MODEL PENGUKURAN TINGKAT KESADARAN KEAMANAN INFORMASI DI UNIVERSITAS AMIKOM YOGYAKARTA

Senie Destya

Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta
Jl. Ring Road Utar, Condong Catur, Depok, Sleman, Yogyakarta 55281
Email : seniedestya@amikom.ac.id

Abstrak

Keamanan system informasi menjadi topic yang penting untuk dibahas, hal ini disebabkan oleh kompleksitas permasalahan yang terbagi menjadi dua bagian utama, yaitu keamanan system dan keamanan pengguna. Paper ini focus membahas keamanan pengguna dengan menggunakan model RBS (Risky Behavior Scale), CBS (Conservative Behavior Scale), dan EOS (Exposure Offense Scale). Penggunaan tiga model ini menghasilkan alat ukur yang konkrit untuk pengukuran kesadaran pengguna tentang keamanan system informasi.

Kata kunci: *Pengukuran, kesadaran keamanan, RBS, CBS, EOS.*

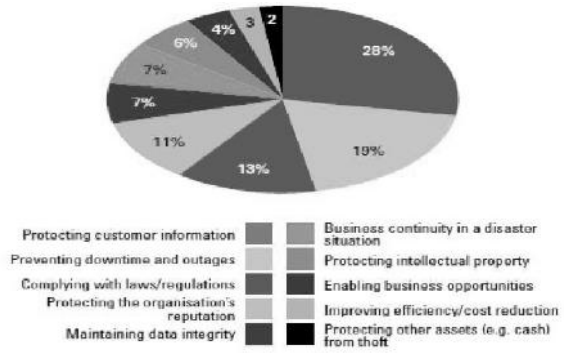
1. Pendahuluan

Di zaman yang semakin berkembang, setiap orang mempunyai kesempatan untuk mengakses informasi sebanyak banyaknya dan dapat memanfaatkan teknologi-teknologi baru. Dalam beberapa tahun terakhir, Asia telah menjadi 'kawasan superlatif' jika dikaitkan dengan teknologi informasi dan komunikasi. Pada kenyataannya kehidupan manusia saat ini sangat bergantung pada teknologi informasi dan komunikasi. Hal ini membuat individu dan organisasi di lingkungan kampus sangat rentan akan serangan terhadap system informasi, seperti *hacking, cyberterrorism, cybercrime,* dan lain-lain.

Kerugian yang terjadi pada penggunaan system informasi disebabkan oleh kesalahan pengguna [1], hal ini disebabkan oleh kelalaian, kebiasaan, dan pengetahuan pengguna tentang keamanan system informasi [2]. Pengukuran tingkat kesadaran keamanan pada pengguna system informasi menjadi penting seiiring berkembangnya konsep BYOD *(Bring Your Own Device)* karena dapat berpengaruh pada keamanan system informasi perusahaan[3].

Pengukuran tingkat kesadaran keamanan system informasi memiliki cakupan yang luas, hal ini dikarenakan oleh multi disiplin ilmu yang digunakan pada proses penghitungan[4]. Untuk itu dibutuhkan penelitian khusus untuk membahas model apa yang tepat digunakan pada pengukuran kesadaran keamanan pada suatu instansi.

Information Security Awareness di sektor Educational institutions awareness pemberian pelajaran kepada institusi perguruan tinggi tentang pentingnya keamanan informasi. Beberapa hal yang harus disampaikan kepada mahasiswa di universitasnya adalah security awareness, security policy, procedures, and guidelines,disaster recovery planning support, dan system monitoring and response. Hal tersebut relevan dengan data dari InfoSecurity Europe yang telah mengklasifikasikan 10 faktor pemicu pentingnya diterapkan system keamanan informasi. Berdasarkan laporan teknis survei pelanggaran keamanan informasi tahun 2010 terhadap 539 perusahaan (besar dan kecil), diperoleh diagram komposisi tingkat urgensi dari ke-10 faktor tersebut seperti yang tertera di Gambar 1.



Gambar 1. *Diagram komposisi faktor pemicu Pentingnya kemanan informasi*

Dari gambar 1 terlihat bahwa tiga besar faktor utama perlu diterapkanya keamanan informasi adalah untuk mengamankan informasi pelanggan, faktor kepatuhan hukum (regulasi) serta menjaga integritas data. Sementara faktor lainnya tidak terlalu signifikan. Peneliti melakukan studi literature pada beberapa peneliti lain yang meneliti tentang kesadaran keamanan informasi untuk menemukan peluang penelitian yang relevan dengan tema yang akan dikerjakan. Tertulis di tabel 1, enam peneliti yang penelitiannya di publish di jurnal ACM dan Semnasteknomedia pada tahun 2015-2017. Berdasarkan dari literature review tersebut, maka peneliti memilih topic tentang metode pengukuran kesadaran keamanan informasi untuk digunakan di Universitas Amikom Yogyakarta. Proses tersebut dilakukan dengan cara membandingkan beberapa metode pengukuran yang kemudian dicari yang paling relevan untuk digunakan di lingkungan Universitas Amikom Yogyakarta.

Rumusan Masalah

Rumusan masalah yang diangkat oleh penulis berdasarkan latar belakang penelitian dapat dilihat ke dalam poin berikut ini :

1. Model apakah yang tepat untuk pengukuran tingkat kesadaran keamanan informasi di lingkungan Universitas Amikom Yogyakarta ?

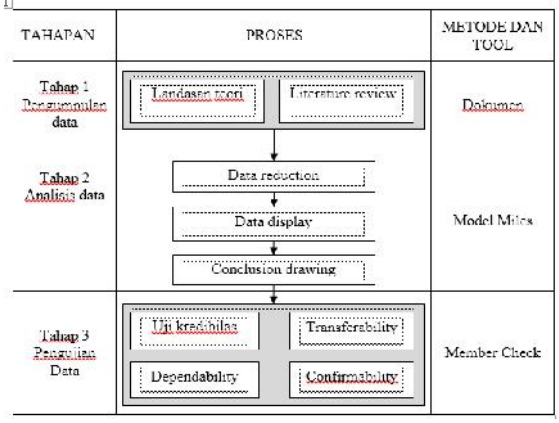
Tujuan Penelitian

Berdasarkan rumusan masalah penelitian, penulis menentukan dua tujuan penelitian yang akan dicapai yaitu :

1. Melakukan perbandingan dan analisis model pengukuran tingkat kesadaran keamanan informasi untuk digunakan di lingkungan Universitas Amikom Yogyakarta.
2. Meningkatkan penelitian dosen pemula pada Direktorat Penelitian Universitas Amikom Yogyakarta.

Metode Penelitian

Penelitian ini dilakukan dalam beberapa tahap yang dijelaskan pada gambar 2.



Gambar 2. *Metode Penelitian*

Pada gambar 2 menjelaskan proses alur penelitian, tahap 1 pengumpulan data yang proses pengerjaannya mengumpulkan landasan teori dan literature review yang menggunakan metode dokumentasi. Pada tahap 2 melakukan analisis data dengan melakukan proses pengolahan data secara bertahap, mulai dari memproses *data reduction*, lanjut proses *data display* baru melanjutkan keproses *conclusion drawing* menggunakan metode model Miles. Tahap 3 pengujian data, pada tahap pengujian melakukan proses *Uji kredibilas*, *transferability*, *dependability dan confirmability* yang menggunakan metode *Member Check.*

Tinjauan Pustaka

Penelitian berjudul "Analisis Hubungan Kesadaran Keamanan, Privasi Informasi, Perilaku Keamanan Pada Para Pengguna Media Sosial *Line"*. Hasil dari penelitian ini membahas tentang Faktor yang memengaruhi perilaku keamanan *(security behavior)* pada pengguna *LINE* adalah persepsi pengguna terhadap ancaman keamanan *(perceived security threat).*

Penelitian berjudul "Improving Security Awareness In The Government Sector". Hasil dari penelitian ini adalah melakukan pengukuran kesadaran keamanan informasi pada pengguna mobile device pada bidang berikut: OS demographics and malware, Password security measures. Unauthorized use and data loss, Wifi-connectivity, Applications from untrusted sources, Phishing

Penelitian berjudul "Evaluasi Penerapan Teknologi Informasi Pada Stie – Amik Lembah Dempo Pagaralam Menggunakan *Framework Information Technology Infrastructure Library (Itil Versi 3)"*. Hasil dari penelitian ini membahas tentang Pengukuran kematangan tata kelola keamanan informasi untuk melihat apakah metode yang telah distandarkan dalam penyelesaiannya, dan telah mendefinisikan dengan jelas langkah-langkah yang akan dipergunakan dalam menunjang pelayanan keamanan informasi.

Penelitian berjudul "Implementasi Standar Pengelolaan Sumber Daya Teknologi Informasi Guna Mendukung Tata Kelola Teknologi Informasi Di Lembaga Pemerintahan". Hasil dari penelitian ini membahas tentang optimalisasi tata kelola Teknologi Informasi (TI) yang ideal bagi lembaga pemerintahan berdasarkan hasil Pemeringkatan e-Government Indonesia (PeGI) tingkat propinsi pada akhir tahun 2013 dengan menerapkan standar pengelolaan sumber daya TI yang mengacu kepada best practice internasional yaitu framework Control Objective for Information and Related Technology (COBIT).

Penelitian berjudul "The Urgent Need for an Enforced Awareness Programme to Create Internet Security Awareness in Nigeria". ". Hasil dari penelitian ini membahas tentang Mendesain program dan material untuk meningkatkan kesadaran keamanan informasi di Negara berkembang. Dilakukan untuk memberikan masyarakat pemahaman yang lebih baik tentang isu keamanan, ancaman keamanan, dan cara untuk menghindarinya.

Landasan Teori

a. Konsep Umum Keamanan Informasi

Ada beberapa konsep keamanan informasi yang dipaparkan oleh Chan dan Mubarak (2011) yang antara lain:

1. *Phishing*. Phising adalah usaha untuk mendapatkan informasi rahasia atau melakukan pencurian identitas dengan menggunakan e-mail atau website palsu yang meniru alamat situs atau alamat e-mail yang sebenarnya.
2. *Spam*. *Spam* adalah surat atau pesan elektronik komersial yang tidak diinginkan oleh penerimanya.
3. *Social Engineering*. Dalam konteks keamanan informasi, *Social Engineering* adalah penggunaan sarana non-teknis untuk melakukan pencurian identitas atau untuk memperoleh informasi rahasia.

4. *Strong Password*. Password adalah kunci untuk otentikasi pengguna dan untuk mencegah akses tidak sah kedalam sistem.

b. Kesadaran Keamanan Informasi

Keamanan sistem informasi tidak hanya melibatkan kontrol keamanan teknis, namun juga melibatkan kontrol administratif, prosedural dan manajerial (Papagiannakis, Pijl, & Visser, 2011). Cara pengguna (karyawan, manajer, personel IT) dalam menggunakan sistem informasi organisasi memainkan peranan penting dalam menjaga kelangsungan aset informasi perusahaan. Program pelatihan dan kesadaran keamanan dapat dibagi dalam tiga bagian yang berbeda (Schlienger & Teufel, 2003):

1. Pendidikan: Karyawan harus memahami, mengapa keamanan informasi dangat penting bagi organisasi. Mereka harus memahami bahwa setiap orang bertanggung jawab atas keamanan yang mempengaruhi lingkungan mereka masing-masing. Pendidikan dapat diimplementasikan melalui kursus keamanan informasi. Dapat juga menjadi pendidikan keamanan informasi dasar di sekolah atau perguruan tinggi.
2. Pelatihan: Karyawan harus mengetahui bagaimana mereka bisa merasa aman. Mereka harus tahu bagaimana menggunakan fungsi keamanan didalam sebuah aplikasi dan dalam proses kerja mereka. Pelatihan tentang peralatan atau fitur keamanan didalam aplikasi perlu diberikan.
3. Kesadaran : Pendidikan dan pelatihan adalah dasar untuk program keamanan. Meskipun demikian, hal ini tidak menjamin perilaku keamanan dalam kehidupan sehari-hari. Pengukuran keamanan diluar kelas mengingatkan karyawan pada pelajaran yang telah diperoleh. Perkakas seperti poster, mouse-pads, dan bolpoin dengan slogan keamanan membantu menghadirkan topik keamanan dimana-mana.

c. Pengukuran Kesadaran Keamanan Informasi

Beberapa penelitian telah melakukan pengukuran kesadaran keamanan informasi. Hong Chang dalam tesisnya yang berjudul "*Information Security Awareness Levels of TAFE South Australia Employees*" melakukan pengukuran kesadaran informasi pada karyawan dengan cara mengukur pengetahuan dan behavior karyawan terhadap aspek-aspek keamanan informasi yang telah dijelaskan pada Bagian 2.2 (Chan & Mubarak, 2011). Pengukuran dilakukan dengan cara sederhana berdasarkan presentasi jawaban responden. Metode ini mengadopsi metode yang sebelumnya sudah pernah dilakukan (*Kruger, Flowerday, Drevin, & Steyn, 2011*). Sebelumnya, Kruger dan Kearney telah memperkenalkan sebuah prototipe untuk mengukur kesadaran keamanan informasi. Penelitian ini mengukur kesadaran keamanan informasi para karyawan di sebuah perusahaan tambang internasional (*Krugger & Kearney, 2006*).

2. Pembahasan

Penelitian diawali dengan mengumpulkan beberapa paper yang berhubungan dengan Security awareness, dari beberapa paper yang ada kemudian dikategorikan menjadi tiga bagian sebagai berikut.

Tabel 1. *Data Reduction*

RBS	*Risky Behavior Scale*	Mengukur tingkat risiko pengguna IS sehubungan dengan perilaku mereka	Naomi Sadeh and Arielle Baskin-Sommers, 2016 [5]
CBS	*Conservative Behavior Scale*	Seberapa berhati-hati pengguna saat menggunakan teknologi informasi atau IS	Christophe Chalons, Frédéric Coquel, 2017
EOS	*Exposure to Offence Scale*	Mengukur pengguna IS terkena insiden keamanan cyber karena tingkah lakunya.	Aytes, Kregg, and Terry Connolly. 2005 [6]

Tabel 1 menjelaskan tentang paper dan penjelasan singkat model pengukuran yang digunakan. Terdapat tiga model yang digunakan, yaitu *Risky Behavior Scale*, *Conservative Behavior Scale*, dan *Exposure to Offence Scale*. Masing-masing model tersebut memiliki karakteristik dan kelebihan model ukur yang berbeda.

Tabel 2. *Data Display*

Pengukuran	RBS	CBS	EOS
1	Penggunaan system informasi (Chat, email, social media)	Penggunaan dan perubahan password secara berkala	Kerugian finansial
2	Aktivitas transaksi	Kesadaran software	Permasalahan

	online	(software berlisensi)	dengan virus
3	Memberikan akses (informasi personal, password)	Keamanan berlapis (password kuat, antivirus)	Phising (penipuan)
4	Konsumsi fasilitas internet (download, game online, nonton video)		

Tabel 2 adalah data display yang berisi poin-poin yang digunakan pada masing-masing metode. Langkah selanjutnya yang dilakukan adalah menganalisis poin-poin tersebut dengan menimbang kekurangan dan kelebihannya. Hasil dari analisi poin inilah yang akan digunakan untuk membuat bank soal pertanyaan.

Tabel 3. Perbandingan model

Pengukuran	Resiko	Kewaspadaan	Insiden
RBS	☑		
CBS		☑	
EOS			☑

Tabel 3 Menjelaskan bahwa masing-masing metode pengukuran memiliki poin yang unik, sehingga pengukuran menggunakan ketiga metode dapat meningkatkan akurasi hasil. Langkah selanjutnya adalah membuat daftar pertanyaan menggunakan ke tiga model tersebut untuk digunakan pada kuisioner.

Tabel 4. *Pertanyaan Model RBS*

1	Saya menggunakan program chat (Messenger, GTalk, Skype, dll).
2	Saya menggunakan situs jejaring sosial (Facebook, Twitter, dll)
3	Saya belanja di Internet.
4	Saya bermain game online.
5	Saya mendownload / menyimpan musik, film, program dan file.
6	Saya membuka e-mail atau mendownload lampiran dari orang asing

Tabel 4 adalah model pertanyaan yang menggunakan model *Risky Behavior Scale*, dimana model *Risky Behavior Scale* ini mengukur tingkat resiko penggunaan sistem informasi berdasarkan perilaku atau kebiasaan pengguna SI.

Tabel 5. *Pertanyaan Model CBS*

1	Saya menggunakan lebih dari satu alamat e-mail.
2	Saya mencoba menggunakan perangkat lunak asli (berlisensi) di komputer saya komputer.
3	Saya menggunakan program seperti virus screening, spy software, dll.
4	Saya punya password untuk menyalakan komputer saya.
5	Saya sering mengganti kata sandi saya.
6	Saya mengganti kata sandi modem nirkabel saya.

Tabel 5 adalah model pertanyaan yang menggunakan model *Conservative Behavior Scale*, dimana model *Conservative Behavior Scale* ini mengukur tingkat seberapa berhati-hati pengguna saat mengunakan teknologi informasi atau sistem informasi.

Tabel 6. *Pertanyaan Model EOS*

1	Saya mengalami masalah karena virus komputer.
2	Saya pernah mengalami kerugian finansial akibat belanja online.
3	Saya mengalami masalah karena saya berbagi informasi pribadi saya di Internet.
4	Saya mengalami kerugian akibat situs jejaring sosial.
5	Saya mengalami masalah karena saya berbagi informasi pribadi saya di Internet.

Tabel 6 adalah model pertanyaan yang menggunakan model *Exposure to Offence Scale*, dimana model *Exposure to Offence Scale* ini mengukur pengguna sistem informasi terkena insiden atau dampak keamanan cyber karena tingkah lakunya sendiri.

3. Kesimpulan

Hasil dari penelitian ini menunjukkan bahwa model pengukuran yang paling tepat untuk digunakan pada tingkat kesadaran keamanan informasi di lingkungan Universitas Amikom Yogyakarta adalah dengan menggunakan gabungan beberapa metode. Hal ini dilakukan untuk memperoleh gambaran secara menyeluruh hasil observasi lapangan.
Saran untuk peneliti selanjutnya adalah menggunakan metode lain untuk meningkatkan akurasi pengukuran, selain itu, peneliti selanjutnya diharapkan dapat mengukur validasi soal yang akan digunakan pada kuisioner. Pengukuran pada bidang selain kampus juga perlu diadakan untuk mengevaluasi keberhasilan ketiga metode ini.

Daftar Pustaka

[1] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and Information Security Awareness," *Comput. Human Behav.*, 2017.
[2] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks," *Comput. Secur.*, 2017.
[3] L. Gerhold, G. Bartl, and N. Haake, "Security culture 2030. How security experts assess the future state of privatization, surveillance, security technologies and risk awareness in Germany," *Futures*, 2017.
[4] S. Allam, S. V. Flowerday, and E. Flowerday, "Smartphone information security awareness: A victim of operational pressures," *Comput. Secur.*, 2014.
[5] N. Sadeh and A. Baskin-sommers, "Risky , Impulsive , and Self-Destructive Behavior Questionnaire (RISQ): A Validation Study," 2016.
[6] G. Öğütçü, Ö. M. Testik, and O. Chouseinoglou, "Analysis of personal information security behavior and awareness," *Comput. Secur.*, 2016.

Biodata Penulis

Senie Destya, memperoleh gelar Sarjana Teknik (ST), Jurusan Teknik Informatika UNIVERSITAS PALANGKARAYA, lulus tahun 2013. Memperoleh gelar Magister Komputer (M.Kom) Program Pasca Sarjana Magister Teknik Informatika STMIK AMIKOM Yogyakarta, lulus tahun 2016. Saat ini menjadi Dosen di UNIVERSITAS AMIKOM Yogyakarta.

ISSN : 2302-3805