BAB II

LANDASAN TEORI

2.1 Pengertian Perilaku

Pengertian umum perilaku adalah segala perbuatan atau tindakan yang dilakukan oleh makhluk hidup. Pengertian perilaku dapat dibatasi sebagai keadaan jiwa untuk berpendapat, berfikir, bersikap, dan lain sebagainya yang merupakan refleksi dari berbagai macam aspek, baik fisik maupun non fisik.

Perilaku juga diartikan sebagai suatu reaksi psikis seseorang terhadap lingkungannya, reaksi yang dimaksud dibagi menjadi dua, yaitu: (Notoatmodjo, 2003).

- Pasif (tanpa tindakan nyata atau konkrit)
- Aktif (dengan tindakan konkrit)

Pengertian Perilaku adalah tindakan atau aktivitas dari manusia itu sendiri yang mempunyai bentangan arti yang sangat luas antara lain : berjalan, berbicara, menangis, tertawa, bekerja, kuliah, menulis, membaca, dan sebagainya. Dari uraian tersebut bisa disimpulkan bahwa perilaku manusia adalah semua kegiatan atau aktivitas manusia, baik yang diamati langsung, maupun yang tidak dapat diamati oleh pihak luar (Notoatmodjo, 2003).

2.2 Keamanan Informasi

Informasi adalah data yang telah diproses atau data yang memiliki arti (Mc Leod, 2004). Informasi dibentuk dari kombinasi data yang diharapkan memiliki arti bagi penerima.(Whitten, 2004). *Information security management system* bahwa keamanan informasi adalah upaya perlindungan dari berbagai macam ancaman untuk memastikan kelanjutan bisnis, meminimalisir resiko bisnis, dan meningkatkan investasi dan peluang bisnis (ISO/IEC, 2005).

Keamanan data adalah perlindungan data di dalam suatu sistem melawan terhadap otorisasi tidak sah, modifikasi, atau perusakan dan perlindungan sistem komputer terhadap penggunaan tidak sah atau modifikasi. Ada empat aspek utama dalam keamanan data dan informasi yaitu (Raharjo Budi, 2017):

1. *Privacy/Confidentiality* adalah aspek yang biasa dipahami tentang keamanan. Aspek *confidentiality* menyatakan bahwa data hanya dapat diakses atau dilihat oleh orang yang berhak. Biasanya aspek ini yang paling mudah dipahami oleh orang. Jika terkait dengan data pribadi, aspek ini juga dikenal dengan istilah *Privacy*. Serangan terhadap aspek *confidentiality* dapat berupa penyadapan data (melalui jaringan), memasang keylogger untuk menyadap apa-apa yang diketikkan di keyboard, dan pencurian fisik mesin / disk yang digunakan untuk menyimpan data. Perlindungan terhadap aspek *confidentiality* dapat dilakukan dengan menggunakan kriptografi, dan membatasi akses (segmentasi jaringan). (Raharjo Budi, 2017)

2. *Integrity* Aspek *integrity* mengatakan bahwa data tidak boleh berubah tanpa ijin dari yang berhak. Sebagai contoh, jika kita memiliki sebuah pesan atau data transaksi di bawah ini (transfer dari rekening 12345 ke rekening 6789 dengan nilai transaksi teretentu), maka data transaksi tersebut tidak dapat diubah seenaknya. (Raharjo Budi, 2017)

Serangan terhadap aspek *integrity* dapat dilakukan oleh *man-in-the-middle,* yaitu menangkap data di tengah jalan kemudian mengubahnya dan meneruskannya ke tujuan. Data yang sampai di tujuan (misal aplikasi di web server) tidak tahu bahwa data sudah diubah di tengah jalan. Perlindungan untuk aspek *integrity* dapat dilakukan dengan menggunakan message authentication code. (Raharjo Budi, 2017)

3. *Availability* Ketergantungan kepada sistem yang berbasis teknologi informasi menyebabkan sistem (beserta datanya) harus dapat diakses ketika dibutuhkan. Jika sistem tidak tersedia, not available, maka dapat terjadi masalah yang menimbulkan kerugian finansial atau bahkan nyawa. Itulah sebabnya aspek *availability* menjadi bagian dari keamanan. Serangan terhadap aspek *availability* dilakukan dengan tujuan untuk meniadakan layanan atau membuat layanan menjadi sangat lambat sehingga sama dengan tidak berfungsi. Serangannya disebut *Denial of Service* (DOS). Perlindungan terhadap aspek *availability* dapat dilakukan dengan menyediakan redundansi. Sebagai contoh, jaringan komputer dapat menggunakan layanan dari dua penyedia jasa yang berbeda. Jika salah satu penyedia jasa jaringan mendapat serangan (atau rusak), maka masih ada satu jalur lagi yang dapat digunakan. (Raharjo Budi, 2017).

2.3 *Data Leakage* (Kebocoran Data)

Kebocoran Data, sederhananya, adalah transmisi data yang tidak sah (atau informasi) dari dalam suatu organisasi dengan tujuan eksternal atau penerima lain. Kebocoran data mungkin terjadi melalui media secara elektronik, atau mungkin melalui metode fisik. Kebocoran data dapat terjadi secara disengaja atau tidak disengaja. Berikut beberapa tipe dari kebocoran data atau informasi yang sering dibocorkan, antara lain : (Sans, 2007)

1. Informasi Rahasia
2. Kekayaan Intelektual
3. Data Pelanggan
4. Informasi Kesehatan

2.4 *Data Theft* (Pencurian Data)

Pencurian data adalah tindakan mencuri informasi yang disimpan di komputer, server, atau perangkat lain dari korban yang tidak diketahui dengan maksud untuk berkompromi dengan privasi atau mendapatkan informasi rahasia. (Digital Guardian, 2017). Ketika infeksi *virus* di perangkat pribadi Anda mengarah ke pencurian informasi penting, ini dapat mengakibatkan: (Kaspersky, 2017)

- Pelanggaran serius privasi Anda
- Pencurian dana dari rekening bank Anda

Sedangkan kerugian dari *Data Theft* apabila di sisi bisnis adalah :

- Pangkalan data pelanggan
- Informasi keuangan
- Dokumentasi teknis

- Detail perbankan perusahaan

2.5 *Social Cost* (Biaya Sosial)

Biaya untuk melakukan perilaku keamanan (dalam fungsionalitas, kenyamanan atau waktu) mengurangi daya tarik perilaku keamanan dan membuatnya kurang mungkin dilakukan, Manfaat biaya untuk menanggapi ancaman terhadap keamanan *smartphone*. Sebagai biaya sosial yang timbul dari penolakan untuk menggunakan fitur dan aplikasi yang digunakan oleh teman seseorang tidak terikat pada ancaman tertentu.(Das and Khan, 2016)

2.6 *Trust* (Kepercayaan)

Kepercayaan adalah suatu proses menghitung *(calculative process)* antara biaya yang dikeluarkan dengan hasil yang diperoleh. Pelayanan yang baik yang diterima sekarang akan berlanjut untuk ke depannya, sehingga *service quality* berpengaruh positif berpengaruh positif terhadap *trust*. (Aydin dan Ozer, 2005)

Dalam menggunakan teknologi sosial, pengguna *smartphone* mungkin terpengaruh oleh keseluruhan tingkat kepercayaan mereka pada pengguna lain. Kepercayaan, dalam pengertian ini, sangat penting bagi keamanan informasi (yang mana bertujuan untuk membangun dan mempertahankan kepercayaan), dan ada seruan untuk menjadikan peran seperti itu sebagai kepercayaan yang jelas (Jensen, 2012) dan tidak ambigu (Gollmann, 2006).

2.7 *User Shophistication* (Kecangihan Pengguna)

User shophistication adalah pengetahuan teknologi atau keakraban."latar belakang dan keterampilan teknologi" dari individu. (Duncan, 1972) . Kedua dimensi ini penting dalam mengidentifikasi tingkat kecanggihan pengguna teknologi informasi. (Napoliello, 1987).

Kecanggihan pengguna dapat diwakili dengan jumlah aplikasi yang terpasang di *smartphone.*(Das and Khan, 2016).

2.8 Virus

Virus adalah sebuah program perangkat lunak kecil yang menyebar dari satu komputer ke komputer lain dan mengganggu pengoperasian komputer. *Virus* komputer dapat merusak atau menghapus data di sebuah komputer, menggunakan program email untuk menyebarkan *virus* ke komputer lain, atau bahkan menghapus apa pun yang ada di dalam harddisk.*Virus* komputer seringnya menyebar melalui lampiran pesan email atau pada pesan instan. Oleh karena itu, Anda tidak boleh membuka lampiran email kecuali jika Anda mengetahui siapa yang mengirim pesan atau kecuali jika Anda memang mengharapkan lampiran email. *Virus* dapat menyamar sebagai lampiran gambar lucu, kartu ucapan, atau file audio dan video. *Virus* komputer juga menyebar melalui unduhan di Internet. *Virus* dapat bersembunyi di dalam perangkat lunak bajakan atau di file lainnya yang Anda unduh (Microsoft, 2016).

Virus komputer, seperti virus flu, dirancang untuk menyebar dari *host* ke *host* dan memiliki kemampuan untuk mereplikasi dirinya sendiri. Demikian pula, dengan cara yang sama bahwa virus tidak dapat mereproduksi tanpa sel induk, virus

komputer tidak dapat mereproduksi dan menyebar tanpa pemrograman seperti file atau dokumen. Dalam istilah yang lebih teknis, *virus* komputer adalah jenis kode atau program jahat yang ditulis untuk mengubah cara mengoperasikan komputer dan yang dirancang untuk menyebar dari satu komputer ke komputer lain. *Virus* beroperasi dengan menyisipkan atau menempelkan dirinya sendiri ke program atau dokumen yang sah yang mendukung makro untuk mengeksekusi kode. Dalam prosesnya suatu *virus* berpotensi menimbulkan efek yang tidak diharapkan atau merusak, seperti merusak perangkat lunak sistem dengan merusak atau menghancurkan data.(Norton, 2017)

2.9 Malware

Malware adalah singkatan dari perangkat lunak berbahaya dan biasanya digunakan sebagai istilah untuk menangkap semua perangkat lunak yang dirancang untuk menyebabkan kerusakan pada satu komputer, server, atau jaringan komputer (Microsoft, 2016).

Istilah *malware* adalah kontraksi dari perangkat lunak berbahaya. Sederhananya, *malware* adalah bagian dari perangkat lunak yang ditulis dengan maksud merusak data, perangkat atau orang.(AVG, 2015)

2.10 Trojan

Trojan merupakan program perangkat lunak berbahaya yang bersembunyi di dalam program lain. Program ini memasuki komputer dengan bersembunyi di dalam program yang sah, seperti *screen saver*. Kemudian dia akan menaruh kode ke dalam sistem operasi yang memungkinkan hacker untuk mengakses komputer

yang terinfeksi. *Trojan* biasanya tidak menyebar sendiri. Mereka disebar oleh *virus*, *worm*, atau perangkat lunak yang diunduh (Microsoft, 2016).

Trojan adalah tipe *malware* yang dapat menghapus, mencuri, mengunci, merubah data secara diam-diam dan memiliki akses *user* terhadap perangkat anda, tidak seperti *virus* atau *worm*, *trojan* tidak dapat mengandakan dirinya sendiri (Kaspersky, 2017).

2.11 Spyware

Spyware dapat diinstal pada komputer tanpa sepengetahuan Anda. Program ini dapat mengubah konfigurasi komputer Anda atau mengumpulkan data iklan dan informasi pribadi. *Spyware* bisa melacak kebiasaan pencarian internet dan juga dapat mengarahkan *browser web* Anda ke situs-situs yang berbeda dari yang Anda ingin kunjungi (Microsoft, 2016).

Spyware adalah *malware* yang dirancang untuk memata-matai Anda. Ia bersembunyi di latar belakang dan mencatat apa yang Anda lakukan secara online, termasuk kata sandi Anda, nomor kartu kredit, kebiasaan berselancar, dan banyak lagi (AVG, 2015).

2.12 Teknik Pengumpulan Data

Teknik pengambilan sampel atau disebut juga sebagai teknik sampling pada dasarnya dikelompokan menjadi dua jenis sampel, yaitu sampel probabilitas dan sampel non probabilitas (Johar Ariffin, 2017).

Kuesioner adalah sejumlah pertanyaan tertulis yang digunakan untuk memperoleh informasi dari responden dalam arti laporan tentang pribadinya, atau hal – hal yang diketahui (Suharsimi Arikunto, 1999).

2.13 Regresi Linear Berganda

Analisis regresi merupakan salah satu teknik analisis data dalam statistika yang seringkali digunakan untuk mengkaji hubungan antara beberapa variabel dan meramal suatu variabel (Kutner, Nachtsheim dan Neter, 2004). Istilah "regresi" pertama kali dikemukakan oleh Sir Francis Galton (1822-1911).

Regresi sederhana pada dasarnya terdiri dari dua variabel, satu variabel terikat atau tergantung atau dependent (Y) dan satu variabel bebas atau independent (X). Pada regresi berganda inilah yang banyak digunakan karena banyak variabel yang perlu dianalisis selain lebih relevan digunakan. Analisis diperlukan untuk mengetahui arah hubungan (positif atau negatif) antara variabel bebas dengan variabel terikat dengan data berskala interval atau rasio (Johar Arifin, 2017).

Berikut rumus dari Regresi berganda :

$$Y' = a + b_1X_1 + b_2X_2 + ... + b_nX_n$$

2.14 Teori Validitas Dan Realibilitas

Validitas berasal dari kata *validity* yang mempunyai arti sejauh mana ketepatan dan kecermatan suatu alat ukur dalam melakukam fungsi ukurannya (Azwar, 1986). Selain itu validitas adalah suatu ukuran yang menunjukkan bahwa variabel yang diukur memang benar-benar variabel yang hendak diteliti oleh peneliti (Cooper dan Schindler, dalam Zulganef, 2006).

Validitas berhubungan dengan suatu peubah mengukur apa yang seharusnya diukur. Validitas dalam penelitian menyatakan derajat ketepatan alat ukur penelitian terhadap isi sebenarnya yang diukur. Uji validitas adalah uji yang digunakan untuk menunjukkan sejauh mana alat ukur yang digunakan dalam suatu mengukur apa yang diukur. (Sugiharto dan Sitinjak, 2006). Uji validitas digunakan untuk mengukur sah, atau valid tidaknya suatu kuesioner. Suatu kuesioner dikatakan valid jika pertanyaan pada kuesioner mampu untuk mengungkapkan sesuatu yang akan diukur oleh kuesioner tersebut. (Ghozali,2009).

Reliabilitas berasal dari kata reliability. Pengertian dari *reliability* (reliabilitas) adalah keajegan pengukuran (Walizer, 1987). reliabilitas adalah alat untuk mengukur suatu kuesioner yang merupakan indikator dari peubah atau konstruk. Suatu kuesioner dikatakan reliabel atau handal jika jawaban seseorang terhadap pernyataan adalah konsisten atau stabil dari waktu ke waktu. Reliabilitas suatu test merujuk pada derajat stabilitas, konsistensi, daya prediksi, dan akurasi. Pengukuran yang memiliki reliabilitas yang tinggi adalah pengukuran yang dapat menghasilkan data yang reliabel (Ghozali,2009). Berikut rumus uji validitas dengan rumus *pearson,* sebagai berikut :

$$r_{xy} = \frac{N\sum XY - \sum X \sum Y}{\sqrt{N\sum X^2 - (\sum X)^2}\sqrt{N\sum Y - (\sum Y)^2}}$$

Keterangan :
r_{xy} = koefisien regresi | x = skor item | y = skor total | n = banyaknya subjek

2.15 Penelitian Terdahulu

Tabel 2. 1 Tabel Penelitian Terdahulu

No	Nama	Thn	Judul	Metode	Hasil	Kesimpulan
1	Amit Das and Habib Ullah Khan	2016	*Security behaviors of smartphone users*	*Expectancy-based models* dan *protection motivation model*	Keamanan pengguna *smartphone* berdasarkan kebiasaan masih rendah.	Memberikan pengajaran tentang penggunaan *smartphone* yang baik dan benar untuk mengurangi risiko.
2	Xiao Juan zhang, Zhen Li *and* Hepu Deng	2017	*Information security behaviors of smartphone users in China: an empirical analysis*	*Empirical Analysis*	Pengukuran terhadap perilaku keamanan pengguna *smartphone* di china	Hasil dari penelitian ini melihat bahwa ada pengaruh serius dari kebiasaan pengguna di China yang mengabaikan keamanannya
3	Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F.	2014	*Current challenges in information security risk management*	*Expectancy-based Framework*	menerapkan pendekatan manajemen resiko keamanan informasi, berhasil mengidentifikasi bidang aset dan inventarisasi penanggulangan, penugasan nilai	Pendekatan manajemen resiko yang ditinjau tidak secara eksplisit menyediakan mekanisme untuk mendukung pengambil keputusan dalam membuat resiko yang sesuai dibandingkan

No	Nama	Thn	Judul	Metode	Hasil	Kesimpulan
					aset, prediksi resiko, efek terlalu percaya, berbagi pengetahuan dan resiko vs. biaya *trade-off*.	dengan pertukaran biaya, dan mengidentifikasi pendekatan akademis yang memenuhi kebutuhan ini.
4	Teodor Sommestad,Henrik Karlzén dan Jonas Hallberg	2014	*The sufficiency of the theory of planned behavior for explaining information security policy compliance*	*Theory of planned behavior* dan *protection motivation model*	TPB dapat dijadikan acuan dalam pembuatan kebijakan keamanan baru	Adanya hubungan antara *Theory of Planned Behavior* terhadap pembuatan kebijakan keamanan baru
5	Waldo Rocha Flores, Hannes Holm, Marcus Nohlberg, *and* Mathias Ekstedt	2014	*Investigating personal determinants of phishing and the effect of national culture*	*Sampling* dan *survey*	Survey terhadap 2.099 karyawan di Swedia,US, dan India	Memiliki niat untuk menghindari *Social Engineering* dan memiliki kesadaran keamanan informasi yang cukup baik, korelasi antara faktor penentu phising dan karyawan masing-masing tempat menunjukan respon yang berbeda

No	Nama	Thn	Judul	Metode	Hasil	Kesimpulan
6	Jonathan Trull, CISA, CFE, OSCP	2012	*Security Through Effective Penetration testing*	*IT Security*	Pengujian terhadap keamanan Sistem melalui 3 pilar IT Security	Hasil dari *penetration testing* dapat menjadi masukan untuk pengamanan sistem di masa yang akan datang
7	Patricia Cohen, Stephen G. West, Leona S. Aiken	2014	*Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*	*Multiple Reggresion*	Pengukuran perilaku menggunakan *multiple regression*	Dalam penelitian perilaku dapat dilakukan pengukuran menggunakan *multiple regression*

Pada Jurnal Pertama terdapat pembahasan mengenai pengukuran keamanan pengguna smartphone (Android,Blackberry dan iOS), penelitian ini berada di daerah timur tengah yaitu Qatar, penelitian ini melakukan penyebaran kuisioner terhadap responden sebesar kurang lebih 500 orang yang data ini akan digunakan untuk diukur apakah behavior memiliki pengaruh terhadap keamanan pengguna dalam penelitian diatas juga terlihat bahwa beberapa bahaya-bahaya yang mengancam pada pengguna smartphone hampir mirip dengan pengguna komputer atau laptop hanya saja pola serangan yang mengancam sedikit berbeda.

Pada jurnal kedua penelitian ini hampir sama seperti jurnal pertama tetapi menggunakan metode yang berbeda dan tempat penelitian yang berbeda dengan penelitian sebelumnya, penelitian ini mendapatkan 338 kuesioner yang *valid* dan menemukan bahwa banyak pengguna *smartphone* di China yang mengabaikan keamanan melalui penggunaan *smartphone* yang tidak benar.

Pada jurnal ketiga penelitian ini melihat penerapan *risk management* menggunakan *expectancy framework* menemukan bahwa *risk management* berhasil melihat bidang aset dan inventarisasi penanggulangan, penugasan nilai aset, prediksi resiko, efek terlalu percaya, berbagi pengetahuan, resiko dan harga yang harus dibayar, dengan *expectancy framework* ditemukan bahwa tidak adanya solusi atau pendukung keputusan dalam mencegah resiko secara langsung.

Pada jurnal keempat penelitian mencoba untuk melihat apakah *behavior* dapat dijadikan acuan dalam membuat aturan atau kebijakan di sebuah perusahaan atau bisnis, penelitian ini juga melihat apakah dengan *behavior* aturan atau kebijakan dapat dijadikan model dalam menyusun kebijakan, model yang

digunakan dalam penelitian ini adalah *Theory of planned behavior* dan *protection motivation model.*

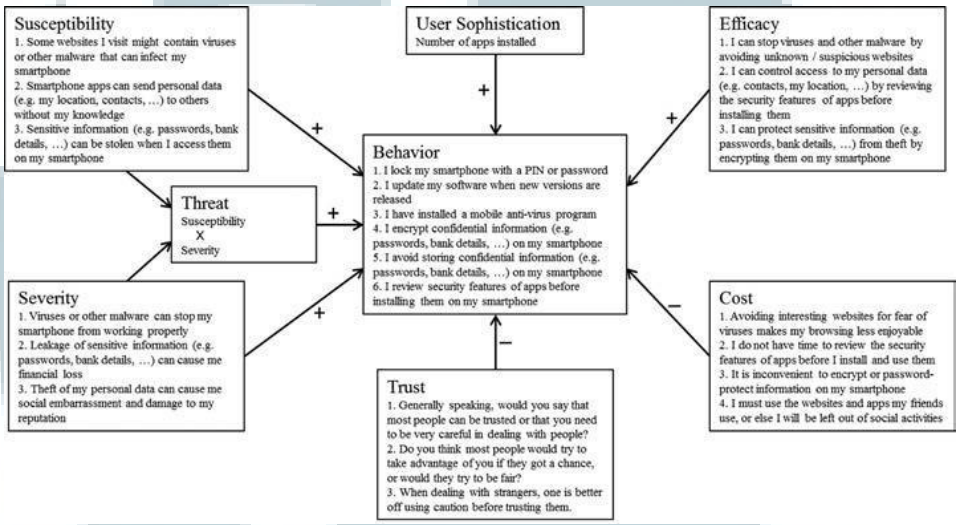
Pada jurnal kelima penelitian melihat bagaimana para pekerja di perusahaan memiliki niat dalam menghindari *phising* pada penelitian ini dapat dilihat hasilnya adalah para pekerja memiliki niat dalam menghindari *social engineering* dimana *social engineering* ini biasanya digunakan sebagai cara menyebarkan *phising* mengingat pola serangan melalui *social engeering* selalu berubah dan cara yang paling benar dalam menghindari serangan tersebut adalah kesadaran keamanan dan niat dari para pekerja untuk menghindarinya.

Pada jurnal keenam penelitian ini melihat bagaimana keamanan sebuah sistem diuji melalui 3 pilar keamanan IT dan hasil dari *penetration testing* dapat dijadikan acuan bagian perusahaan dalam mengamankan sistemnya di masa yang akan datang dengan menerima rekomendasi dari hasil *penetration testing*.

Jurnal ketujuh menjelaskan tentang penggunaan metode perhitungan regresi untuk mengukur perilaku terhadap variabel-variabel lain, metode ini digunakan untuk melihat bagaimana pengaruh atau korelasi dari varibel-variabel yang diukur terhadap perilaku.

Dari beberapa jurnal di atas dapat dilihat bahwa terdapat persamaan dan perbedaan, salah satu persamaan dari penelitian ini terhadap penelitian sebelumnya adalah mengamati kebiasaan pengguna dapat mempengaruhi keamanan pengguna, serta penggunaan *alternative threat based model* yang juga digunakan di dalam penelitian ini, sedangkan perbedaan antara penelitian ini terhadap penelitian sebelumnya adalah lokasi penelitian ini dilakukan di Indonesia, dimana secara

geografis, pendidikan, sosial dan budaya cukup berbeda dari penelitian sebelumnya. Kemudian penelitian sebelumnya mengamati 3 jenis *operating system Android, iOS* dan *BlackBerry* sedangkan pada penelitian ini akan berfokus kepada pengguna *Android*. Pada penelitian ini juga akan ditambahkan metode pengambilan data secara observasi untuk mengukur perilaku keamanan pengguna *Android*.

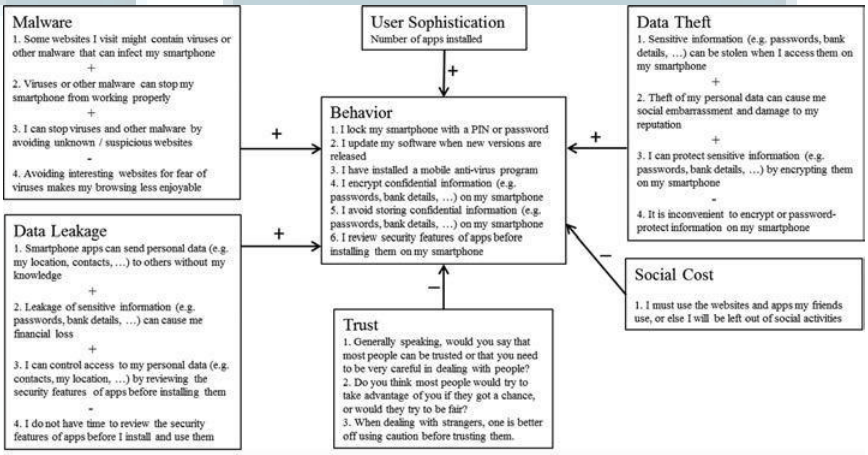


Gambar 2. 1 ***Expectancy-based model and operationalization***
Sumber *:* (Das and Khan, 2015)

Model *expectancy based model* pada penelitian ini disusun berdasarkan *expectancy framework* dimana *expectancy based model* disusun ulang agar dapat memenuhi tujuan penelitian, masing-masing variabel pertanyaan dilandaskan berdasarkan ancaman-ancaman yang menjadi fokus pada masalah keamanan pada *smartphone*, kemudian model kedua dibentuk berdasarkan *expectancy framework* yang disusun ulang variabelnya untuk dijadikan perbandingan dalam penelitian ini jika pada model pertama melihat *behavior* berdasarkan ancaman-ancaman seperti *susceptibility, severity, efficacy* maka pada model kedua akan melihat *behavior* berdasarkan serangan langsung seperti *malware, data leakage* dan *data theft*,

sedangkan untuk variabel *trust* tetap di masukan kedalam kedua model dan tidak terjadi perubahan sama sekali, kemudian untuk variabel *cost* dan *social cost* dibentuk ulang untuk model pertama *cost* disusun berdasarkan biaya yang harus dibayar ketika menghindari ancaman serta biaya yang terjadi ketika ancaman telah terjadi, jadi dalam penelitian sebelumnya kedua model ini digunakan untuk membandingkan masing-masing perilaku dari sisi berbeda.

Penelitian terdahulu ingin melihat, apakah pengguna cenderung melihat perilaku pengguna terhadap ancaman-ancaman dan biaya yang dirasakan pada model pertama kemudian kuesioner model kedua dibentuk ulang untuk melihat kontribusi relatif dari tiga ancaman *malware, data leakage* dan *data theft* terhadap perilaku pengguna.



Gambar 2. 2 *Alternative Threat Based Model*
Sumber *:* (Das and Khan, 2015)

2.16 Pengertian *Android*

Android merupakan sistem operasi untuk telepon seluler yang berbasis Linux. *Android* menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam peranti

bergerak. *Android* umum digunakan di *smartphone* dan juga tablet PC. Fungsinya sama seperti sistem operasi *Symbian* di Nokia, *iOS* di *Apple* dan BlackBerry OS. (Nazaruddin, 2012)

Android merupakan OS *(Operating System) Mobile* yang tumbuh ditengah OS lainnya yang berkembang dewasa ini. OS lainnya seperti *Windows Mobile*, *iOS*, *Symbian*, dan masih banyak lagi. Akan tetapi, OS yang ada ini berjalan dengan memprioritaskan aplikasi inti yang dibangun sendiri tanpa melihat potensi yang cukup besar dari aplikasi pihak ketiga.