IT Security Awareness Assessment

Lidya Jessica - 18217037

Program Studi Sistem dan Teknologi Informasi

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Bandung 40132, Indonesia

18217037@std.stei.itb.ac.id

***Abstract*–Pada zaman ini, manusia tidak lepas dari teknologi. Komunikasi, produksi, transaksi, dan hal lainnya dapat berjalan dengan bantuan teknologi informasi. Dari berbagai hal positif yang didatangkan oleh teknologi, tetap saja ada sisi negatif dalam penggunaannya, salah satunya adalah berkaitan dengan aspek keamanannya. Kesadaran terhadap keamanan teknologi informasi (TI) perlu ditingkatkan. Apakah tolak ukur untuk menilai bahwa seseorang telah memiliki tingkat kesadaran akan keamanan TI yang baik? Pada tulisan kali ini akan dibahas apa itu kesadaran akan keamanan TI dan metode apa yang bisa digunakan untuk mengukurnya.**

***Index Terms*–tingkat kesadaran, keamanan, teknologi informasi (TI), ukur**

I. Pendahuluan

I.1 Latar Belakang

Kesadaran akan keamanan teknologi informasi (TI) sangat penting untuk dimiliki oleh semua orang. Terutama saat ini, saat teknologi berkembang dengan pesatnya, ketika orang-orang tidak terlepas dari *handphone* mereka masing-masing, membuat akun di sana-sini, dan bahkan dapat melakukan transaksi secara *online*. Kesadaran bahwa keamanan TI dapat terancam bahkan dari langkah kecil, seperti menekan sebuah link bisa mengekspos informasi pribadi dan bahkan membuat *device* dapat diretas, harus dimiliki oleh setiap orang. Saat ini masih belum jelas apa tolak ukur untuk menilai kesadaran akan keamanan TI yang dimiliki oleh seseorang atau sekelompok orang dan cara mengukurnya. Pada tulisan ini akan dibahas apa itu kesadaran akan keamanan TI dan metode yang bisa digunakan untuk mengukur tingkat kesadaran keamanan TI dari seseorang maupun sekelompok orang.

I.2 Rumusan Masalah

Berikut adalah rumusan masalah dari penulisan ini.

1. Apa itu kesadaran akan keamanan TI?
2. Bagaimana cara mengukur tingkat kesadaran akan keamanan TI?

I.3 Tujuan

Berdasarkan rumusan masalah di atas, maka tujuan dari penulisan ini adalah:

1. Memahami kesadaran akan keamanan TI.
2. Mengetahui cara mengukur tingkat kesadaran akan keamanan TI.

I.4 Metodologi

Berikut adalah kerangka isi dari penulisan ini.

Tabel 1 Metodologi

No	Bagian	Deskripsi	Isi Bagian
1.	Pendahuluan	Berisi penjelasan singkat mengenai penulisan makalah.	- Latar Belakang - Rumusan Masalah - Tujuan - Metodologi
2.	Pembahasan	Berisi inti dari pembahasan penulisan makalah, yaitu penjelesan mengenai kesadaran akan keamanan TI dan metode pengukuran tingkat kesadaran akan keamanan TI dalam suatu organisasi atau individu.	- Kesadaran Akan Keamanan TI - Metode Pengukuran Tingkat Kesadaran Akan Keamanan TI
3.	Penutup	Berisi kesimpulan dari penulisan ini dan saran untuk penulisan selanjutnya yang akan menggunakan tulisan ini sebagai referensi.	- Kesimpulan - Saran
4.	Daftar Pustaka	Berisi daftar referensi yang digunakan dalam membuat tulisan ini. Referensi diurutkan berdasarkan nama penulis.	- Daftar Pustaka

II. Pembahasan

II.1 Kesadaran Akan Keamanan TI

Dengan semakin berkembangnya teknologi saat ini dan terjadinya pandemi COVID-19, membuat banyak orang semakin memanfaatkan teknologi. Media sosial, *mobile banking*, *video conference*, *e-commerce*, dan media lainnya sering digunakan, tetapi apakah para pengguna media tersebut paham akan hal-hal yang perlu dilakukan untuk menjaga privasi mereka? Sudah banyak tersebar di internet hal-hal yang perlu diperhatikan untuk menjaga / mengamankan akun yang dibuat, seperti jangan menggunakan tanggal lahir sebagai *password*, jangan menggunakan *username* sebagai *password*, dan lainnya. Saran-saran tersebut tidak muncul dengan sendirinya, tetapi muncul dari peristiwa-peristiwa yang pernah terjadi. Sekarang jika ditelusuri di internet, ada banyak sekali saran-saran dalam menjaga keamanan dalam menggunakan teknologi informasi, sehingga dapat dilihat bahwa aspek keamanan itu sangat penting.

Keamanan sistem informasi menurut David Icove dapat diklasifikasikan menjadi empat bagian, yaitu:

1. Fisik (*physical security*)
2. Manusia (*people* / *personnel security*)
3. Data, media, teknik komunikasi
4. Kebijakan dan prosedur (*policy and procedures*)

Hal yang berkaitan tentang keamanan selanjutnya adalah tiga prinsip utama dalam keamanan informasi, yaitu *confidentiality*, *integrity*, dan *availability* (CIA), berikut adalah penjabarannya.

1. *Confidentiality* / *Privacy*

   Memastikan data terlindungi dan data sensitif hanya dapat dilihat oleh pihak yang telah diberi otorisasi. Perlindungan data yang sensitif, seperti data pribadi atau data pelanggan, dengan menggunakan proteksi, seperti *firewall*, enkripsi, *policy*, dan sebagainya. Perlindungan ini dilakukan untuk mencegah serangan, seperti *sniffer*, *keylogger*, kelemahan aplikasi, kebijakan yang tidak jelas, dan sebagainya.

2. *Integrity*

   Memastikan informasi telah sesuai dengan format yang ditentukan dan sesuai dengan tujuan pembuatannya. Menjaga agar informasi tidak berubah tanpa ijin dengan memberikan proteksi, seperti *message authentication code* (MAC), *digital signature*, *hash function*, dan *logging*. *Integrity* informasi dapat terancam karena serangan *spoof*, virus yang mengubah data, dan sebagainya.

3. *Availability*

   Memastikan bahwa informasi tersedia ketika dibutuhkan. Proteksi yang dapat dilakukan adalah *firewall*, *backup*, *filtering router*, dan lainnya untuk mencegah serangan, seperti *Denial of Service* (DoS) *attack*, listrik mati, dan jaringan terputus.

Keamanan harus menyeluruh (*holistic approach*), mulai dari *people* dalam hal *awareness* dan *skill*, *process* dalam hal menyertakan keamanan dalam proses bisnis, dan *technology* yang memperhatikan aspek keamanan dalam pembangunannya (Rahardjo, 2020).

Kesadaran akan keamanan TI adalah pengetahuan yang dimiliki orang dalam suatu organisasi mengenai perlindungan aset fisik dan informasi dari organisasi tersebut. Kesadaran akan keamanan TI juga dapat dilihat dari perilaku dan motivasi orang dalam suatu organisasi dalam memahami dan menangani berbagai masalah keamanan, bagaimana dia sadar bahwa ada orang yang mungkin secara sengaja / tidak sengaja mencuri, merusak, atau menyalahgunakan data / aset TI lainnya. Kesadaran untuk menjaga aset informasi agar sesuai dengan prinsip CIA (Banerjee & Pandey, 2010).

Dalam tulisan Gábor Vanderer, salah satu aspek yang dapat mempengaruhi kesadaran akan kemanan TI adalah kesenjangan generasi. Para pekerja dapat dibagi menjadi empat kelompok generasi berdasarkan tahun lahirnya, yaitu:

1. *Baby boom generation* (1946 - 1965)

   Anggota kelompok ini umumnya sudah pensiun dan memiliki masalah dalam beradaptasi dengan perkembangan teknologi informasi saat ini.

2. *Generation* X (1965 - 1980)

Anggota generasi X bergerak secara independen, sering mengabaikan standar keamanan, merasa lebih paham, sehingga dapat menyebabkan kerusakan yang disengaja dan jahat. Generasi X sadar akan bahaya yang ada, tetapi merasa lebih paham sehingga bertindak sesuai pemahamannya.

3. *Generation* Y (1980 - 1995)

   Kelompok ini peka terhadap teknologi informasi, tetapi tidak sabar. Cenderung mencari solusi melalui internet dan mengunduh dokumen sensitif ke *device* tanpa pikir panjang. Generasi Y bisa saja tidak sadar atas bahaya yang ada, mereka memegang prinsip: selama tujuan yang diinginkan tercapai, maka tidak ada masalah.

4. *Generation* Z (1995+)

   Generasi ini mengharapkan dan membutuhkan kehadiran internet terus-menerus. Generasi ini sama sekali tidak sadar atas bahaya yang ada.

Perbedaan generasi dalam karakteristik kelompok umur harus diperhitungkan dalam membuat peraturan keamanan informasi (Vanderer, 2015).

Kesadaran akan keamanan TI sangat penting untuk dimiliki oleh seluruh generasi, karena telah banyak terjadi tindak kriminal melalui internet, yang disadari maupun tidak disadari. Semakin berkembangnya teknologi, semakin banyak pula celah yang dapat disusupi pelaku *cybercrime*.

II.2 Metode Pengukuran Tingkat Kesadaran Akan Keamanan TI

Metode pengukuran tingkat kesadaran akan keamanan TI yang akan dibahas di bawah ini adalah prototipe penilaian yang dibuat oleh H.A. Kruger dan W.D. Kearney. Langkah-langkah yang harus diambil dalam mengukur tingkat kesadaran akan keamanan TI adalah (Kruger & Kearney, 2006):

1. Memahami latar belakang organisasi.

   Pertama kali yang harus dilakukan adalah memahami apa yang dikerjakan oleh organisasi, struktur organisasi, kebijakan dan prosedur yang diterapkan, teknologi apa saja yang digunakan, dan kondisi keamanan yang ada di organisasi saat ini.

2. Membuat program kesadaran akan keamanan informasi.

   Pembuatan program ini bertujuan untuk memastikan bahwa pengguna teknologi mengetahui risiko terkait dengan penggunaan teknologi informasi serta memahami dan mematuhi kebijakan dan prosedur yang ada. Dalam tahap ini, harus dilakukan penentuan enam fokus area dari program agar dapat dikelola. Fokus area ini ditentukan berdasarkan pertimbangan dari risiko-risiko yang mungkin terjadi pada organisasi.

   Kemudian dilakukan pelaksanaan program, yaitu dengan menggunakan fokus area yang ada, disampaikan melalui media, seperti presentasi, video, poster, dan brosur kepada orang-orang yang terlibat dalam penggunaan teknologi informasi di organisasi tersebut. Presentasi dibuat dengan pesan inti yang sama, tetapi disampaikan sesuai dengan tipe audiens. Untuk media lainnya, harus dipastikan bahwa semua pihak dapat mengerti apa yang ingin disampaikan, contohnya jika dalam suatu organisasi di Amerika terdapat anggota-anggota yang berasal dari Spanyol, pembuatan video harus mendukung bahasa Spanyol.

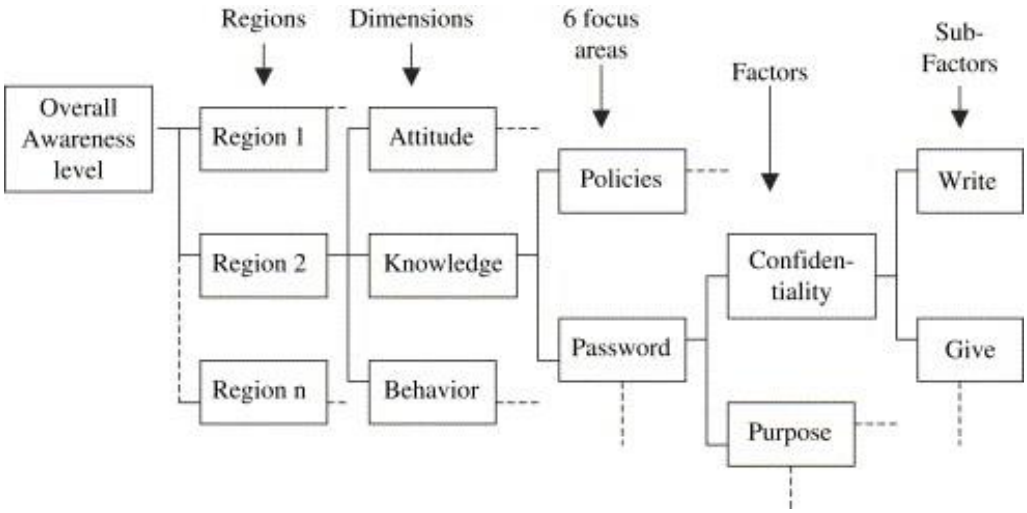
   Setelah pelaksanaan program selesai, dilakukanlah evaluasi dari program tersebut dengan mengukur kesuksesan dan keefektifannya. Untuk mengukur dua aspek tersebut, dibentuklah alat ukur berupa survei kuesioner yang terdiri atas pertanyaan pilihan ganda yang harus dijawab oleh responden. Jumlah jawaban yang benar yang digunakan sebagai indikasi kesadaran akan keamanan TI di wilayah tertentu.

   Pada langkah selanjutnya akan dilakukan pengembangan alat ukur. Alat ukur dikembangkan berdasarkan teknik psikologi sosial, yang melihat kecenderungan untuk merespon dengan cara puas atau tidak puas untuk objek tertentu, respon tersebut memiliki tiga komponen, yaitu pengaruh (emosi positif atau negatif), perilaku (niat untuk bertindak dengan cara tertentu), dan kognisi (keyakinan dan pemikiran). Tiga komponen ini digunakan sebagai dasar dan model dikembangkan pada tiga dimensi yang setara, yaitu apa yang diketahui seseorang (*knowledge*),

bagaimana perasaan seseorang terhadap suatu topik (*attitude*), dan apa yang mereka lakukan (*behavior*). Langkah yang harus dilalui untuk mengembangkan alat ukur adalah menetapkan apa yang harus diukur dan bagaimana cara mengukurnya.

3. Menetapkan apa yang harus diukur.

   Tingkat kesadaran akan keamanan TI global untuk organisasi adalah ukuran utama yang diperlukan, sehingga dilakukan pengukuran tingkat kesadaran di masing-masing regional yang kemudian akan digabungkan menjadi ukuran keseluruhan. Langkah awal yang harus dilakukan adalah identifikasi *key factors* yang akan menjadi dasar evaluasi. Untuk membantu dalam proses penataan masalah, hierarki kriteria diidentifikasi menggunakan struktur pohon seperti yang ada pada Gambar 1 berikut.



Gambar 1 - Contoh struktur pohon

Dalam penggunaan struktur pohon, dapat dilakukan pendekatan secara *top-down* atau *bottom-up*. Jika dilakukan pendekatan secara *top-down*, identifikasi dimulai dari regional menuju ke tiga dimensi (*knowledge*, *attitude*, dan *behavior*), dari masing-masing dimensi dibagi lagi menjadi enam fokus area yang ditetapkan pada langkah kedua, enam fokus area dapat dibagi menjadi faktor yang lebih spesifik, dan faktor tersebut dapat dibagi lagi menjadi sub-faktor yang lebih spesifik.

Setelah faktor yang akan diukur diidentifikasi, setiap faktor yang ada pada struktur pohon perlu diukur tingkat kepentingannya, sehingga didapatkan tingkat kepentingan dari tiap bagian mungkin berbeda, contoh pada bagian 1 lebih mementingkan dimensi *knowledge*, yang mementingkan fokus area *policies*, dan sebagainya.

4. Melakukan pengukuran.

   Dengan menggunakan struktur pohon, pengukuran dilakukan dari level terendah ke level teratas. Proses pengukuran ini dapat dilakukan dengan menggunakan aplikasi *spreadsheet*.

   Berikut adalah rumus yang digunakan untuk melakukan pengukuran.

$$V(a) = \sum_{i=1}^{n} v_i(a)\ w_i$$

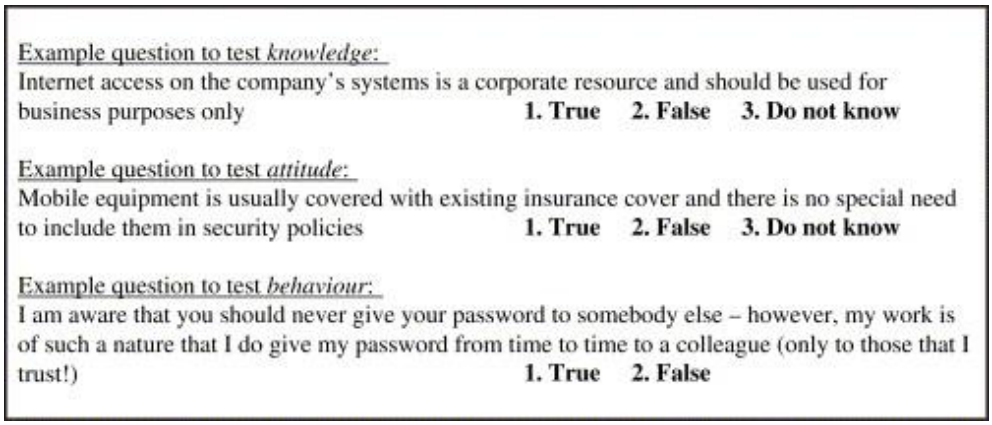
   Keterangan:

   $V(a)$ = keseluruhan nilai alternatif a

   $v_i(a)$ = skor nilai yang mencerminkan kinerja alternatif a pada kriteria i

   w_i = bobot yang diberikan untuk mencerminkan pentingnya kriteria i

   Kinerja ditentukan menggunakan kuesioner. Kuesioner berisi 35 pertanyaan yang didesain untuk menguji *knowledge*, *attitude*, dan *behavior* responden terkait dengan enam fokus area utama beserta faktor dan sub-faktornya. Contoh dari pertanyaan kuesioner yang dapat dilihat pada Gambar 2 di bawah ini.



Example question to test *knowledge*:
Internet access on the company's systems is a corporate resource and should be used for business purposes only **1. True 2. False 3. Do not know**

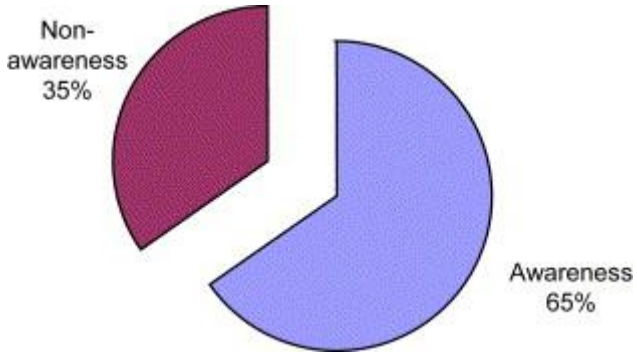
Example question to test *attitude*:
Mobile equipment is usually covered with existing insurance cover and there is no special need to include them in security policies **1. True 2. False 3. Do not know**

Example question to test *behaviour*:
I am aware that you should never give your password to somebody else – however, my work is of such a nature that I do give my password from time to time to a colleague (only to those that I trust!) **1. True 2. False**

Gambar 2 - Contoh pertanyaan kuesioner

Bobot ditentukan menggunakan *analytic hierarchy process* (AHP). Pendekatan AHP menggunakan *pairwise comparison* untuk memberikan evaluasi subjektif terhadap faktor berdasarkan penilaian dan pendapat profesional dari pihak manajemen. Perbandingan dibuat menggunakan skala preferensi, yang memberikan nilai numerik ke berbagai tingkat preferensi. Dari *pairwise comparison* dapat dihasilkan matriks kuadrat dan skala diekstraksi berdasarkan *eigenvector* dengan *eigenvalue* terbesar. Ketika vektor ini dinormalisasi menjadi satu, solusi yang dihasilkan unik dan mewakili ukuran numerik dari persepsi pembuat keputusan tentang kepentingan relatif kriteria. Setelah ini, indeks konsistensi dapat dihitung untuk mengukur tingkat inkonsistensi dalam *pairwise comparison* (Saaty, 1980).

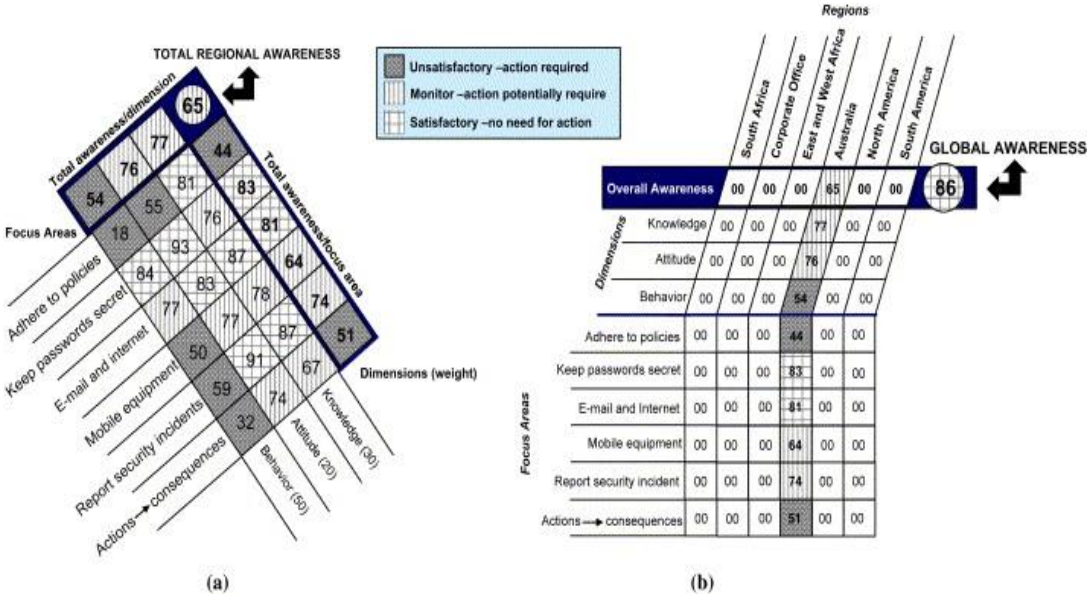
5. Melakukan pemetaan berdasarkan area fokus yang ditetapkan pada langkah kedua.
   Dari langkah keempat, hasil keluaran dari pengolahan data berupa grafik dan *awareness maps*. Grafik menggambarkan tingkat kesadaran secara keseluruhan yang diukur dengan alat prototipe. Grafik yang serupa juga dapat dihasilkan untuk menampilkan hasil untuk setiap dimensi dan setiap fokus area. Gambar 3 di bawah ini merupakan contoh grafik yang menampilkan tingkat kesadaran secara keseluruhan pada suatu regional.



Gambar 3 - Contoh grafik

Hasil dari pengukuran dan skala *awareness* dapat digunakan untuk membuat kode warna pada peta kesadaran regional. Kode warna dibagi menjadi tiga, yaitu kode warna yang menyatakan puas (*satisfactory*) sehingga tidak diperlukan tindak lebih lanjut, monitor yang artinya berpotensi membutuhkan tindak lebih lanjut, dan tidak

puas (*unsatisfactory*) sehingga membutuhkan tindak lebih lanjut. Berikut adalah contoh peta kesadaran regional yang dapat dilihat pada Gambar 4(a) dan ilustrasi ketika dipetakan pada peta kesadaran global yang dapat dilihat pada Gambar 4(b).



Gambar 4 - (a) Peta keadaran regional; (b) peta kesadaran global

Catatan:

Angka 86 pada Gambar 4(b) yang merupakan nilai total dari kesadaran global dimasukkan untuk kebutuhan ilustrasi, bukan hasil dari perhitungan yang sebenarnya.

Lima langkah di atas harus dipenuhi ketika ingin mengukur tingkat kesadaran akan keamanan TI dalam suatu organisasi. Bagaimana jika ingin mengukur tingkat kesadaran akan keamanan TI dari seseorang? Bisa juga dengan menggunakan langkah-langkah di atas, namun berfokus pada orang yang ingin diukur kesadaran akan teknologi informasinya. Contoh langkah yang harus dilalui:

1. Memahami latar belakang individu.

   Paham tentang orang yang akan diukur kesadaran akan teknologi informasinya, latar belakang pendidikan, umur, dan aspek lainnya yang dapat mempengaruhi.

2. Membuat program kesadaran akan keamanan informasi.

   Berbeda dengan program untuk suatu organisasi, program untuk individu ini dibuat lebih simpel, tetapi tetap berfokus pada tujuan utamanya. Fokus area yang ditentukan,

bergantung pada yang melakukan penilaian, fokus area apa yang ingin dinilai oleh peneliti.

3. Menetapkan apa yang harus diukur.
   Tetap menggunakan struktur pohon, tetapi langsung masuk ke area dimensi, tidak lagi mulai dari regional karena yang diuji hanya satu orang.

4. Melakukan pengukuran.
   Tetap menggunakan rumus yang sudah ada dan membuat pertanyaan berdasarkan enam fokus area yang telah ditentukan pada langkah kedua. Kuesioner diberikan kepada orang yang hendak diuji, lalu data diolah menggunakan aplikasi *spreadsheet*.

5. Melakukan pemetaan berdasarkan area fokus yang ditetapkan pada langkah kedua.
   Dari pengolahan data, dapat dihasilkan grafik dan peta kesadaran akan teknologi dari orang yang diuji. Dengan demikian dapat diketahui fokus area mana yang perlu ditingkatkan.

III. Penutup

III.1 Kesimpulan

Kesadaran akan keamanan TI itu sangat penting, terutama pada zaman sekarang di mana teknologi semakin berkembang. Keamanan TI diklasifikasikan menjadi empat bagian, yaitu fisik, manusia, data, dan kebijakan. Prinsip keamanan yang harus diperhatikan adalah CIA, yaitu *confidentiality*, *integrity*, dan *availability*. Keamanan harus diterapkan secara menyeluruh, mulai dari manusia, proses, dan teknologi yang terlibat. Kesadaran akan keamanan TI juga dipengaruhi oleh kesenjangan generasi. Dengan banyaknya kasus kriminalitas yang terjadi karena kurangnya kesadaran akan keamanan TI, dapat dilihat bahwa kesadaran akan kemanan TI sangat penting dan harus dimiliki oleh setiap orang.

Metode yang dilakukan untuk mengukur tingkat kesadaran adalah dengan menggunakan prototipe penilaian yang dibuat oleh H.A. Kruger dan W.D. Kearney. Prototipe penilaian tersebut memiliki tiga bagian utama, yaitu analisis kondisi, pengumpulan data melalui survei kuesioner, dan pengolahan data yang pada akhirnya akan menghasilkan grafik dan peta kesadaran. Dengan demikian dapat diketahui pada area mana kesadaran akan keamanan TI masih rendah dan pada dimensi apa rendahnya, apakah dimensi *knowledge*, *attitude*, atau *behavior*.

III.2 Saran

Metode yang ada untuk mengukur tingkat kesadaran akan keamanan TI sangat jarang ditemukan. Dalam melakukan studi mengenai topik ini, yang sering muncul adalah metode pengukuran tingkat keamanan TI dalam suatu perusahaan yang tujuannya adalah mencegah risiko yang mungkin terjadi dalam penerapan TI pada perusahaan. Belum ada metode yang secara spesifik digunakan untuk mengukur tingkat kesadaran akan keamanan TI secara individu, yang ada adalah metode pengukuran untuk suatu organisasi. Tingkatan kesadaran akan keamanan TI juga masih belum ada tolak ukur yang jelas, masih berupa penilaian dan pendapat profesional dari anggota organisasi yang dinilai.

Untuk penulisan selanjutnya, akan sangat bagus jika dilakukan penemuan metode lain yang dapat digunakan dan penetapan tolak ukur yang pasti untuk mengukur tingkat kesadaran akan keamanan TI.

IV. Daftar Pustaka

Banerjee, C., & Pandey, S. (2010). Research on Software Security Awareness: Problems and Prospects. *ACM*, 5. From https://dl.acm.org/doi/pdf/10.1145/1838687.1838701

Kruger, H., & Kearney, W. (2006). A Prototype for Assessing Information Security Awareness. *Elsevier*, 8. From https://www.sciencedirect.com/science/article/pii/S0167404806000563?via%3Dihub#bib1

Rahardjo, B. (2020, February 20). Prinsip-Prinsip Keamanan. Bandung, Jawa Barat, Indonesia.

Saaty, T. (1980). *What is the Analytic Hierarchy Process?* Pittsburgh: McGraw-Hill.

Vanderer, G. (2015). Security Awareness and Social Responsibility. *IEEE*, 4. From https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7208226&tag=1