BAB III

METODOLOGI PENELITIAN

3.1 Objek Penelitian

Penelitian ini akan melakukan pengukuran keamanan melalui kebiasaan pengguna terutama pada pengguna *Android*, untuk itu dirasa perlu untuk mengetahui respon dari para pengguna *Android* dalam mengamankan perangkatnya dan mengukur bagaimana respon tersebut dalam mencegah atau memberikan perlindungan terhadap data atau informasi penting, pada penelitian ini akan dilakukan penyebaran kuesioner kepada calon responden secara acak dengan rentang umur 18-25 tahun. Dengan tingkat pendidikan rata-rata pada rentang umur tersebut sedang menempuh pendidikan S-1 atau telah lulus S-1, penyebaran kuesioner ini akan dilakukan di beberapa kota-kota besar antara lain Palangka Raya, Malang, Solo, Bandung, Jakarta, Tangerang, Yogyakarta dan Semarang.

Pemilihan rentang umur 18-25 tahun dikarenakan pengguna internet pada tahun 2017 terbesar ada pada rentang usia 18-34 tahun dengan presentase sekitar 49,52%, kemudian pengguna *smartphone* pada tahun 2017 mencapai 50,08%, sedangkan menurut tingkat pendidikan pengguna internet berpendidikan S-1 sekitar 79,23% dan SMA sekitar 70,54% (APJII, 2017), sehingga rentang umur 18-25 tahun dirasa cukup dijadikan sebagai contoh objek dalam penelitian ini karena pada kisaran umur tersebut rata-rata masih berpendidikan SMA, atau sedang menempuh pendidikan S-1(strata-1) dan sebagiannya telah menyelesaikan studi S-1(strata-1).

3.2 Populasi dan Sample

Populasi bisa diartikan wilayah generalisasi yang terdiri atas: objek atau subjek yang mempunya kualitas dan karakteristik tertentu yang ditetapkan oleh peneliti untuk dipelajari dan kemudian ditarik kesimpulannya. Jadi populasi bukan hanya orang, tetapi juga objek dan benda-benda alam yang lain. Populasi juga bukan sekedar jumlah yang ada pada objek/subjek yang dipelajari, tetapi meliputi seluruh karakteristik atau sifat yang dimiliki oleh subjek atau objek itu. (Sugiono, 2011). Populasi pada penelitian ini adalah keseluruhan responden yang memiliki *smartphone Android* .

Sampel adalah suatu bagian dari populasi tertentu yang menjadi perhatian (Suharyadi dan Purwanto, 2004). Sampel dalam penelitian ini berumur antara 18-25 tahun. Total responden diawal ditentukan sebanyak 200 orang dengan menggunakan rumus perhitungan jumlah sampel yang *representative* menurut Hair et al (Kiswati, 2010) adalah tergantung pada jumlah indikator dikali 5 (lima) sampai 10 (sepuluh). Apabila populasi tidak diketahui, menurut hair et al (Prawira, 2010) merekomendasikan jumlah sampel minimal adalah 5-10 kali dari jumlah item pertanyaan yang terdapat di kuesioner. Penelitian ini memiliki indikator pertanyaan sebanyak 31 pertanyaan dengan 5 indikator variabel, maka dapat dihitung sebagai berikut :

Sampel minimum = 31 x 5 = 155 Responden

Berdasarkan perhitungan diatas di dapat untuk *sample* minimum dalam penelitian ini sebanyak 155 responden, namun penelitian ini tetap akan mengambil *sampel* sebanyak 200 untuk mengurangi resiko kesalahan.

3.3 Metode Penelitian

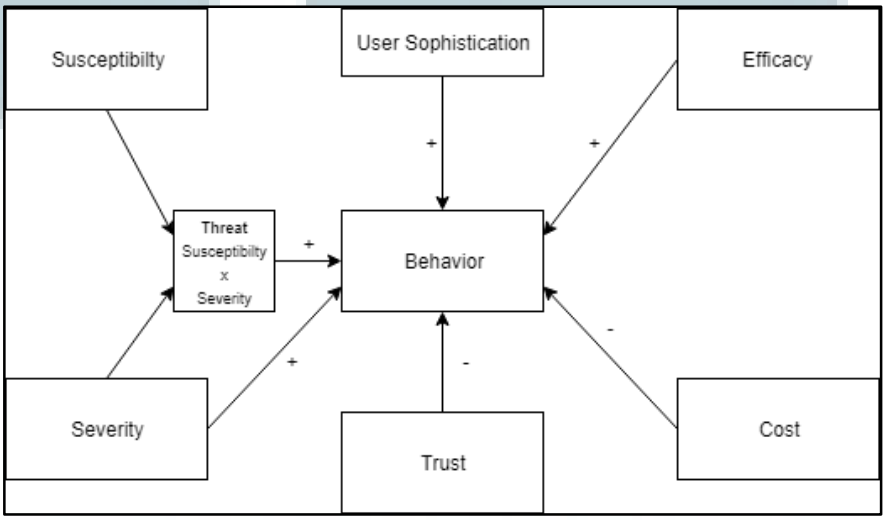
Metode pada penelitian yang digunakan mengacu pada metode sebelumnya dalam metode penelitian ini model yang digunakan adalah *Expectacy Based Model* untuk mengukur perilaku pengguna terhadap penggunaan *smartphone Android*. Model ini dibentuk dengan menilai dari berbagai ancaman yang ada, Berbagai ancaman keamanan terhadap *smartphone (FCC: Federal Communications Commision, 2012; Ofcom, 2013; ENISA: European Union Agency for Network and Information Security, 2010)* dapat dikelompokkan menjadi setidaknya menjadi tiga kategori (He, 2013):

(1) *Malware,* seperti *worm* dan *virus,* ditujukan untuk merusak perangkat atau membuatnya tidak tersedia. *Malware* dapat menghapus file penting, menguras baterai atau mengganggu kemampuan komunikasi *smartphone*.

(2) *Data Leakage,* yaitu pengumpulan dan pengiriman data yang tidak sah seperti lokasi, kontak dan perilaku pemakaian. Banyak aplikasi pihak ketiga (dan penyedia sistem operasi, berpotensi) mengumpulkan data pengguna secara diam-diam, tanpa atau di luar persetujuan pengguna, mengirimkan kembali data ini ke perusahaan untuk maksud data pertambangan atau pemasaran, sehingga melanggar privasi pengguna.

(3) *Data Theft,* seperti password dan kartu kredit data. Serangan *hacking* yang ditargetkan untuk mencegat dan mendekripsi komunikasi, pemasangan *trojans* dan *spyware,* serta serangan *phishing* dengan *spoofing* atau peniruan identitas, bisa digunakan untuk mencuri informasi rahasia untuk pengintaian, pemerasan atau tebusan.

Bagian 1 mencakup perangkat lunak berbahaya yang dirancang untuk merusak / menurunkan *smartphone* atau perangkat itu sendiri. Pada bagian 2 mengacu pada pemungutan data pengguna yang tidak sah oleh penulis sistem operasi dan aplikasi. Pada bagian 3 mengacu pada pencurian informasi yang ditargetkan dari penyimpanan (misalnya foto) atau transit (misalnya kata sandi). Perbedaan antara bagian 2 dan 3 adalah bahwa bagian 2 mempengaruhi semua pengguna *Android*, sementara bagian 3 merujuk ke Serangan yang ditargetkan pada individu (kemungkinan sasaran lunak dan / atau bernilai tinggi).



Gambar 3. 1 *Expectacy-Based Model*
Sumber : (Das and Khan, 2015)

Susceptibility, dioperasionalkan dengan pertanyaan tentang kerentanan terhadap masalah keamanan: satu untuk *malware*, yang lain untuk *data leakage* dan yang ketiga untuk *data theft*. Hal yang sama berlaku untuk tingkat *Severity*: terdiri dari satu item masing-masing untuk potensi kerusakan yang diakibatkan oleh *malware*, *data leakage* dan *data theft*. Selain memiliki efek langsung terhadap *susceptibility*

dan *severity* pada perilaku keamanan, model ini disebut sebagai istilah interaksi multiplikatif yang dibentuk oleh dua variabel independen.(Das and Khan, 2016) Tiga item untuk merespon *efficacy* mengacu pada efektivitas tindakan pengamanan yang dirasakan terhadap *Malware*, *data leakage* dan *data theft*. Juga mencakup item keempat selain hilangnya kenyamanan, fungsionalitas dan waktu untuk melindungi perangkat dari *malware*, *data leakage* dan *data theft*. *Cost* ini mengacu pada *cost* sosial yang tidak digunakan (Das and Khan, 2016).

User Shopiscation atau kecanggihan pengguna digunakan untuk mempelajari perilaku keamanan pengguna. *Self-efficacy* adalah ukuran kemampuan pengguna untuk membela diri terhadap ancaman keamanan. Dalam penelitian ini, (Das and Khan, 2016) menggunakan jumlah aplikasi terinstal di ponsel cerdas pengguna sebagai *proxy* untuk *User Shopiscation*. Penulis mengharapkan "*Power User*" untuk memasang lebih banyak aplikasi daripada pengguna pemula lainnya.

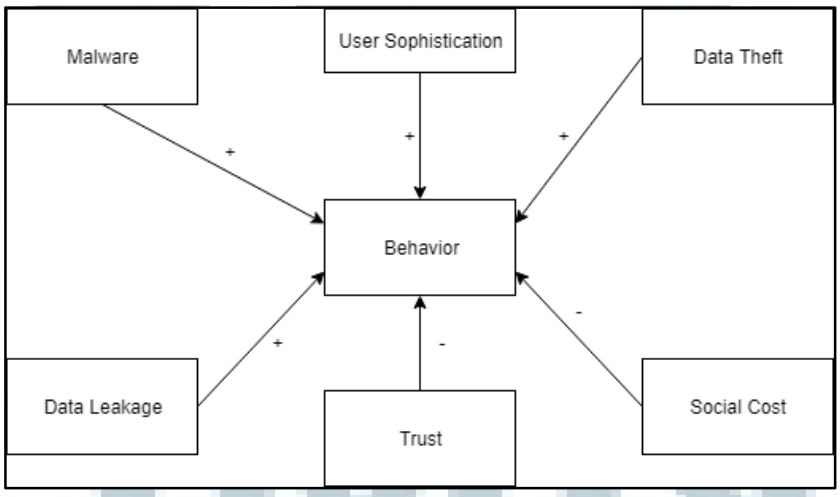
Ukuran variabel dependen, *behavior security*, diadaptasi dari *Microsoft's Computing Safety Index* (Microsoft, 2014). Pertanyaan dibuat berdasarkan perlindungan kata sandi, menjaga sistem perangkat lunak *up-to-date*, penggunaan perangkat lunak *anti-virus*, penyampaian pesan dengan kata sandi, tidak menyimpan informasi yang sensitif dan meninjau fitur keamanan aplikasi sebelum menginstal mereka. Semakin banyak perilaku keamanan yang dilakukan, semakin tinggi skornya.

Trust, sangat penting bagi keamanan informasi (yang bertujuan untuk membangun dan mempertahankan kepercayaan), dan untuk membuat peran

kepercayaan semacam itu menjadi eksplisit dan tidak ambigu ((Jensen, 2012),(Gollmann, 2006)).

Untuk tiga item ukuran *trust* yang berasal dari Survey Umum Sosial Amerika (GSS), 2014) dan Kuesioner Panel Sosial Ekonomi Jerman (SOEP: Panel Sosial Ekonomi, 2014). Pengguna *smartphone* yang lebih percaya diharapkan dapat menampilkan tingkat perilaku keamanan yang lebih rendah, karena mereka cenderung tidak mendapatkan tindakan jahat dari orang lain.

Untuk mengukur bagaimana ketiga ancaman dapat memberikan kontribusi relatif, ketiga ancaman *malware, data theft* dan *data leakage* maka dalam penelitian sebelumnya memodelkan ulang model I (*Expectacy Based Model)* menjadi model alternatif yang disebut *Expectacy Based Model* yang disebut juga model II, dimana pada kuesioner sebelumnya disusun ulang menyesuaikan model.



Gambar 3. 2 ***Alternative Threat-Based Model***
Sumber : (Das and Khan, 2015)

3.4 Teknik Pengumpulan Data

Teknik pengumpulan data pada penelitian ini menggunakan metode kuesioner dimana kuesioner tersebut disebar secara acak menggunakan *google form* dengan jumlah sampel yang akan diambil sebesar 200 orang berumur 18-25 tahun, tersebar di beberapa kota-kota seperti : Palangka Raya, Malang, Solo, Bandung, Jakarta, Tangerang, Yogyakarta dan Semarang.

Pengumpulan data ini menggunakan skala likert sebagai indikator pengukuran dimana setiap indikator dibentuk sebagai berikut :

1 = Sangat Tidak Setuju	diberi skor 1
2= Tidak Setuju	diberi skor 2
3 = Netral	diberi skor 3
4 = Setuju	diberi skor 4
5 = Sangat Setuju	diberi skor 5

Pertanyaan-pertanyaan pada penelitian ini juga telah dibentuk sesuai dengan penelitian sebelumnya, dimana kuesioner ini terdiri dari 30 pertanyaan yang menjadi indikator mewakili ke-lima variabel independen dan satu variabel dependen, adapun butir-butir pertanyaan yang dibentuk sebagai berikut :

Tabel 3. 1 Pertanyaan Model 1 *Expectacy Based Model*

	User Shopiscation
P1	Jumlah aplikasi yang anda gunakan
	Behavior
P2	Saya mengunci *smartphone Android* saya dengan Finger Print/Password/Pin/Patttern
P3	Saya mengupdate aplikasi secara berkala
P4	Saya menginstall antivirus di *smartphone Android*
P5	Saya melakukan enkripsi pada data-data sensitif saya
P6	Saya tidak menyimpan data-data rahasia di *smartphone*
P7	Saya melihat *Review/Rating* dari aplikasi sebelum menginstal sebuah aplikasi
	Susceptibility
P8	Beberapa aplikasi/Website yang saya gunakan mengandung *VIRUS* dan dapat menginfeksi *smartphone* saya
P9	Beberapa aplikasi/Website yang saya kunjungi mengandung *MALWARE* dan dapat menginfeksi *smartphone* saya
P10	Aplikasi *smartphone* bisa saja mengirim data pribadi (Seperti Lokasi saya, kontak saya, dll) tanpa sepengetahuan saya
P11	Informasi sensitif saya dapat dicuri ketika saya mengakses Aplikasi/Web/Email dari semua jenis *smartphone*
	Severity
P12	*VIRUS* dapat mengakibatkan fungsi *smartphone* saya tidak berjalan dengan semestinya
P13	*MALWARE* dapat mengakibatkan fungsi *smartphone* saya tidak berjalan dengan semestinya
P14	Kebocoran informasi sensitif dapat mengakibatkan saya mengalami kerugian secara materi (password, data bank, dll)
P15	Pencurian data dapat mengakibatkan masalah yang cukup sulit
	Efficacy
P16	Saya dapat menghentikan *VIRUS* dengan cara menghindari sumber "Aplikasi/Website tidak dikenal"
P17	Saya dapat menghentikan *MALWARE* dengan cara menghindari sumber "Aplikasi/Website tidak dikenal"
P18	Saya dapat menghentikan *VIRUS* dengan cara menghindari sumber Aplikasi/Website "mencurigakan"
P19	Saya dapat menghentikan *MALWARE* dengan cara menghindari sumber Aplikasi/Website "mencurigakan"
P20	Saya dapat menentukan akses terhadap data personal saya (Seperti Kontak, Lokasi, dll) dengan mereview fitur keamanan aplikasi sebelum di install pada *smartphone* saya
P21	Saya dapat melindungi data-data sensitif saya dengan melakukan enkripsi di *smartphone* saya
	Cost

P22	Menghindari rasa ingin tahu terhadap Aplikasi/Website karena takut akan *VIRUS* membuat saya menjadi kurang nyaman
P23	Menghindari rasa ingin tahu terhadap Aplikasi/Website karena takut akan *MALWARE* membuat saya menjadi kurang nyaman
P24	Saya tidak memiliki waktu untuk melakukan review keamanan pada aplikasi sebelum di install dan digunakan
P25	Saya merasa kurang nyaman dengan mengenkripsikan data-data saya
P26	Saya menggunakan aplikasi yang digunakan oleh Keluarga/Teman
	Trust
P27	Pada umumnya saya berbicara mengenai informasi sensitif saya kepada orang yang saya percaya
P28	Saya sangat berhati-hati dalam membuat kesepakatan dengan orang lain
P29	Saya berpikir orang lain dapat mengambil keuntungan dari saya apabila diberikan kesempatan
P30	Orang lain bersikap adil terhadap saya
P31	Saya perlu mempercayai orang sebelum melakukan kesepakatan dengan orang yang tidak di kenal

Tabel 3. 2 Pertanyaan Model 2 (*Alternative Threat Based Model)*

	User Shopiscation
P1	Jumlah aplikasi yang anda gunakan
	Behavior
P2	Saya mengunci *smartphone Android* saya dengan Finger Print/Password/Pin/Patttern
P3	Saya mengupdate aplikasi secara berkala
P4	Saya menginstall antivirus di *smartphone android*
P5	Saya melakukan enkripsi pada data-data sensitif saya
P6	Saya tidak menyimpan data-data rahasia di *Smartphone*
P7	Saya melihat *Review/Rating* dari aplikasi sebelum menginstal sebuah aplikasi
	Malware
P8	Beberapa Aplikasi/Website yang saya gunakan mengandung *VIRUS* dan dapat menginfeksi *smartphone* saya
P9	Beberapa Aplikasi/Website yang saya kunjungi mengandung *MALWARE* dan dapat menginfeksi *smartphone* saya
P10	*VIRUS* dapat mengakibatkan fungsi *smartphone* saya tidak berjalan dengan semestinya
P11	*MALWARE* dapat mengakibatkan fungsi *smartphone* saya tidak berjalan dengan semestinya
P12	Saya dapat menghentikan *VIRUS* dengan cara menghindari sumber "Aplikasi/Website tidak dikenal"
P13	Saya dapat menghentikan *MALWARE* dengan cara menghindari sumber "Aplikasi/Website tidak dikenal"

P14	Saya dapat menghentikan *VIRUS* dengan cara menghindari sumber Aplikasi/Website "mencurigakan"
P15	Saya dapat menghentikan *MALWARE* dengan cara menghindari sumber Aplikasi/Website "mencurigakan"
P16	Menghindari rasa ingin tahu terhadap Aplikasi/Website karena takut akan *VIRUS* membuat saya menjadi kurang nyaman
P17	Menghindari rasa ingin tahu terhadap Aplikasi/Website karena takut akan *MALWARE* membuat saya menjadi kurang nyaman
	Data Leakage
P18	Aplikasi *smartphone* bisa saja mengirim data pribadi (Seperti Lokasi saya, kontak saya, dll) tanpa sepengetahuan saya
P19	Kebocoran informasi sensitif dapat mengakibatkan saya mengalami kerugian secara materi (password, data bank, dll)
P20	Saya dapat menentukan akses terhadap data personal saya (Seperti Kontak, Lokasi, dll) dengan mereview fitur keamanan aplikasi sebelum di install pada *smartphone* saya
P21	Saya tidak memiliki waktu untuk melakukan review keamanan pada aplikasi sebelum di install dan digunakan
	Data Theft
P22	Informasi sensitif saya dapat dicuri ketika saya mengakses Aplikasi/Web/Email dari semua jenis *smartphone*
P23	Pencurian Data dapat mengakibatkan masalah yang cukup sulit
P24	Saya dapat melindungi data-data sensitif saya dengan melakukan enkripsi di *smartphone* saya
P25	Saya merasa kurang nyaman dengan mengenkripsikan data-data saya
	Social Cost
P26	Saya menggunakan aplikasi yang digunakan oleh Keluarga/Teman
	Trust
P27	Pada umumnya saya berbicara mengenai informasi sensitif saya kepada orang yang saya percaya
P28	Saya sangat berhati-hati dalam membuat kesepakatan dengan orang lain
P29	Saya berpikir orang lain dapat mengambil keuntungan dari saya apabila diberikan kesempatan
P30	Orang lain bersikap adil terhadap saya
P31	Saya perlu mempercayai orang sebelum melakukan kesepakatan dengan orang yang tidak di kenal

Pertanyaan-pertanyaan ini dibentuk berdasarkan keberhasilan dalam menanggapi ancaman-ancaman yang terjadi, sehingga dapat diasumsikan pertanyaan-pertanyaan ini mewakilkan pengetahuan pengguna terhadap ancaman-ancaman yang ada, apakah pengguna telah memahami ancaman, resiko serta biaya yang dapat mereka rasakan (Das and Khan, 2016).

3.5 Teknik Analisis Data

Data yang telah disebarkan dan dikumpulkan kepada semua responden, akan diolah dan diukur agar nantinya dapat ditentukan apakah terdapat keterkaitan antara perilaku pengguna terhadap keamanan pengguna, teknik analisis data yang akan digunakan adalah *Multiple Regression* (Regresi linier berganda) dimana variabel kriteria (DV) adalah *Behavior* dan varibel prediktor (IV) adalah *User Sophistication*, *Malware*, *Data Leakage*, *Data Theft*, *Social Cost* dan *Trust*.

Penelitian ini menggunakan *Multiple regression* (regresi linier berganda) dimana variabel bebas yang digunakan lebih dari satu sehingga apabila menggunakan *Linear regression* (regresi linier) tidak terlalu cocok untuk digunakan, karena tidak dapat mengukur secara keseluruhan variabel bebas lebih dari satu sedangkan pada metode *Multiple regression* (regresi linier berganda) variabel bebas lebih dari satu sangat memungkinkan untuk dianalisis. Setelah ditemukan hasil dari perhitungan *Multiple regression* maka hasilnya tersebut akan diuji sesuai dengan hipotesa yang telah ditentukan. Berikut rumus dari *Multiple regression* (regeresi linier berganda) :

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

Keterangan:
Y' = Variabel dependen (nilai yang diprediksikan)
X_1 dan X_2 = Variabel independen
a = Konstanta (nilai Y' apabila X_1, X_2…..X_n = 0)
b = Koefisien regresi (nilai peningkatan ataupun penurunan)

Kemudian untuk *tools* yang digunakan adalah SPSS banyak tools lain yang dapat dijadikan sebagai *tools* pengolahan data antara lain *Microsoft Excel* namun

keterbatasan fungsi pada *Microsft Excel* membuat penelitian ini lebih baik menggunakan SPSS.

3.6 Variabel Penelitian

Dari kedua model diatas dapat ditentukan variabel dependen dan independen yang akan digunakan antara lain :

Tabel 3. 3 Variabel Dependen dan Independen

Dependen Variabel Model 1	**Independen *Expectacy Based Model* (Model I)**	**Dependen Variabel Model 2**	**Independen Variabel *Alternative Threat Based Model* (Model II)**
Behavior	*User Sophistication*	*Behavior*	*User Sophistication*
	Susceptibility		*Malware*
	Severity		*Data Leakage*
	Susceptibility X Severity		*Data Theft*
	Efficacy		*Social Cost*
	Cost		*Trust*
	Trust		

3.7 Hipotesis

Hipotesis yang akan disusun dalam penelitian adalah hipotesi H_1 dimana terjadinya pengaruh (penerimaan) antara variabel independen terhadap variabel dependen untuk masing-masing model dengan signifikasi sebesar 5%, berikut dapat dapat dijelaskan variabel masing-masing dari tiap model, sebagai berikut :

1. *User Shopiscation*

User Shopiscation atau disebut juga kecanggihan pengguna, merupakan salah satu variabel yang akan diukur, menurut penelitian terdahulu, *user shopiscation* yang semakin tinggi di harapkan akan membuat pengguna jauh lebih

mengerti dalam pemanfaatan teknologi, sehingga semakin tinggi *user shopiscation* maka di harapkan *behavior* pengguna akan semakin baik (Das and Khan, 2015), maka dari itu hipotesis yang akan diajukan mengenai *user shopiscation* sebagai berikut :

H_1 = *User shopiscation* berpengaruh signifikasi positif terhadap *behavior*.

2. *Susceptibility*

Susceptibility atau disebut juga kerentanan adalah salah satu variabel yang akan diukur, *susceptibility* dibentuk berdasarkan ancaman-ancaman yang dapat menjadi dampak bagi para pengguna, sebagian besar penelitian sebelumnya mengenai perilaku keamanan secara implisit atau eksplisit mengangkat *expectacy framework* dimana *susceptibility* yang dirasakan dan *efficacy* yang dirasakan bergabung mendorong proses penilaian ancaman yang melengkapi penilaian dari menanggulangi tanggapan berdasarkan analisis *cost-benefit* dari tindakan pengamanan dan seberapa besar kemungkinannya langkah-langkah tersebut untuk berhasil menetralisir ancaman. Ini menjadi sama dengan sejumlah kerangka kerja bisnis yang digunakan untuk manajemen risiko keamanan informasi yang juga melihat perilaku keamanan sebagai *tradeoff* antara risiko - dioperasionalkan sebagai kerugian tahunan harapan dan biaya (Fenz et al., 2014), dengan memahami ancaman-ancaman yang dapat menyebabkan masalah bagi para pengguna, maka di harapkan *behavior* pengguna akan semakin baik (Das and Khan, 2015), maka dari itu hipotesis untuk variabel *susceptibility* dapat dibentuk sebagai berikut :

H_1 = *Susceptibility* berpengaruh signifikasi positif terhadap *behavior*

3. *Severity*

Penelitian terdahulu menunjukkan bahwa *susceptibility* yang dirasakan, *severity* yang dirasakan, *efficacy* dan respon *cost* mempengaruhi niat perilaku untuk menggunakan perangkat lunak *anti-spyware* sebagai teknologi pelindung (Chenoweth et al, 2009). Penelitian selanjutnya yang menemukan bahwa *severity*

Adanya pengaruh ini dari penelitian terdahulu membuat variabel *severity* dapat dibentuk menjadi sebuah hipotesa sebagai berikut :

H_1 = *Severity* berpengaruh signifikasi positif terhadap *behavior*

4. *Susceptibility x Severity*

Penelitian terdahulu menyelidiki penyimpangan keamanan dalam organisasi dan menemukan bahwa tingkat *susceptibility* dan tingkat *severity* yang dirasakan, dan *self-* dan tanggapan *efficacy* yang tinggi mengurangi kemungkinan kelalaian yang dapat membahayakan keamanan (Workman, 2008). Adanya pengaruh ini semakin memperkuat bahwa variabel *Susceptibility x Severity* dapat membentuk hipotesis sebagai berikut :

H_1 = *Susceptibility x Severity* berpengaruh signifikasi positif terhadap *behavior*

5. *Efficacy*

Penelitian tentang niat pengguna untuk menggunakan *anti-spyware*, menemukan bahwa niat tersebut dipengaruhi secara langsung oleh respon yang keberhasilan, *self-efficacy* dan norma sosial, namun tidak dengan kerentanan dan tingkat keparahan ancaman seperti yang digambarkan dalam ketakutan banding (Johnston dan Warkentin, 2010). Penelitian lain menemukan pemenuhan niat bergantung pada persepsi *efficacy* keamanan dan juga tanggapan pengguna *self-efficacy* dalam hal melakukan tanggapan (Ifinedo, 2012).

Berdasarkan penelitian-penelitian terdahulu maka variabel *efficacy* dapat membentuk sebuah hipotesis sebagai berikut :

H_1 = *Efficacy* berpengaruh signifikasi positif terhadap *behavior*

6. *Cost*

Penelitian terdahulu mengembangkan dan menguji model penghindaran ancaman teknologi menemukan bahwa motivasi untuk menghindari *spyware* dipengaruhi secara positif oleh ancaman yang dirasakan (*susceptibility* dan *severity*), *self-efficacy* dan secara negatif terhadap *cost* (Liang dan Xue, 2010). Variabel *cost* dapat di bentuk hipotesis sebagai berikut :

H_1 = *Cost* berpengaruh signifikasi negatif terhadap *behavior*

7. *Trust*

Penelitian terdahulu yang menggunakan variabel *trust* menemukan bahwa kualitas informasi kebijakan keamanan memiliki dampak positif terhadap niat dan penyesuaian perilaku, terlepas dari sikap kebijakan pengguna, kepercayaan dan kebiasaan (Pahnila et al, 2007), berdasarkan penelitian diatas dapat dibentuk sebuah hipotesis sebagai berikut :

H_1 = *Trust* berpengaruh signifikasi negatif terhadap *behavior*

8. *Malware, Data Leakage dan Data theft*

Penelitian terdahulu yang mempelajari tentang pemakaian perangkat lunak *anti-malware* pada eksekutif dari perusahaan kecil dan menengah. Menemukan bahwa efek positif dari *severity* yang dirasakan, *susceptibility* yang dirasakan, *efficacy*, *social cost*, dukungan vendor dan anggaran TI pada niat untuk memakai perangkat lunak *anti-malware*, dan hubungan yang positif antara niat yang diungkapkan dan perilaku pemakaian yang aktual (Lee and Larsen, 2009).

Pertanyaan-pertanyaan tentang *susceptibility* terhadap masalah keamanan antara lain mewakilkan ketiga variabel berikut: satu untuk *malware*, satu lagi untuk *data leakage* dan yang ketiga untuk *data theft*. Hal yang sama berlaku untuk *severity*: terdiri dari satu untuk dampak kerusakan yang dirasakan dari potensi *malware*, *data leakage* dan data theft (Das and Khan, 2015), berdasarkan penelitian diatas dapat dibentuk hipotesis yang mewakilkan masing-masing variabel sebagai berikut :

H_1 = *Malware* berpengaruh signifikasi positif terhadap *behavior*

H_1 = *Data leakage* berpengaruh signifikasi positif terhadap *behavior*

H_1 = *Data theft* berpengaruh signifikasi positif terhadap *behavior*

9. *Social Cost*

Cost juga termasuk hal keempat di samping hilangnya kenyamanan, fungsionalitas dan waktu dalam melindungi *malware*, *data leakage* dan data theft. Unsur biaya ini mengacu pada *social cost* yang tidak digunakan dari fitur *smartphone* atau aplikasi yang populer di kalangan seseorang: kemungkinan tertinggal dari percakapan, diskusi dan kegiatan yang dilakukan melalui media sosial (Das and Khan, 2015), dari penelitian terdahulu dapat dibentuk sebuah hipotesis sebagai berikut :

H_1= *Social Cost* berpengaruh signifikasi negatif terhadap *behavior*

Penjelasan-penjelasan dari masing-masing variabel diatas maka akan disusun kedalam masin-masing model, pada model I (*Expectacy Based Model*) kesimpulan hipotesis yang dibentuk sebagai berikut:

Tabel 3. 4 Hipotesis Model I

	Deskripsi
H1	*User Sophicisation* berpengaruh signifikasi positif terhadap *behavior*

	Deskripsi
H2	*Susceptibilty* berpengaruh signifikasi positif terhadap *behavior*
H3	*Severity* berpengaruh signifikasi positif terhadap *behavior*
H4	*Susceptibility x Severity* berpengaruh signifikasi positif terhadap *behavior*
H5	*Efficacy* berpengaruh signifikasi positif terhadap *behavior*
H6	*Cost* berpengaruh signifikasi negatif terhadap *behavior*
H7	*Trust* berpengaruh signifikasi negatif terhadap *behavior*

Model II (*Alternative Threat Based Model*) memiliki hipotesis yang sama seperti model 1 dimana terjadi pengaruh (penerimaan) dari variabel independen terhadap variabel dependen, yang masing-masing variabelnya disusun ulang untuk melihat kontribusi dari ancaman-ancaman yang ada.

Tabel 3. 5 Hipotesis Model II

	Deskripsi
H1	*User Sophicisation* berpengaruh signifikasi positif terhadap *behavior*
H2	*Malware* berpengaruh signifikasi positif terhadap *behavior*
H3	*Data Leakage* berpengaruh signifikasi positif terhadap *behavior*
H4	*Data Theft* berpengaruh signifikasi positif terhadap *behavior*
H5	*Social Cost* berpengaruh signifikasi negatif terhadap *behavior*
H6	*Trust* berpengaruh signifikasi negatif terhadap *behavior*