Penelitian ini bertujuan untuk melihat pengaruh variabel *risk tolerance* dan *risk perception* terhadap perilaku Keamanan Informasi sehingga diperoleh gambaran kondisi PNS di Jakarta Pusat terhadap Keamanan Informasi. Hasil dari penelitian ini diharapkan dapat dijadikan rujukan dalam meningkatkan kesadaran pegawai terhadap kemanan data dan informasi. Serta diharapkan dapat menjadi masukan dalam menyusun kebijakan terkait keamanan informasi di Direktorat Keamanan Informasi, Ditjen Aptika, Kementerian Komunikasi dan Informatika.

II. PEMBAHASAN

A. Kerangka Teori

1. Literatur Review

Penelitian yang dilakukan oleh Pattison dan Anderson (2006) dilatarbelakangi adanya *Risk perception* individu terkait sistem informasi yang ditentukan oleh adanya kemungkinan individu tersebut beresiko ketika menggunakan komputer. Perilaku bisa dimanipulasi dengan *Framing* sebagai sebuah komunikasi terkait sikap dalam risiko keamanan informasi. Tulisan ini membahas bagaimana *cognitive style framing* individu perlu dipertimbangkan ketika menyusun pesan resiko. Tujuan dari penelitian ini adalah menekankan pentingnya perilaku sebagai pelaksana dalam level penerima keamanan informasi di organisasi. Tujuan lainnya untuk menunjukkan dengan pendekatan resiko komunikasi dengan *cognitive style framing*, sehingga pihak manajemen bisa

mempertimbangkan untuk mengubah perilaku pengguna dalam mengambil resiko saat menggunakan komputer disemua level. Hasilnya adalah perubahan positif dalam berperilaku dapat mengurangi resiko, jika *risk perception* pengguna komputer turun maka tingkat keamanan informasinya meningkat. Paper ini mendukung pandangan bahwa level penerimaan keamanan informasi terbaik yang bisa dicapai adalah dengan melibatkan semua komponen sistem informasi terutama yang berhubungan dengan manusia. Penelitian ini juga berkontribusi untuk aspek sosiologi terhadap resiko terkait keamanan informasi. Selain itu, melihat konsep yang lebih baik dalam risiko komunikasi dengan mengembangkan konsep *framing* untuk memitigasi aktual risiko informasi.

Penelitian dengan judul "*Risk Perception and Cloud Computing Security*" dilakukan dengan pendekatan psikometri ini bertujuan untuk mencari tau faktor-faktor yang mempengaruhi *risk perception cloud computing* di militer dan organisasi sipil. Pengambilan data dilakukan dengan menampilkan aplikasi-aplikasi *cloud computing* dan meminta responden memberikan penilaian terhadap resiko dengan skala likert. Hasilnya bahwa informasi bisa meningkatkan pemahanan tentang peran *risk perception* dalam analisis resiko *cloud computing* dan memberikan dukungan kepada organisasi pemerintah dan strategi *cloud computing*.

Penelitian yang dilakukan oleh Skotnes (2015) bertujuan untuk melihat *risk perception* antara pengguna baik manajer dan pegawai dalam sistem TIK dan mendiskusikan faktor-faktor yang mempengaruhi *risk perception*. Sistem *electric power supply* adalah infrastruktur penting dikehidupan modern saat ini dan kerusakan pada sistem ini bisa berpengaruh terhadap keuangan dan kerusakan pada keamanan dan kesehatan masyarakat. Hasil survey menunjukkan bahwa *risk perception* responden relative rendah. Faktor yang mempengaruhinya adalah kompleksitas sistem TIK dan kurangnya komunikasi antara subculture dengan perbedaan fokus. Penelitian terdahulu menunjukkan bahwa besar perusahaan, pengetahuan dan kesadaran akan kemanan TIK dan pengalaman menjadi faktor yang mempengaruhi *risk perception*.

Penelitian yang dilakukan oleh Anthony dkk (2014) didasarkan bahwa *Risk perception* pengguna memiliki dampak yang penting terhadap keamanan informasi karena aksi pengguna dapat berkompromi dengan seluruh sistem. Oleh karena itu diperlukan pemahaman bagaimana persepsi dan respon pengguna terhadap risiko keamanan informasi. Penelitian ini akan mendemontrasikan bahwa perilaku mengambil resiko efektif untuk memprediksi penggunaan *electroencephalography* (EEG) dengan *even-related potentials* (ERPs). Hasilnya adalah prediksi *risk perception* keamanan informasi tidak efektif disaat keamanan informasi dianggap tidak penting.

Penelitian sebelumnya yang dilakukan oleh (Dupuis, Crossler, Popovsky ,2015) adalah menguji perilaku individu terhadap keamanan informasi dengan variabel dependen yang digunakan adalah *backing up* informasi. Variable-variabel independen dalam penelitian ini adalah *risk tolerance, risk perceptions, past experiences severity, past experiences frequency*, dan dilihat hubungannya dengan variable *severity* dan *likelihood*. Metode penelitian yang digunakan adalah penelitian kuantitatif. Responden kuesioner adalah pengguna Amazon's Mecahnical Turk. Hasil dari penelitian ini menunjukkan bahwa *individual's risk tolerance, risk perception* dan *past experience* berpengaruh secara signifikan untuk memprediksi perilaku *back up* data individu.

Long Huang, dkk (2010) melakukan penelitian untuk menyelidiki persepsi tentang keamanan informasi dan mencari factor-faktor yang mempengaruhinya. Survey dilakukan pada 602 responden. Analisis data menggunakan analisis factor eksloratori. Hasilnya adalah persepsi orang terhadap keamanan informasi adalah signifikan terkait dengan pengalaman memakai komputer dan jenis-jenis kerugian yang dialami.

Dari penelitian-penelitian tersebut masih terbatas pada risk perception dan saat ini masih sedikit penelitian yang berhubungan dengan *risk tolerance* dan *risk perception* dalam Keamanan Informasi. Oleh karena itu dalam penelitian ini akan membahas korelasi atau hubungan antara *risk perception* dan *risk tolerance* terhadap perilaku keamanan informasi.

2. Konsep-Konsep Teoritik

a. Keamanan Informasi

Informasi adalah data yang telah diolah menjadi bentuk yang berguna bagi penerimanya dan nyata, berupa nilai yang dapat dipahami didalam keputusan sekarang maupun masa depan (Tipton dan Krause, 2005). Informasi dapat dikatakan sebagai keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik maupun non elektronik (Undang-Undang No. 14 Tahun 2008). Informasi yang merupakan aset harus dilindungi keamanannya. Keamanan informasi adalah melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, serta mempercepat kembalinya investasi dan peluang usaha (Tipton dan Krause, 2005). Keamanan informasi merupakan upaya melindungi informasi dan sistem informasi dari akses yang dilakukan oleh pihak yang tidak bertanggung jawab, penggunaan, penyingkapan, gangguan, modifikasi, atau perusakan untuk menjaga integritas, kerahasiaan, dan ketersediaan informasi (NIST SP 800-59).

Pengertian lain berdasarkan ISO 17799:2005, Keamanan Informasi adalah perlindungan terhadap informasi untuk memastikan kelangsungan bisnis, meminimalkan resiko, memaksimalkan keuntungan dalam berinvestasi dan keuntungan bisnis. Karakteristik yang harus dipenuhi pada Keamanan Informasi adalah *confidentiality, integrity,* dan *availability* serta dikenal sebagai CIA triangle. Konsep CIA triangle ini dikembangkan oleh industri keamanan komputer dan digunakan sebagai suatu pedoman dalam perlindungan keamanan informasi (Mattord & Whitman, 2012). Keamanan Informasi didefinisikan sebagai usaha melindungi informasi dengan menjaga *confidentiality, integrity,* dan *availability.*

Confidentiality dapat diartikan sebagai hanya orang yang memiliki hak yang bisa melihat atau membuka informasi. *Confidentiality* memastikan bahwa hanya orang yang berhak yang bisa mengakses informasi jadi jika seseorang tanpa hak akses bisa membuka informasi maka *Confidentiality* sudah diterobos (Mattord & Whitman, 2012). *Integrity* adalah informasi yang seluruhnya lengkap dan tidak ada informasi yang rusak *(corrupted). D*engan kata lain informasi yang digunakan adalah asli dan otentik, tidak ada orang yang bisa menghapus atau memodifikasi informasi tanpa izin. *Availability* memungkinkan pengguna bisa mengakses informasi tanpa interfensi dan mendapatkan sesuai format yang diinginkan (Mattord & Whitman, 2012).

b. *Risk Tolerance* dan *Risk Perception*

Berdasarkan KBBI, risiko bisa diartikan sebagai akibat yang kurang menyenangkan (merugikan, membahayakan) dari suatu perbuatan atau tindakan. Risiko ini bisa diartikan berbeda-beda tergantung dari sudut pandang atau bidang apa yang digunakan. Sebagai contoh dibidang keuangan risiko bisa diartikan sebagai kemungkinan diperoleh hasil dari investasi lebih kecil daripada yang diharapkan. Pada bidang asuransi, risiko adalah suatu situasi dimana kemungkinan terjadinya suatu peristiwa yang merugikan dapat diukur tetapi dimana peristiwa itu terjadi tidak dapat ditentukan. Dalam bidang teknologi informasi, risiko bisa diartikan sebagai adanya potensi dari ancaman yang ada yang akan dapat melakukan eksploitasi pada celah keamanan yang ada, yang mungkin akan memberikan ancaman tersendiri pada organisasi tersebut. Pengertian resiko menurut ISO/IEC Guide 73:2009 adalah dampak dari ketidakpastian pada tujuan. Resiko ini dapat berupa resiko positif dan resiko negatif. Risiko biasa dikategorikan berdasarkan pada peristiwa yang mungkin terjadi dan konsekuensinya maupun gabungan antara keduanya. Risiko bisa disampaikan dalam bentuk konsekuensi dari suatu peristiwa serta berhubungan dengan tingkat kemunculannya.

Perilaku seseorang ditentukan oleh *risk perception* dan bukan berdasarkan probabilitas terbaru (Kokolakis, Spyros. 2011). Persepsi resiko (*risk perception*) dapat diartikan sebagai sudut pandang stakeholder dalam melihat resiko (ISO/IEC Guide 73).

Risk tolerance merupakan kesiapan organisasi untuk menghadapi resiko setelah proses pengembangan, pemilihan, dan implementasi kontrol untuk mencapai tujuannya.

Risk tolerance perception dari individu bisa diperoleh dari berbagai aspek seperti *threat severity* dan *threat probability* dalam kerangka teori *Protection Motivation Theory* (Dupuis, Crossler, Popovsky ,2015). Evaluasi terhadap resiko telah dilakukan diberbagai konteks dalam berbagai bidang. Salah satu contoh penelitian untuk menentukan resiko dan penggunaannya dalam melakukan evaluasi resiko adalah dengan mencari dan mengevaluasi seberapa dekat hubungan antar variabel. Jika seseorang mengetahui karakteristik orang lain, dia bisa membuat kesimpulan yang sama pada karakteristik orang lainnya juga.

Mengacu pada teori-teori sebelumnya, maka hipotesis dalam penelitian ini adalah sbb :

H1 : *risk tolerance* berpengaruh positif terhadap Perilaku Keamanan Informasi

H2 : *risk perception* berpengaruh positif terhadap Perilaku Keamanan Informasi.

3. Defini konsep dan operasional

a. Definisi konsep

Yang dimaksud dengan konsep : *Risk tolerance* dalam riset ini adalah tingkat toleransi terkait resiko yang akan ditanggung pengguna. *Risk perception* adalah persepsi terhadap resiko yang akan terjadi terkait keamanan informasi. Perilaku Keamanan Informasi adalah perilaku yang dilakukan oleh pengguna dalam Keamanan Informasi. Hal ini dapat dilakukan seperti password yang digunakan dengan rumit sehingga tingkat keamanannya tinggi, berhati-hati dalam menggunakan akses internet ditempat umum, memperhatikan peraturan terkait Keamanan Informasi dsb.

b. Definisi operasional

Dalam melakukan pengukuran terhadap variabel *risk tolerance, risk perception*, dan Keamanan Informasi ini dilakukan dengan menggunakan pertanyaan terkait keamanan Informasi dengan skala Likert 1 sampai 4. Pilihan yang diberikan dalam kuesioner adalah Sangat Tidak Setuju, Tidak Setuju, Setuju, dan Sangat Setuju.

B. Metode Penelitian

Penelitian ini korelatif[1] ini dilakukan dengan pendekatan kuantatif. Penentuan sampel berdasarkan populasi PNS di Satuan Kerja Pemerintah Daerah di Kotamadya Jakarta Pusat. Penghitungan sampel dilakukan dengan menggunakan rumus Solvin. Jumlah populasi PNS di Jakarta Pusat sebanyak 1.494 orang sehingga diperoleh sampelnya menjadi 94 orang.

Berikut ini adalah rumus Solvin :

$$n = \frac{N}{1 + Ne^2}$$

Keterangan : n = jumlah sampel yang diambil
N = jumlah populasi
e = taraf nyata 0,1

Perhitungan jumlah sampel dalam penelitian sebagai berikut :

Jakarta Pusat :

$$n = \frac{1.494}{1 + 1.494 * 0.1^2}$$

= 94

[1] Analisis korelasi adalah analisis yang dilakukan untuk melihat tingkat keeratan hubungan antara dua variabel. Tingkat hubungan ini dibedakan menjadi tiga kriteria yaitu mempunyai hubungan positif, mempunyai hubungan negatif, dan tidak memiliki hubungan. Kuatnya suatu korelasi ditunjukkan dengan nilai koefisiean korelasi. Nilai koefisien korelasi ini antara -1 sampai dengan 1. Hubungan antar variabel disebut memiliki hubungan yang erat jika nilainya mendekati 1.

Metode pengambilan sampel dilakukan dengan *non-probability sampling* berupa *convenience sampling* adalah dengan cara memilih responden yang ditemui dan menanyakan kesediannya untuk mengisi kuesioner. Analisis data dilakukan dengan bantuan SPSS 18.

Guna kepentingan uji korelasi, maka secara prosedural penelitian ini sebelumnya melakukan proses uji Reliabilitas dan Uji Validitas kuesioner dan Uji Linieritas. Hasil uji Reliabilitas dan Validitas menunjukkan kuesioner penelitian ini bernilai andal dan valid sebagai kuesioner namun tidak terdapat asosiasi yang linier diantara variabel (lihat tabel 1; 2; dan 3).

Tabel 1
Out put reliabilitas Keamanan Informasi

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.824	.828	13

Tabel 2
Output reliabilitas *Risk Perception*

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.820	.810	12

Tabel 3
Output reliabilitas *Risk Tolerance*

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.881	.882	13

Uji validitas untuk variabel *Risk Perception* untuk setiap item yaitu berdasarkan pada nilai r tabel 92 dengan signifikansi 5% adalah 0.2028. Nilai item dikatakan valid jika nilai r tabel lebih kecil dari nilai r hitung.

Pada nilai hitung untuk RP1 adalah -0.179 artinya nilai hitung lebih kecil dari pada nilai r tabel sehingga RP1 tidak valid maka tidak perlu dimasukkan dalam analisis selanjutnya. Untuk nilai r hitung pada item RP2, RP3, RP4, RP5, RP6, RP7, dan RP8 masing-masing adalah 0.361, 0.764, 0.797, 0.804, 0.766, 0.834, dan 0.497. Nilai r hitung untuk RP9 adalah 0.175 yaitu lebih kecil dari nilai r tabel 0,2028 sehingga item RP9 tidak valid. Untuk nilai r hitung RP 10 yaitu 0.665, RP11 memiliki nilsi r hitung 0.774, dan RP12 nilai r hitungnya adalah 0.543. Nilai-nilai tersebut diatas nilai r tabel sehingga item RP10, RP11, dan RP12 adalah valid. Dapat disimpulkan bahwa Item-item pertanyaan yang valid untuk variabel *Risk Perception* berdasarkan

perhitungan korelasi antar item dengan total variabel adalah RP2, RP3, RP4, RP5, RP6, RP7, RP8, RP10, RP11, RP12. Untuk lebih jelasnya dalam melihat uji validitas dapat dilihat pada tabel 4.

Tabel 4
Uji validitas variabel *Risk Perception*

Variabel	R hitung	Signifikansi
RP1	-0.179	Tidak valid
RP2	0.361	Valid
RP3	0.764	Valid
RP4	0.797	Valid
RP5	0.804	Valid
RP6	0.766	Valid
RP7	0.834	Valid
RP8	0.497	Valid
RP9	0.175	Tidak valid
RP10	0.665	Valid
RP11	0.774	Valid
RP12	0.543	Valid

Sama seperti variabel Keamanan Informasi dan *Risk Perception*, maka variabel *Risk Tolerance* juga perlu dilakukan uji validitas. Pada variabel *Risk Tolerance* untuk RT1 memiliki nilai r hitung 0.506, RT2 memiliki nilai r hitung sebesar 0.552, RT3 memiliki nilai r hitung sebesar 0.424, nilai r hitung untuk item RT4 yaitu 0.467, r hitung untuk RT5 adalah 0.720, r hitung untuk RT6 yaitu 0.530, r hitung untuk RT7 yaitu 0.487, r hitung untuk RT8 adalah 0.731, nilai r hitung untuk RT9 yaitu 0.550, RT10 memiliki r hitung sebesar 0.383, RT11 memiliki nilai r hitung sebesar 0.441, nilai RT12 memiliki r hitung sebesar 0.258, dan RT 13 memiliki r hitung sebesar 0.491. Nilai-nilai item-item t r hitung untuk *Risk Tolerance* tersebut menunjukkan nilai yang lebih besar dari nilai r tabel sehingga item-item untuk RT tersebut adalah valid. Varibel RT1, RT2, RT3, RT4, RT5, RT6, RT7, RT8, RT9, RT10, RT11, RT12, dan RT13 adalah valid. Tabel 5. merupakan ringkasan untuk uji validitas variabel *Risk Tolerance.*

Tabel 5
Uji validitas variabel *Risk Tolerance*

Variabel	R hitung	Signifikansi
RT1	0.506	Valid
RT2	0.552	Valid
RT3	0.424	Valid
RT4	0.467	Valid
RT5	0.720	Valid
RT6	0.530	Valid
RT7	0.487	Valid
RT8	0.731	Valid
RT9	0.550	Valid
RT10	0.383	Valid
RT11	0.441	Valid
RT12	0.258	Valid
RT13	0.491	Valid

Terkait dengan Uji Linearitas, maka ini dimaksudkan sebagai uji yang dilakukan untuk melihat linier tidaknya hubungan dua variabel. Hipotesis yang diajukan untuk Ho adalah data dua variabel mempunyai hubungan linier. Hal ini dipenuhi dengan syarat nilai signifikansi kurang dari 0.05. Untuk melihat hubungan linieritas antara variabel Keamanan Informasi dan *Risk Perception* dilakukan uji linieritas. Berdasarkan hasil pengolahan data dengan SPSS diperoleh nilai signifikansi untuk linieritas adalah 0.084 dan lebih besar dari 0.05. Hal ini berarti bahwa Ho ditolak dan variabel tidak berhubungan linier, sehingga untuk melihat uji korelasinya dilakukan dengan uji statistik nonparametrik.

III. PEMBAHASAN

A. Hasil Penelitian

Dalam penelitian ini data diolah dengan bantuan SPSS. Sebelum dilakukan uji korelasi terlebih dahulu dilakukan uji validitas dan uji reliabilitas terhadap kuesioner. Berdasarkan hasil pengolahan data dengan SPSS 18 untuk uji validitas diperoleh nilai korelasi untuk item pertanyaan terhadap item total variabel keamanan Informasi adalah signifikan atau valid. Hal ini bisa disimpulkan berdasarkan nilai signifikansi yang lebih kecil daripada 0,05. Selain itu, dapat juga dilihat dari nilai r tabel yaitu untuk r tabel 92 dengan signifikansi 5% adalah 0.2028, nilai item dikatakan valid jika nilai r tabel lebih kecil dari nilai r hitung.

1. Analisis Korelasi variabel Risk Tolerance dan Risk Perception terhadap Keamanan Informasi,

Analisis korelasi dilakukan untuk membuktikan hipotesis sebagai permasalahan yang diangkat dalam penelitian ini. Hipotesis akan diterima jika nilai signifikansinya lebih kecil dari 0.05. Dengan analisis korelasi akan dilihat apakah *risk tolerance* berpengaruh positif terhadap Perilaku Keamanan Informasi dan apakah ada hubungan/korelasi antara *risk perceptions* dengan Perilaku Keamanan Informasi. Dari tabel 6 dapat dilihat korelasi antara *Risk Perception* dan Keamanan Informasi memiliki nilai signifikansi 0.014 dan lebih kecil dari 0.05. Hipotesis diterima jika nilai signifikansinya lebih kecil dari 0.05, hal ini bisa disimpulkan bahwa hipotesis diterima. Artinya ada hubungan antara *Risk tolerance* terhadap Keamanan Informasi. Koefisien korelasinya adalah -0.253 menunjukkan bahwa terdapat hubungan negatif yang signifikan antara *Risk Perception* dengan Keamanan Informasi. Semakin rendah *risk perception* seseorang maka akan semakin tinggi kemanan Informasi orang tersebut.

Tabel 6
Korelasi antara variabel *Risk Tolerance*, dan *Risk Perception* terhadap Keamanan Informasi

Correlations

			KI	RPel	RT
Spearman's rho	KI	Correlation Coefficient	1.000	-.253*	-.264*
		Sig. (2-tailed)	.	.014	.010
		N	94	93	94
	RPel	Correlation Coefficient	-.253*	1.000	.810**
		Sig. (2-tailed)	.014	.	.000
		N	93	93	93
	RT	Correlation Coefficient	-.264*	.810**	1.000
		Sig. (2-tailed)	.010	.000	.
		N	94	93	94

*. Correlation is significant at the 0.05 level (2-tailed).
**. Correlation is significant at the 0.01 level (2-tailed).

Analisis korelasi Spearman's digunakan untuk melakukan uji hipotesis terhadap hubungan antara *risk tolerance* dengan Perilaku Keamanan Informasi. Dari tabel 6. diperoleh nilai signifikansinya adalah 0.010 dan lebih kecil dari 0.05. Hal ini menunjukkan bahwa Ho diterima, artinya ada hubungan antara *risk tolerance* dengan Perilaku Keamanan Informasi. Nilai koefisien dari hubungan ini adalah -0.264. Nilai koefisien tersebut menunjukkan bahwa terdapat hubungan negatif yang signifikan antara *Risk tolerance* dengan Keamanan Informasi. Semakin rendah tingkat *risk tolerance* seseorang maka akan semakin tinggi kemanan Informasi orang tersebut.

B. Diskusi

Berdasarkan uji hipotesis tersebut dapat disimpulkan bahwa variabel *risk perception* dan *risk tolerance* berpengaruh negatif tehadap perilaku keamanan informasi. Hubungan negatif ini menunjukkan bahwa semakin rendah *risk tolerance* dan semakin rendah *risk perception* seseorang maka akan semakin tinggi tingkat keamanan informasi dari orang tersebut. Dengan kata lain toleransi terhadap resiko yang rendah yaitu toleransi terhadap adanya potensi ancaman pada celah keamanan informasi yang rendah berpengaruh terhadap tingginya tingkat keamanan informasi seseorang. Orang yang tidak bisa mentolerir adanya risiko maka perilaku keamanan informasinya tinggi, sebagai contoh orang tersebut tidak akan mudah meminjamkan flash disk kepada orang lain, membagi-bagi password kepada orang lain, jika akan meninggalkan komputernya selalu log out sehingga tidak bisa digunakan orang lain dengan mudah. Hal ini menunjukkan perilaku keamanan informasi yang tinggi. Begitu pula dengan persepsi terhadap resiko yang rendah mempengaruhi tingkat perilaku keamanan informasi. Jika seseorang memiliki toleransi yang tinggi terhadap resiko maka akan mempengaruhi tingkat keamanan informasinya menjadi rendah. Hal ini bisa dilihat seperti melakukan back up data dan mengganti password tidak dilakukan atau melakukan back up data dan mengganti password tapi tidak sering atau bisa dilakukan satu tahun sekali dan tidak terjadwal menjadikan perilaku keamanan informasinya rendah.

Dengan adanya hubungan antara variabel *risk perception* dan *risk tolerance* berpengaruh negatif tehadap perilaku keamanan informasi ini perlu ditingkatkan kesadaran akan pentingnya keamanan informasi bagi PNS di Kota Administrasi Jakarta Pusat. Hal ini juga disebutkan dalam tulisan Skotnes (2015) bahwa kesadaran akan keamanan TIK dan pengalaman menjadi faktor yang berpengaruh dalam keamanan informasi. Sebaiknya dibuatkan SOP untuk menjaga informasi dan data-data penting yang menjadi tanggung jawab masing-masing pegawai. Penggunaan email instansi untuk urusan pekerjaan perlu dijadikan prioritas agar keterjaminan data-data penting tidak mudah disimpan dan diambil oleh pihak asing. Disamping itu sosialisasi akan pentingnya keamanan informasi dan langkah-langkah yang harus ditempuh untuk menjaga informasi sangat diperlukan. Jika dibutuhkan dibuatlah edaran, atau pengumuman bagaimana untuk menjaga data dan informasi. Kampanye atau sosialisasi yang terjadwal dan berkelanjutan menjadi penting agar upaya penyadaran akan pentingnya keamanan informasi ini bisa terwujud.

IV. PENUTUP

A. Kesimpulan dan Saran

Variabel Keamanan Informasi dipengaruhi oleh variabel *risk tolerance* dan *risk perception*. Koefisien korelasi untuk variabel *risk perception* adalah -0.253 dapat disimpulkan bahwa semakin rendah *risk perception* seseorang maka akan semakin tinggi Kemanan Informasi orang tersebut. Untuk nilai koefisien korelasi dari variabel *risk tolerance* terhadap keamanan Informasi adalah -0.264. Hal ini menunjukkan bahwa terdapat hubungan negatif yang signifikan antara *Risk tolerance* dengan Keamanan Informasi. Semakin rendah *risk tolerance* seseorang maka akan semakin tinggi Kemanan Informasi orang tersebut.

Penelitian ini masih terbatas untuk menggali korelasi antara dua variabel independen *Risk perception* dan *risk tolerance* terhadap variabel dependen Keamanan Informasi, sehingga perlu dikembangkan untuk menambahkan variabel-variabel lain yang mempengaruhi Perilaku Keamanan Informasi. Penelitian lanjutan masih perlu dilakukan untuk menggali lebih dalam variabel-variabel yang mungkin berpengaruh dan jika dimungkinkan bisa dilakukan analisis lebih jauh seperti analisis regresi, dan *Structural Equation Model.*

Ucapan terima kasih : Penulis mengucapkan terima kasih kepada Kementerian Komunikasi dan Informatika atas kesempatan yang diberikan untuk menyelesaikan penelitian ini.

Daftar Pustaka

Dupuis Marc J., Crossler Robert E., Popovsky Barbara Endicott. 2015. "*The Information Security Behavior of Home Users : Exploring a User's Risk Tolerance and Past Experiences in the Context of Backing Up Information*" http://faculty.washington.edu/marcjd/pubs/risk-tolerance.pdf diakses 11 Maret 2016 jam 14.00.

Elena, Gianfranco. 2012. Risk Perception and Cloud Computing Security. University of Glasgow, UK

Hal Tipton and Micki Krause. 2005. *Handbook of Information Security Management*, CRC Press LLC.

ISO 27000 : 2012. 2012. *Information technology, security techniques, Information Security Management System Overview and vocabulary*.

Jantin, Suhar. 2014. Analisis Validitas dan Reliabilitas Dengan Skala Likert Terhadap Pengembangan SI/TI Dalam Penentuan Pengambilan Keputusan Penerapan Strategic Planning pada Industri Garmen. *Prosiding* Seminar Nasional Aplikasi Sains & Teknologi (SNAST) 2014 ISSN: 1979-911X, Yogyakarta. 15 November

Kokolakis, Spyros. 2011. *Risk Perception, Psychology and Economics of Information Security:A multi methodological exploration*. Dept. of Information & Communication Systems Engineering, University of the Aegean Bristol, February 2011

Long Huang, Ding. Rau, Patrick Pei-Luen. Salvendy, Gayvriel. 2010. Perception of Information Security. Journal Behaviour & Information Technology, Volume 29, 2010. Issue 3 Pages 221-232

Mattord, H. J. & Whitman, M.E. 2012. *Principles of information security*. (4th edition). Course Technology : Cengage Learning.

National Institute of Standards and Technology Special Publication (NIST SP) 800-59. 2003. *Guideline for Identifying an Informastion System as a National Security System.*

Pattinson, Malcolm & Anderson, Grantley. 2006. Risk Communication, Risk Perception and Information Security. https://www.researchgate.net/publication/45816163_Risk_Communication_Risk_Perception_and_Information_Security diakses 6 Oktober 2016.

Skotnes, Ruth stgaard. 2015. Risk perception regarding the Safety and Security of ICT System in Electric Power Supply Network Companies. Safety Science Monitor Issue 1. 2015. Vol. 19. Article 4.

Vance, Anthony. Anderson, Bonnie Brinton. Kirwan, C. Brock. Eargle, David. 2014. Using Measuring of Risk Perception to Predict Information Security Behavior : Insights from Electroenceph (EEG). Jurnal of The Assosiation for Information System (JAIS) Volume 15, Special Issue, pp. 679-722, October 2014