Pengukuran Kesadaran Keamanan Informasi dan Privasi Pada Pengguna *Smartphone* Android di Indonesia

Robbi Akraman[a], Candiwan[b] , Yudi Priyadi[c]

[abc]Program Studi Manajemen Bisnis Telekomunikasi dan Informatika,
Fakultas Ekonomi dan Bisnis, Universitas Telkom

Naskah Diterima : 22 Desember 2017; Diterima Publikasi : 16 September 2018

DOI : 10.21456/vol8iss2pp115-122

Abstract

Based on statistical data, it is known that Android is the most popular smartphone with the largest number of users in the world, which is about 1.8 billion users. The high number of users also invite the many cases of information security and privacy caused by the lack of awareness of the user such as : spam, spoofing/phising, network incident, malware, uploading something personal data such as photos, phone numbers, addresses or having no antivirus. The research aims to find out about the awareness of the security of information and privacy of Android smartphone users by doing measurement of problem. The awareness has some dimensions such as attitude, knowledge and behavior with the seven focus areas of information security namely trust in app repository, misconception about app testing, security and agreement message, pirated application, adoption Security control, spam sms and report of security incidents and three focus areas of privacy are perceived surveillance, perceived intrusion, secondary use of information. This research uses analytical hierarchy process (AHP) to measure the level of awareness of information security and privacy of smartphone users. Overall, the results of the research show that information security has an average level of awareness (71%) but the focus area of report for security incidents has a poor level of awareness (37%) this occur because users prefer to solve their own information security issues experienced and privacy has an average level of awareness (76%). However, for secondary use of information in attitude dimension has low awareness level (66%). Based on the results of this study, it can be concluded that smartphone users in Indonesia have a poor awareness level in maintaining security and privacy of their information.

Keywords **:** Information Security; Privacy; Awareness; Measurement; Smartphone Users

Abstrak

Berdasarkan data statistik, diketahui bahwa Android merupakan *smartphone* terpopuler dengan jumlah pengguna terbanyak di dunia, yaitu sekitar 1,8 miliar pengguna. Tingginya jumlah pengguna juga mengundang banyaknya kasus keamanan informasi dan privasi yang dikarenakan oleh kurangnya kesadaran dari pengguna seperti *spam, spoofing/phising, network incident, malware,* mengunggah sesuatu yang bersifat pribadi seperti foto, nomor telepon, alamat atau tidak memiliki antivirus. Penelitian ini bertujuan untuk mengetahui tentang keamanan informasi dan privasi pengguna *smartphone* Android dengan melakukan pengukuran masalah dari dimensi kesadaran (*attitude, knowledge* dan *behaviour*) dengan tujuh fokus area keamanan informasi yaitu *trust in app repository, misconception about app testing, security and agreement message, pirated application, adoption security control, spam sms* dan *report of security incidents* dan tiga fokus area privasi yaitu *perceived surveillance, perceived intrusion, secondary use of information.* Penelitian ini menggunakan metode *analytical hierarchy process* (AHP) untuk mengukur tingkat kesadaran keamanan informasi dan privasi dari pengguna *smartphone*. Secara keseluruhan, hasil dari penelitian menunjukkan bahwa keamanan informasi memiliki tingkat kesadaran rata-rata (71%). Namun pada fokus area *report for security incidents* memiliki tingkat kesadaran yang buruk (37%) hal ini karena pengguna lebih memilih untuk menyelesaikan sendiri masalah keamanan infomasi yang dialami dan privasi memiliki tingkat kesadaran rata-rata (76%). Sedangkan *secondary use of information* dalam dimensi *attitude* memiliki tingkat kesadaran yang rendah (66%). Berdasarkan temuan tersebut, dapat disimpulkan bahwa pengguna *smartphone* di Indonesia memiliki tingkat kesadaran yang buruk dalam menjaga keamanan informasi dan privasinya.

Kata Kunci : Kemanan Informasi; Privasi; Kesadaran; Pengukuran; Pengguna *Smartphone*

1. Pendahuluan

Di era teknologi informasi ini smartphone menjadi kebutuhan untuk bisa berkomunikasi dan berbagi informasi seperti mengirim SMS atau email, *entertainment*, media sosial tanpa mengkhawatirkan jarak dan waktu. Menurut data yang dilansir *website* Statista, di awal tahun 2016, Android merupakan *smartphone* terpopuler dengan jumlah pengguna terbanyak di dunia, yaitu sekitar 1,8 miliar.

*) Penulis korespondensi: candiwan@telkomuniversity.ac.id

Kemudian diikuti oleh pesain seperti Apple dengan IOS milikinya yaitu sekitar 463 juta penguna, Windows dengan 45 juta pengguna, disusul Blackberry dengan jumlah pengguna sebanyak 19 juta, serta jenis *smartphone* lainnya dengan 31 juta pengguna. Di Indonesia sendiri, Menurut *website* Statista (2016), pangsa pasar yang dimiliki oleh sistem operasi *mobile* di Indonesia, pada awal bulan Januari 2016, 74,2% dari total pengguna *smartphone* dimiliki oleh sistem operasi Android berarti sekitar 82.140.000 orang menggunakan smartphone Android dari total pengguna *smartphone* di Indonesia.

Dilansir Gemalto (2015), sektor teknologi menduduki peringkat keempat (12%) yang memiliki jumlah laporan pelanggaran sebanyak 84.394.833 laporan (top 7 sektor dengan jumlah laporan pelanggaran). Berdasarkan data dari *Indonesia Computer Emergency Response Team* atau IDCERT (2015), dengan beberapa responden dari penyedia telekomunikasi, dilaporkan bahwa insiden mulai bulan Januari sampai Februari 2015 adalah 30,99% *spam*; 27.31% respon terhadap laporan yang masuk. 15.67% hak kekayaan intelektual; 4,53% *spoofing/phising*; 3,98% *network incident*; dan 3.18% adalah *malware*. Dilansir Symantec (2015) jumlah jenis *malware* yang ditemukan dalam sistem operasi Android terus meningkat tahun dari 2011 yang hanya 71 jenis *malware*; 174 jenis *malware* di tahun 2012; 231 jenis *malware* di tahun 2013; 277 jenis *malware* di tahun 2014; 295 jenis *malware* di tahun 2015 dan akan terus bertambah jenis *malware* yang akan ditemukan sistem operasi Android tiap tahunnya.

Dilansir oleh laporan Symantec (2015), 46%, mayoritas pelanggaran yang disebabkan oleh *attacker/hacker*. Namun, 22% lebih dari pelanggaran diklasifikasikan sebagai "tidak sengaja dibuat publik," dan 21% adalah karena pencurian atau kehilangan komputer atau perangkatnya dan 10% adalah karena adanya keterlibatan orang dalam. Semua jenis pelanggaran data dapat dicegah jika data dienkripsi, secara efektif dapat menghilangkan dampak dari data ini jatuh ke tangan yang salah.

Menurut Al-Sehri (2012), salah satu faktor yang menjadi pemicu terjadinya pelanggaran keamanan informasi dan privasi adalah karena pengguna *smartphone* memiliki kesadaran yang tidak memadai dalam menggunakan *smartphone* dengan aman, beberapa dari mereka memiliki pengetahuan yang cukup memadai dalam penggunaan smartphone tetapi mereka tidak menerapkannya dengan baik.

Menurut Xu *et al.* (2012), praktik agresif seperti akses data yang digunakan oleh pengembang aplikasi *mobile* dan sistem operasi telah memperburuk masalah privasi di antara pengguna (*smartphone*). Kekhawatiran ini terkait dengan 'koleksi otomatis' dari pengguna perangkat mobile, informasi keberadaan secara *real-time*, dan kerahasiaan data yang dikumpulkan seperti lokasi, identitas pribadi, dan perilaku sehari-hari. Berbeda dengan internet konvensional, *platform mobile* memungkinkan untuk *real-time* dan komunikasi data dan transmisi yang selalu menyala, yang menimbulkan ancaman privasi. Informasi Privasi menjadi kekhawatiran pengguna tentang kemungkinan kehilangan privasi sebagai akibat dari pengungkapan informasi kepada pihak ketiga seperti pengembang aplikasi. Teori ini memaparkan bahwa *smartphone* yang sangat dikenal khususnya Android merupakan sistem operasi *mobile phone* yang memiliki resiko yang besar, masih banyak pengguna *smartphone* yang belum menyadari aturan keamanan dan privasi yang harus diperhatikan dalam menggunakan *smartphone.* Padahal, banyak kasus-kasus terjadi seputar dampak negatif karena kurangnya kesadaran kemanan dan privasi dalam menggunakan *smartphone*, termasuk di Indonesia, diakibatkan oleh faktor ketidakpahaman akan keamanan informasi dan privasi ketika mendapatkan SMS/email dari orang tidak dikenal yang menyertakan link palsu yang merupakan *website* buatan penyerang untuk membuat *smartphone* terkena serangan malware yang mengakibatkan pengambilan data secara illegal sampai rusaknya internal dari perangkat (*smartphone*) yang digunakan.

2. Kerangka Teori

Menurut Whitman dan Mattord (2011), keamanan informasi merupakan upaya untuk melindungi informasi dan elemen-elemen penting yang ada didalamnya, baik berupa sistem atau perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi. Menurut McLeod dan Schell (2008) keamanan informasi ditujukan untuk mencapai tiga tujuan utama, yaitu kerahasiaan ketersediaan, dan integritas . Dalam penelitian ini, keamanan informasi dibagi menajadi 7 indikator 5 diantaranya *trust in application repository, misconception about app testing, security and agreement message, pirated applicaion*, dan *adoption of security control* (Mylonas, 2013) ditambah 2 indikator seperti *spam sms* dan *report of security incidents* (Sari *et al.*, 2014).

Menurut Smith *et al.* (2011), terdapat empat definisi privasi informasi yaitu privasi sebagai hak asasi manusia, privasi sebagai komoditas, privasi sebagai keadaan akses terbatas, dan privasi sebagai kemampuan untuk mengendalikan informasi tentang diri sendiri.

Menurut Xu *et al.* (2012), persepsi pengguna *smartphone* dari sudut pandang pengawasan terhadap pengguna bisa sangat menonjol karena kegiatan pengumpulan data yang agresif oleh aplikasi *mobile*. Kedua, persepsi intrusi dapat dipicu ketika aturan kepemilikan dilanggar, yaitu, ketika aplikasi *mobile* mampu membuat keputusan independen tentang memiliki atau meminta informasi pribadi pengguna. Dalam penelitian ini dan berdasarkan penelitian sebelumnya privasi terdiri dari tiga indikator yaitu *perceived surveillance, perceived intrusion, secondary use information* (Xu *et al.*, 2012).

Menurut Whitman dan Mattord (2011), *security Awareness* adalah kontrol/aturan yang dirancang untuk mengurangi insiden pelanggaran terhadap

keamanan informasi, akibat dari kelalaian maupun tindakan yang telah direncanakan. Menurut Kruger & Kerney (2006), menggunakan teori psikologi sosial membagi tiga komponen untuk mengukur objek yakni *cognition, affection* dan *behaviour.* Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai *Knowledge* (pengetahuan seseorang), *Attitude* (sikap seseorang) dan *Behaviour* (perilaku seseorang).

3. Metode

Jenis penelitian yang digunakan adalah penelitian kuantitatif dimana data dikumpulkan dengan menggunakan kuesioner. Penelitian ini memiliki 42 pertanyaan dari kesadaran keamanan informasi dan 27 pertanyaan dari kesadaran privasi untuk menguji *attitude, knowledge* dan *behavior* dalam perspektif penggunaan *smartphone* Android. Beberapa pertanyaan dijawab dalam skala 3 poin yaitu setuju, tidak tahu dan tidak setuju (dimensi *attitude* dan *knowledge*), sementara yang lain hanya membutuhkan jawaban yang setuju atau tidak setuju (dimensi *behavior*). Contoh pertanyaan yang diajukan dapat dilihat di Tabel 1. Kuesioner disebar secara online.

Tabel 1. Contoh Pertanyaan

Dimensi	Pertanyaan	Jawaban
Attitude	Saya mempertimbangkan keamanan sebelum menginstal Aplikasi dari repositori aplikasi	1. Setuju 2. Tidak Tahu 3. Tidak
Knowledge	Jika saya tidak mempertimbangkan keamanan sebelum menginstall aplikasi dari repository aplikasi, saya bisa mengalami gangguan keamanan informasi	1. Setuju 2. Tidak Tahu 3. Tidak
Behavior	Saya selalu mempertimbankan sebelum menginstal aplikasi dari repository aplikasi	1. Setuju 2. Tidak

Variabel operasional dalam penelitian ini terdiri dari tiga dimensi, yaitu pengetahuan (apa yang mereka ketahui tentang keamanan dan privasi), Sikap (bagaimana perasaan mereka tentang keamanan dan privasi), Dan perilaku (apa yang mereka lakukan terhadap keamanan dan privasi) Masing-masimg dimensi tersebut kemudian terbagi menjadi tujuh fokus area keamanan informasi yaitu *trust in application repository, misconception about app testing, Security and agreement message, pirated applicaion, adoption of security control spam sms* dan *report of security incidents*. dan tiga fokus area privasi yaitu *perceived surveillance, perceived intrusion* dan *secondary use information*.

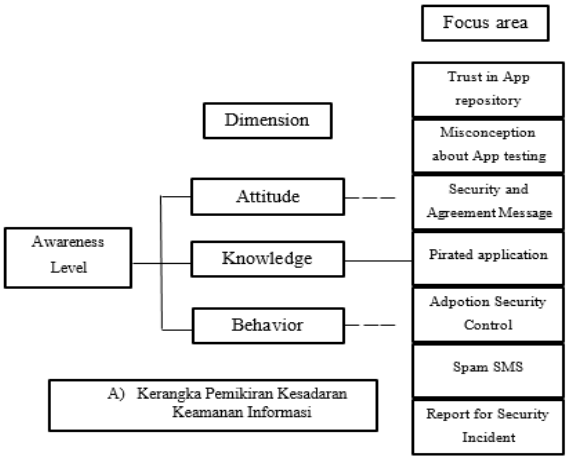
Untuk menguji validitas setiap item dalam kuesioner, penulis menggunakan korelasi Pearson Product Moment dimana setiap item yang memiliki koefisien korelasi sama atau lebih dari 0,3 adalah valid. Untuk pengujian reliabilitas penulis menggunakan metode Alpha Cronbach, dimana koefisiennya harus sama atau lebih dari 0,5.

Sari *et al.* (2014) mengatakan bahwa pembobotan ditentukan dengan menggunakan *analytical hierarchy process* (AHP). Pendekatan AHP menggunakan perbandingan berpasangan untuk memberikan evaluasi subyektif terhadap faktor berdasarkan pertimbangan dan pendapat profesional manajemen. Setiap dimensi memiliki bobot yang akan digunakan dalam pehitungan skor kesadaran. Bobot tersebut didefinisikan pada Tabel 2. sebagai berikut.

Tabel 2. Pembobotan Dimensi

Dimensi	Bobot
Attitude	20
Knowledge	30
Behavior	50

Kerangka pemikiran dari penilitian ini menggunakan model Krueger dan Kerney (2006) yang mengadaptasi teori psikologi sosial yang mengusulkan tiga komponen untuk mengukur cara yang menguntungkan atau tidak menguntungkan terhadap objek tertentu. Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai *knowledge* (pengetahuan seseorang), *attitude* (sikap seseorang) dan *behaviour* (perilaku seseorang. Dimensi *knowledge* digunakan untuk mengetahui bagaimana pengetahuan pengguna. Sedangkan Dimensi *attitude* digunakan untuk mengetahui bagaimana sikap pengguna dan dimensi *behaviour* untuk mengetahui hal-hal yang dapat dilakukan oleh pengguna. Masing-masing dimensi tersebut kemudian terbagi menjadi tujuh fokus area keamanan informasi dan tiga fokus area privasi. Berikut ini adalah metode yang diadopsi dari model Kruger dan Kearney seperti yang ditunjukan pada Gambar 1.

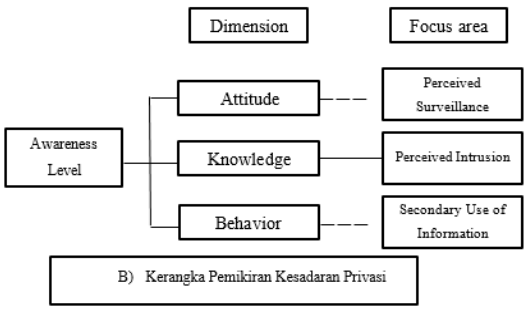


Gambar 1. Kerangka Pemikiran Kesadaran Keamanan Informasi

Kerangka pemikiran kesadaran keamanan informasi pada Gambar 1 dengan menggunakan model Krueger dan Kerney (2006) untuk mengukur

tingkat kesadaran dari tiap-tiap fokus area yang lima diantaranya diadaptasi dari Mylonas *et al.* (2013) yaitu *trust in app repository, misconception about app testing, security and agreement message, prirated application,* dan a*doption of security control* dimana *trust in app repository* bisa dilihat dari rasa percaya pengguna *smartphone* untuk mengunduh aplikasi di toko aplikasi atau *repository* aplikasi yang sudah disediakan oleh sistem operasi dari *smartphone* yang digunakan. Lalu *misconception about app testing* yang bisa dilihat dari kesadaran pengguna untuk menguji aplikasi pada *repositorty* aplikasi. *Security and agreement message* yang diketahui dari kesadaran pengguna tentang persetujuan keamanan aplikasi, persetujuan lisensi, dan konsekuensi penggunaan aplikasi. Selanjutnya *prirated application* berupa kekhawatiran pengguna untuk menginstal aplikasi bajakan dan banyaknya aplikasi bajakan yang mengandung *malware.* Kemudian *adoption security control* yang terlihat dari kontrol keamanan yang digunakan pengguna, anti virus *smartphone* pengguna, adanya kehadiran virus, dan lain sebagainya.

Adapun dua fokus area lainya dari kerangka pemikiran kesadaran keamanan informasi pada Gambar 1 yang diadaptasi dari Sari *et al.* (2014) yaitu *spam sms* dan *report for security incident*. Ketujuh fokus area yang telah disebutkan di atas, digabungkan bertujuan agar penelitian lebih konprehensif untuk mengukur kesadaran kaamanan informasi. Sedangkan kerangka pemikiran kesadaran privasi dapat dilihat pada Gambar 2.



Gambar 2. Kerangka Pemikiran Kesadaran Privasi

Pada Gambar 2, kerangka pemikiran kesadaran privasi juga di adaptasi dari model Krueger dan Kerney (2006) dan fokus areaya diadaptasi dari Xu *et al.* (2012) yang menggunakan *perceived surveillance, perceived intrusion,* dan *secondary use of information* untuk mengukur kesadaran privasi pengguna *smartphone.* Fokus area *perceived surveillance* adalah untuk mengetahui apakah perangkat lokasi yang ada di *smartphone* memantau kegiatan pengguna, aplikasi *mobile* yang dapat mengumpulkan banyak informasi pengguna menimbulkan kekhawatiran pengguna, dan aplikasi *mobile* pada perangkat *mobile* yang dapat memantau kegiatan pengguna menimbulkan kekhawatiran pengguna. Sedangkan fokus area *perceived intrusion* adalah untuk mengetahui apakah penggunaan aplikasi *mobile* menimbulkan rasa tidak nyaman bagi penggunaya, informasi pribadi pengguna yang lebih mudah tersedia untuk orang lain, dan akibat dari penggunaan aplikasi *mobile.* Kemudiaan untuk fokus area *secondary use of information* adalah untuk mengetahui apakah Aplikasi *mobile* dapat menggunakan informasi pribadi pengguna untuk tujuan lain tanpa izin otoritas dari pengguna, aplikasi dapat menggunakan informasi pribadi pengguna untuk tujuan lain, dan aplikasi *mobile* dapat berbagi informasi pribadi pengguna dengan entitas lain tanpa otorisasi pengguna. Pengukuran kesadaran privasi ini perlu dilakukan untuk mengetahui sejauh mana pengguna dapat mengendalikan informasi pribadi pengguna terhadap hak akses yang diminta oleh aplikasi *mobile* dan kekhawatiran penyalahgunaan informasi oleh pengembang aplikasi dan pihak ketiga.

4. Hasil dan Pembahasan

Penelitian ini mengambil sampel sebanyak 100 responden dimana kuesioner didistribusikan oleh peneliti pada bulan Maret 2017 di Indonesia. Di bawah ini merupakan karakteristik dari responden yang menggunakan *smartphone* Android (Tabel 3).

Tabel 3. Jenis kelamin responden

No	Jenis Kelamin	Persentase
1	Laki-laki	52%
2	Perempuan	48%

Pada Tabel 3 menggambarkan responden bedasarkan jenis kelamin dimana jumlah responden laki-laki lebih banyak dari responden perempuan. Hal ini memperlihatkan bahwa mayoritas responden pada penelitian adalah laki-laki. Kemudian untuk karakteristik responden dilihat dari segi usia dapat dilihat pada Tabel 4.

Tabel 4. Usia responden

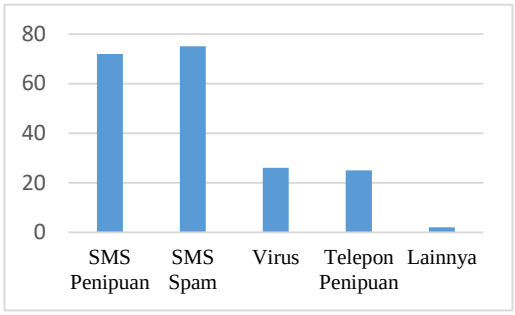
No	Usia	Persentase
1	< 16 Tahun	2%
2	16-18 Tahun	8%
3	18-23 Tahun	81%
4	23-30 Tahun	8%
5	30-40 Tahun	1%

Pada Tabel 4 diatas menunjukan jumlah responden penelitian ini didominasi oleh kategori usia 18-23 tahun. Selain itu, data ini juga memperlihatkan bahwa pengguna *smartphone* Android kebanyakan berasal dari kalangan anak muda. Dari banyaknya pengguna *smartphone* yang menjadi responden pada penelitian ini, diketahui juga bahwa pengguna tersebut pernah mengalami gangguan informasi pada saat menggunakan *smartphone*. Detail data dapat dilihat pada Tabel 5.

Tabel 5. Pengalaman Ganguan Keamanan informasi

No	Pengalaman Gangguan	Persentase
1	Ya	91%
2	Tidak	9%

Berdasarkan hasil survei, responden yang pernah mengalami gangguan keamanan informasi ada sebanyak 91% sedangkan 9% sisanya belum pernah mengalami gangguan keamanan informasi. Sehingga dapat diketahui bahwa harpir semua pengguna *smartphone* Android pernah mengalami gangguan keamanan informasi. Gangguan keamanan informasi ini bisa berasal beberapa faktor seperti sms penipuan, sms *spam*, virus, telepon penipuan, dan lain-lain. Data pengalaman gangguan keamanan informasi pengguna *smartphone* berdasarkan jenis ancaman gangguannya dapat dilihat pada Gambar 3.



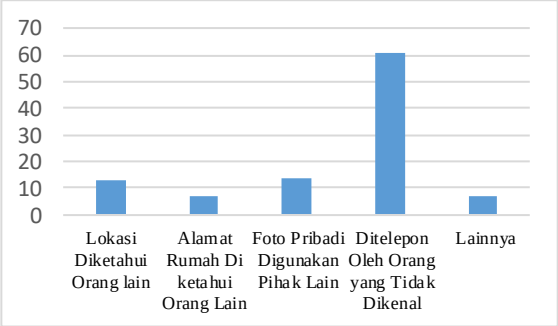
Gambar 3. Ancaman Gangguan Keamanan Informasi

Responden banyak mengalami gangguan keamanan informasi berupa sms *spam* dengan jumlah 75 responden, lalu pada gangguan keamanan informasi berupa sms penipuan sebanyak 72 responden, lalu responden yang gangguan keamanan informasi berupa virus sebanyak 26 responden, dan sebanyak 25 responden telah mengalami gangguan berupa telepon penipuan. Berdasarkan data yang ditampilkan pada Gambar 6, dapat diketahui bahwa pengguna *smarphone* Android merasa terganggu oleh sms *spam* yang bermunculan pada ponselnya dan mayoritas responden mengalami gangguan tersebut. Adapun gangguan lain dialami oleh responden. Salah satunya adalah gangguan privasi. Data mengenai jumlah reponden yang mengalami gangguan privasi dapat dilihat pada Tabel 6.

Tabel 6. Pengalaman Ganguan Privasi

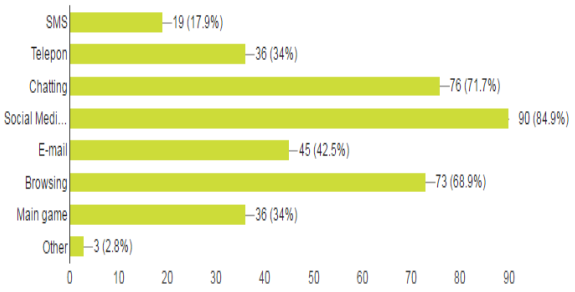
No	Pengalaman Gangguan	Persentase
1	Ya	67%
2	Tidak	33%

Pada Tabel 7 menunjukan persentase jumlah responden yang pernah mengalami gangguan privasi yaitu ada sebanyak 67%. Sedangkan 33% sisanya belum pernah mengalami gangguan privasi. Sehingga dapat diketahui bahwa harpir semua pengguna *smartphone* Android pernah mengalami gangguan privasi. Gangguan keamanan informasi ini bisa disebabkan oleh beberapa hal seperti lokasi pengguna yang diketahui oleh orang lain, alamat rumah yang diketahui oleh orang lain, foto pribadi yang digunakan orang lain tanpa izin, adanya telepon dari orang yang tidak dikenal, dan lain-lain. Data hasil survei berdasarkan gangguan keamanan informasi pengguna smartphone berdasarkan jenis gangguan privasi yang dialami responden dapat dilihat pada Gambar 4.



Gambar 4. Ancaman Ganguan Privasi

Banyaknya jumlah responden yang mengalami gangguan privasi berupa telepon dari orang yang tidak dikenal ada sebanya 61 responden. Lalu banyaknya responden yang mengalami gangguan privasi berupa foto pribadi digunakan oleh pihak lain ada sebanyak 14 responden. Kemudian jumlah responden yang mengalami gangguan privasi berupa lokasi diketahui oleh orang lain ada sebanyak 13 responden, dan sebanyak 7 responden telah mengalami gangguan privasi berupa alamat rumah diketahui orang lain. Berdasarkan data yang ditampilkan pada Gambar 6, dapat diketahui bahwa pengguna *smarphone* Android merasa terganggu oleh telepon dari orang yang tidak dikenal muncul di ponselnya dan mayoritas responden mengalami gangguan tersebut.



Gambar 6. Penggunaan *Smartphone*

Berdasarkan hasil survei yang diperlihatkan pada Gambar 7, pengguna menggunakan *smartphone* untuk *social media* (84,9%), *chatting* (71,7%), browsing (69,8%), email (42,5%), main *game* dan telepon (34%), SMS (17,9%), lainnya (2,8%). Hal tersebut menunjukkan bahwa pengguna *smartphone* yang menggunakan internet semakin meningkat dan untuk telpon dan SMS menurun..

Tabel 7. Kriteria Kesadaran

Kriteria	Nilai (%)	Tindakan
Baik	77, 78- 100	Tidak dibutuhkan tindakan
Rata-rata	55,56-77,77	Berpotensi tindakan diperlukan
Buruk	33,33-55,55	Tindakan diperlukan

Menurut Sari *et al.* (2014), skor hasil masing-masing fokus area dan dimensi kemudian dikelompokkan sebagai kriteria kesadaran yang sesuai dengan Tabel.3. Nilai interval dari kriteria tersebut didasarkan pada nilai garis kontinum dimana nilai maksimumnya adalah 100% dan skor minimumnya adalah 33,33%. Setiap kriteria juga mengidentifikasikan apakah suatu focus area memerlukan tindakan untuk perbaikan atau tidak.

Tabel 8. Tingkat Kesadaran Keamanan Informasi

Fokus Area	**Dimensi (Bobot)**			
	A	**K**	**B**	**Total**
	20	**30**	**50**	**100**
User's trust in app repository	50	58	82	**68**
Misconception about application testing	85	59	78	**74**
Security Agreement Messages	58	81	87	**80**
Pirated Application	81	88	83	**84**
Adoption of Security Control	67	67	50	**58**
Spam SMS	73	70	94	**83**
Report for Security Incidents	61	56	37	**50**
Total Awareness/ Dimensi	**69**	**68**	**73**	**71**

Keterangan
A = Attitude; K = Knowledge; B = Behavior;

Dari tingkat kesadaran keamanan informasi yang didapat seperti pada Tabel 8, dengan hasil sebagai berikut :

1. Total keseluruhan tingkat kesadaran keamanan informasi adalah 71%. Hal ini mengindikasikan bahwa tingkat kesadaran keamanan informasi di tingkat rata-rata atau berada ditingkat memuaskan. Tingkat kesadaran tertinggi terdapat pada dimensi *behavior* yaitu 73%, lalu dimensi *attitude* dengan 69% dan dimensi *knowledge* memiliki tingkat kesadaran terkecil yaitu 68%. Hal ini menunjukkan bahwa *attitude*, *knowledge*, dan *behavior* memiliki kriteria rata-rata.
2. Pada fokus area *security agreement messages*, *pirated application*, dan *spam SMS* memiliki kritetria kesadaran yang baik dan tidak memerlukan tindakan untuk perbaikan.

Dari hasil yang didapatkan dari tingkat kesadaran keamanan informasi menunjukkan bahwa fokus area yang memerlukan tindakan maupun yang masih berpotensi (tingkat rata-rata dan buruk) sebagai berikut :

1. *User's trust in app repository*
   Pada dimensi *attitude* memiliki kriteria kesadaran buruk (50%). Berdasarkan pertanyaaan yang diberikan, sebagian pengguna tidak menganggap mengunduh aplikasi di *play store* aman dipasang pada *smartphone* pengguna. Hal ini dikarenakan setiap aplikasi memiliki hak akses pada *smartphone* pengguna dan aplikasi dapat mengambil data mereka kapanpun. Kekhawatiran ini membuat responden menganggapnya tidak aman. Hal ini perlu dilakukan tindakan untuk perbaikan. Pada dimensi *knowledge* memiliki kriteria kesadaran rata-rata (58%) akan tetapi tingkat kesadarannya hampir berada di kriteria buruk. Berdasarakan pertanyaan yang telah diberikan beberapa responden tidak mengetahui jika mengunduh melalui *app repository* (*play store*) lebih aman daripada mengunduh ditempat lain. Walaupun begitu responden tetap mengunduh melalui *app repository* terlihat pada dimensi *behavior* yang memiliki kriteria bagus.
2. *Misconception about application testing*
   Pada dimensi *knowledge* memiliki kriteria kesadaran rata-rata (59%) hal tersebut menunjukkan dimensi tersebut harus mendapatkan perhatian. Berdasarkan pertanyaan yang telah diberikan, sebagian pengguna tidak mengetahui apakah aplikasi yang telah di instal pada *smartphone* mereka telah diuji dulu keamanannya atau belum. Hal ini menunjukkan bahwa pengguna percaya menginstal aplikasi melalui *app repository* (*Play Store*).
3. *Security agreement messages*
   Pada dimensi *attitude* memiliki kriteria kesadaran rata-rata (58%) dengan kriteria kesadaran tersebut menujukkan bahwa dimensi *attitude* harus mendapatkan perhatian karena mendekati kriteria kesadaran yang buruk. Berdasarkan pertanyaan yang telah diberikan, sebagian pengguna mungkin jarang membaca informasi tentang kebijakan keamanan yang muncul sebelum menginstal aplikasi. Ini mungkin dikarenakan memakan waktu terlalu jika pengguna membaca semua item dalam kebijakan keamanan saat mereka menginstal aplikasi baru. Namun pada dimensi *behavior* memiliki kriteria kesaradaran yang baik dimana pengguna mematuhi informasi tentang kebijakan keamanan. Hal ini mungkin karena pengguna sudah memahami kebijakan keamanan yang umum.
4. *Adoption security control*
   Pada dimensi *attitude* dan *knowledge* memiliki kriteria kesadaran yang sama yaitu memuaskan (67%) hal ini menunjukkan kedua dimensi tersebut harus mendapatkan perhatian karena berpotensi diperlukannya tindakan. Sedangkan pada dimensi *behavior* memiliki kriteria kesadaran yang buruk (50%). Berdasarkan pertanyaan yang telah diberikan, pengguna sebagian besar tidak memasang *antivirus*, password maupun mekanisme keamanan informasi lainnya untuk melindungi *smartphone* mereka dan pengguna yang memiliki aplikasi *antivirus* tidak mengupdate secara rutin. Selain itu, rendahnya tingkat *behavior* mungkin

disebabkan karena kurangnya pengetahuan tentang *antivirus* itu sendiri.

5. *Spam SMS*
   Pada dimensi *attitude* dan *knowledge* memiliki kriteria kesadaran rata-rata (73% dan 70%). Berdasarkan pertanyaan yang telah diberikan, beberapa pengguna tidak mengetahui bahwa SMS premium dapat mengurangi sejumlah pulsa yang dimiliki pengguna dan beberapa pengguna masih memilih menanggapi SMS dari pihak yang tidak dikenal. Walaupun penyebab rendahnya tingkat kesadaran dimensi *attitude* dan *behavior* adalah kurangnya pengetahuan tentang SMS premium, pengguna tidak berlangganan SMS premium dapat dilihat dari tingkat kesadaran pada dimensi *behavior* sebesar 94% dan memiliki kriteria kesadaran yang baik.
6. *Report for security incidents*
   Pada dimensi *attitude* dan *knowledge* memiliki kriteria kesadaran rata-rata (61% dan 56%). Hal tersebut menujukkan bahwa kedua dimensi tersebut harus mendapatkan perhatian dan berpotensi diperlukannya tindakan untuk perbaikan, sedangkan pada dimensi *behavior* memiliki kriteria yang buruk (37%). Hal tersebut menunjukkan diperlukannya tindakan untuk perbaikan karena rendahnya tingkat kesadaran. Berdasarkan pertanyaan yang telah diberikan dalam hal melaporkan insiden keamanan sebagaian besar pengguna mungkin lebih memilih untuk menyelesaikan sendiri insiden keamanan informasi yang dialami daripada melaporkan kepada pihak *developer* aplikasi melalui *feedback* karena telah mengalami gangguan keamanan informasi. Selalin itu pengguna *smartphone* jarang sekali melapor ke *call center* operator telekomunikasi terkait penipuan SMS atau *spam SMS.*

Tabel 9. Tingkat Kesadaran Privasi

Fokus Area	**Dimensi (bobot)**			
	A	**K**	**B**	**Total**
	20	**30**	**50**	**100**
Perceived Surveillance	75	78	80	**78**
Perceived Intrusion	68	72	71	**71**
Secondary Use of Information	78	66	83	**77**
Total Awareness/ Dimension	**74**	**72**	**78**	**76**

Keterangan
A = Attitude; K = Knowledge; B = Behavior;

Dari tingkat kesadaran privasi pada Tabel 5 didapatkan hasil sebagai berikut :

1. Total keseluruhan tingkat kesadaran privasi adalah 76%. Hal ini mengindikasikan bahwa tingkat kesadaran keamanan informasi di tingkat ditingkat memuaskan.
2. Tingkat kesadaran tertinggi terdapat pada dimensi *behavior* yaitu 78%, lalu dimensi *attitude* dengan 74% dan dimensi *knowledge* memiliki tingkat kesadaran terkecil yaitu 72%. Hal ini menunjukkan bahwa *attitude*, *knowledge* memiliki kriteria rata-rata atau memuaskan, sedangkan dimensi *behavior* memiliki kriteria kesadaran yang baik.
3. Pada fokus area *perceived surveillance* memiliki kritetria kesadaran yang baik dan tidak memerlukan tindakan untuk perbaikan.
4. Tidak ada satupun fokus area dan dimensi dari tingkat kesadaran privasi yang kriteria kesadaran yang buruk (tingkat kesadaran dibawah 55,56%).

Dari hasil yang didapatkan dari tingkat kesadaran privasi menunjukkan fokus area yang memerlukan tindakan maupun yang masih berpotensi (tingkat rata-rata dan buruk) sebagai berikut :

1. *Perceived surveillance*
   Pada dimensi *attitude* memiliki kriteria kesadaran yang memuaskan (75%). selain itu, pada dimensi *knowledge dan behavior* sudah memiliki kriteria yang baik dan tidak diperlukan tindakan untuk perbaikan. Berdasarkan pertanyaan yang telah diberikan sebagian besar pengguna sudah mengetahui bahwa aplikasi dapat mengumpulkan informasi pengguna *smartphone* dari hak akses yang diberikan oleh aplikasi terutama pada fitur *global positioning system* (GPS) yang dapat mengetahui lokasi pengguna ketika menyalakan fitur tersebut. Selain itu, pengguna juga sudah paham untuk selalu mematikan fitur GPS ketika sudah tidak diperlukan lagi.
2. *Perceived intrusion*
   Pada dimensi *attitude*, *knowledge*, dan *behavior* memiliki kriteria kesadaran rata-rata, dimana tingkat kesadaran *attitude* sebesar 68% *knowledge* sebesar 72% dan *behavior* sebesar 71%. Hal tersebut menunjukkan bahwa dimensi *attitude*, *knowledge*, *behavior* berpotensi perlu dilakukan tindakan untuk perbaikan. Berdasarkan pertanyaan yang telah diberikan sebagian besar pengguna sudah menyadari bahwa informasi pribadi pengguna lebih tersedia untuk orang lain seperti foto, alamat dan nomor telepon pengguna. Contohnya aplikasi *path* orang lain dapat menyimpan foto yang telah diunggah oleh pengguna. Selain itu sebagian besar pengguna sudah menyadari bahwa situs dapat mengetahui minat pengguna berdasarkan *history* dan *cookies* penulusaran dan selalu rutin menghapus agar situs tidak mengoleksi data pengguna.
3. *Secondary use of information*
   Pada dimensi *attitude* dan *behavior* sudah memiliki kriteria kesadaran yang baik sedangkan, pada dimensi *knowledge* memiliki kriteria kesadaran rata-rata (66%). Hal tersebut menunjukkan bahwa dimensi *knowledge* berpotensi perlu dilakukan tindakan untuk perbaikan. Berdasarkan pertanyaan yang telah diberikan sebagian pengguna kurang pengetahuan bahwa aplikasi bisa saja menggunakan informasi pribadi pengguna tanpa izin terlebih dahulu pengguna juga kurang menyadari bahwa aplikasi

bisa memberikan informasi pribadi pengguna kepada entitas lain atau untuk tujuan lain. Walaupun kurangnya pengetahuan akan aplikasi yang dapat bersifat intrusi pengguna hanya memberikan informasi mana yang akan diberikan pada aplikasi terlihat pada dimensi *behavior* yang memiliki kriteria kesadaran yang baik.

5. Kesimpulan

Berdasarkan penelitian kami, dinyatakan bahwa tingkat kesadaran keamanan informasi dan privasi pengguna smartphone di Indonesia ada berada pada kriteria rata-rata. Hal ini ditunjukkan oleh tingkat kesadaran keamanan informasi sebesar 71% dan privasi 76%. Namun terdapat beberapa fokus area yang harus diperbaiki agar bisa mengalami peningkatan potensial terutama pada *report for security incidents* (37%) yang memiliki kriteria kesadaran yang buruk Dengan menerapkan program kesadaran keamanan informasi bagi pengguna smartphone, penulis berharap pengguna *smartphone* dapat mengerti tentang keamanan dan pengamanan informasi mereka dalam penggunaan *smartphone* yang biasanya mereka gunakan untuk email, layanan di media sosial, sms, *chatting*, dan lain-lain. Program kesadaran keamanan ini penting karena Jumlah pengguna smartphone selalu meningkat setiap tahunnya dan mereka menggunakannya untuk berbagai keperluan.

Tingkat kesadaran privasi memiliki kriteria kesadaran rata-rata (76%). Hal ini menunjukkan bahwa secara umum bagus. Namun terdapat beberapa fokus area berpotensi diperlukan tindakan perbaikan yaitu; *secondary use of information* (66%) pada dimensi *knowledge*. Pengguna *smartphone* kurang mengetahui bahwa aplikasi bisa saja menggunakan informasi pribadi pengguna tanpa izin terlebih dahulu, pengguna juga kurang menyadari bahwa aplikasi bisa memberikan informasi pribadi pengguna kepada entitas lain atau untuk tujuan lain.

Terdapat ketimpangan yaitu dimana responden yang mengalami gangguan keamanan informasi (sebesar 91%) hal ini kemungkinan bisa terjadi karena pada fokus area *report for security incidents* memiliki kriteria kesadaran yang buruk. Oleh karena itu, diharapkan untuk penelitian selanjutnya dapat dikembangkan untuk menganalisis faktor-faktor tersebut seperti mengapa pelanggaran keamanan informasi terhadap pengguna *smartphone* masih tergolong tinggi.

Daftar Pustaka

Al-Sehri, 2012. Information security awareness and culture, British Journal of Arts and Social Sciences; 6(1): 61-69.

Gemalto, 2015. Information Security Threat Annual Reports. Gemalto Corporation. 2015; 43.

IDCERT, 2015. Laporan Dwi Bulan I 2015. Indonesia Computer Emergency Response.

McLeod, Raymond & Schell, George P. 2008. Sistem Informasi Manajemen, Edisi 10. Jakarta: Salemba Empat.

Kruger, H.A., Kearney W., D., 2006. A prototype for assessing information security Awareness. Computer & Security Volume 25 : 289-29.

Mylonas, A., Kastania, A., Gritzalis, D., 2013. Delegate the smartphone user? Security awareness in smartphone platforms. Computer & Security Volume 34 : 47-66.

Sari, Kencana, P., Candiwan, 2014. Measuring Information Security Awareness of Indonesian Smartphone.Users.TELKOMNIKA..Vol.12,No.2, June 2014,pp.493-500.

Smith, H.J., Dinev, T., Xu, H., 2011. Information Privacy Research: An Interdisciplinary Review, MIS Quarterly (35:4), pp 989-1015.

Statista, 2016. Market Share Smartphone. https://www.statista.com/statistics/266136/global-marketshare-held-by-smartphone-operating-systems/ diakses tanggal 23 September 2016.

Statista, 2016. Market share OS mobile Smartphone Indonesia.https://www.statista.com/statistics/262205/marketshare-held-by-mobile-operating-systems-in-indonesia/ diakses tanggal 23 September 2016

Symantec, 2015. Information Security Threat Reports. Symantec Corporation. 2015; 18.

Witman, M. E., Mattord, H. J., 2011. Principles of Information security, 4th Edition. Atlanta: Cengage Learning.

Xu, H., Gupta, S., Rosson, M.B., Carroll, J.M., 2012. Measuring Mobile Users' Concerns for Information Privacy. Thirty Third International Conference on Information Systems, Orlando.