DAMPAK PENGGUNAAN BROADBAND TERHADAP PERILAKU KEAMANAN INFORMASI
(Sebuah Proposal Disain Penelitian)

IMPACT OF BROADBAND ON THE USE OF INFORMATION SECURITY BEHAVIOR
(A Research Design Proposal)

Dewi Hernikawati
Peneliti Bidang TIK Lainnya pada Balai Pengkajian dan Pengembangan Komunikasi dan Informatika Jakarta,
Jln. Pegangsaan Timur No. 19 B Jakarta Pusat, Provinsi DKI Jakarta, Indonesia
Telp. 31922337, dewi005@kominfo.go.id,
(Naskah diterima 17-5-206, revisi pasca editing redaksi . 8-8-2016, diperiksa PR 11-8-2016,
direvisi pasca editing mitra bestari 20-8-2016, disetujui PR terbit 19-8-2016)

ABSTRACT

Broadband give high speed to surfing, downloading, uploading and using data. Humans are the weakess point in security that needs to be educated in order to minimize the impact of security attach to organization. This paper will purpose design of research the impact of broadband to information security behavior. Literature study used as a method. Result of this design are risk tolerance, risk perception, past experience severity, past experience frequency, use of broadband as independen variable and information security as dependen variable.
Keywords : Impact; Use, Broadband, Behavior, Information security, Research Design

ABSTRAK

Broadband memberikan kecepatan tinggi dalam berinternet dan penggunakan data. Manusia sebagai titik terlemah dari rantai kemananan yang perlu selalu dibina agar dapat meminimalisasi dampak serangan keamanan yang bisa menjadi ancaman untuk organisasi. Oleh karena itu, dalam tulisan ini akan merumuskan desain penelitian dampak penggunaan broadband terhadap perilaku keamanan informasi. Metode yang digunakan adalah studi literatur. Hasilnya pada desain penelitian ini melibatkan variabel *risk tolerance, risk perception, past experience severity, past experience frequency*, penggunaan broadband sebagai variable independen sedangkan variabel Keamanan informasi sebagai variable dependen.
Kata kunci : Dampak, Penggunaan, Broadband, Perilaku, Keamanan informasi, Disain penelitian.

PENDAHULUAN

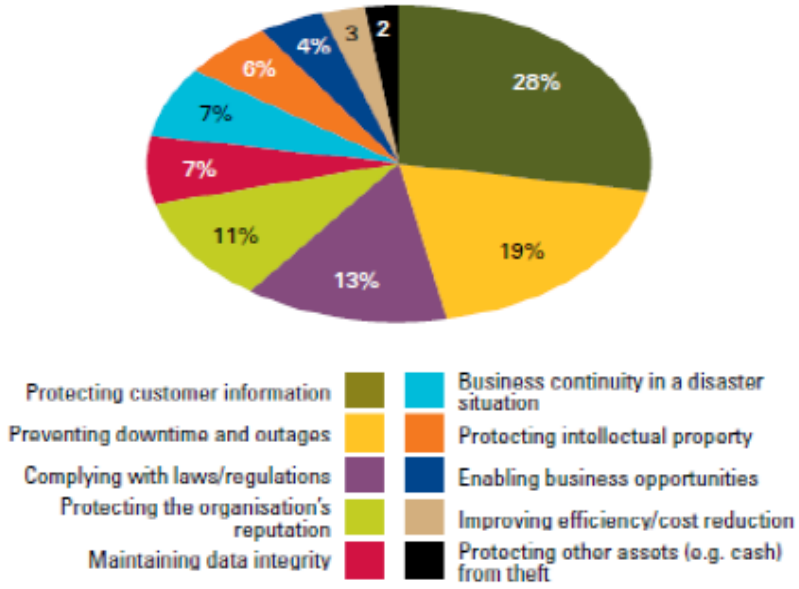
Komunikasi berasal dari kata-kata (bahasa) Latin *communis* yang berarti umum *(common)* atau bersama. Apabila kita berkomunikasi, sebenarnya kita sedang berusaha menumbuhkan suatu kebersamaan *(commonnes)* dengan seseorang. Dalam berkomunikasi kita berusaha berbagai informasi, ide atau sikap, sebagai contoh, misalnya saya sedang berusaha berkomunikasi dengan para pembaca untuk menyampaikan ide bahwa hakikat sebuah komunikasi sebenarnya adalah usaha membuat penerima atau pemberi komunikasi memiliki pengertian (pemahaman) yang sama terhadap pesan tertentu" (Suprapto, 2006 : 2-3). Secara umum dapat diartikan bahwa komunikasi adalah penyampaian informasi dan pengertian dari seseorang kepada orang lain. Proses-proses yang ada dalam komunikasi antara lain adanya *source* (sumber), *communicator* (penyampai pesan), *Message* (Pesan), *Channel* (saluran), *Communican* (penerima pesan), dan *Effect* (hasil). Saluran komunikasi (*channel*) merupakan saluran komunikasi untuk menyampaikan pesan yang dapat diterima oleh panca indra atau disampaiakan dengan media. Komunikasi dapat terjadi melalui dua *channel*/saluran yaitu saluran formal dan tidak formal. Saat ini komunikasi bahkan lebih mudah bisa dilakukan tanpa harus bertemu langsung. Komunikasi ini bisa dilakukan dengan telepon, berkirim surat, dan menggunakan internet. Dengan adanya internet memungkinkan pengguna untuk memiliki banyak pilihan media online untuk berkomunikasi. Komunikasi ini bisa dilakukan dengan email, ruang chat, situs jejaring sosial, forum komunikasi, blog yang memiliki fasilitas koneksi komunikasi dll. Dengan adanya perkembangan saluran komunikasi ini membutuhkan dukungan infrastruktur internet yang baik dan handal.

Saat ini internet sudah menjadi kebutuhan salah satunya untuk berkomunikasi. Teknologi Broadband mampu menyediakan layanan data, suara, dan video dalam satu pipa sehingga akses internet menjadi lebih cepat, dan bisa melakukan panggilan pada saat sedang berselancar dengan internet. Dengan adanya broadband memberikan banyak keuntungan bagi pengguna. Dampak penggunaan broadband menurut Seymour dan Naido (2013) antara lain komunikasi menjadi lebih mudah, lebih

hemat waktu dan bisa mengerjaan pekerjaan lain, hemat biaya, dan memudahkan untuk melakukan pekerjaan dari rumah. Banyak keuntungan yang diperoleh dengan teknologi broadband ini, namun ada juga kerugian-kerugian yang ditimbulkan. Kerugian atau kekurangan dari teknologi broadband ini antara lain dari sisi ancaman keamanan, biaya layanan yang lebih tinggi jika dibandingkan dengan dial-up dan belum tersedia diseluruh wilayah pedesaan.

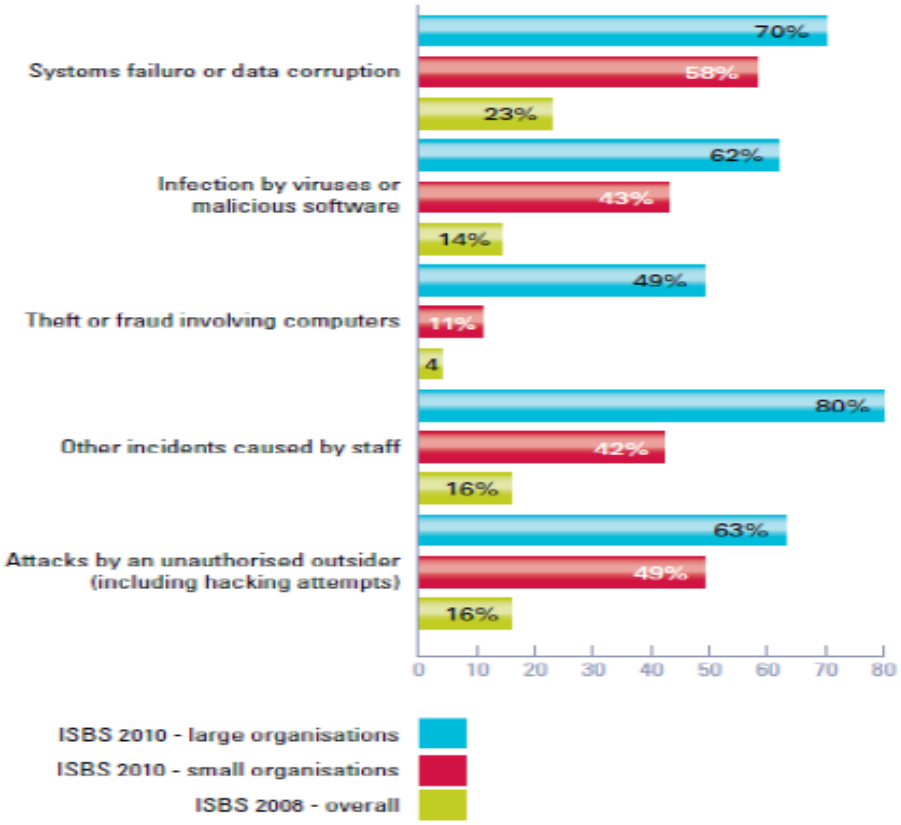
Broadband yang memberikan keuntungan hemat waktu, murah, dan cepat ini menyebabkan perubahan pada perilaku pengguna. Jika sebelumnya data disimpan secara lokal di hard disk, flash disk, atau hardisk external dengan adanya broadband memungkinkan pengguna untuk menyimpan data di cloud sehingga bisa diakses kapan saja dan dimana saja sehingga tidak perlu repot untuk membawa peralatan kemana-mana. Ancaman dari cloud ini adalah jika data tiba-tiba tidak bisa diakses atau di hack, adanya eror, fraud dan pencurian data baik oleh pihak berwenang maupun yang tidak berwenang, karyawan melakukan sabotase, dan sebagainya. Dengan akses yang bisa lebih cepat, tidak hanya data yang bisa cepat diakses namun penyebaran virus juga bisa lebih cepat. Selain itu pengguna juga diuntungkan dengan lebih mudah untuk mengunduh software, film, game meskipun keamanannya belum bisa dijamin. Dengan adanya broadband ini menyebabkan perubahan perilaku pengguna baik dari segi pola penggunaan internet, dari segi keamanan informasi, dari segi konsumsi yang dilakukan, dsb. Dari segi keamanan informasi dilihat karena Informasi merupakan aset penting dalam organisasi yang perlu dikelola dengan sebaik-baiknya dan bisa berperan dalam pengambilan keputusan pimpinan organisasi.

Peran penting informasi dalam organisasi perlu diperhatikan terkait ancaman dan kerawanan terhadap informasi semakin meningkat seiring munculnya persaingan antar organisasi. Pengamanan informasi sangat dibutuhkan agar kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi (Ronald dan Russell, 2007) dapat terjaga sehingga tidak mengganggu kinerja dan operasional organisasi. Seberapa pentingkah diterapkannya sistem keamanan informasi di suatu organisasi atau perusahaan? Dan faktor apa saja yang menjadi tujuan dari sistem keamanan informasi? InfoSecurity Europe telah mengklasifikasikan 10 faktor pemicu pentingnya diterapkan sistem keamanan informasi. Berdasarkan laporan teknis survey pelanggaran keamanan informasi tahun 2010 terhadap 539 perusahaan (besar dan kecil) yang dilakukan oleh InfoSecurity Europe, diperoleh diagram komposisi tingkat urgensi dari ke 10 faktor tersebut seperti yang tertera di Gambar 1. (InfoSecurity Europe, 2010).



Gambar 1. Diagram Komposisi Faktor Pemicu Pentingnya Keamanan Informasi

Dari gambar terlihat bahwa tiga besar faktor utama perlu diterapkannya keamanan informasi adalah untuk mengamankan informasi pelanggan, faktor kepatuhan hukum (regulasi) serta menjaga integritas data. Sementara faktor lainnya tidak terlalu signifikan. Kegagalan proses pengamanan informasi akan berefek langsung terhadap kepercayaan pelanggan atau masyarakat yang dampaknya dapat mengganggu hingga membawa bencana bagi institusi bahkan keamanan nasional. Di sisi lain perkembangan teknologi telah merubah lingkungan bisnis menjadi lebih terbuka dalam jaringan interkoneksi global (e-World), yang sangat rawan terhadap ancaman. Pertukaran informasi dalam jaringan global telah menjadi target potensial bagi para penyerang baik secara pasif maupun aktif. Hasil survey dari InfoSecurity Europe pada Information Security Breaches Survey 2010 terhadap tipe-tipe pelanggaran keamanan informasi dapat dilihat pada Gambar 2. (InfoSecurity Europe, 2010).



Gambar 2. Diagram Tingkat Serangan Keamanan Informasi

Serangan terhadap keamanan informasi dapat berasal dari dalam (*insider attacks*) dan dari luar (*outsider attacks*). Berdasarkan data pelanggaran dari gambar 2, terlihat bahwa penyebab mayoritas pelanggaran adalah manusia baik secara individu maupun berkelompok. Pelanggaran paling besar justru dilakukan oleh staf, baik karena faktor kelalaian hingga faktor kriminal (*white collar criminal*). Berdasarkan hal tersebut diatas, manusia memegang peranan kunci dalam penerapan sistem keamanan informasi. Mitnick dan Simon (2002) menyatakan manusia merupakan faktor utama dan penting dalam pengamanan informasi selain teknologi, karena manusia merupakan rantai terlemah dalam rantai keamanan. Oleh sebab itu, dimensi manusia perlu selalu dibina dengan baik agar segala bentuk ancaman dapat dihindari. Salah satu cara yang dapat dilakukan adalah dengan menumbuhkan kesadaran akan pentingnya keamanan informasi.

Perumusan Masalah

Dari latar belakang tersebut, dengan adanya broadband yang memberikan kecepatan tinggi dalam berinternet ini memberikan kemudahan dalam berkomunikasi. Selain itu, telah diketahui bahwa manusia sebagai titik terlemah dari rantai kemananan yang selalu perlu dibina agar dapat meminimalisasi dampak serangan keamanan yang bisa menjadi ancaman untuk organisasi. Terkait dengan fenomena perkembangan *channel* berkomunikasi dalam hubungannya dengan titik kelemahan manusia sebagai pengguna tadi, maka tulisan ini akan berupaya merumuskan desain penelitian tentang

dampak penggunaan broadband terhadap perilaku keamanan informasi? Mengingat hasil literature review yang memperlihatkan masih relatif minimnya pelaksanaan studi tentang perilaku keamanan informasi baik di dunia dan apalagi di Indonesia, maka tulisan ini bertujuan untuk membuka horison baru bagi para akademisi tentang studi keamanan informasi dalam kaitannya dengan broadband. Dengan upaya dimaksud maka diharapkan hasilnya dapat membantu para akademisi yang tertarik mempelajari persoalan perilaku keamanan informasi.

Tinjauan Pustaka

Penelitian terkait perilaku keamanan informasi, dari literatur yang ada pada hakekatnya ternyata bukanlah suatu fenomena yang belum pernah dipelajari secara ilmiah oleh para akademisi. Akan tetapi jumlahnya masih belum banyak dijumpai. Diantara penelitian itu, antara lain tersebutlah seperti penelitian dengan judul "*The Information Security Behavior of Home Users : Exploring a User's Risk Tolerance and Past Experiences in the Context of Backing Up Information"*

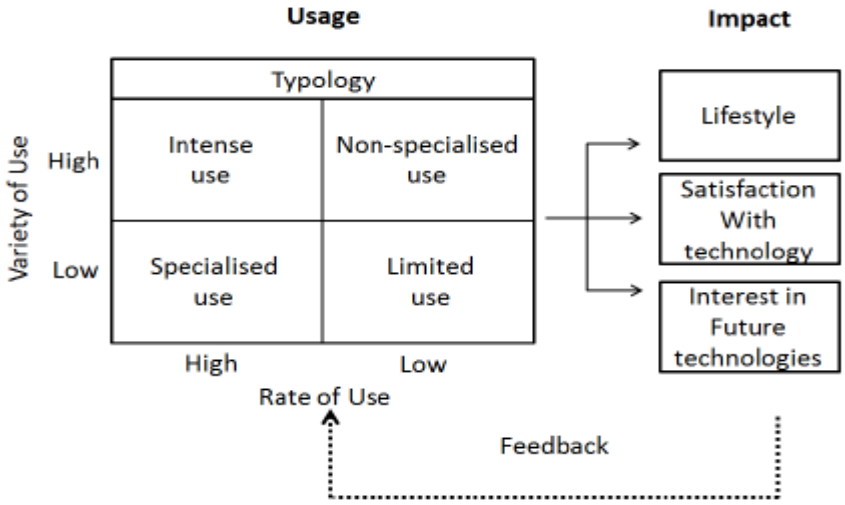
Penelitian ini dilatarbelakangi oleh adanya banyak keuntungan yang ditimbulkan oleh penggunaan komputer bagi pengguna namun terdapat banyak resiko akibat penggunaan tersebut. Penelitian ini untuk menguji perilaku individu terhadap keamanan informasi dengan variabel dependen yang digunakan adalah *backing up* informasi.

Teori yang digunakan pada penelitian ini adalah *Protection Motivation Theory* (PMT) yang telah disesuaikan dengan Sistem Informasi. Variable dalam penelitian ini adalah *individual risk tolerance* dan *risk perception*. 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.

Selain itu ada juga hasil penelitian yang sudah dipublikasikan melalui jurnal ilmiah yang ditulis oleh Seymour dan Naidoo (2013). Penelitian mereka sendiri berjudul "*The Usage and Impact of Broadband: A South African Household analysis*". Latar belakang penelitian ini adalah masih sedikitnya penelitian yang fokus terhadap adopsi broadband dan dampak layanan broadband di Afrika Selatan. Penelitian ini bertujuan untuk menyelidiki penggunaan dan dampak layanan broadband. Penelitian ini diakukan secara literatur riview kemudian dilaksanakan wawancara untuk mengambil data dan dilakukan validasi dengan kuantitatif.

Hasil dari studi ini menunjukkan bahwa pengguna broaband di Afrika Selatan sebagian besar adalah pengguna eksperimental. Penggunaan broadband yang tinggi memberikan kemudahan pengguna untuk bekerja dari rumah sehingga menghemat waktu dan hidupnya lebih nyaman. Pengguna lebih puas dengan teknologi dan menunjukkan minat ketertarikan terhadap teknologi komunikasi yang berorientasi ke masa depan. Model yang diperoleh dapat menjadi sumber literatur dan masukan kepada pemerintah, *Internet Service Provider*, bisnis, dan organisasi publik untuk membuat keputusan pada investasi infrastruktur broadband.



Gambar 3. *Proposed model for broadband use and impact in the household* (Seymour dan Naidoo,2013)

Penelitian lainnya yaitu penelitian yang dilakukan oleh Crossler (2010). Penelitian ini berjudul "*Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data*". Penelitian ini menggunakan *Protection Motivation Theory (PMT)* sebagai *framework* yang digunakan untuk melihat perilaku pengguna dalam melakukan back up data pada komputernya. Penelitian ini dilakukan dengan survey kepada 112 responden yang dilakukan secara online dan langsung menyebarkan kuesioner. Hasil dari penelitian ini adalah *self-efficacy* dan *response efficacy* berpengaruh positif terhadap back up data. Sedangkan untuk variabel *prevention cost , perceived security vulnerability* dan *perceived security threat* berpengaruh negative atau tidak ada pengaruh terhadap back up data.

Kemudian penelitian yang dilakukan oleh Chenoweth, Minch, dan Gattiker (2009) dengan judul "*Application of Protection Motivation Theory to Adoption of Protective Technologies*". Protection Motivation Theory (PMT) merupakan model yang potensial untuk digunakan dalam memprediksi adopsi proteksi teknologi. PMT digunakan untuk menghindari kerugian dari dampak negative perkembangan teknologi seperti malware. Dalam penelitian ini PMT digunakan untuk mengadopsi anti-spyware software dan menguji model pada pengguna. Responden dalam penelitian ini adalah mahasiswa pengguna komputer. Hasil dari penelitian ini menunjukkan bahwa *perceived vulnerability, perceived severity, response efficacy,* dan *response cost* berpengaruh terhadap perilaku untuk menggunakan software anti-spyware sebaga protektor teknologi. Maladaptive coping hanya dipengaruhi oleh response cost dan pengaruhnya sangat kecil.

Berdasarkan hasil tinjauan literatur sebelumnya diketahui bahwa studi terkait keamanan informasi pada dasarnya masih relatif sedikit dilakukan para akademisi. Berdasarkan hasil studi tersebut juga menunjukkan bahwa variabel/konsep yang diamati juga berbeda. Dengan kondisi empirik tersebut, bahwa masih sedikit yang melakukan penelitian terkait keamanan informasi di Indonesia maka penelitian ini menjadi signifikan/penting untuk dilakukan.

Konsep-Konsep Teoritik

1. 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 industry keamanan computer 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).

2. Perilaku Keamanan Informasi

Perilaku keamanan informasi bagi pengguna dalam rumah tangga dan di organisasi bisa berdeda. Dari sisi pengguna pribadi (dalam rumah tangga) terkait dengan pencegahan yang telah dilakukan pengguna untuk mengamankan informasi, atau peralatan yang digunakan seperti 82iteratu dan laptop. Dalam melindungi informasi ini pengguna bisa mengapdate firewall, tidak membuka email dari pengirim yang tidak jelas, membuat password yang sulit, dan lain-lain. Dari segi organisasi bisa dihubungkan dengan kebijakan dalam suatu organisasi yaitu dengan mematuhi aturan yang ada atau tidak mematuhi aturan terhadap kemanan informasi yang telah ditetapkan. Penelitian yang dilakukan oleh Siponen dan Vance (2010) menyatakan bahwa pelanggaran yang paling umum dan penting dalam keamanan Informasi di organisasi antara lain kegagalan dalam mengunci atau log out 82iteratu, menulis password ditempat yang bisa dilihat orang lain, membagi-bagi password dengan teman, menduplikasi (copy) data 82iteratur di USB yang tidak aman, meyebarkan informasi rahasia keluar, mematikan konfigurasi keamanan, memakai laptop sembarangan diluar perusahaan, mengirim informasi rahasia yang tidak terinkripsi, dan membuat password yang mudah ditebak.

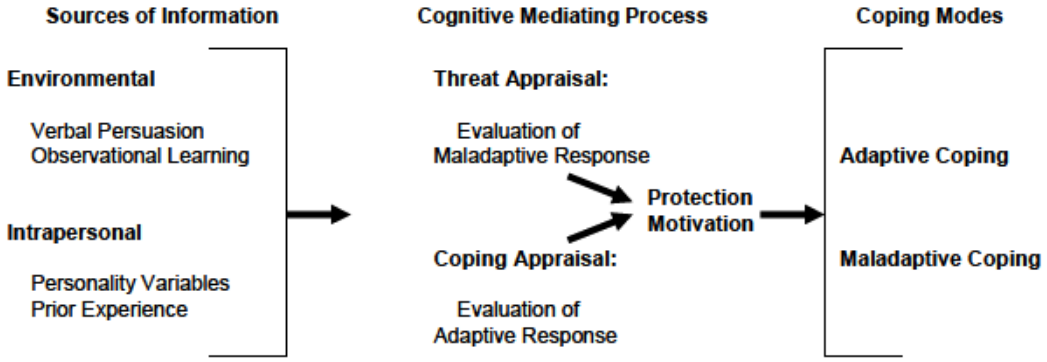
3. Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) merupakan teori yang dikembangkan oleh Roger pada tahun 1975 sebagai pengembangan dari *expectancy-value theory* untuk melengkapi pemahaman dampak ketakutan yang muncul pada perubahan tingkah laku. PMT adalah suatu proses penilaian ancaman dan proses penilaian tanggapan yang mengakibatkan niat untuk melaksanakan tanggapan adaptif (motivasi perlindungan) atau mal adaptif (menempatkan seseorang pada resiko). PMT merupakan teori perilaku yang berfungsi mengembangkan intervensi untuk mengurangi ancaman pada individu dengan penelitian dan mengintegrasikan konsep psikologis, sosiologis, dan bidang-bidang lainnya yang terkait. PMT awalnya diterapkan pada bidang kesehatan. Teori ini menyatakan bahwa perilaku yang berhubungan dengan kesehatan dibentuk oleh 4 komponen yaitu vulnerability (kerentanan), severity (ancaman), response effectiveness (tingkat efektivitas respon), dan self efficacy (keyakinan diri). PMT mengukur dua variable independen yaitu threat appraisal dan coping appraisal. Threat appraisal berhubungan dengan severity dan vulnerability. Pada coping appraisal berhubungan dengan response effectiveness dan self efficacy. PMT ini melibatkan 2 sumber informasi yaitu lingkungan dan intrapersonal. Contoh sumber informasi lingkungan adalah persuasi verbal dan belajar dari observasi, sedangkan contoh untuk informasi intrapersonal adalah pengalaman penting.

Menurut Floyd (2000) dalam Crossler (2010), Premis pada PMT adalah bahwa informasi pertama yang diterima (*sources of information*), yang mengarah pada evaluasi dengan orang yang menerima (*cognitive mediating process*), dan terakhir sampai kepada orang yang akan bereaksi terhadap informasi yang diterima (*coping mode*). Sumber informasi adalah variabel input ke model termasuk lingkungan dan intrapersonal. Lingkungan disini mencakup *verbal persuasion* dan *observational learning*. Sumber intrapersonal antara lain aspek kepribadian dan umpan balik dari pengalaman sebelumnya termasuk pengalaman terkait perilaku yang menarik. *Cognitive mediating processes* memiliki 2 tipe yaitu *threat appraisal process* dan *coping appraisal process*. *Threat appraisal* terdiri dari *threat perception (severity* dan *vulnerability*) dan dilanjutkan dengan *maladaptive response*.

a) *Security Threat Appraisal*
   Security Threat Appraisal bisa dikatakan sebagai persepsi terhadap resiko dimana terdapat konsep ketidakpastian dan konsekuensi. Security Threat Appraisal mengarah pada ketidakpastian dan mengarah untuk mengetahui bagaimana pemikiran orang yang memiliki resiko terhadap suatu ancaman.
b) *Security Coping Appraisal*
   Security Coping Appraisal terdiri dari *security self-efficacy, response efficacy,* dan *prevention cost*. *Security self-efficacy* adalah kepercayaan individu pada kemampuannya untuk mencegah atau mengurangi peristiwa keamanan yang

mengancam. *Response efficacy* adalah keyakinan individu terhadap perilaku yang direkomendasikan untuk mencegah atau mengurangi keamanan. *Security Coping Appraisal* terdiri dari *security self-efficacy, response efficacy,* dan *prevention cost*. *Security self-efficacy* adalah kepercayaan individu pada kemampuannya untuk mencegah atau mengurangi peristiwa keamanan yang mengancam. *Response efficacy* adalah keyakinan individu terhadap perilaku yang direkomendasikan untuk mencegah atau mengurangi keamanan. *Respon cost* akan meningkatkan *likelihood* dan menurunkan *adaptive coping response*.



Gambar 4. *Protection Motivation Theory* (Floyd (2000) dalam Crossler, 2010)

PMT telah digunakan pada penelitian dibidang Sistem Informasi. Model yang diajukan oleh Liang dan Xue dalam Dupuis, Crossler, Popovsky untuk penelitian Sistem Informasi adalah sebuah model yang terdiri dari 4 konstruk dan berakibat langsung pada pengelakan motivasi. Variable ini terdiri dari perceived threat, safeguard effectiveness, safeguard cost, dan self efficacy. Perceived threat ditentukan oleh dua sub konstruk yaitu perceived severity dan perceived susceptibility. Hipotesis yang diajukan pada penelitian ini adalah adanya interaksi antara perceived severity dan perceived susceptibility seperti interaksi antara perceived threat dan safeguard effectiveness. Pengelakan motivasi dicatat untuk mendapatkan efek langsung pada pengelakan perilaku. Hasil dari penelitian ini adalah bahwa interaksi antara perceived severity dan susceptibility tidak signifikan atau dapat dicatat bahwa back up informasi secara teratur dapat mengurangi kerentanan dan bahaya.

4. Broadband

Kecepatan transfer data adalah jumlah bit yang melewati suatu medium dalam satu detik. Kecepatan akses internet dibedakan menjadi 2 kategori yaitu *Dial Up Connection* dan *Broadband connection*. *Dial up connection* mampu mentransfer data maksimal dengan kecepatan 56 Mbps. Broadband merupakan jaringan atau servis internet dengan kecepatan transfer data yang lebih tinggi jika dibandingkan dial-up karena memiliki lebar jalur data yang besar. Teknologi broadband dengan jalur lebar ini akan membagi-bagi jalur lebar yang ada dengan pengguna lain, namun jika tidak ada pengguna lain yang memakai maka jalur tersebut sepenuhnya akan digunakan sendiri sehingga kecepatannya menjadi lebih besar.

Broadband atau pita lebar ini merupakan media transmisi yang bisa membawa banyak sinyal dan membagi kapasitas besarnya dalam beberapa kanal bandwith. Setiap kanal akan beroperasi dengan frekuensi yang spesifik. Jalur lebar yang umum digunakan ada dua jenis yaitu DSL dan kabel modem yang bisa mentransfer 512 Kbps atau lebih. Broadband memiliki kelebihan dibandingkan dial up yaitu akses data multimedia dengan kecepatan tinggi. Akses data ini antara lain layanan gambar, audio, dan video termasuk video streaming, video downloading, video telephony, dan video messaging. Selain itu, dengan perangkat yang mendukung teknologi ini maka pengguna bisa mengakses hiburan mobile TV, mengunduh music, dan berkomunikasi secara real-time dengan teknologi fixed mobile seperti webcam. Broadband adalah koneksi dengan kecepatan tinggi yang memungkinkan akses internet secara cepat dan selalu terkoneksi (*always on*).

Metodologi

Metodologi merupakan langkah-langkah yang dilakukan untuk menyusun penelitian dalam hal ini adalah langkah-langkah yang dilakukan untuk membuat desain penelitian. Pada tahap ini penulis melakukan studi literature untuk mendapatkan bahan-bahan yang dibutuhkan untuk membuat desain penelitian. Studi literature tentang teori terkait penelitian dan penelitian terdahulu dijadikan dasar penyusunan desain penelitian. Survey bisa dilakukan di lingkungan pemerintah dalam hal ini PNS, dunia pendidikan untuk pelajar atau mahasiswa, masyarakat umum, pegawai swasta sehingga bisa dilihat perilakunya secara luas dan ada keterwakilan dari semua sektor.

PEMBAHASAN

Pada rancangan penelitian ini akan mengadopsi model dari penelitian sebelumnya "The Usage and Impact of Broadband : A South African Household analysis oleh Lisa F Seymour dan Mogen Naidoo" untuk melihat dampak Broadband pada gaya hidup yang dihubungkan dengan keamanan informasi dengan menggunakan *Protection Motivation Theory* yang telah digunakan pada penelitian-penelitian sebelumnya. Tabel 1. Menunjukkan penelitian sebelumnya dan perbedaan dengan penelitian yang akan dilakukan.

Tabel 1. Perbandingan dengan penelitian terdahulu.

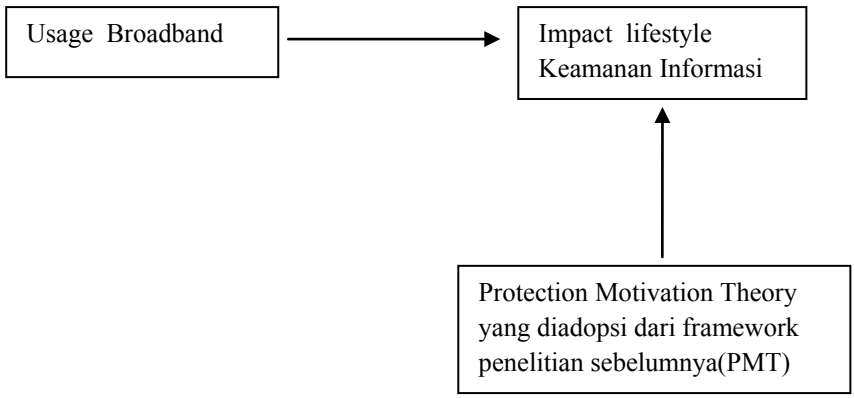
No	Penelitian	Judul	Sampel	Variabel	Hasil
1.	Dupuis Marc J., Crossler Robert E., Popovsky Barbara Endicott	*The Information Security Behavior of Home Users : Exploring a User's Risk Tolerance and Past Experiences in the Context of Backing Up Information*	Amazon's Mecahnical Turk	*risk tolerance, risk perceptions, past experiences severity, past experiences frequency, variable severity dan likelihood*	*risk tolerance, risk perception* dan *past experience* berpengaruh secara signifikan untuk memprediksi perilaku *back up* data.
2.	Lisa F Seymour dan Mogen Naidoo	The Usage and Impact of Broadband: A South African Household analysis	Pengguna Internet	*Variety of use, rate of use, life style, satisfaction with technologi, interest in future technology*	Pengguna broaband di Afrika Selatan sebagian besar adalah pengguna eksperimental. Penggunaan broadband yang tinggi memberikan kemudahan pengguna untuk bekerja dari rumah sehingga menghemat waktu dan hidupnya lebih nyaman.
3	Crossler	Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data	Penonton tournament soccer, pegawai , mahasiswa paska sarjana	*self-efficacy, response efficacy, prevention cost, perceived security vulnerability, perceived security threat, backup data*	*self-efficacy* dan *response efficacy* berpengaruh positif terhadap back up data

4	Chenoweth, Tim. Minch, Robert. Gattiker, Tom	Application of Protection Motivation Theory to Adoption of Protective Technologies	mahasiswa pengguna komputer	*perceived vulnerability, perceived severity, Fear Appraisal, response efficacy, self efficacy, response cost, maladaptive coping, behavioral Intention*	*perceived vulnerability, perceived severity, response efficacy,* dan *response cost* berpengaruh terhadap perilaku
5	Penelitian ini	Dampak Penggunaan Broadband terhadap perilaku Keamanan Informasi	PNS	*risk tolerance, risk perceptions, past experiences severity, past experiences frequency, variable severity dan likelihood, penggunaan broadband, Keamanan Informasi*	Desain penelitian

Desain Penelitian

Pada penelitian ini perubahan perilaku keamanan Informasi akan diperoleh sebagai akibat dari penggunaan broadband yang memberikan kemudahan dan kecepatan dalam transfer data serta berkomunikasi melalui internet. Broadband merupakan salah satu variabel independen untuk menentukan perilaku keamanan Informasi. Variabel-variabel independen lain yang mempengaruhi perilaku keamanan informasi diperoleh dengan menggunakan teori *Protection Motivation Theory* yang sudah diadopsi untuk penelitian Sistem Informasi.

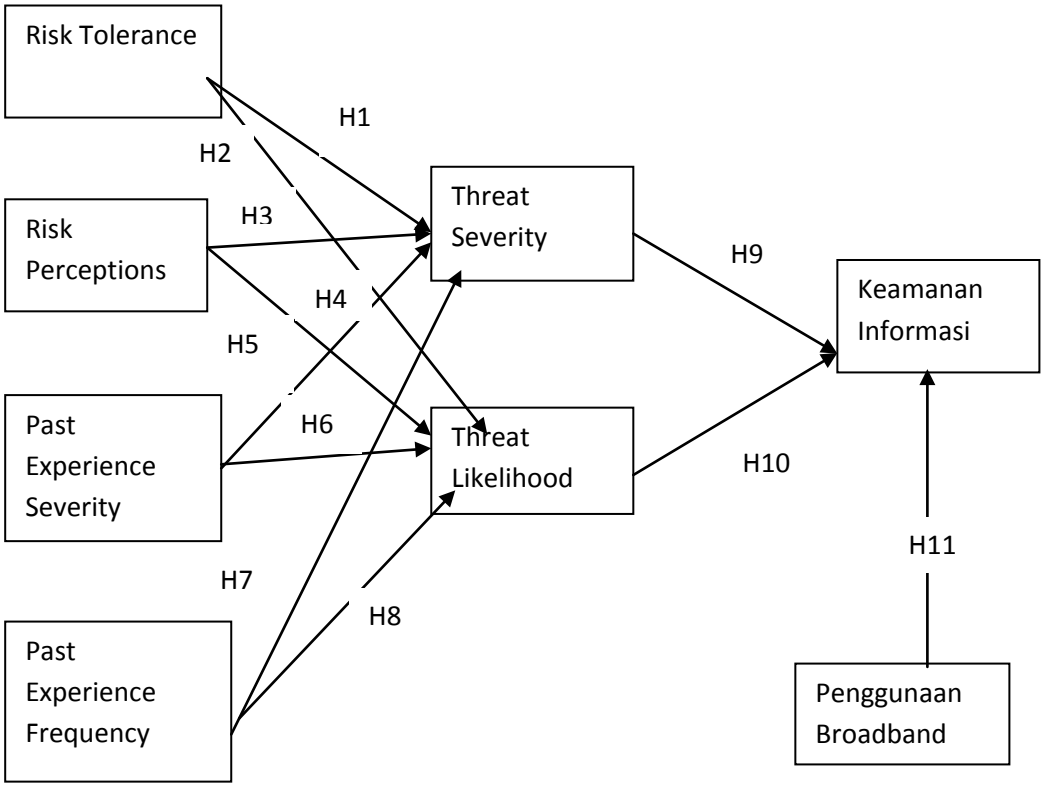
.



Gambar 4. Kerangka konsep penelitian

Berdasarkan *Protection Motivation Theory,* variabel yang akan digunakan sebagai variabel independen adalah *risk tolerance, risk perception, past experience severity,* dan *past experience frequency*. Variabel *risk tolerance* merupakan toleransi terhadap resiko-resiko yang akan terjadi terkait dengan keamanan informasi. *risk perception* adalah persepsi atau pandangan terhadap resiko yang akan terjadi. *Past experience severity* adalah pengalaman yang telah terjadi dan memberikan kerugian. *Past experience frequency* adalah banyaknya pengalaman terkait kejadian keamanan informasi yang telah dialami. Variabel *Threat Severity* dan *Threat Likelihood* merupakan variabel Mediasi. *Threat Severity*

adalah adanya insiden keamanan informasi yang akan menimbulkan pengaruh atau memberikan dampak negatif (merugikan). *Threat Likelihood* adalah ancaman yang akan timbul terkait keamanan informasi.variabel dependennya adalah Keamanan Informasi yaitu perilaku keamanan informasi. Untuk melihat variabel dengan lebih detail dapat dilihat pada gambar dibawah ini :



Gambar 5. Desain Penelitian Penggunaan Broadband terhadap perubahan Perilaku

Berdasarkan pada gambar 5. tersebut maka Hipotesis yang akan diuji pada penelitian ini adalah :
H1 : Risk Tolerance berpengaruh positif terhadap Threat Severity
H2 : Risk Tolerance berpengaruh positif terhadap Threat Likelihood
H3 : Risk Perceptions berpengaruh positif terhadap Threat Severity
H4 : Risk Perceptions berpengaruh positif terhadap Threat Likelihood
H5 : Past Experience Severity berpengaruh positif terhadap Threat Severity
H6 : Past Experience Severity berpengaruh positif terhadap Threat Likelihood
H7 : Past Experience Frequency berpengaruh positif terhadap Threat Severity
H8 : Past Experience Frequency berpengaruh positif terhadap Threat Likelihood
H9 : Threat Severity berpengaruh positif terhadap Perilaku Keamanan Informasi
H10 : Threat Likelihood berpengaruh positif terhadap Perilaku Keamanan Informasi
H11 : Penggunaan Broadband berpengaruh positif terhadap Perilaku Keamanan Informasi

PENUTUP

Kesimpulan

Pada desain penelitian ini variabel-variabel independen yang terlibat adalah *risk tolerance, risk perception, past experience severity, past experience frequency*, penggunaan broadband sedangkan variable dependennya adalah Keamanan informasi. Variabel mediasinya adalah *Threat Severity* dan *Threat Likelihood*.

Saran

Penelitian ini masih perlu dikembangkan untuk menggali variabel-variabel lain yang berpengaruh terhadap perilaku Keamanan Informasi, hal ini terkait masih sedikitnya penelitian Keamanan Informasi di Indonesia. Variabel-variabel itu diantaranya terkait variabel anteseden berupa variabel koneksivitas internet dan variabel intervening seperti variabel perpasive. Penelitian ini sebaiknya dilakukan tidak hanya dikalangan PNS namun bisa dilakukan dengan sampel pelajar atau mahasiswa untuk melihat perilaku keamanan Informasi dilingkungan pendidikan sehingga bisa membuat kebijakan dan solusi terkait Keamanan Informasi.

Ucapan terima kasih : Penulis tidak lupa mengucapkan terima kasih kepada tim redaksi beserta anggota mitra bestrai yang telah banyak mengarahkan penulis dalam proses penyelesaian karya tulis ilmiah ini.

Daftar Pustaka

Chenoweth, Tim. Minch, Robert. Gattiker, Tom. Application of Protection Motivation Theory to Adoption of Protective Technologies. Proceedings of the 42nd Hawaii International Conference on System Sciences. 2009.

Dupuis Marc J., Crossler Robert E., Popovsky Barbara Endicott, "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

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

InfoSecurity Europe. Information SecurityBreaches Survey 2010 (ISBS-2010) : Technical Report, www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf.2010.

ISO/IEC 17799:2005 : Information technology, security techniques, Code of practice for information security management.2005.

Kevin D. Mitnick and William L. Simon. The Art of Deception, Wiley Publishing, Inc. 2002.

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

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

Ronald L. Krutz and Russell Dean Vines. The CISSP and CAP Prep Guide: Platinum Edition, John Wiley & Sons. 2007.

Seymour, Lisa F and Naidoo , Mogen **"**The Usage and Impact of Broadband: A South African Household analysis" The *Electronic Journal Information Systems Evaluation* Volume 16 Issue 2. 2013. (134-147) , available online at www.ejise.com diakses 6 Januari 2016

Siponen, M. T. & Vance, A. Neutralization: new insights into the problem of employee information systems security policy violations. MIS *Quarterly*, 34(3), 487–502. 2010.

Suprapto, Tommy. *Pengantar Teori Komunikasi.* Cetakan Ke-1. Yogyakarta: Media Pressindo, 2006.

Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik (KIP). 2008.

Teori Kekayaan Media

Teori kekayaan Media didasarkan pada teori kontingensi dan teori pemrosesan informasi (Galbraith 1977). Pendukung pertama teori ini dibuat oleh Daft & Lengel (1984). Asumsi inti teori adalah bahwa media komunikasi memiliki berbagai kapasitas untuk menyelesaikan ambiguitas, negosiasi berbagai interpretasi, dan memfasilitasi pemahaman.

Dua asumsi utama teori ini yaitu : orang ingin mengatasi ketidakjelasan dan ketidakpastian dalam organisasi dan berbagai media yang biasa digunakan dalam organisasi bekerja lebih baik untuk tugas-tugas tertentu daripada yang lain. Menggunakan empat kriteria, Daft dan Lengel menyajikan hirarki Media kekayaan, diatur dari tinggi ke derajat rendah kekayaan, untuk menggambarkan kapasitas jenis media untuk proses komunikasi ambigu dalam organisasi.

Kriteria tadi adalah (a) ketersediaan umpan balik instan; (b) kapasitas media untuk mengirimkan beberapa isyarat seperti bahasa tubuh, nada suara, dan infleksi; (c) penggunaan bahasa alami; dan (d) fokus pribadi medium. Komunikasi tatap muka merupakan media komunikasi terkaya di hirarki dan diikuti oleh telepon, surat elektronik, surat, catatan, memo, laporan khusus, dan akhirnya, flier dan buletin.

Dari perspektif manajemen strategis, teori media kekayaan menunjukkan bahwa manajer yang efektif membuat pilihan rasional yang cocok dengan media komunikasi tertentu untuk tugas tertentu atau tujuan dan untuk tingkat kekayaan yang diperlukan oleh tugas yang (Trevino, Daft, & Lengel, 1990, di Kedelai 2001). (http://www.tcw.utwente.nl/theorieenoverzicht/Theory%20clusters/Mass%20Media/Media_Richness_Theory.doc/.