STUDI PERBANDINGAN KESADARAN, PENGETAHUAN, DAN PERILAKU CYBER SECURITY DI INDONESIA

Rizki Dewantara[1*], Dwi Rizky April Yadi[2]
[1]Program Studi Sains Data, Institut Teknologi Bisnis dan Kesehatan Bhakti Putra Bangsa,Indonesia
[2]Program Studi Informatika, Universitas Perwira Purbalingga, Indonesia
[1]dewantararizki@ibisa.ac.id
[2]dwirizky@gmail.com

ABSTRAK

Berdasarkan statistik, Android adalah smartphone paling populer dengan hampir 1,8 juta pengguna di seluruh dunia. Tingginya jumlah pengguna juga mengundang banyaknya kasus keamanan informasi dan privasi yang disebabkan oleh kurangnya kesadaran dari pengguna seperti spam, spoofing/phishing, insiden jaringan, malware, mengunggah sesuatu yang bersifat pribadi seperti gambar, nomor telepon, alamat, atau tidak saya. mengetahui tentang keamanan informasi dan privasi pengguna smartphone Android dengan melakukan pengukuran masalah dari dimensi kesadaran (sikap, pengetahuan dan perilaku) dengan tujuh area fokus informasi keamanan yaitu trust in app repository, miskonsepsi tentang pengujian aplikasi, keamanan dan pesan persetujuan, aplikasi bajakan, adopsi keamanan kontrol, sms spam, dan laporan insiden keamanan dan tiga fokus area privasi Proses hierarki analitik (AHP) digunakan untuk mengukur keamanan informasi dan kesadaran privasi pengguna smartphone. Penelitian menunjukkan bahwa keamanan informasi memiliki tingkat pengetahuan rata-rata (71%). Namun, laporan area fokus untuk acara keamanan memiliki kesadaran yang buruk (37%) karena pengguna lebih suka menyelesaikan masalah keamanan informasi dan privasi mereka sendiri. Penggunaan informasi sekunder pada sikap memiliki pengetahuan yang rendah (66%). Berdasarkan survei tersebut, pengguna smartphone Indonesia memiliki keterampilan keamanan informasi dan privasi yang buruk.

Kata kunci: Kesadaran, Pengetahuan, Perilaku cyber

ABSTRACT

Based on statistics, Android is the world's most popular smartphone with 1.8 billion users. Due to user ignorance, many information security and privacy issues arise, such as spam, spoofing/phishing, network incidents, malware, uploading personal data like images, phone numbers, addresses, or having no antivirus. The study measures Android smartphone owners' understanding of data security and privacy. Information security's seven priority areas include trust in app repository, misconception about app testing, security and agreement message, pirated program, adoption, and Security control, spam sms, and reporting security incidents are privacy's three focus areas. Analytical hierarchy process (AHP) is used to test smartphone users' understanding of information security and privacy. The research found that information security has an average level of knowledge (71%), but the focus area of report for security incidents has a poor level of awareness (37%), perhaps because users prefer to solve their own information security issues. Privacy awareness is average (76%). However, attitude dimension secondary information usage awareness is 66%. Based on this study, Indonesian smartphone users have little understanding of data security and privacy.

Keywords: *Cyber Awareness, Knowledge, Behavior*

PENDAHULUAN

Perkembangan teknologi dan informasi yang sedemikian pesatnya telah menimbulkan perubahan kebutuhan serta gaya hidup masyarakat yang semakin tergantung dengan teknologi. Perkembangan teknologi dalam kehidupan sehari-hari dapat dirasakan di berbagai aktivitas terutama dalam situasi pandemi *covid* 19 ini yang tidak bisa lepas dari teknologi. Sehingga perlindungan data pribadi di dunia digital semakin penting karena penggunaan dokumen elektronik dan jaringan internet semakin meningkat terutama sejak pandemik *covid* 19 hampir semua orang bekerja, belajar, bertransaksi dari rumah dengan mengandalkan jaringan internet. Pemanfaatan akan teknologi dan informasi dapat dirasakan manfaatnya baik di bidang pendidikan dan perekonomian dan lain-lain, hal-hal yang berkaitan dengan perkembanagan ilmu pengetahuan, sains dan lain sebagainya yang dengan mudah dapat di akses, sehingga milyaran bahkan triliyunan informasi dapat kita terima dengan cepat. Dalam bidang pekerjaan, pengelolaan data yang berjumlah sangat banyak dapat dikelola dengan baik, cepat, efektif dan efisien serta meminimalisir kesalahan. Dalam bidang perekonomian, promosi-promosi dan potensi-potensi dalam meningkatkan kesejahteraan masyarakat dilakukan degan cepat tanpa batasan tempat atau wilayah dan menjangkau semua lapisan masyarakat baik nasional maupun internasional. Akan tetapi perkembangan teknologi dan informasi ini tidak saja memberikan manfaat melainkan juga mengakibatkan masalah yang dapat merugikan masyarakat, seperti halnya penyalahgunaan *data*, pencurian *data* pribadi, penjualan *data* pribadi, penipuan dan lain-lain karena seringnya server mengalami masalah seperti layanan yang rusak dan perhitungan yang salah, server sekunder harus mengambil alih server utama.(Dewantara & Fatwanto, 2019).

Pelaku usaha atau penyelenggara sistem elektronik bisa mengumpulkan *data* pribadi dari pelanggan atau calon pelanggan secara luring atau daring, dimana *data* digital dapat diperjualbelikan tanpa sepengetahuan dan seizin pemilik *data* atau disalahgunakan (untuk tujuan di luar pemberian, penyerahan data pribadi digital), bisa juga terjadi *data* pribadi yang terkoneksi dibajak, dicuri (hack) oleh pihak ketiga. Saat membahas keamanan komputer, administrator akan sering mengangkat topik yang sudah dikenal masyarakat umum namun masih memiliki beberapa pertanyaan yang perlu dijawab (Khairunnisa & Sutarti, 2018). Internet di mana dan kapan pun dapat digunakan, seperti mengakses informasi, menghubungi kerabat, bahkan jual beli barang (Hafid, 2019).Dengan adanya penyalahgunaan *data* pribadi, maka dapat terlihat adanya kelemahan sistem, kurangnya pengawasan, sehingga *data* pribadi dapat disalahgunakan dan mengakibatkan kerugian bagi pemilik data tersebut. Penyalahgunaan, pencurian, penjualan *data* pribadi merupakan suatu pelanggaran hukum dalam bidang teknologi informasi dan juga dapat dikategorikan sebagai pelanggaran atas hak asasi manusia, karena *data* pribadi merupakan bagian dari hak asasi manusia yang harus dilindungi. Berkaitan hal tersebut, terdapat beberapa contoh kasus dalam penyalahgunaan *data* pribadi, diantaranya yaitu:

1. Penyalinan *data* dan informasi kartu ATM nasabah (*skimming*) dimana pelaku *skimming* melakukan penarikan dana di tempat lain.
2. Pinjaman *online*, dimana mekanisme transaksinya mengisi data secara online akan tetapi dalam hal keterlambatan pembayaran tidak jarang menggunakan kolektor untuk

melakukan intimidasi kepada nasabah, keluarga nasabah, pimpinan tempat nasabah bekerja dan bahkan dapat mengakses *data* dari handphone nasabah.

3. Transportasi *online*, dimana konsumen mengalami pelecehan seksual melalui nomor whatshap.

Berdasarkan peristiwa tersebut dapat disimpulkan bahwa terdapat metadata berupa data pribadi yang diberikan untuk berbagai kepentingan (perbankan, e-commerce, dll.), diserahkan secara sukarela dan disimpan sbagai data digital oleh pelaku usaha (atau siapapun yang menerima dan menyimpan data pribadi, *metadata* rentan untuk disalahgunakan penerima-penyimpan data atau dicuri (hack) pihak ketiga dan terbuka untuk disalahgunakan, digunakan untuk tujuan-tujuan lain di luar kesepakatan. Penyalahgunaan data pribadi merupakan perbuatan yang memenuhi unsur-unsur perbuatan pidana seperti unsur tindak pidana pencurian dan unsur tindak pidana penipuan serta tindak pidana lainnya baik dari sisi unsur objektif maupun unsur subjektif. Dengan terpenuhinya unsur-unsur tersebut, maka sanksi administratif, sanksi perdata maupun sanksi pidana belum cukup untuk mengakomodir tindak pidana penyalahgunaan data pribadi yang senyatanya merupakan bentuk kejahatan yang sempurna.

Kejahatan adalah perbuatan manusia yang melanggar atau bertentangan dengan apa yang ditentukan dalam kaidah hukum, tegasnya perbuatan yang melanggar larangan yang ditetapkan dalam kaidah hukum dan tidak memenuhi atau melawan perintah-perintah yag telah ditetapkan dalam kaidah hukum yang berlaku dalam masyarakat dimana yang bersangkutan bertempat tinggal.

Berdasarkan permasalahan diatas, penting untuk diperhatikan terkait perlindungan serta kepastian hukum dalam pemanfaatan teknologi agar dapat berjalan dengan optimal. Berdasarkan dari penjelasan latar belakang di atas, maka yang menjadi permasalahan untuk diteliti adalah:

1. Bagaimana pengaturan perlindungan hukum atas penyalahgunaan *data* pribadi sebagai bentuk kejahatan yang sempurna dalam upaya memberikan kepastian hukum kepada masyarakat?
2. Bagaimana peran penegak hukum dalam pencegahan tindak pidana penggunaan *data* pribadi dimasa yang akan datang ditinjau dari perspektif pembaharuan hukum pidana.

Perbedaan mendasar antara tulisan ini dengan kedua tulisan ilmiah tersebut diatas terletak pada obyek penelitian mengenai perlindungan hukum, dimana penelitian yang pertama terkait dengan akibat hukum penyalahgunaan *data* pribadi pengguna aplikasi pinjaman dana berbasis *fintech*, sedangkan penelitian kedua terkait dengan pengaturan privasi konsumen daring dalam *online marketplace system.* Sementara dalam tulisan ini, penulis akan mengkaji mengenai perlindungan hukum atas penyalahgunaan *data* pribadi serta peran penegak hukum dalam pencegahan tindak pidana penggunaan *data* pribadi.

METODE PENELITIAN

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. Kuesioner disebar secara online

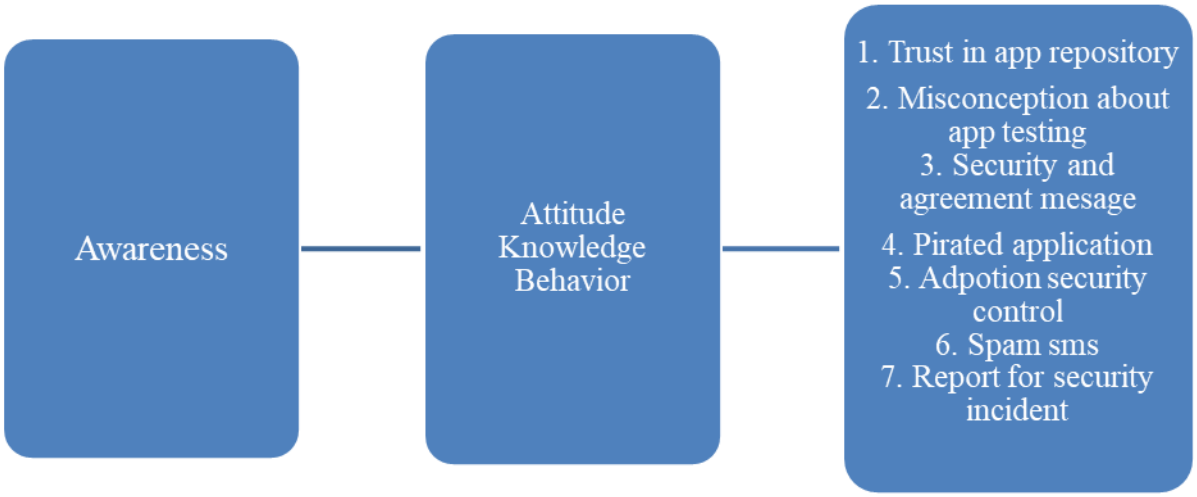
Dimensi	Pertanyaan	Jawaban
Attitude	Saya mempertimbangkan keamanan sebelum menginstal *Aplikasi* dari repositori aplikasI	1.Setuju 2.Tidak Tahu 3.Tidak
Knowledge	Jika saya tidak mempertimbangkan keamanansebelum menginstall aplikasi dari *repository* aplikasi, saya bisa mengalami gangguan keamanan informasi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

Tabel 2. Model KAB

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

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*, *priratedapplication*, dan *adoption 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.

Aplikasi *mobile* menimbulkan rasa tidak nyaman bagi penggunanya, 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.

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. Karakteristik Responden

Jenis kelamin	Persentasi
Laki – lakli	52%
Perempuan	48%

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 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 itusendiri.
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 sebagian 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.

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* penelusuran 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.

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

Abidin, D. Z. (2015). Kejahatan dalam Teknologi Informasi dan Komunikasi. Jurnal Ilmiah Media Processor, Vol. 10, No. 2, 509-516.

Agus, A. A. (2016). Penanganan Kasus Cyber Crime di Kota Makassar. Jurnal Supremasi, Vol. XI, No. 1, 20-29. doi: https://doi.org/10.26858/supremasi.v11i1.3023

Akub, M. S. (2018). Peraturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia. Jurnal Ilmiah Hukum, Vol. 21, No. 2, 85-93. Doi: https://doi.org/10.33096/aijih.v21i2.19

Arianto, A. R., & Anggraini, G. (2019). Membangun Pertahanan dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team nn Internet Infrastructure (ID-SIRTII). Jurnal Pertahanan & Bela Negara Vol. 9 No. 1 , 13-29. doi:10.33172/jpbh.v9i1.497

Dewantara, R., & Fatwanto, A. (2019). Availability Analysis with Failover Computer Cluster Method Case Study in Academic Information System of UIN Sunan Kalijaga. 6(2), 1–4.

Hafid, H. (2019). Investigasi Log Jaringan Untuk Deteksi Serangan Distributed Denial of Service (Ddos) Dengan Menggunakan Metode General Regression Neural Network. http://etheses.uin-malang.ac.id/16609/

Khairunnisa, & Sutarti. (2018). Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan DDOS (Distributed Denial of Service) Berbasis Honeypot. Jurnal PROSISKO, 4(2), 8.